BEDRIJFSECONOMISCHE WETENSCHAPPEN

2010
2011

master in de toegepaste economische wetenschappen:
accountancy en financiering

Masterproef

Informatiesystemen binnen het auditproces

Promotor :
dr. Mieke JANS

Copromotor :
Prof. dr. Tensie STEIJVERS

Kevin Bervoets

Masterproef voorgedragen tot het bekomen van de graad van master in de toegepaste economische wetenschappen , afstudeerrichting accountancy en financiering

universiteit hasselt
UNIVERSITEIT VAN DE TOEKOMST

Universiteit Hasselt | Campus Diepenbeek | Agoralaan Gebouw D | BE-3590 Diepenbeek
Universiteit Hasselt | Campus Hasselt | Martelarenlaan 42 | BE-3500 Hasselt

universiteit hasselt
UNIVERSITEIT VAN DE TOEKOMST

2010
2011

BEDRIJFSECONOMISCHE WETENSCHAPPEN

master in de toegepaste economische wetenschappen: accountancy en financiering

Masterproef

Informatiesystemen binnen het auditproces

Promotor :
dr. Mieke JANS

Copromotor :
Prof. dr. Tensie STEIJVERS

Kevin Bervoets

Masterproef voorgedragen tot het bekomen van de graad van master in de toegepaste economische wetenschappen , afstudeerrichting accountancy en financiering

universiteit hasselt
UNIVERSITEIT VAN DE TOEKOMST

Voorwoord

Deze eindverhandeling kwam tot stand in het kader van mijn opleiding Toegepaste Economische Wetenschappen, afstudeerrichting Accountancy en Financiering, aan de Universiteit Hasselt. Het gebruik van informatiesystemen– en technologieën en de toepassingen ervan binnen een bedrijfscontext, hebben mij steeds sterk geïnteresseerd. Gedurende mijn opleiding heb ik daarenboven een interesse ontwikkeld voor het externe auditgebied. In deze verhandeling kreeg ik de kans om beide nader te onderzoeken en te linken aan elkaar.

Tijdens het opstellen van mijn eindverhandeling werd ik door heel wat mensen bijgestaan. Langs deze weg wil ik hen dan ook mijn oprechte dank betuigen voor hun steun en begeleiding.

Vooreerst wil ik mijn promotor dr. Mieke Jans en mijn co-promotor prof. dr. Tensie Steijvers bedanken voor hun deskundige begeleiding en raadgevingen.

Hiernaast zou ik ook ik graag een woord van dank richten aan de bevoorrechte getuigen. Het gaat om Jan Borzée, Jeroen Decroos, Koen Claessens en Peter Leyman. Zij hebben de benodigde tijd vrijgemaakt om al mijn vragen te beantwoorden. Door hun bijdrage kon ik de bevindingen uit de literatuur vergelijken met de praktijksituatie.

Ten slotte wil ik ook nog mijn ouders, zus en vrienden bedanken voor de morele steun tijdens mijn opleiding en bij de realisatie van deze masterproef.

Samenvatting

Het belang van een goed werkend auditsysteem werd duidelijk na een reeks fraudeschandalen in 2001 en 2002. Om het vertrouwen in de markt te herstellen, werd in Amerika de Sarbanes-Oxley wetgeving ingevoerd. Deze wet voerde onder meer onafhankelijkheidsvoorschriften in voor de externe auditor en verplichte ondernemingen om een intern beheersingssysteem op te zetten rondom hun financiële verslaggeving. De externe auditor dient dit systeem vervolgens te controleren op efficiëntie en effectiviteit. Het grote belang van de audit werd hiermee bevestigd en vastgelegd in een regelgeving. Ook in België volgde men het Amerikaanse voorbeeld met de invoering van de Belgische Corporate Governance Code.

Het is dan ook niet verwonderlijk dat er binnen de auditstandaarden steeds meer aandacht wordt besteed aan technieken die in staat zijn om de audit efficiëntie te verhogen. Eén van de belangrijkste hiervan zijn CAATTs of 'computer assissted Audit tools and techniques'. Een verwijzing hiernaar is onder meer terug te vinden in SAS - Statement on Auditing Standards - nr. 99 en nr. 104-111. Maar ook in de interne auditstandaarden zoals Institute of Internal Auditors Standard 1210 en 1220.A2.

