IT audit en Sarbanes-Oxley

ius summum saepe summa inuria - Cicero

Michiel le Comte
2007

Interne begeleider : Michel Zandbergen
Externe begeleider : Tjakko de Boer

vrije Universiteit amsterdam

Inhoudsopgave

1 Inleiding 3

1.1 Introductie en achtergrond 3

1.2 Vraagstelling en scope 3

1.3 Onderzoeksaanpak 4

1.4 Opbouw van de scriptie 4

2 Samenvatting en conclusie 5

3 De geschiedenis van IT audit 7

3.1 Het ontstaan van het EDP audit vakgebied (1965 – 1975) 7

3.2 Het tijdperk van de centrale systemen (1970 – 1990) 7

3.3 Het netwerk is het systeem – client/server (1990 – 2002) 11

3.3.1 Veranderingen door de client/server architectuur 11

3.3.2 Veranderingen in de IT audit aanpak als gevolg van Client/Server 14

3.3.3 Overige ontwikkelingen 15

3.4 Recente ontwikkelingen (2002 – heden) 16

3.5 De Nederlandse IT audit geschiedenis in een oogopslag 17

4 De ontwikkeling van Sarbanes Oxley 18

4.1 Het ontstaan van de SOX wetgeving 18

4.2 De interpretatie en implementatie van de SOX in het bedrijfsleven 18

4.3 De toekomstvisie op SOX vanuit de Verenigde Staten 19

5 Overlap en toekomst (onderzoeksvraag 3 en 4) 21

5.1 De overlap en verhoudingen tussen EDP audit en SOX 21

5.2 Aanpassing onderzoeksvraag 4 22

5.3 De integratie van EDP audit en SOX 23

5.3.1 Bepaling van de audit planning 23

5.3.2 Applicatie en rekencentrum audits 24

5.3.3 Project audits 25

5.3.4 Samenwerking met de business 26

5.4 Samenvatting 27

Persoonlijke terugblik 28

Annex A 29

SOX – section 404 29

SOX – section 302 29

Referenties 30

1 Inleiding

1.1 Introductie en achtergrond

Het Enron schandaal was de directe aanleiding tot de Sarbanes Oxley wetgeving. SOX heeft een significante impact op de activiteiten die een bedrijf moet uitvoeren om aan te tonen dat ze de processen beheersen die leiden tot de financiële cijfers. Het doel hiervan is om aan de aandeelhouders te tonen dat de financiële cijfers betrouwbaar zijn. De wet heeft met name sterkere eisen gesteld aan de bewijsvoering voor het vaststellen van deze beheersing.

Een onderdeel van de beheersing van de financiële processen is de beheersing van de ondersteunende IT omgeving. Hierdoor worden de activiteiten van de EDP auditors in Nederland direct geraakt, met name de activiteiten van de externe auditors en interne auditors van de grotere bedrijven die in de VS aan de beurs genoteerd staan.

Sinds de invoering van de wet (juli 2002) is er veel geschreven en gesproken over hoe de wet geïnterpreteerd moet worden, met name door de extern accountantskantoren en IT consultancy bedrijven. Deze interpretatie is in de afgelopen jaren ook vrijwel continu aangepast om tot een haalbare inspanning te komen. Het hoofd van de New York Stock Exchange (NYSE) heeft op 10 november 2006 opgeroepen tot een nog verdere reductie van de SOX inspanningen (Cox, 2006-1), wat aangeeft dat de SOX interpretatie waarschijnlijk nog niet definitief is.

Doordat IT audit als vakgebied zich al heeft kunnen ontwikkelen, wordt bij de uitleg van de SOX vereisten rekening gehouden met de huidige werkwijzen. Initieel had de SOX insteek veel overlap met de IT audit aanpak van een 30 jaar terug, maar door nieuwe inzichten over de SOX aanpak is de aanpak al aanzienlijk “verjongd”. Het is echter nog een feit dat de huidige aanpak voor SOX IT testen niet gelijk is aan de huidige IT audit aanpak. De impact van SOX op IT projecten, en daarmee op de audit van IT projecten, is bijvoorbeeld nog niet uitgewerkt.

1.2 Vraagstelling en scope

Deze scriptie kijkt naar de achtergronden van zowel IT audit als vakgebied en SOX als specifiek onderdeel daarvan, om de waarschijnlijke veranderingen in de SOX aanpak in 2007 te voorspellen.

Gebaseerd op bovenstaande achtergrond zal het onderzoek zich op de volgende vraag richten:

Centrale vraag: Wat is de relatie tussen de geschiedenis van IT audit en de huidige rol en aanpak van IT audit binnen de Sarbanes Oxley wet van 2002 en wat zegt deze relatie over de mogelijke toekomstige rol en werkwijze van IT audit binnen Sarbanes Oxley?
Subvragen:
1. Hoe heeft IT audit zich als vakgebied de afgelopen 40 jaar ontwikkeld? Wat waren de drivers voor de veranderingen?
2. Hoe is de Sarbanes-Oxley wet ontstaan en welke wijzigingen zijn er in de laatste jaren geweest qua aanpak?
3. Hoe verhoudt de verandering in SOX aanpak zich tot de evolutie van IT audit in de afgelopen 30/40 jaar?

4. Welke wijzigingen kunnen verwacht worden in de IT Audit SOX aanpak, op basis van de overeenkomsten met de IT audit geschiedenis?

De vraagstelling spreekt over de geschiedenis van IT Audit. In het specifiek zal dit onderzoek zich richten op de ontstaansgeschiedenis van het vakgebied in Nederland, maar de relatie met IT audit in de Verenigde Staten wordt, waar relevant, ook meegenomen.

De doelgroep van deze scriptie is zijn Nederlandse (IT) auditors, vandaar dat een aantal termen als bekend verondersteld worden.

1.3 Onderzoeksaanpak

Het onderzoek is een beschrijvend onderzoek en valt in twee onderdelen uiteen. Het eerste onderdeel is de geschiedenis van de IT audit. Deze geschiedenis van het IT audit vakgebied is vastgesteld via 6 interviews met voormalig en huidige IT auditors, aangevuld met literatuur over de ontwikkeling van de technische componenten van IT. Op basis hiervan wordt de eerste onderzoeksvraag beantwoord.

De ontwikkeling van SOX in de afgelopen jaren is besproken tijdens interviews maar is met name gebaseerd op literatuuronderzoek, in het specifiek informatie over de vereisten die aan IT audit worden gesteld vanuit de SOX wetgeving en additionele bronnen (PCAOB en ITGI)). Dit heeft geleidt tot de beantwoording van onderzoeksvraag 2.

De verzamelde informatie is vergeleken en op basis van deze verschillenanalyse gemaakt is een werkwijze ontwikkeld die de mogelijkheid van integratie van SOX en de IT audit aanpak uitwerkt. Het resultaat hiervan zijn de antwoorden op onderzoeksvragen 3 en 4.

1.4 Opbouw van de scriptie

Deze scriptie is als volgt opgebouwd: Hoofdstuk 2 bevat een management samenvatting van de daaropvolgende hoofdstukken. In hoofdstuk 3 en 4 wordt respectievelijk de geschiedenis van EDP audit in Nederland en van SOX beschreven. Daarna volgt hoofdstuk 5 waarin de verschillen tussen SOX en standaard IT audit aanpak worden beschreven en uitgewerkt wordt hoe SOX en de huidige standaard IT audit aanpak geïntegreerd kunnen worden. De scriptie eindigt met een persoonlijke terugblik op de scriptie en overzicht van de gebruikte referenties. Deze zijn opgenomen in de annex.

2 Samenvatting en conclusie

Vanaf ongeveer 1970 tot 1990 is EDP Audit als vakgebied ontwikkeld. De EDP audit aanpak was in die tijd sterk gestructureerd, gebaseerd op het Mainframe en de waterval ontwikkelmethode. De IT auditor was met name betrokken bij projecten en de activiteiten waren primair gericht op het beoordelen van de opzet. In de jaren 80 ontstond noodgedwongen meer aandacht voor de technische aspecten van de informatiesystemen.

De introductie van de client/server architectuur begin jaren 90 heeft een significante impact gehad op vrijwel alle activiteiten van de EDP auditor. Door de toenemende complexiteit heeft de EDP auditor zich, noodgedwongen, in toenemende mate gericht op de audit van de processen om de IT componenten heen, in plaats van de IT componenten zelf. Waar de technische kant werd getest verplaatste de nadruk zich van beoordeling van de opzet naar beoordeling van de werking. Hierdoor verminderde de aandacht voor de techniek zelf.
In de afgelopen jaren verschenen nog steeds in een significant tempo nieuwe ontwikkelingen op het gebied van techniek, maar dit heeft (nog) niet geleid tot vergelijkbaar grote veranderingen in de EDP audit aanpak.
Vanuit een aantal bedrijfs- en accountingschandalen is in Juli 2002 de Sarbanes-Oxley wet in de VS aangenomen. Deze wet stelt onder andere als eis dat de Chief Financial Officer (CFO) aftekent voor de juistheid en volledigheid van de financiële cijfers en dat er een uitspraak gedaan wordt over de effectiviteit van de interne controles die de correctheid en volledigheid van de financiële cijfers garanderen. De wet is van toepassing voor alle bedrijven die beursgenoteerd zijn in de VS. SOX heeft een aanzienlijke impact gehad op het bedrijfsleven. Dit komt deels doordat bedrijven dezelfde rigoureuze stappen hebben genomen als de externe accountantskantoren.Vanuit verscheidene kanten (SEC, ITGI) wordt nu aangegeven dat bedrijven minder activiteiten hoeven te ontplooien als ze een “top-down, risk-based” aanpak gebruiken om SOX efficiënter te maken.

Er bestaan drie hoofdverschillen tussen de SOX aanpak en de huidige EDP audit aanpak:

- De link tussen audit activiteiten en de jaarrekening is sterker bij SOX.
- De grootte van steekproeven bij audit testwerkzaamheden is groter bij SOX
- SOX heeft op dit moment vrijwel geen rol bij project audits, maar des te meer bij audits van de bestaande organisatie

Op basis van deze verschillen heb ik op hoog niveau een model uitgewerkt hoe de reguliere EDP aanpak en SOX elkaar kunnen aanvullen en versterken. Hierbij zijn de doelstellingen die de organisatie moet bereiken het uitgangspunt (principe), en niet uitputtende lijsten van regels waaraan voldaan moet worden.
Het model bevat de volgende onderdelen:

- De financiële risico’s voor de vaststelling van de audit en SOX planning moeten door audit en de business gezamenlijk vastgesteld worden.
- De aanpak van audits van individuele entiteiten moet uitgebreid worden zodat steekproefgroottes en vereisten aan vastlegging en rapportage geïntegreerd zijn.
- De project audit aanpak voor SOX relevante projecten moet een standaard onderdeel hebben voor de SOX impact, voor zowel functioneel en technisch ontwerp, en ook voor de bijbehorende testen. De IT auditor moet hier tijdens het project al bij betrokken zijn.