Deze eindverhandeling heeft als doel een overzicht te geven van de belangrijkste informatiesystemen die ter beschikking staan van de auditor en de mogelijke toepassingen ervan binnen het auditproces. De centrale onderzoeksvraag luidt dan ook als volgt: "Welke rol spelen informatiesystemen in het auditproces?". Het auditproces verwijst hierin zowel naar de interne, als naar de externe audit. Het praktijkprobleem, de centrale onderzoeksvraag en de deelvragen worden nog in meer detail besproken in **hoofdstuk één**. Ook wordt er een overzicht gegeven van de toegepaste methodiek voor wat betreft de literatuurstudie en het empirisch onderzoek.

Hoofdstuk twee en drie geven een korte uiteenzetting van de werking van en de begrippen rondom een audit. In **hoofdstuk twee** wordt een korte beschrijving gegeven van de verschillende auditfasen, gaande van de planningsfase tot de opvolging van aanbevelingen. Nadien wordt een vergelijking gemaakt tussen het interne en het externe auditgebied. Er wordt gezocht naar de belangrijkste verschillen en overeenkomsten tussen beide gebieden, die een invloed kunnen uitoefenen op het gebruik van informatiesystemen. In **hoofdstuk drie** wordt deze basisinformatie verder uitgebreid met een omschrijving van de belangrijkste beheersings- en auditbegrippen in relatie tot continuous auditing. Het gaat om begrippen zoals interne controle, beheersing, continuous auditing, e.d..

In het **vierde hoofdstuk** wordt er overgegaan tot de eigenlijke bespreking van de gebruikte audit informatiesystemen. In eerste instantie wordt er nagegaan welke wijzigingen in de bedrijfsomgeving hebben geleid tot de ontwikkeling en invoering van dit soort systemen. Nadien wordt een beschrijving gegeven van de huidige auditomgeving en de informatiesystemen die erbinnen gebruikt worden. Deze systemen kunnen worden onderverdeeld in twee categorieën, namelijk audit productiviteit tools en de meer data gerichte CAATTs. Hoewel beide worden besproken, wordt de focus voornamelijk gelegd op de CAATTs. Deze tools zullen immers een grotere positieve invloed uitoefenen op de audit efficiëntie dan de audit productiviteit tools. Naast een overzicht van de beschikbare CAATTs, wordt ook het gebruik ervan binnen de interne en externe audit besproken, samen met de voor- en nadelen ervan.

In **hoofdstuk vijf** wordt er verder ingegaan op het begrip continuous auditing. Er wordt nagegaan hoe dergelijke technieken binnen de audit kunnen worden toegepast en aan welke voorwaarden moet zijn voldaan om een succesvol CA systeem op te zetten. Naar de focus van deze verhandeling wordt er meer aandacht besteed aan de technologische vereisten waaraan voldaan moet zijn. Aan de hand van deze voorwaarden en de audit doelstellingen, wordt vervolgens een CA model opgesteld met een detailbespreking van de mogelijke onderliggende architecturen. Ook wordt de implementatie van een dergelijk model besproken en geïllustreerd aan de hand van twee praktijkvoorbeelden uit de literatuur. Het systeem dient immers steeds stapsgewijs te worden afgestemd op de specifieke bedrijfseigenschappen, succesfactoren en risicofactoren van de onderneming in kwestie.

Hoewel het gebruik van CA technieken verschillende voordelen met zich meebrengt, wordt er op dit moment nog geen intensief gebruik van gemaakt. Vooral binnen de externe audit lijkt CA enkele bijkomende problemen met zich mee te brengen. Deze problemen worden verder besproken in **hoofdstuk zes**. Hiernaast wordt er ook aandacht besteed aan de compatibiliteit van de verschillende CA architecturen met de externe auditstandaarden.

In **hoofdstuk zeven** wordt overgegaan naar het empirisch onderzoek. Dit onderzoek werd uitgevoerd in de vorm van een bevraging van bevoorrechte getuigen, actief binnen de interne- of de externe audit. Om te verzekeren dat de verkregen informatie zo breed mogelijk toepasbaar is, wordt binnen de interne audit geopteerd voor één beursgenoteerde onderneming, aangevuld met interne audit consultants. De externe audit wordt bestudeerd binnen een combinatie van Big Four auditkantoren en een kleiner auditkantoor. Aan de hand hiervan kunnen de bevindingen uit de literatuurstudie worden gekoppeld aan de praktijksituatie binnen België.