- Samenwerking met de business is essentieel voor een efficiënte uitvoering van de testwerkzaamheden, en ook voor de vaststelling van de controles op het juiste niveau zijn er een aantal concrete aspecten waarin de huidige EDP audit aanpak en SOX te integreren zijn.
- Om de grootste voordelen te halen is samenwerking tussen audit en de overige bedrijfsonderdelen noodzakelijk. Deze samenwerking is zeker realiseerbaar omdat deze samenwerking niet alleen leidt tot een efficiëntere SOX test aanpak, maar tot een verbeterde risicobeheersing in het algemeen.

3 De geschiedenis van IT audit

In dit hoofdstuk wordt het ontstaan en de ontwikkeling van het Electronic Data Processing (EDP) audit[1] vakgebied uitgewerkt. Specifiek wordt de eerste onderzoeksvraag beantwoord: "*Hoe heeft IT audit zich als vakgebied de afgelopen 40 jaar ontwikkeld? Wat waren de drijfveren voor de veranderingen?*"
Over de geschiedenis van EDP audit bestaat weinig literatuur. Daarom is beschrijving van de geschiedenis gebaseerd op interviews die gehouden zijn met prominenten van het vakgebied die zowel vanuit interne audit afdelingen als accountantskantoren komen. Hierbij is het uitgangspunt geweest dat alleen de punten die in meerdere interviews zijn teruggekomen opgenomen zijn in dit hoofdstuk, om eventuele subjectiviteit te verminderen.

3.1 Het ontstaan van het EDP audit vakgebied (1965 – 1975)

Vanaf 1964 tot 1973 boekten managers van de "Equity funding Corporation of America" incorrecte verzekeringspolissen af om de winst, en daarmee de aandelenkoers, omhoog te duwen. Deze praktijk kwam aan het licht door een klokkenluider. Toch kostte het de auditors van Touche Ross twee jaar om het bestaan van de fictieve polissen in het IT systeem aan te tonen. Dit was een van de eerste fraudegevallen waarbij de auditors gedwongen werden om "door de computer heen" te auditen, in plaats van "om de computer heen".

In Nederland ontstond eind jaren 60 ook het besef dat de informatiesystemen steeds sterker een integraal onderdeel van de business vormden en daarmee ook een onderdeel van controle moesten zijn. Dit was een grote stap, zeker bij de accountantscontrole van de financiële instellingen, waarvan voorheen sommige accountants van mening waren dat deze überhaupt niet gecontroleerd konden worden vanwege de afwezigheid van een waardekringloop gebaseerd op de doorstroom van goederen.

De accountants ondernamen daarom stappen om grip te krijgen op de juistheid en volledigheid van de automatisering. De automatisering bestond op dat moment uit een centrale mainframe, waarbij mutaties werden aangebracht via afgetekende ponskaarten. Een logische aanpak was dan ook het "closed shop" principe, oftewel de volledige controle op alle inkomende en uitgaande informatiestromen. De eerste aanpak van accountants was dan ook om zelf de ponskaarten te beheren. Al snel werd echter duidelijk dat er specifieke kennis en kunde nodig was om de automatisering in de greep te houden. In deze fase kwam vanuit de accountancy het idee van een netwerk van controletotalen in computersystemen tot ontwikkeling. Ook ontstonden ideeën over het beoordelen van de automatiseringsorganisatie en de informatiesystemen als onderdeel van de beoordeling van de administratieve organisatie. Als gevolg hiervan specialiseerden bepaalde accountants zich in de ontwikkelende wereld van de IT. De EDP auditor was geboren.

3.2 Het tijdperk van de centrale systemen (1970 – 1990)

1970/1980

In het begin van de jaren 70 was de EDP auditor ondersteunend aan de jaarrekening controle. De activiteiten waren dan ook voornamelijk gericht op "controle met behulp van de computer" in

[1] In deze scriptie worden "EDP audit" en "IT audit" afwisselend gebruikt, deze verwijzen naar hetzelfde vakgebied.

plaats van “controle van de computer zelf”, en met name ter ondersteuning van de controle van de administratieve organisatie. Dit kwam vanwege de accountancy achtergrond die elke IT auditor op dat moment primair had. De externe accountantskantoren onderzochten de transactiebestanden met behulp van specifiek ontwikkelde software. Een van de voorbeelden van de gebruikte audit tools is Auditape (Cangemi, Singleton, 2003), wat informatie uit Mainframes kon halen, waarna auditors transactiegerichte controles op deze files konden uitvoeren. Hierbij werd de aanname gemaakt dat de cijfers die zich in het Mainframe bevonden volledig waren, wat steunde op de “closed shop” gedachte met handmatige controle op de ponskaarten. Andere tools die gebruikt werden zijn data analyse tools zoals SAS en ACL.

Er zijn twee gedachten die tot een wijziging op de bovenstaande aanpak hebben geleid:

1. De opkomst van de 3270 terminals
2. De noodzaak tot rekencentrum audits

De 3270-terminal

Door de komst van de 3270 “domme” terminal kregen gebruikers de mogelijkheid om direct met het Mainframe te communiceren via een beeldscherm van 32x70 karakters. Initieel kregen gebruikers alleen de mogelijkheid om informatie uit het Mainframe op te vragen, maar al snel werd de mogelijkheid tot het toevoegen van mutaties ook aangeboden. Mutaties konden nu “real-time” ingevoerd worden, hoewel deze mutaties net zoals de ponskaarten pas aan het eind van de dag door een batch verwerkt werden. De terminal met de real-time mutatie kon echter de ponskaarten vervangen, en door de verwijdering van de bijbehorende logistiek van papier het mutatieproces aanzienlijk efficiënter maken.
Aan de andere kant viel hiermee de authenticatie van de mutaties weg. De ponskaarten werden immers afgetekend, maar dit gold niet meer voor de mutaties. Hierdoor had de accountant geen zekerheid meer over de juistheid en volledigheid van de financiële stromen. Dit probleem leidde dan ook tot het ontstaan van afgedwongen functiescheidingen en autorisaties in het systeem en de bijbehorende autorisatiematrix.

Rekencentrum audits

Tussen 1972 en 1975 werden de rekencentrum audits geïntroduceerd, om ook de ondersteunende processen te beoordelen. Binnen AMRO vormden de rekencentra al snel een onderdeel van het IT audit universe, vanwege de leidende insteek die Margaret van Biene-Hershey[2] had. In andere gevallen kostte het de externe accountant soms jaren om de klant van het nut van de rekencentrum audit te overtuigen.

De aanpak van de initiële rekencentrum audits bestond uit de controle van de volgende onderdelen:

- Uitwijkmaatregelen
- Functiescheidingen
- Fysieke beveiliging (toegangsbeveiliging)
- Brandbeveiliging
- Aanwezigheid van gesloten tape magazijn

[2] Voormalige hoofd van IT audit AMRO en mede-oprichster van de EDP audit opleiding aan de VU.

Dit wil dus zeggen dat onderdelen als het Operating System, de logische toegangsbeveiliging voor systeembeheerders en de beheerprocessen (zoals ITIL) nog geen onderdeel vormden van de originele rekencentrum audit aanpak.

Samenvattend ontstond in de jaren 70 de functie van EDP auditor als specialisatie van de register accountant. De controle van de autorisaties in het systeem kregen een plaats in de audit aanpak, de audit van het besturingsysteem ontstond en de rekencentrum audit werd gemeengoed. Hierbij namen een paar auditors de rol van voortrekker, wat gebruikelijk is bij opstartende bedrijven en vakgebieden. Zo was bijvoorbeeld Herman Roos (KPMG) een van de voortrekkers in het opzetten van het Mainframe audit kader, en Margaret van Biene-Hershey (AMRO) sterk betrokken bij de invoering van rekencentrum audits.

1980/1990

In de 80er jaren vond een verfijning van de audit aanpak uit de jaren 70 plaats. Dit gebeurde op basis van de volgende onderdelen:

- De waterval ontwikkelmethode vormde een solide basis voor de EDP audit werkzaamheden
- Externe eisen werden gesteld aan IT
- Het EDP audit vakgebied professionaliseerde via centrale opleidingen

IT projecten via de waterval methode

Het Mainframe was een gestructureerde omgeving en ontwikkeling van applicaties verliep op een even gestructureerde wijze. De standaard ontwikkelmethodiek was de waterval methode, met welgedefinieerde projectfases en bijbehorende opbrengsten per fase. Interne EDP-auditors waren betrokken bij alle projecten en gaven positieve zekerheid per document ("Dit functioneel ontwerp is van voldoende kwaliteit om verder te gaan naar de volgende fase"). De project audit vormde de hoofdmoot van het audit werk, 80% van de interne EDP werkzaamheden werd eraan besteed.

De externe IT auditors name ook deel aan projecten, in een 1 op 10 verhouding ten opzichte van de interne auditors. De externe auditor volgde projecten meestal op het niveau van de projectgroep, net als de interne IT auditors, maar behield vanwege de tijdsbeperkingen een hoger abstractieniveau dan de interne auditor. In andere woorden: de interne auditors hadden meer mogelijkheden om dieper in de materie te duiken. Dit past ook bij de rol van de interne IT auditor die een verdergaande taak heeft dan alleen dat doen wat voor de jaarrekeningcontrole nodig is.

In deze periode lag de nadruk van de EDP audit activiteiten dus op de beoordeling van de opzet van informatiesystemen. Via het testtraject werd ook gekeken naar het bestaan van controles in de applicatie, maar de werking van applicatie controles werd nog niet getest.

Externe eisen aan IT en IT audit

Op 20-9-1988 gaf De Nederlandsche Bank (DNB) het memorandum "Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen" uit. Dit memorandum gaf aan hoe DNB vond dat de rol en positie van IT gezien moest worden. Dhr. Frielink (voormalig accountant van de DNB) gaf hierbij aan: "*voor banken is IT niet een positie an sich, maar het is een ondersteuning van de liquiditeit en solvabiliteit en daarmee een essentieel onderdeel van de banken*".

Het memorandum was vrij gedetailleerd in het omschrijven van de noodzakelijk geachte maatregelen (bijvoorbeeld Sectie 5, B, 2.9: Beveiligen van gevoelige informatie tijdens transport tegen ongeautoriseerd raadplegen of veranderen (datatransmissie met behulp van communicatienetwerken, tape-transport, transport van PC-gegevensdragers enz.)

Dit memorandum bevestigde dat de rol van de EDP auditor essentieel is voor een goede beoordeling van de stand van zaken binnen de financiële instellingen. (Het memorandum is vervangen door de "Regeling Organisatie en Beheersing" (ROB) van DNB d.d. 29 maart 2001)

Bij de internationale accountantskantoren was er sprake van kruisbestuiving tussen de EDP auditors in de Verenigde Staten en in Nederland. In de VS ontstond het vak met name na de fraude bij de Equity Funding Corporation of America (zie paragraaf 3.1) en is van de grond af opgebouwd. In Nederland had de EDP audit functie een snelle start omdat het voortbouwde op de methodieken en principes van de accountancy. De auditors in de VS hadden over het algemeen uitputtende lijsten met testen, terwijl de Nederlandse auditors de achterliggende filosofie als basis hadden. Hierdoor konden de Nederlandse auditors via hun Amerikaanse collega's relatief gemakkelijk aan concrete testaanpak uitwerkingen komen voor nieuwe systemen. De internationale samenwerking leidde tot een wederzijdse toenadering.

Deze kruisbestuiving zorgde er ook voor dat de Nederlandse EDP audit aanpak beïnvloed is door de verscheidene wetten die in de VS aangenomen waren op het gebied van computer criminaliteit. In Nederland werd de eerste wet over computercriminaliteit pas in 1993 aangenomen.
Uiteraard zijn er ook vanuit andere landen invloeden geweest, zoals bijvoorbeeld vanuit de EDPAC vanuit Canada, die al vroeg richtlijnen hebben opgesteld voor EDP werkzaamheden.

Professionalisering van de auditors via centrale opleidingen

Omdat de IT audit functie ontstaan is als specialisatie van het reguliere accountancy vak werden de EDP auditors in het algemeen als accountant (RA) opgeleid, en leerden ze de "EDP kennis" intern. Hierbij was de hoofdgedachte binnen de accountantskantoren en interne accountantsdiensten om tijdelijke werkgroepen op te richten die antwoord gaven op de vraag "Wat moet de accountant bijleren om ook de computer mee te kunnen auditen?". Deze tijdelijke groepen zijn in feite nooit opgeheven. De conclusie was al vrij snel dat het onmogelijk is elke accountant zo op te leiden dat deze de audit in zwaar geautomatiseerde omgevingen even goed beheerst als de audit van de verslaggevingskant. De aanvankelijk tijdelijke studiegroepen hebben zich ontwikkeld tot een zelfstandig beroep waarmee accountants, zowel externe als interne, intensief samenwerken in het kader van de jaarrekeningcontrole.
Om IT auditors adequater op te leiden is in Nederland de eerste EDP opleiding in 1986 opgericht, als vakgroep aan de Vrije Universiteit, waarbij Hans de Lange en Margaret van Biene-Hershey oprichters waren. Door het ontstaan van centrale opleidingen werd EDP kennis verspreid tussen bedrijven, voorheen hadden alleen accountantskantoren hun eigen interne opleidingen.

In het eerste jaar van de opleiding werd voornamelijk les gegeven aan andere hoofden van audit. Hierdoor werd de inhoud van de opleiding geverifieerd en werd de opleiding een resultaat van aanpakken vanuit de verschillende bedrijven. De initiële opbouw was gebaseerd op het uitwerken van het principe van het netwerk van controletotalen, want de opleiding moest antwoord geven op "Wat moet de accountant bijleren om ook de computer "even" mee te kunnen auditen?" Op deze vraag is nooit een voldoeninggevend antwoord gevonden, en daarmee werd beseft dat de EDP audit een vak apart is.

Dit kwam daarna ook in de opleiding naar voren. Margaret van Biene-Hershey introduceerde bijvoorbeeld het begrip technische auditor, oftewel een IT auditor die niet accountancy als achtergrond had. De opkomst van aparte EDP Audit opleidingen zorgde voor een professionalisering van de EDP audit rol en voor een duidelijkere positionering van IT audit als een op zichzelf staand vakgebied. Als gevolg hiervan verplaatste de aandacht van de audits zich. Was EDP audit initieel ondersteunend aan de beoordeling van de administratieve organisatie (AO) en de jaarrekening controle, door de aparte positionering en professionalisering op IT gebied verplaatste de nadruk van de IT audit zich naar de technische kant.

Samenvatting 1970-1990
Vanaf ongeveer 1970 tot 1990 is EDP Audit als vakgebied naast de traditionele accountancy ontstaan omdat de accountant niet langer meer om het informatiesysteem heen kon controleren. In deze eerste periode was een gestructureerde aanpak ontstaan, gebaseerd op de inrichting van het Mainframe en de waterval ontwikkelmethode, en in principe werden alle IT projecten door een EDP Auditor gevolgd. Daarnaast keek de EDP auditor ook naar de omgeving waarin een informatie systeem zich bevond, via de besturingssysteem audit en de rekencentrum audit.
De IT audits waren in deze periode gericht op het beoordelen van de opzet. De beoordeling van bestaan en werking kregen minder aandacht. Initieel waren de EDP audits ondersteunend aan de beoordeling van de administratieve organisatie, maar in de loop van de 80er jaren is de focus verplaatst naar de technischere kant. Er kwam zo dus meer focus op de operationele risico's naast de jaarrekening controle.

3.3 Het netwerk is het systeem – client/server (1990 – 2002)

Was eind jaren 80 het leven van een EDP auditor overzichtelijk, de 90er jaren brengen daar een drastische wijziging in. In deze periode verschijnt de client/server architectuur (CS), met kleinere midrange servers en intelligente clients, die allemaal aan elkaar geknoopt konden worden via TCP/IP netwerken. Deze ontwikkeling maakte veranderingen in IT ontwikkeltechnieken mogelijk en veranderingen in IT beheertechnieken noodzakelijk. De flexibiliteit die client/server leverde zorgde ook voor een verandering in de relatie tussen business en IT, waarbij met name de business zich veel prominenter met IT ging bezig houden.

Paragraaf 2.3.1 beschrijft de drie belangrijkste veranderingen vanuit het oogpunt van IT audit die hebben plaats gevonden binnen IT. Paragraaf 2.3.2. laat zien hoe de IT audit aanpak door deze veranderingen aangepast is.

3.3.1 Veranderingen door de client/server architectuur

De introductie van de client/server architecture heeft tot een de volgende drie hoofdveranderingen geleid.

1. Technische veranderingen van de client/server architectuur
2. Veranderingen in IT ontwikkelmethodes (methodes en organisatie)
3. Veranderingen in de IT beheermethodologie , door implementatie van ITIL en bijbehorende processen

De impact van de client/server architectuur op de techniek
De eerste hoofdverandering ten gevolge van de komst van de client/server architectuur was technisch van aard. Door de nieuwe midrange servers verloor het Mainframe zijn positie als centrale server en verzamelaar van informatie. In plaats daarvan verscheen een scala aan

verschillende server types, met bijbehorende eigen protocollen. Voorheen had een organisatie bijvoorbeeld een Mainframe met terminals en een SNA netwerk. Door client/server kon een combinatie ontstaan van bijvoorbeeld Mainframe, Tandem, Unix, OS/2, Windows NT, die benaderd werden via clients die draaiden op DOS, Olivetti, OS, en Windows en het totaal was verbonden via een netwerk van SNA, Token ring, Ethernet en Novell Netware. Het werd hierdoor significant lastiger om een totaal oordeel over de informatiebeveiliging te geven.

Voor de EDP auditor met kennis van het Mainframe was het een uitdaging om op de hoogte te blijven van alle nieuwe ontwikkelingen binnen deze stroom van nieuwe IT componenten. Een tweede uitdaging was een simpel numeriek feit. De nieuwe infrastructuur groeide exponentieel. Chargerend gezegd bracht elk IT project een nieuwe server de organisatie binnen, met applicatie specifieke settings qua netwerk en OS, waardoor de IT auditor bij een hoop projecten niet kon voortbouwen op al eerder beoordeelde technische componenten.
De derde uitdaging is dat de EDP auditor gevraagd werd om een mening over de combinatie van een applicatie, OS en infrastructuur, in plaats van een nieuwe applicatie gebaseerd op een bekende omgeving. De beveiliging van de applicaties werd meer en meer een combinatie van allerlei componenten met allemaal onderlinge afhankelijkheden. Hierdoor werd de scope van IT audits standaard groter dan voorheen.

Overall kan gesteld worden dat door deze nieuwe technologie het principe van de centrale veilige omgeving definitief vervangen is door de decentrale IT infrastructuur.

De verandering in IT ontwikkelmethodes en organisatie

De tweede verandering die het gevolg was van de opkomst van de client/server architectuur heeft betrekking op de manier waarop projecten gedaan werden. De client/server architectuur werd door de business in het algemeen met open armen ontvangen. De hoofdbelofte van client/server was namelijk dat het de doorlooptijd van IT projecten drastisch zou verkorten. Dit vertaalde zich in de mogelijkheid om als bedrijf flexibel met IT om te gaan, snel nieuwe producten te introduceren en hierdoor een strategisch voordeel te behalen. Doorlooptijd van projecten werd aldus tot een strategisch punt gemaakt en client/server beloofde dat het dit kon realiseren, en wel omdat het de volgende dingen mogelijk maakt:

- Het flexibel ontwikkelen door middel van iteratieve ontwikkelmethodes
- Het aanbieden van standaard oplossingen (in de vorm van één pakket van applicatie en alle infrastructuur die daar bij hoort)
- Het directer invloed uitoefenen op applicatie functionaliteit door business medewerkers

De eerste ontwikkeling was de promotie van iteratieve ontwikkelmethodes. Hierdoor kon al snel een eerste versie van een applicatie opgeleverd worden die al een deel van de functionaliteit leverde. Hierdoor werd de totale doorlooptijd van een project dus opgeknipt in kleinere delen met kortere doorlooptijd. Eigenlijk was het idee van de iteratieve ontwikkelmethode niet nieuw want de geestelijk vader van de watervalmethode, Winston Royce, publiceerde in 1970 al een artikel[3] waarin de iteratieve methode werd aangeprezen (Royce, 1970).

[3] "Managing the Development of Large Software Systems", Winston Royce, 1970: "*If the computer program in question is being developed for the first time, arrange matters so that the version finally delivered to the customer for operational deployment is actually the second version insofar as critical design/operations areas are concerned.*"

Als gevolg van de iteratieve ontwikkelmethode werd inderdaad de doorlooptijd van projecten verkort, wat leidde tot minder aandacht voor documentatie, met name geconsolideerde documentatie over meerdere iteraties heen ("ieder project documenteert voor zich"). Daarnaast kregen auditors minder tijd om een mening te vormen over de formele project documenten.

De tweede manier om doorlooptijd te verkorten was door standaard oplossingen te kopen en deze aan te passen aan de bedrijfsspecifieke processen. De aankoop van standaard oplossingen leidde tot nieuwe processen zoals leverancier selectie en contract management. Was het voor de EDP auditor al lastiger om tijdens een project de combinatie van infrastructuur, OS en applicatie te beoordelen, dit werd nog lastiger als de tijd hiervoor drastisch gereduceerd werd wanneer een standaard combinatie geïntroduceerd werd. Hoe garandeert de EDP auditor of de leverancier inderdaad het gewenste niveau van zekerheid en beveiliging in zijn pakket heeft verwerkt?