De bevindingen uit de literatuurstudie en het empirische onderzoek worden in **hoofdstuk acht** samengebracht om een voorspelling te kunnen maken omtrent de toekomst van informatietechnologieën binnen de audit. In het **negende hoofdstuk** worden tot slot de conclusies geformuleerd en worden er enkele voorstellen gegeven voor toekomstig onderzoek.

Inhoudsopgave

Lijst van tabellen en figuren

Hoofdstuk 1: Probleemstelling

1.1. Praktijkprobleem: omschrijving en situering

Het begrip audit is zeker niet nieuw. Volgens historici werd er reeds in 4000 B.C. een soort van registratie- en controlesysteem toegepast binnen ondernemingen en regeringen. Richard Brown (1905) beschrijft de wortels van auditing als volgt:

"The origin of auditing goes back to times scarcely less remote than that of accounting…Whenever the advance of civilization brought about the necessity of one man being in trusted to some extent with the property of another, the advisability of some kind of check upon the fidelity of the former would become apparent." (Ramamoorti, 2003).

Het is echter pas sinds de invoering van de Sarbanes-Oxley (SOX) wetgeving in Amerika (2002) dat de audit sterk aan belang gewonnen heeft. Tot die tijd had men vertrouwd op de eerlijkheid van het management bij het opstellen van de financiële verslagen. Na een reeks van schandalen werd het echter duidelijk dat het voeren van een deugdelijk ondernemingsbeleid geen evidentie is. De bekendste voorbeelden hiervan zijn Enron, een Amerikaans energiebedrijf (2001) en WorldCom, een Amerikaanse telecom-onderneming (2002). In beide bedrijven werd de winst telkens opnieuw kunstmatig verhoogd, werden verliezen verborgen gehouden en keerden managers zichzelf hoge verloningen uit. Toen deze fraude aan het licht kwam, volgden de faillissementen elkaar snel op en verloor het publiek alle vertrouwen in de bedrijfswereld. Zowel het interne als het externe controlesysteem had immers jarenlang gefaald.

Om dit soort falingen in de toekomst te vermijden en om het vertrouwen in de markt te herstellen, werd de Sarbanes-Oxley wetgeving ingevoerd. Deze wet, opgesteld door Paul Sarbanes en Michael Oxley, focust op 'corporate governance'. Bedrijven worden verplicht tot het voeren van een deugdelijk ondernemingsbeleid met onder meer een doorlopende informatieverplichting, regels voor het vermijden van belangenconflicten en verplichtingen in verband met de onafhankelijkheid van de audit. Ook wordt de oprichting en werking van de Public Company Accounting Oversight Board besproken. Een nieuw orgaan dat zal instaan voor de controle op het onafhankelijke en informatieve karakter van de auditrapporten (Dumortier, 2005).

Ook in andere landen ging men over tot de invoering van soortgelijke wetten. In België ontstond zo de 'Belgische Corporate Governance Code' (BCGC, 2005), voor beursgenoteerde ondernemingen en 'Code Buysse' (2005), voor niet-beursgenoteerde ondernemingen. In tegenstelling tot de SOX wetgeving, waar er geldboetes en gevangenisstraffen volgen bij niet naleving, zijn deze codes 'soft

law'. Dit houdt in dat ze juridisch niet bindend zijn en er geen sancties zijn voorzien voor eventuele slechte bestuurders. De codes zijn gebaseerd op het 'pas toe of leg uit' principe. Een onderneming mag dus van de voorschriften afwijken, zolang er een verklaring wordt gegeven waarom men dit doet. Het toezicht op de naleving van deze richtlijnen berust bij de raad van bestuur, de aandeelhouders van de vennootschap, de commissaris en de Commissie voor het Bank-, Financiën- en Assurantiewezen (CBFA)[1], eventueel aangevuld met andere mechanismen (Belgische Corporate Governance Code, BCGC, 2009).

Eén van de belangrijkste artikelen van de SOX wetgeving is artikel 404. Dit artikel bevat regels met betrekking tot de financiële rapportering en de interne beheersing van bedrijven. Het 'Committee of Sponsoring Organizations of the Treadway Commission' (COSO, 1992) definieert interne beheersing als een proces, gericht op het verkrijgen van een redelijke mate van zekerheid omtrent het bereiken van doelstellingen in de volgende categorieën:

- De effectiviteit en efficiëntie van bedrijfsprocessen
- De betrouwbaarheid van de financiële informatieverzorging
- De naleving van relevante wet- en regelgeving