Het derde onderdeel van de client/server belofte was organisatorisch van aard. De nieuwe methodieken stelden de business in staat zelf directer bij de IT ontwikkelprojecten betrokken te zijn, waardoor sneller de beste/gewenste oplossing zou ontstaan. De client/server projecten werden inderdaad in toenemende mate gedreven vanuit de business, gebaseerd op een concrete business vraag. De business zag "Time to market", oftewel de project doorlooptijd, inderdaad als een van de belangrijkste factoren. De business zag een duidelijk strategisch voordeel om als bedrijf als eerste nieuwe functionaliteit op de markt kon brengen. IT kreeg hierbij een leverplicht toebedeeld en verloor zijn rol als leidende partij binnen projecten. Dit leidde onder andere tot:

1) Minder formele investeringsbesluiten, want de business kon directer over investeringen besluiten, waar voorheen de IT afdeling een sterk onderbouwd investeringsvoorstel moest maken om geld voor investeringen te verkrijgen.
2) Een verhoging van de mate waarin risico's binnen projecten geaccepteerd werden want de business medewerkers keken meer naar kansen dan bedreigingen. Dit telt voor zowel project risico's als de business risico's.
3) Verminderde aandacht voor het beheren van applicaties, want het applicatiebeheer is niet een verantwoordelijkheid van de business, en dus speelde dit minder als argument bij projecten. Dit leidde tot de eerder genoemde wildgroei aan infrastructuur, operating systemen en applicaties.

Implementatie van formele IT beheersprocessen (bijv. ITIL)

De derde significante wijziging ten gevolge van de opkomst van client/server heeft betrekking op het beheer van de nieuwe applicaties en infrastructuur. De IT organisaties werden geconfronteerd met een sterke groei aan infrastructuur en applicaties. De beheermethodieken die volstonden voor het Mainframe waren hier niet op berekend en daarom werd gekeken naar methodieken die hierbij konden helpen. Iets na 1980 had het CCTA (Central Computer and Telecoms Agency) de GITIM, (Government Information Technology Infrastructure Management) ontwikkeld. Deze methodiek was de voorloper van de IT Infrastructure Library (ITIL). Begin jaren 90 werd deze onder de nieuwe naam ITIL massaal omarmd door het bedrijfsleven. Ieder bedrijf had uiteraard zijn eigen specifieke variant van ITIL, maar ITIL vormde wel de de-facto standaard voor het beheer van rekencentra. De introductie van deze formele beheermethodiek was nodig om het overzicht van de explosief groeiende IT infrastructuur te behouden.

Samengevat heeft de opkomst van de client/server architectuur significante wijzigingen tot gevolg gehad voor 1) de IT techniek, 2) de IT ontwikkelmethodieken en 3) de IT beheermethodieken. De volgende paragraaf legt uit welke veranderingen dit tot gevolg had voor de IT audit aanpak.

3.3.2 Veranderingen in de IT audit aanpak als gevolg van Client/Server

De client/server invoering zorgde voor veranderingen in alle aspecten van de IT bedrijfsvoering. Dit gebeurde in een rap tempo en stelde daarmee de EDP auditers voor de lastige vraag hoe zij het veranderde landschap konden controleren. Hierbij was het maar de vraag of het management van IT zelf nog wel als "in control" beschouwd mocht worden. Het was in elk geval duidelijk dat de periode voorbij was dat alle projecten gevolgd kon worden en dat de EDP auditor nog een volledig beeld had van de gehele IT infrastructuur.

Als reactie op de client/server golf is binnen de EDP audit aanpak het concept van het auditen op basis van risico ontstaan. Dit is een logische stap, want als niet meer alle projecten en alle IT componenten geaudit kunnen worden, dan gaat de voorkeur uit naar onderdelen die de meeste impact hebben op de organisatie.
Merk op dat voor een deel van de EDP audit gemeente er een groot voordeel was. De meeste client/server applicaties waren gericht op de front-office, maar de daadwerkelijke transactieverwerking en het grootboek draaide nog op het vertrouwde Mainframe. In de vastleggin in het grootboek zitten "uiteraard" de grootste risico's, dus een audit aanpak op basis van een risico-inschatting zorgde voor een verantwoorde manier om de lastige client/server omgeving buiten beschouwing te laten.
Deze vorm van redeneren heeft mogelijk een tijdelijke uitkomst geboden, maar de orde van grootte van groei en impact van client/server zorgde er al snel voor dat de hedendaagse EDP auditor zich niet meer op alleen het Mainframe kon richten. Dit geldt uiteraard nog veel sterker voor bedrijven waarvan de IT infrastructuur volledig uit midrange servers bestaat.

De introductie van client/server heeft tot een aantal problemen met bijbehorende wijzigingen in de IT audit aanpak geleid:

- Het concept van auditen op basis van risico werd geïntroduceerd.
- De wildgroei aan nieuwe systemen, zowel technisch maar ook qua aantallen, die nog niet allemaal volwassen waren (e.g. Unix, NT) heeft geleid tot technische specialisatie binnen het EDP audit vak.
- Iteratieve ontwikkelmethodes kenden minder structuur, en een groter aantal projecten van kortere duur. De EDP auditor kon niet meer elk project inhoudelijk volledig volgen en richtte daarom de aandacht op het controleren van de project aansturing. De nadruk verschoof daardoor van de beoordeling van de inhoud van ontwerpen naar het beoordelen van het totstandkomingsproces van de ontwerpen en projectopbrengsten. In andere woorden: de IT auditor keek meer naar het project als een aantal stappen die goed uitgevoerd moeten worden, en minder naar de karakteristieken van het eindproduct wat via de stappen gebouwd wordt. Hierdoor ontstond onder andere de audit van de QA aspecten van projecten.
- De combinatie van applicatie, operating system en infrastructuur vereiste een integrale audit. De aandacht verplaatste van het testen van applicatie controles of OS controles naar het testen van een stelsel van elkaar aanvullende controles. Hierdoor testte de EDP auditor in toenemende mate ook de werking van de controles, wat vroeger nog door operationele auditors of accountants gedaan werd. Een voorbeeld hiervoor is de beoordeling van de autorisaties binnen een systeem. De autorisaties werden in de jaren 70/80 door de operationele auditors beoordeeld, maar deze beoordeling werd in toenemende mate naar de IT auditor verplaatst. Hierdoor is het werkgebied van de IT auditor sluipenderwijs groter gegroeid.

- De formalisering van beheermethodieken leidde tot een algemene standaard en deze werd toegevoegd aan de rekencentrum audits. Dit maakte het mogelijk om de beheerprocessen binnen rekencentra te auditen, wat noodzakelijk was omdat het aantal servers dat beheerd werd te groot werd om ze allemaal te auditen.
- Vanwege de toenemende complexiteit werd de expertise van de IT auditor in toenemende mate ingezet voor advies en consultancy werkzaamheden. Met name bij de externe accountants ontstonden significante adviesafdelingen.

Door al deze wijzigingen werd het werk van de EDP wel minder gestructureerd, waardoor de EDP auditor ook gedwongen werd om minder sterke waarborgen te geven. Werd in het jaren 80 bij projecten aangegeven dat bepaalde documentatie of een ontwerp een goede basis vormde voor een vervolgfase van een project, in de jaren 90 was het maximaal haalbare om aan te geven dat er geen extreem grote fouten of lacunes in de documentatie of het ontwerp zitten. De EDP auditor verzwakte dus zijn inbreng bij projecten van positieve zekerheid naar negatieve zekerheid.

Daarnaast verminderde ook de zekerheid bij rekencentra audits. Zoals gezegd werd de nadruk meer gelegd op de processen, omdat de infrastructuur te omvangrijk werd voor volledige controle. Steekproeven vonden wel plaats, maar het was goed mogelijk dat er applicaties waren die nooit geaudit waren. In principe zijn dit dan de minder kritieke applicaties, maar als deze groep van applicaties te groot wordt kan er een kritieke massa ontstaan aan applicaties die buiten de conclusie en zekerheid van de EDP auditor vallen.

De laatste significante wijziging betreft de rol van de IT auditor. Tot begin van de 90er jaren waren de activiteiten van de IT auditor gericht op de attest functie. Vanaf ongeveer 1993 werden vooral externe IT auditors ook ingezet als consultant of adviseur bij IT projecten, wat na enkele jaren een significant grotere markt bleek dan puur de IT audit functie. Deze ontwikkeling creëerde een potentieel conflict tussen de onafhankelijkheid van de IT auditor en het commerciële belang. De activiteiten van Arthur Andersen voor Enron zijn hiervan een duidelijk voorbeeld.

3.3.3 Overige ontwikkelingen

De technische ontwikkelingen hebben een significante impuls gegeven aan het EDP audit vakgebied, maar er zijn uiteraard meer invloeden geweest. Zoals al eerder genoemd heeft de Nederlandse overheid in 1993 de wet computercriminaliteit aangenomen. Daarnaast is het vakgebied ook vanuit een interne impuls verder ontwikkeld. De professionalisering via uniforme opleidingen is verder gezet naar de oprichting van de Nederlandse Orde van Register EDP auditors in 1992 (NOREA). De NOREA heeft onder andere standaarden vastgelegd in Studierapport 2 en geschrift 1.

Samenvatting 1990-2002

De introductie van de Client/Server architectuur heeft een impact gehad op vrijwel alle activiteiten van de EDP auditor. Door de toenemende complexiteit heeft de EDP auditor zich, noodgedwongen, in toenemende mate gericht op het audit van de processen om de IT componenten heen, in plaats van de IT componenten zelf. Waar de technische kant werd getest verplaatste de nadruk zich van beoordeling van de opzet naar beoordeling van de werking. Hierdoor verminderde de aandacht op de techniek zelf, en kwam de aandacht voor de administratieve organisatie weer terug. In het totaal is de zekerheid die de EDP auditor kon bieden wel verminderd.

3.4 Recente ontwikkelingen (2002 – heden)

In Juli 2002 werd in de Verenigde Staten de Sarbanes-Oxley (SOX) wetgeving aangenomen. Hoe en waarom SOX ontstaan is wordt in hoofdstuk 4 uitgewerkt want in dit hoofdstuk ligt de nadruk op de geschiedenis van EDP audit zelf.