Aangestuurd door het grote belang van corporate governance, kijkt men hier naar interne beheersing vanuit een risico gebaseerde benadering (Weidenmier en Ramamoorti, 2006). Volgens COSO (2004) bestaat interne beheersing uit vijf met elkaar in verband staande delen:

1. De controleomgeving: de controleomgeving is de cultuur in een organisatie met betrekking tot de interne beheersing. Het vormt de basis voor hoe risico's binnen de onderneming worden beschouwd en aangepakt.
2. Risicobeoordeling: met een risicoanalyse probeert men het risico dat beheersingsproblemen zich voordoen, doordat zowel preventieve als repressieve beheersingsmaatregelen ineffectief zijn, terug te brengen tot een aanvaardbaar niveau. Er dient hier een afweging te worden gemaakt de beheersingskosten en de mogelijke voordelen van beheersing.
3. Controlemaatregelen: controlemaatregelen zijn bedoeld om afwijkingen van vooraf vastgestelde criteria te detecteren en/of te voorkomen. Het gaat dan respectievelijk over repressieve en preventieve maatregelen.
4. Informatie en communicatie: het opzetten van een goede informatiedeling en interne communicatie is essentieel om interne beheersing mogelijk te maken. Bovendien moet de informatie van kwalitatief goede aard zijn. Informatie vormt dus zowel een object van beheersing als een beheersingsinstrument.

[1] In 2010 veranderde de CBFA van naam en werd FSMA: "Financial Services and Markets Authority".

5. Bewaking van de goede werking: beter bekend onder zijn Engelse term monitoring. De efficiënte werking van het risicomanagementsysteem wordt bewaakt en waar nodig worden wijzigingen aangebracht. Er zijn twee vormen van monitoring, namelijk als continu proces en als specifieke evaluatie op een bepaald moment. (Vaassen et al., 2007).

Sectie 404 van de SOX wetgeving vereist dat ondernemingen de interne beheersing rond hun financiële verslaggeving op een dusdanige manier hebben ingericht, dat materiële onjuistheden in de jaarrekening voorkomen of gedetecteerd worden (Steegers, 2008). Ze dienen dit systeem naar efficiëntie te beoordelen en het resultaat hiervan in de financiële verslaggeving op te nemen. De externe auditor dient vervolgens deze uitspraken te verifiëren (PwC, 2008).

Ook de BCGC heeft een soortgelijke verplichting. Dit is af te leiden uit volgende artikels:

5.2./14 - De monitoring van de doeltreffendheid van de interne controle- en risicobeheerssystemen van de vennootschap, ingesteld door het uitvoerend management, wordt minstens een keer per jaar uitgevoerd en heeft tot doel de doeltreffende identificatie, beheer en publicatie van de belangrijkste risico's te verzekeren (met inbegrip van de risico's m.b.t. fraude en de naleving van de bestaande wetgeving en reglementen) overeenkomstig het door de raad van bestuur goedgekeurde kader.

5.2./17 - Er wordt een onafhankelijke interne auditfunctie opgericht die de middelen en de know-how tot haar beschikking heeft welke zijn aangepast aan de aard, de omvang en de complexiteit van de vennootschap. Indien de vennootschap niet beschikt over een interne auditfunctie, wordt minstens jaarlijks beoordeeld of daartoe een noodzaak bestaat.

5.2./18 - Het auditcomité beoordeelt het werkprogramma van de interne auditor, rekening houdend met de complementaire rol van de interne en externe auditfuncties. Het ontvangt de interne auditverslagen of een periodieke samenvatting ervan. (BCGC, 2009)

Uit bovenstaande uiteenzetting blijkt duidelijk dat zowel de interne controlefunctie als de interne en externe auditfunctie van groot belang is binnen het bedrijfsleven. Elke methode die in staat is om de efficiëntie binnen deze gebieden te vergroten, dient dan ook voldoende aandacht te krijgen.

Sinds het jaar 1945 is er binnen ondernemingen een evolutie merkbaar van manuele naar geautomatiseerde bedrijfsprocessen. Ook binnen de interne beheersingsprocessen werd er daarom overgeschakeld op een door informatiesystemen[2] (IS) ondersteund proces. COSO (2009) vermeldt

[2] In deze context verwijst IS naar alle op computer gebaseerde informatiesystemen die door organisaties worden gebruikt en de onderliggende technologieën ervan (Laudon, 2008).

informatietechnologie (IT) dan ook expliciet als tool om de interne beheersing te kunnen verbeteren (Marks en Jay, 2009). De nieuwe omgeving waarin bedrijven actief zijn vereist immers dat controles automatisch, dynamisch, geïntegreerd, preventief en in real-time verlopen (Weidenmier en Ramamoorti, 2006).

Deze evoluties hebben ook binnen de audit geleid tot de toepassing van IT ter verbetering van de traditionele audit. Een voorbeeld hiervan is terug te vinden in SAS - Statement on Auditing Standards - Nr. 48 dat handelt over de audit van bedrijven waarbinnen computergestuurde accountingsystemen worden toegepast. Het gebruik van 'Computer Assisted Audit tools and techniques' oftewel CAATTs wordt hierin besproken en aangeraden om de efficiëntie van de audit verhogen (Lovata, 1990).

Indien informatiesystemen correct gebruikt worden, stellen ze een auditor in staat om over te schakelen naar een meer continu controleproces, beter bekend als 'continuous auditing' (CA):

"A methodology for issuing audit reports simultaneously with, or a short period after, the occurrence of the relevant events" (Vaserhelyi en Halper, 1991).

De voordelen van een continu proces werden reeds in 1991 besproken en aangetoond door Vasarhelyi en Halper in twee piloot implementatieprojecten bij Siemens en een Amerikaanse zorgaanbieder. Tegelijkertijd duidden ze echter ook op de implementatiemoeilijkheden die zich kunnen voordoen, met één van de grootste hiervan de zeer hoge implementatiekosten (Debreceny et al., 2005).

Sinds de adoptie van Enterprise Rescource Planning (ERP) systemen zijn deze kosten echter sterk afgenomen (Debreceny et al., 2005). ERP- systemen bieden één informatiesysteem voor de organisatiebrede coördinatie en integratie van belangrijke bedrijfsprocessen. Het systeem verzamelt gegevens uit alle bedrijfsprocessen en slaat ze op in één gegevenssysteem of database. Interne controle en auditing systemen kunnen vervolgens worden gebaseerd op deze database, waardoor de implementatiekosten afnemen (Laudon, 2006).

Een studie van PwC (2006) toonde aan dat al 50% van de Amerikaanse bedrijven gebruik maakt van continuous auditing technieken en 31% van de resterende bedrijven had plannen om in de nabije toekomst een CA systeem te implementeren.

Uit dit alles blijkt duidelijk dat informatiesystemen een waardevolle bijdrage kunnen leveren aan het auditproces. In combinatie met het grote belang van de audit, is verder onderzoek omtrent de beschikbare IS dan ook aangewezen.

1.2. Onderzoeksopzet

1.2.1. Centrale onderzoeksvraag

Deze masterproef heeft als doelstelling het bepalen van de rol en het belang van informatiesystemen binnen het auditproces. Er wordt nagegaan op welke manier deze systemen het domein van de interne en externe audit hebben beïnvloed en in de toekomst nog zullen beïnvloeden. De centrale onderzoeksvraag luidt als volgt:

Welke rol spelen informatiesystemen in het auditproces?

1.2.2. Deelvragen

Om de centrale onderzoeksvraag beter te kunnen beantwoorden worden er enkele deelvragen opgesteld. Deze deelvragen vormen een uitbreiding op de centrale onderzoeksvraag en zullen leiden tot een beter onderbouwd antwoord.

1. Hoe worden informatiesystemen gebruikt binnen het auditgebied?

De complexiteit en automatisering van accounting systemen is zodanig sterk toegenomen dat het gebruik van zogenaamde computer assisted audit tools and techniques (CAATTs) sterk wordt aangeraden door de meer recente auditstandaarden (Lovata, 1990).

Binnen deze deelvraag wordt er vooraleerst nagegaan welke IS momenteel aangewend kunnen worden ter verbetering van het auditproces. Er wordt nagegaan of er reeds ten volle gebruik wordt gemaakt van deze mogelijkheden, of opdat er wordt vastgehouden aan minderwaardige legacy systemen.

Daarnaast worden ook de voor- en nadelen van het gebruik van IS bij een audit onderzocht. Er wordt bepaald in welke mate deze systemen kunnen bijdragen aan het opzetten van een efficiënt en effectief auditsysteem dat voldoet aan de voorschriften van de SOX en/of de Belgische Corporate Governance Code 2009.