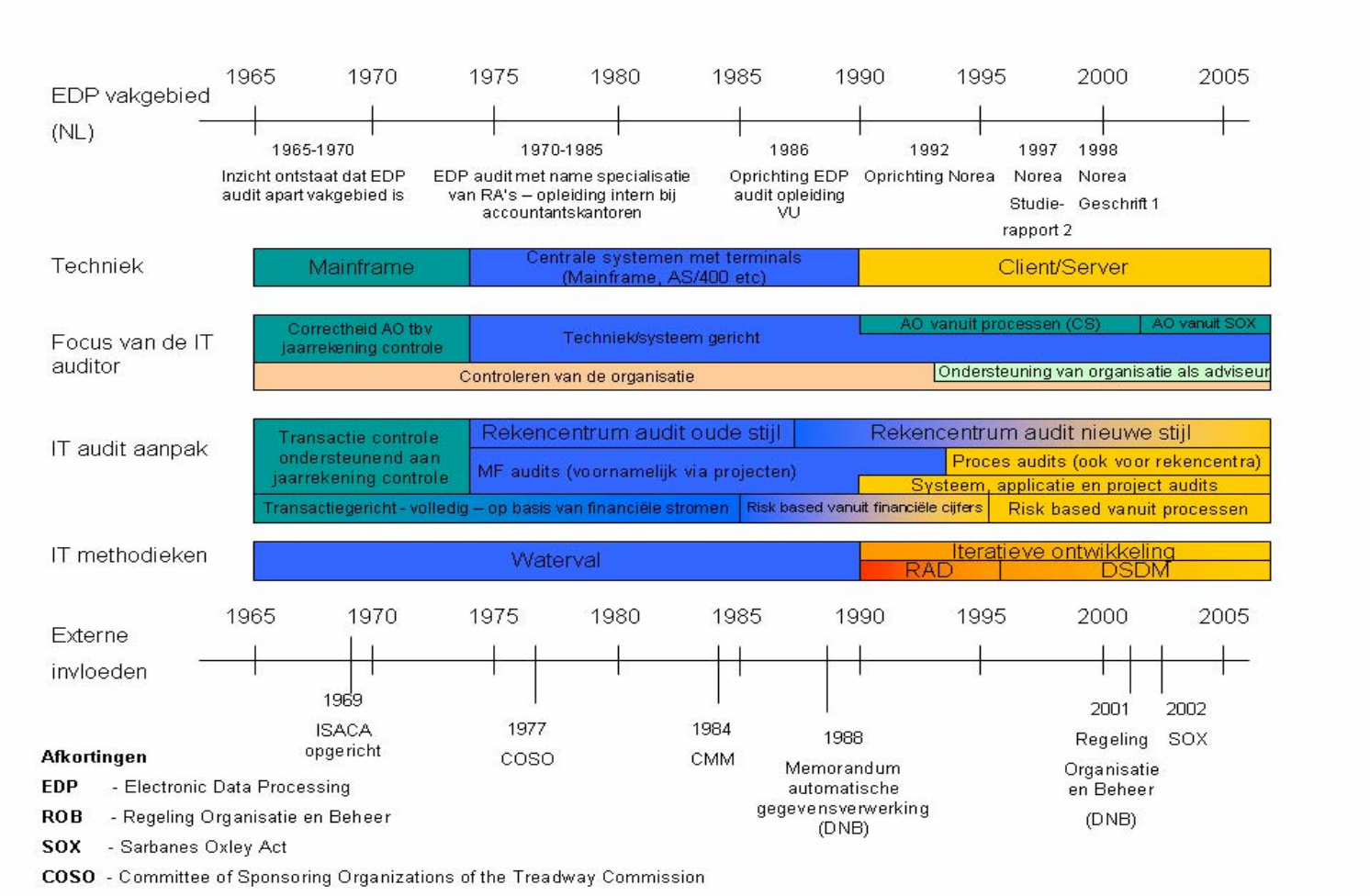
Hoewel SOX en EDP audit een groot raakvlak hebben is er tot op heden weinig tot geen integratie van beide onderdelen geweest. Specifieker: bij Nederlandse bedrijven wordt een audit planning gedefinieerd. Deze ontstaat vanuit een audit universum waar, op basis van risico overwegingen, de belangrijkste objecten uit geselecteerd worden en deze worden aangevuld met de SOX verplichtingen. De daarin vastgelegde audits zijn reguliere audits waar enkele extra activiteiten aan toegevoegd zijn om de SOX verplichtingen af te dekken. Dit resulteert dan ook in separate rapportages voor SOX en de audit zelf. Deze gang van zaken is ietwat bevreemdend als gerealiseerd wordt dat het idee achter SOX op hoog niveau hetzelfde is als de filosofie die vanuit de Nederlandse accountancy ontstaan is. Hoofdstuk 4 gaat hier dieper op in.

Naast SOX zijn er de laatste jaren continu wijzigingen in het IT domein, zoals bijvoorbeeld *e*-commerce en XML met alle bijbehorende toepassingen. Typerend is wel dat deze ontwikkelingen nieuwe technieken zijn maar deze hebben weinig impact gehad op de overall EDP audit aanpak. De onderliggende architectuur heeft namelijk nog steeds de karakteristieken van client/server.

Een andere ontwikkeling is de virtualisatie van de IT functionaliteiten. Applicaties worden hierdoor langzaam maar zeker combinaties van bestaande modules, aangevuld met nieuwe onderdelen, bijvoorbeeld volgens de objectgeoriënteerde gedachte (J2EE) of bij sterk configureerbare applicaties (SAP). Hiervoor geldt ook dat er wel bestaande EDP audit technieken zijn die worden toegepast om een mening te geven over dergelijke applicaties, maar dit gebeurt met behulp van de al bestaande EDP audit technieken zoals eens standaard applicatie werkprogramma.

Samenvattend geldt voor de laatste jaren dat er nog steeds in een significant tempo nieuwe ontwikkelingen zijn op het gebied van techniek, maar dit heeft niet geleidt tot vergelijkbaar grote veranderingen in de EDP audit aanpak als in de jaren daarvoor.

3.5 De Nederlandse IT audit geschiedenis in een oogopslag



4 De ontwikkeling van Sarbanes Oxley

Dit hoofdstuk werkt de tweede onderzoeksvraag uit: "*Hoe is SOX ontstaan en welke wijzigingen zijn er in de laatste jaren geweest qua aanpak?*". Daarnaast zijn enkele recente ontwikkelingen opgenomen om een beeld te geven hoe de toekomst van SOX er mogelijk uit kan zien. Dit beeld geeft richting aan de wijze waarop de IT audit rol binnen SOX in de volgende jaren ingevuld wordt.

4.1 Het ontstaan van de SOX wetgeving

In de periode 2000-2002 waren er verscheidene bedrijfs- en accountingschandalen in de VS. Enron is de meest bekende, maar ook Worldcom en Tyco International haalden de kranten. De overheid wilde het vertrouwen van aandeelhouders weer terugwinnen, en de Democratisch Senator Sarbanes werkte aan een voorstel om het bedrijfsleven aanzienlijk meer controles op te leggen, zodat ze adequater konden en moesten rapporteren naar de aandeelhouders. Omdat Senator Sarbanes wel erg drastische maatregelen wilde opleggen is volksvertegenwoordiger Oxley (republikein) gevraagd om Sarbanes te helpen om tot een werkbare wet te komen (in de VS maakt de republikeinse partij zich sterk voor minder regels voor het bedrijfsleven).

De rechtzaken en parlementaire enquêtes in de VS naar aanleiding van Enron, Worldcom en Tyco werden nauw gevolgd, en het volgende argument was veel mensen een doorn in het oog. Jeffrey Skilling, voormalig CEO van Enron noemde zichzelf een "control freak" die desalniettemin niet op de hoogte was van de dubieuze financiële praktijken die plaats vonden en die het uiteindelijke bankroet hebben bepaald. De betrokken CEO's en CFO's claimden onschuld door onwetendheid, hoe kan immers verwacht worden dat zij op hun niveau op de hoogte zijn van alles?
De uitkomst van de rechtzaken was in 2002 nog niet duidelijk, maar de Sarbanes-Oxley wetgeving heeft een duidelijke sectie toegevoegd om specifiek dit argument in het vervolg te ondervangen. In andere woorden, de CEO en CFO staan niet alleen in voor de correctheid van de financiële cijfers (sectie 302), maar moeten ook tekenen dat ze op de hoogte zijn van eventuele zwakheden die deze correctheid negatief kunnen beïnvloeden. Het kunnen aantonen van een adequate beheersing van de financiële processen is hiervoor een vereiste. En aldus deed SOX 404[4] zijn intrede in het bedrijfsleven.

4.2 De interpretatie en implementatie van de SOX in het bedrijfsleven

SOX tot op heden
Na alle schandalen was het voor de meeste Amerikaanse bedrijven wel duidelijk dat er iets moest veranderen en dat dit een impact zou hebben op hun bedrijfsvoering. In juli 2002 werd duidelijk wat de nieuwe juridische werkelijkheid was, maar het was nog verre van duidelijk hoe de wet geïnterpreteerd moest worden. Het enige wat men wist is dat SOX secties 302 en met name 404 een grote impact zouden hebben.

Dat SOX 404 inderdaad een grote impact had werd al spoedig duidelijk. Als gevolg hiervan is de datum waarop bedrijven moeten voldoen aan SOX meerdere keren vooruit geschoven. Initieel was de startdatum 2004, maar dit schoof naar 2005 voor de grote bedrijven in de VS, en naar

[4] Voor de inhoud van SOX 404, zie de bijlagen, paragraaf 0

2006 voor buitenlandse bedrijven die in de VS aan een beurs geregistreerd staan. Voor de kleine Amerikaanse bedrijven is de datum zelfs recentelijk verplaatst naar Juli 2007.

Voor de EDP auditors was de impact van SOX op IT in het begin niet duidelijk. De Public Company Accounting Overview Board (PCAOB) gaf in Juni 2005 Auditing Standards nr 2 uit waarin beschreven staat hoe bedrijven om moeten gaan met de SOX eisen. Deze standards waren gebaseerd op de accountancy aanpak in de VS en het risico raamwerk COSO werd als model aangeraden. De grote accountantskantoren konden op basis hiervan hun eigen aanpak uitwerken. Hierdoor werd de SOX aanpak vergelijkbaar aan het standaard werk wat gedaan werd voor de jaarrekeningcontrole.

Auditing Standards nr 2 van de PCAOB leidde indirect tot de situatie die hierboven werd beschreven. Omdat er vrijwel geen verdere handvatten aanwezig waren, werd Auditing Standards nr 2 leidend voor alle betrokkenen, waaronder het bedrijfsleven, alhoewel het gericht was op de externe accountant. Concreet betekent het dat bedrijven de volgende 3 activiteiten uitvoerden om hun SOX controles te definiëren:

1. Breng alle organisatieonderdelen in kaart
2. Beschrijf de bijbehorende processen
3. Beschrijf alle risico's binnen deze processen met de controles die deze risico's afdekken

Toen deze insteek voor het concretiseren van SOX controles duidelijk was, werd ook de aanpak voor de EDP auditors duidelijk: het wordt hetzelfde werk als de externe EDP auditors deden ten behoeven van de jaarrekening controle. Dit wil zeggen dat de EDP auditors betrokken raakten bij twee hoofdactiviteiten:

- Het testen van applicatieve, geautomatiseerde controles
- Het testen van rekencentrum controles waarop de geautomatiseerde controles op steunen

De bovenstaande stappen hebben geleid tot de identificatie van de business controles en applicatie controles, maar voor IT was niet volledig duidelijk welke eisen SOX zou stellen aan de IT controles. Een voorbeeld hiervan zijn de rekencentrum controles. De standaard SOX rekencentrum controles van drie Nederlandse banken die aan de NYSE geregistreerd staan variëren sterk in aantal, van 10 tot 25 of zelfs 40 standaard controles. Dit is niet een gevolg van de detaillering van controles (i.e. dat 1 controle eigenlijk 4 controles bevat), maar van daadwerkelijk grotere aandachtsgebieden en processen die als belangrijk worden beschouwd. Of er bij een of meerdere van deze banken sprake is van te weinig of teveel zekerheid is onduidelijk.

SOX heeft wel toegevoegde waarde gehad voor IT audit, want het heeft geleid tot een duidelijke verbinding tussen IT, de jaarrekening en de interne beheersing, waardoor bij bedrijven een beter inzicht en meer begrip is ontstaan voor de rol van IT en IT audit voor de interne beheersing van de bedrijfsvoering.

4.3 De toekomstvisie op SOX vanuit de Verenigde Staten

De vraag is of bedrijven er verstandig aan hebben gedaan om dezelfde stappen te volgen als de externe accountants. Het voordeel van deze keuze is dat in elk geval gegarandeerd is dat de bedrijven hoe dan ook zouden voldoen aan de SOX wetgeving. De bottom-up aanpak heeft namelijk geleid tot een groot aantal beschreven controles. Het daadwerkelijk voldoen aan de controles, inclusief het vereiste vastleggen en testen van de controles, werd hierdoor echter een onmogelijke opgave. In 2005 en 2006 stonden de grootste wijzigingen in de SOX aanpak dan ook volledig in het teken van het reduceren van controles. Dit was niet om SOX te marginaliseren,

maar om het überhaupt haalbaar te maken. De reductie was ook belangrijk om de focus te leggen op de controles die echt relevant zijn voor de jaarrekening, want door de start vanuit de processen waren ook veel operationele controles erin geslopen.

De voorzitter van de SEC (US Securities and Exchange Commission), C. Cox merkte in de meeting van de SEC (13-12-2006) droog op: "Door de afwezigheid van guidance heeft management de PCAOB auditing standaarden gebruikt om hun eigen testen te bepalen, wat nooit de bedoeling is geweest." (SEC, 2006) De SEC heeft recentelijk een aantal uitspraken gedaan om de nieuwe richting van SOX voor de komende jaren te schetsen. Het terugkerende thema hierbij is "top-down, risk-based". C. Hewitt, de hoofdaccountant van de SEC zei in dezelfde meeting letterlijk: "*In particular, the top-down, risk-based guidance would allow for effective, and, importantly, efficient, methods and procedures for conducting evaluations at smaller companies*".

Deze insteek vervangt in feite het COSO framework voor het nieuwere COSO Enterprise Risk Management (COSO ERM) framework. Hierbij wordt eerst op hoog niveau een risico inschatting gemaakt, en daarna worden pas de overgebleven processen en controles beschreven. In andere woorden: "snoeien aan het begin in plaats van snoeien aan het eind". Deze aanpak zal vrijwel zeker leiden tot een reductie van de complexiteit en controles.

De vernieuwde insteek wordt ook gedeeld door het IT Governance Institute (ITGI). In September 2006 heeft het ITGI een herziene versie uitgebracht van hun insteek voor de aanpak van IT binnen SOX. Hierin geven ze expliciet aan dat "*een van de meest belangrijkste geleerde lessen van de eerste jaren van Sarbanes-Oxley is dat de activiteiten op basis van een risico inschatting moeten gebeuren*". (ITGI, 2006) Door de ondersteuning van het ITGI wordt het waarschijnlijker dat de nieuwe richting van de SEC ook door de accountantskantoren gevolgd gaat worden. Dit is belangrijk want de externe accountantskantoren hebben een tegengesteld commercieel belang als het gaat om SOX werkzaamheden. Reductie van de SOX controles leidt immers ook tot minder werk voor externe accountants, terwijl deze de afgelopen jaren aanzienlijk personeel hebben geworven om de SOX testen uit te voeren.

Conclusie

SOX heeft een aanzienlijke impact gehad op het bedrijfsleven. De vraag is echter hoeveel hiervan door SOX komt en hoeveel hiervan komt door de keuzes die de bedrijven zelf hebben gemaakt. Het gebrek aan richting vanuit de SEC heeft de bedrijven in elk geval niet geholpen. Daarnaast hebben de straffen vanuit de Enron en Worldcom rechtzaken duidelijk gemaakt dat incorrecte en/of onvolledige financiele cijfers significante gevolgen kunnen hebben voor de topbestuurders persoonlijk. Dit heeft ertoe geleid dat bedrijven zeker wilden zijn dat ze aan SOX zouden voldoen.
De SEC heeft recentelijk aangegeven dat een "top-down, risk-based" aanpak tot een efficiënte SOX implementatie kan leiden, maar de vraag is of bedrijven bereid zijn om een SOX herstart te maken. Het is waarschijnlijker dat bedrijven de huidige aanpak zullen aanpassen aan de nieuwe uitleg dan dat ze met een schone lei beginnen.

5 Overlap en toekomst (onderzoeksvraag 3 en 4)

In hoofdstuk 2 en 3 is de geschiedenis van respectievelijk het EDP audit vakgebied en Sarbanes-Oxley weergegeven. In dit hoofdstuk worden beide geschiedenissen met elkaar vergeleken en wordt aangegeven hoe beide aanpakken geïntegreerd kunnen worden. Hiermee worden de laatste twee onderzoeksvragen beantwoord:

3. *Hoe verhoudt de verandering in SOX aanpak zich tot de evolutie van IT audit in de afgelopen 30/40 jaar?*
4. *Welke wijzigingen kunnen verwacht worden in de IT Audit SOX aanpak, op basis van de overeenkomsten met de IT audit geschiedenis?*

5.1 De overlap en verhoudingen tussen EDP audit en SOX

Voor de EDP auditors binnen Nederland was de beginsituatie voor SOX nog lastiger dan voor de collega's in de VS. Enerzijds was voor hen de wet initieel even onduidelijk, maar zelfs toen een aanpak duidelijk werd ontstond er frictie. De EDP audit aanpak die door de externe IT auditors voor SOX werd gebruikt was sterk gebaseerd op lijsten van standaard controles voor processen (de zogeheten "rule-based" aanpak die in de VS gebruikelijk is). Dit stond haaks op de EDP audit filosofie zoals deze in Nederland was gegroeid. In Nederland gaat de IT auditor immers uit van algemene principes, waarbij het management aan moet geven hoe zij aan deze principes voldoen (de "principle-based" aanpak).

Tabel 1 geeft aan wat de verschillen zijn tussen de hedendaagse EDP audit aanpak in Nederland en de wijze waarop de SOX werkzaamheden in bedrijven tot op heden plaats vinden:

	EDP audit heden '90 –heden	EDP Audit '70-'90	SOX
Transactiegericht testen	Nee	Ja	Ja
Scope op basis van jaarrekening	Nee (interne auditor) Ja (externe auditor)	Ja	Ja
Risk-based op hoog niveau	Ja	Nee	Nee
Principle/rule based testen	Principle based (int) Rule based (ext)	Principle based	Rule-based

Uit de tabel blijkt dat de SOX aanpak die tot op heden gebruikt is meer raakvlakken heeft met de EDP audit aanpak zoals deze in de jaren 70 en 80 werd gehanteerd, dan met IT audit werk in de jaren 90. Dit verklaart ook waarom voor SOX meestal een aparte aanpak gehanteerd is dan voor de reguliere audit activiteiten. Dit komt met name door de volgende verschillen tussen de SOX vereisten en de 90er jaren EDP audit aanpak:

1. De risico inschattingen die de basis vormen voor de EDP audit activiteiten zijn niet altijd duidelijk verantwoord vanuit de jaarrekening. Hierdoor was het noodzakelijk om voor SOX de link tussen de jaarrekening en controles opnieuw expliciet te maken. Aan de andere kant heeft dit geleid tot een overvloed aan controles, zoals toegelicht in paragraaf 4.2.
2. De huidige EDP audit aanpak maakt in het algemeen gebruik van minder grote steekproeven voor individuele controles, omdat de controles worden beoordeeld als onderdeel van een geheel van elkaar aanvullende en versterkende controles. SOX betreft het specifieke risico met betrekking tot de financiële rapportages en vereist dat de

controles die hier specifiek aan gerelateerd zijn uitputtend getest zijn, met verantwoordde steekproefgroottes.

3. De vastlegging van de testresultaten neemt binnen SOX een prominentere positie in, zo moeten bijvoorbeeld ook positieve resultaten worden opgeslagen. Bij interne auditors was de huidige EDP audit aanpak om met name de negatieve testresultaten goed te documenteren, omdat deze tot discussie kunnen leiden.
4. SOX heeft zich tot nu toe toegespitst op de controles die al bestaan. Vanuit projecten zullen veranderingen komen in het controle raamwerk, en deze nieuwe controles moeten beoordeeld worden op opzet en bestaan tijdens het project, zodat de controle effectief is vanaf het moment van implementatie. De huidige EDP audit project audit aanpak heeft nog geen specifieke onderdelen om de SOX controles al tijdens het project mee te kunnen testen. Als gevolg hiervan worden de applicatie eigenschappen en –instellingen pas getest nadat de applicatie in productie genomen is, in plaats van tegelijk met het al bestaande testtraject.
5. De interne IT auditor heeft per definitie een wat afgezonderde positie binnen het bedrijf om zijn onafhankelijkheid te borgen. De auditor rapporteert aan de raad van bestuur over de werkzaamheden van het management. Voor SOX voert de IT auditor mogelijk dezelfde testwerkzaamheden uit, maar nu namens het management zelf. Het management is immers verantwoordelijk voor het aftekenen voor de SOX 404 verklaring. Dit heeft een directe impact op de positie en werkwijze van de IT auditor.

Paragraaf 4.3 beschrijft hoe deze vijf verschillen opgelost kunnen worden. Eerst is het echter nodig om kritisch naar onderzoeksvraag 4 te kijken.

5.2 Aanpassing onderzoeksvraag 4

Nu de verschillen en overeenkomsten tussen SOX en de huidige EDP audit aanpak helder zijn lijkt het of de 4e onderzoeksvraag beantwoord kan worden. Er is echter een complicerende factor. Bij het begin van dit onderzoek is een viertal onderzoeksvragen geformuleerd. Hierbij werd impliciet de aanname gemaakt dat zowel de geschiedenis van EDP audit en de huidige EDP audit aanpak een gegeven zijn, en dat beiden op dit moment al een vaste vorm hebben. SOX werd beschouwd als een nog variabel proces is waarin wijzigingen kunnen en zullen plaats vinden. De verwachting was dus dat SOX door de EDP audit aanpak zou wijzigen, maar niet andersom. Vandaar dat de onderzoeksvraag luidde: "*Welke wijzigingen kunnen verwacht worden in de IT Audit SOX aanpak, op basis van de overeenkomsten met de IT audit geschiedenis*?"

Uit de interviews naar de geschiedenis van EDP audit is echter naar voren gekomen dat vrijwel alle geïnterviewden vinden dat de huidige EDP audit aanpak een aantal goede onderdelen van de vroegere aanpak heeft verloren. Vanwege de overlap tussen SOX en de vroegere aanpak is dan ook meerdere keren de hoop uitgesproken dat SOX de huidige EDP audit aanpak weer kan voorzien van deze sterke punten. Een verbetering van de EDP audit aanpak is uiteraard altijd welkom, maar dit betekent wel dat de initiële aanname waarop de 4e onderzoeksvraag gebaseerd is incorrect is.

Het vervallen van de geldigheid van de aanname betekent dat de onderzoeksvraag algemener gesteld moet worden. Immers bestaat nu ook duidelijk de optie dat de EDP audit aanpak door SOX beïnvloed wordt. Deze overweging leidt tot de volgende herziene formulering van onderzoeksvraag 4: "*Hoe kunnen de EDP Audit en SOX aanpak efficiënt geïntegreerd worden, uitgaande van de overeenkomsten en verschillen tussen beide aanpakken*?" Deze vraag wordt beantwoord in de volgende paragraaf.

5.3 De integratie van EDP audit en SOX

De slotvraag van deze scriptie betreft hoe de aanpak van EDP audit en SOX het beste geïntegreerd kunnen worden. Voordat dit uitgewerkt wordt moet eerst de kanttekening geplaatst worden dat de uitwerking nooit een "*one size fits all*" oplossing kan zijn.

Ten eerste wordt gesproken over "de EDP audit aanpak" alsof er een unieke EDP aanpak bestaat, maar de realiteit is dat elk groot bedrijf en accountancy kantoor zijn eigen variant heeft. Voor SOX geldt dat de algemene stappen voor het bepalen van de controles eerder al beschreven zijn. Deze stappen zijn echter niet verplicht, SOX stelt alleen maar eisen en elk bedrijf mag zelf invullen hoe ze aan de eisen voldoen. Dit betekent dat elk bedrijf een SOX aanpak heeft die op hoofdlijnen vergelijkbaar maar in de details uniek is.

Ten tweede is een uitwerking alleen een oplossing als deze tot realiseerbare stappen leidt die bedrijven kunnen nemen om tot een geïntegreerde aanpak te komen. Er kunnen echter omstandigheden zijn binnen bedrijven die betekenen dat bepaalde stappen niet haalbaar zijn, zoals bijvoorbeeld de bereidheid om de SOX werkwijze fundamenteel te herzien. Een theoretische uitwerking van een EDP audit aanpak kan niet alle varianten van bedrijfsmoreel, politiek en business strategie meenemen, vandaar dat dit ook niet in deze uitwerking wordt opgenomen.

Als gevolg van de kanttekening is gekozen om de uitwerking hieronder niet tot een diep detailniveau uit te werken. De uitwerking zal op hoog niveau beschrijven hoe de eerder geconstateerde verschillen opgelost kunnen worden. Voor implementatie zullen de daadwerkelijke details per bedrijf en situatie ingevuld moeten worden. Het is hierbij wel van belang om te redeneren vanuit de principes die de basis vormen van SOX en IT veiligheid in zijn algemeen. Met andere wo0rden, het realiseren van een praktische integratie van SOX en IT audit is meer dan het samenvoegen van nieuwe controle lijsten aan een bestaande aanpak. Het meeste voordeel wordt pas bereikt zodra de onderliggende principes als leidraad voor integratie gebruikt worden.

De verschillen die in paragraaf 4.1 genoemd zijn geven de grootste verschillen weer. Aan de andere kant geven ze ook de richting aan hoe SOX en de huidige EDP audit geïntegreerd kunnen worden. Merk op dat deze richting niet nieuw is, maar eerder oud, want de integratie komt neer op het combineren van de sterke punten van de oude EDP audit technieken/SOX technieken met de sterke punten van de huidige EDP audit technieken. De punten zijn een direct gevolg van de eerder genoemde verschillen, de cijfers geven aan welke verschillen uit 4.1 gerelateerd zijn aan de punten:

- Bepaling van de audit planning (1,5)
- Aanpak van audits op applicaties en rekencentra (2,3)
- Project audit aanpak (3,4)
- Samenwerking met de business (5)

5.3.1 Bepaling van de audit planning

De basis voor audit activiteiten wordt bepaald door de risico's te inventariseren voor alle objecten binnen het bedrijf (het audit universum). De grootte van de bruto (inherente) risico's bepaalt welke objecten geaudit moeten worden (de audit planning) In het algemeen gelden hiervoor de volgende hoofdoverwegingen:

- Financiële risico's
- Juridische verplichtingen

- Operationele risico's
- Vorige audit resultaten

In principe sluit SOX hier naadloos op aan, want het voldoen aan SOX is een juridische verplichting, en de activiteiten voor SOX zijn gericht op het verkrijgen van zekerheid omtrent de financiële rapportage, en daarmee nauw verbonden aan de financiële risico's.

De juridische verplichtingen, operationele risico's en vorige audit resultaten beïnvloeden op continue basis het audit universum. Wijzigingen hierin komen immers van duidelijk afgebakende activiteiten zoals een nieuwe wet, een project wat een nieuw bedrijfsproces of IT systeem invoert of een afgeronde audit.

De financiële risico's zijn echter afhankelijk van een externe markt die kan wijzigen zonder dat het bedrijf zelf verandert. In andere woorden: als de afzetmarkt van een bedrijf stevig wijzigt hoeft er geen verandering te zijn in de processen of controles, maar de financiële risico's (en daarmee de nadruk voor de auditor) veranderen wel. Daarnaast geldt voor de financiële risico's dat deze voor SOX niet altijd door de audit afdeling worden bepaald, maar door een financiële afdeling of een separate SOX groep. Om de SOX aanpak al in het begin te integreren met de audit aanpak is het dan ook sterk aan te bevelen om het bepalen van de financiële risico's een gezamenlijke activiteit van alle betrokken afdelingen te maken.

Deze gezamenlijk bepaalde financiële risico's moeten ook leiden tot een overzicht van de daarbij betrokken informatiesystemen, wat een essentieel onderdeel is van de audit planning voor de EDP auditor. Door deze aanpak wordt dus de link tussen het werk van de EDP auditor en de jaarrekeningcontrole weer expliciet gemaakt.

Het audit universum wordt uiteraard nog uitgebreid met IT systemen vanuit de andere drie risicogebieden, maar daar is geen wijziging in huidige aanpak voor nodig. Wel geldt dat er efficiëntie mogelijk is, afhankelijk van de verdere inrichting van de business. Als de operationele risico's binnen de organisatie bijvoorbeeld beheerst worden via het COSO Enterprise Risk Management (COSO ERM) model, dan ligt het voor de hand om de vaststelling van de financiële en operationele risico's te combineren, omdat dit tegelijkertijd in het COSO ERM model plaats vindt. Welk risico model gebruikt wordt is echter een bedrijfsbesluit wat veel verder strekt dan alleen de audit aanpak, en wordt daarom hier niet verder uitgewerkt.

Gegeven een audit planning waarin een SOX integraal onderdeel is, zullen daarna de gedefinieerde objecten daadwerkelijk geaudit moeten worden. Hieronder worden de hoofdpunten uitgewerkt die relevant zijn voor individuele applicatie of rekencentrum audits, project audits en de noodzakelijke samenwerking met de business partijen.

5.3.2 Applicatie en rekencentrum audits

Voor de audits van applicatie audits of rekencentrum audits geldt dat de relevante controles in opzet, bestaan en werking getest moeten worden. De keuze van welke controles getest moeten worden wordt bepaald door de risico's of controle doelstellingen die geïdentificeerd zijn (vanuit de vaststelling van de audit planning). Een deel van de controles van een regulier werkprogramma zal verplicht zijn vanuit SOX. In paragraaf 4.1 is gebleken dat de integratie van SOX en de huidige EDP aanpak met name speelt bij:

- De bepaling van de steekproefgrootte

- De vastlegging van de bewijzen van de test activiteiten
- De rapportage van de testresultaten

Steekproefomvang
Vanuit SOX moet de werking van bepaalde controles binnen een bedrijf aangetoond worden. In het algemeen is voor het verantwoord bepalen van de werking van een controle een omvangrijkere steekproef nodig dan in de huidige EDP audit praktijk gebruikelijk is. Het is aan te raden om de steekproefomvang van SOX ook te gebruiken als minimumeis voor het testen van de overige controles. Door het herintroduceren van significante steekproeven wordt de zekerheid die bij entiteit audits gegeven wordt ondersteund door relevante statistische overwegingen, en krijgt de business een beter zicht op de staat van dienst dan wanneer alleen opzet en bestaan bekeken worden. Omdat tijd uiteraard een beperkende factor is, is het wel van belang om ook voor de niet-SOX controles een duidelijk afbakening te maken welke controles echt belangrijk zijn (zie ook verder bij het onderdeel “samenwerking met management”).

Vastlegging en rapportage
Voor de vastlegging en rapportage van gevonden punten speelt een nog niet eerder genoemd probleem. De SOX resultaten zijn in principe in naam en onder verantwoordelijkheid van management getest en deze moet dus eigenlijk toegang hebben tot deze resultaten ten behoeve van verantwoording. Om hier efficiënt mee om te gaan ligt een pragmatische aanpak het meest voor de hand. De EDP auditor legt 1 dossier aan, waarin bewijs van alle controles van de audit wordt opgeslagen. Door het markeren van de SOX relevante bewijzen kan de EDP auditor achteraf management op efficiënte wijze voorzien van extra informatie, als deze nodig is. Gezien het verschillende publiek voor het audit rapport en SOX rapport is het wel aan te raden om een separaat rapport te maken met alleen de SOX resultaten (een SOX deficiëntie is uiteraard sowieso een audit bevinding).

5.3.3 Project audits

Als een IT auditor een project audit uitvoert kan de auditor vanuit verschillende rollen acteren. Hij kan puur de kwaliteit bewaken, als business partner acteren (advies), de project structuur en project management controleren en als laatste kan de IT auditor de geautomatiseerde controles van het nieuwe systeem beoordelen. Met name de laatstgenoemde rol kan uitgebreid worden om SOX efficiënt te integreren.
Merk op dat hierbij met name de projecten bedoeld worden die impact hebben op systemen die relevant zijn voor SOX. Voor de overige projecten kan de uitbreiding van de rol ook ingevoerd worden ten behoeve van een uniforme werkwijze, maar dit zal op basis van een separaat kosten/baten besluit moeten gebeuren. Voor de SOX relevante projecten zal de EDP auditor twee activiteiten moeten doen:

- De EDP auditor moet meer betrokken worden bij de beoordeling van de opzet van toekomstige controles. Hij zal de nieuwe controles ook moeten beoordelen in relatie tot het al bestaande controle raamwerk. De EDP auditor kan de opzet van de controles het best beoordelen door middel van het functioneel en technisch ontwerp (FO en TO). Dit zal in combinatie met het herschrijven/ vervangen van de bestaande SOX controles moeten gebeuren om te garanderen dat er geen extra risico’s ontstaan. De EDP auditor kan hierdoor tijdig aangeven of het nieuwe informatiesysteem qua opzet voldoende controles heeft om de juistheid en volledigheid van de financiële stromen te garanderen (in samenwerking met de Register Accountant waar nodig).
- Voor SOX moeten de applicatieve controles expliciet getest worden voor bestaan en werking. Dit kan efficiënt in het bestaande project proces ingebed worden, door de SOX relevante controles en functionaliteiten expliciet in het testproces van het project op te

nemen. De EDP auditor kan de testresultaten en documentatie beoordelen, en eventueel een of meerdere testen zelf waarnemen of hertesten. Op basis hiervan kan de EDP auditor het bestaan van de in het FO en TO gedefinieerde controles vaststellen. Hierdoor hoeven deze testwerkzaamheden in productie niet herhaald te worden en wordt de vastlegging van de resultaten al geleverd door het project.

Door de IT auditor te betrekken bij projecten die een impact hebben op SOX relevante systemen wordt de beoordeling van de opzet van de controles op het vroegst mogelijke moment uitgevoerd. De beoordeling van bestaan en werking wordt efficiënt afgehandeld door de integratie met al bestaande activiteiten.

5.3.4 Samenwerking met de business

Eerder is al aangegeven dat SOX, en risicobeheersing in het algemeen, een verantwoordelijkheid zijn van het management van het bedrijf. De EDP auditor geeft slechts aan in welke mate dit succesvol lukt en geeft handvatten om eventuele problemen op te lossen. Dit betekent dan ook meteen dat elke oplossing die de EDP auditor, EDP audit afdeling of zelfs totale audit afdeling bedenkt zeer waarschijnlijk geen ideale oplossing zal zijn als het management en de overige bedrijfsafdelingen hierbij niet betrokken zijn geweest.

Dit blijkt ook uit de eerdere aanbevelingen. De financiële afdelingen en de audit afdelingen moeten gezamenlijk de financiële risico's bepalen. De business projecten zullen zelf expliciet onderdelen in hun project aanpak moeten toevoegen om de SOX onderdelen adequaat mee te nemen. Op hoog niveau moet de business zelf aangeven hoe zij hun risico's willen identificeren en beheersen, en of zij dit bijvoorbeeld via COSO of COSO ERM willen doen. Hier kan de (EDP) auditor wel bij helpen.

Wat echter wel een significante impact heeft op de werkzaamheden van de EDP auditor is het type van controles wat binnen het bedrijf gebruikt wordt om de volledigheid en juistheid van de financiële stromen en rapportages te waarborgen. In zijn algemeenheid kan gesteld worden dat controles van hoger niveau leiden tot een verminderde hoeveelheid testwerk. Het volgende voorbeeld van logische toegangsbeveiliging illustreert dit.

Omdat IT verweven is met bedrijfsvoering is te stellen dat een goede logische toegangsbeveiliging van essentieel belang. Een bedrijf kan het risico op fouten in de gebruikersadministratie verminderen door een geformaliseerd proces te gebruiken voor het toevoegen, wijzigen en verwijderen van gebruikers en rechten. Stel dat dit proces de controle is waar de organisatie op steunt. De auditor zal dan dit proces moeten controleren, wat gezien het aantal wijzigingen al snel een aanzienlijke inspanning kan betekenen. Merk op dat management in deze situatie sterk steunt op een correcte uitvoering van mutaties op de gebruikersadministratie, ze hebben in deze situatie geen direct inzicht in de inhoudelijke correctheid van de administratie.

Een andere mogelijkheid is om een controle op hoger niveau te definiëren, door management periodiek de gebruikersrechten te laten controleren. Enerzijds leidt dit tot een periodieke opschoning van eventuele fouten en interne rapportage van de correctheid van de gebruikersadministratie. Aan de andere kant wordt de hoeveelheid testwerk voor de auditor ook minder, want deze beoordeelt in dit geval of de periodieke controle goed is verlopen. Mocht blijken dat sommige managers mogelijk te lichtzinnig met de controle omgegaan zijn, bijvoorbeeld als ze vrijwel direct hebben aangegeven dat alles in orde is, dan kan de auditor altijd nog een stap verder gaan door terug te vallen op de controle van de administratie zelf.

Uit het bovenstaande blijkt dat de EDP auditor een extra rol heeft als het gaat om het efficiënt uitvoeren van de testwerkzaamheden voor SOX. De auditor zal actief het management moeten ondersteunen in het definiëren van sterke SOX controles op het juiste niveau. De voordelen hiervan strekken zich verder uit dan SOX, want de "juiste" controles zullen management extra inzicht geven in de risico's die zij op dagelijkse basis lopen.

Controles op hoger niveau zijn alleen zinnig als er gebouwd kan worden op een al bestaande laag van goede controles. Het hogere niveau gaat immers ten koste van de detaillering. Als de correctheid van de detaillering echter door een andere controle afgedekt wordt, of de detaillering is achteraf nog op te vragen, dan zijn controles op hoger niveau efficiënter en inzichtelijker voor management. Als een bedrijf bijvoorbeeld een aantal controles op laag niveau laat uitvoeren door middel van continue monitoring, dan kan het management zich concentreren op het resultaat van deze controle in plaats van de controle zelf.

5.4 Samenvatting

De aanpak die voor SOX tot op heden gebruikt is heeft geleid tot een werkwijze die voornamelijk overeenkomsten heeft met EDP audit zoals dit in de periode 1970-1990 werd beoefend. Dit betekent dat voor de integratie van SOX en de huidige EDP audit aanpak geen wezenlijke nieuwe EDP audit technieken bedacht hoeven te worden. De technieken die voor de Mainframe audits gebruikt werden kunnen hergebruikt worden. Om tot een efficiënte integratie te komen is echter meer nodig. De auditors zullen actief betrokken moeten zijn bij het bepalen van de financiële risico's, beoordelen van nieuwe SOX controles tijdens projecten en het (her)definiëren van controles op het juiste niveau.

Persoonlijke terugblik

De afgelopen jaren ben ik betrokken geweest bij SOX, zowel voor het testen als het ontwikkelen van de test methodiek. Bij het herzien van de testmethodiek speelden een aantal discussies en argumenten waarvan ik het gevoel had dat deze al eerder gevoerd waren. Hieruit volgde mijn vermoeden dat er een relatie is tussen enerzijds SOX en de bijbehorende ontwikkelingen en anderzijds de ontwikkeling van EDP audit als vakgebied. Mijn idee was dan ook dat de toekomst van de SOX aanpak in Nederland voor de komende jaren te voorspellen zou zijn door extrapolatie van de relatie. Dit heeft geleid tot de onderzoeksvraag met bijbehorende opsplitsing in onderliggende subvragen.

Bij de interviews bleek dat mijn vermoeden niet volledig klopte. Er is inderdaad een duidelijke relatie tussen SOX en EDP audit, met name tussen SOX en het EDP audit vakgebied zoals dit in de 70/80er jaren bestond. Uit de beschrijving van de ontwikkeling van het EDP audit vakgebied bleek echter dat de algemene indruk van de geïnterviewden was dat de ontwikkelingen van de Client/Server architectuur hadden geleid tot een situatie van verminderde IT risico beheersing. Het gevolg hiervan was dat de EDP auditor ook minder effectief werd. De huidige EDP audit aanpak kon hierdoor ook geen definitieve vorm zijn.

Deze constatering heeft SOX voor mij in een ander daglicht gezet. Uiteraard blijft het voor bedrijven een kostbare verplichting en zijn de SOX testwerkzaamheden niet het spannendste onderdeel van de EPD audit activiteiten. Desalniettemin heeft SOX ook een aantal sterke punten die de zwakheden kunnen opheffen die tijdens de client/server periode ontstaan zijn. De verplichting van SOX zorgt hierbij voor een impuls om ook de vereiste bijbehorende veranderingen in de organisatie te kunnen realiseren.

Om dit voor elkaar te krijgen zal het audit vakgebied wel een grotere rol moeten opeisen dan de huidige rol van beoordeler en tester van controles. In het bijzonder zullen interne auditors zich meer moeten laten gelden in het voortraject van de SOX werkzaamheden, zoals het bepalen van de risicogebieden.

Een ander aspect wat naar voren is gekomen is dat het EDP audit vakgebied initieel gevormd is door een aantal richtinggevende “voortrekkers” (bijv. Margaret van Biene-Hershey). Dit is een standaard fenomeen bij startende bedrijven en mogelijk ook startende vakgebieden. Op een gegeven moment groeit een organisatie tot een formaat dat de rol van dergelijke voortrekkers niet meer voldoende kan zijn, waarna op natuurlijke wijze een soort van “managementstructuur” moet ontstaan. Voor het EDP audit vakgebied kan deze overgang geïnterpreteerd worden via het ontstaan van de NOREA.
De bovenstaande modellering van het ontstaan en de ontwikkeling van bedrijven is bekend als het groeifasemodel van Greiner (Greiner, 1972). Het is zeker interessant om dit aspect van EDP audit te bekijken, zeker omdat het groeifasemodel nog een drietal verdere niveaus van professionalisering onderkent. Dit paste echter helaas niet meer binnen de scope voor deze scriptie.

Annex A

SOX – section 404

S404(a)(1)(2) 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 to contain an Internal control report, which shall— (1) state 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.

S404(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.

SOX – section 302

(a) REGULATIONS REQUIRED.—The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—
(1) the signing officer has reviewed the report;
(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;
(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;
(4) the signing officers

a. are responsible for establishing and maintaining internal controls;
b. have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
c. have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
d. have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

a. (A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and
b. (B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

Referenties

- Managing the Development of Large Software Systems, Winston Royce, 1970.
- The essential handbook of internal auditing, K. H. Spencer Picket, 2005, ISBN 0-470-01316-8.
- Managing the Audit Function: A Corporate Audit Department Procedures Guide, 3rd Edition, M.P. Cangemi, T. Singleton, 2003, ISBN: 978-0-471-28119-1.
- Fundamentals of the internal auditing function, 2003 (http://media.wiley.com/product_data/excerpt/90/04712811/0471281190.pdf)
- Inleiding EDP auditing, van Praat/Suerink, 2003, ISBN 90-44-00199-X.
- PCAOB auditing standard nr 2, 2004, http://www.pcaobus.org.
- The Sarbanes Oxley Act of 2002
- IT Control Objectives for Sarbanes Oxley – The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting, ITGI, 2004.
- IT Control Objectives for Sarbanes Oxley – The role of IT in the design and implementation of internal control over financial reporting, 2nd edition, ITGI, 2006.
- IT Auditing – An object oriented approach, M. van Biene-Hershey, 1995, ISBN 9061557763.
- Bestuurlijke informatiesystemen en automatisering, T.M.A. Bemelmans, 1987, ISBN 90 207 1548 8.
- SEC minutes of meeting 13-12-2006: http://www.sec.gov/news/digest/2006/dig121306.txt
- Vitale Organisaties (5e druk), J. Heijnsdijk, 2004
- Evolution and revolution as organisations grow, Harvard Business Review, 4, 37-46, Greiner, L. E. (1972).
- Management en Organisatie (8e druk), D. Keuning/ D.J. Eppink, ISBN 902073265X.