2. In hoeverre verschilt het interne en externe auditgebied van elkaar met betrekking tot het gebruik van CA systemen?

In tegenstelling tot de verwachting van Alles et al. (2002) voor de doorvoering van de SOX wetgeving, waren het niet de externe auditors maar wel de interne auditors die continuous auditing sterk hebben geadopteerd en gestuurd. Het gebruik van IS is bij een externe audit dan ook veel minder ingeburgerd. De oorzaken hiervan zijn zowel situationeel als juridisch en worden in deze deelvraag nader onderzocht (Alles et al., 2008).

3. Hoe zal dit in de toekomst evolueren?

Binnen deze deelvraag wordt nagegaan op welke manier audit ondersteunende IS zich in de toekomst nog zullen ontwikkelen. Het gaat dan zowel om de systemen op zich, als het gebruik ervan binnen de interne- en externe audit. Omdat deze evolutie deels afhankelijk is van enigszins onvoorspelbare technologische evoluties, worden de voorspellingen gedaan aan de hand van zowel het literatuur- als empirisch onderzoek.

1.3. Toegepaste methodiek

Om bovenstaande vragen te kunnen beantwoorden wordt gebruik gemaakt van verschillende onderzoeksstrategieën. Allereerst wordt er een literatuurstudie uitgevoerd. In de literatuur moet er een onderscheid worden gemaakt tussen primaire, secundaire en tertiaire bronnen. Om de betrouwbaarheid van de informatie te kunnen garanderen, wordt er voornamelijk gebruik gemaakt van secundaire bronnen en meer bepaald wetenschappelijke artikels, boeken en onderzoeksrapporten. Niet- wetenschappelijke bronnen zoals websites worden enkel gebruikt indien deze als betrouwbaar beschouwd kunnen worden.

Deze literatuurstudie zal het in de eerste plaats mogelijk maken om een algemeen kader te schetsen van het onderwerp. Omwille van het grote belang van de audit en het steeds groter wordende belang van informatiesystemen, zijn er reeds heel wat onderzoeken verschenen hieromtrent. Opmerkelijk is dat in deze artikels verschillende auditing begrippen door elkaar worden gebruikt, zonder dat er een eenduidige definitie van wordt gegeven. Interne controle, interne beheersing, continuous audit, continuous assurance,… zijn slechts enkele voorbeelden van begrippen die vaak onterecht met elkaar worden verward. Uit de literatuurstudie zal dan ook een duidelijke definitie van elk van deze begrippen moeten volgen.

De artikels die gebruikt worden in de literatuurstudie worden gezocht met behulp van elektronische databases zoals EBSCOHOST, Google Scholar en ScienceDirect. De artikels die op deze manier gevonden werden handelen voornamelijk over de situatie en wetgeving binnen Amerika en gaan terug tot 1990. Slechts een klein gedeelte heeft betrekking op de Europese situatie. Mits het grote belang van de SOX wetgeving ten opzichte van de verschillende Europese codes, is dit ook niet verwonderlijk.

Naast een literatuuronderzoek wordt er extra informatie verzameld aan de hand van een empirisch onderzoek. De gekozen strategie hierbij is de bevraging van bevoorrechte getuigen. Deze praktijkstudie zal pas worden uitgevoerd na de afronding van de literatuurstudie. Op deze manier kan de literatuur worden gekoppeld aan de praktijksituatie en kan de literatuur verder worden aangevuld waar deze tekortschiet. Na beide onderzoeken zou er voldoende informatie moeten beschikbaar zijn om een antwoord op alle deelvragen te kunnen formuleren.

Hoofdstuk 2: De auditor en het auditproces

Om de rol en het belang van IS binnen een audit te kunnen inschatten, is een basiskennis omtrent het auditproces vereist. Vermits deze eindverhandeling zowel handelt over het interne als het externe auditgebied, dient er bovendien een duidelijk onderscheid te worden gemaakt tussen beide gebieden. In dit hoofdstuk wordt er daarom een korte uiteenzetting gegeven over het auditproces en worden de verschillen en overeenkomsten tussen de auditgebieden besproken.

2.1. Het auditproces

Een audit bestaat steeds uit vier op elkaar volgende stadia. In een eerste fase, de planningsfase, wordt er voldoende informatie verzameld om de onderneming en de ondernemingsprocessen grondig te leren kennen. Op deze manier kunnen de belangrijkste risico- en succesfactoren worden geïdentificeerd en kan er bepaald worden wat de beste manier is om bewijsmateriaal te verzamelen. Gedurende de veldwerkfase worden vervolgens de benodigde bewijsstukken verzameld en geanalyseerd. Onder bewijsstukken wordt onder andere verstaan: CA systeemrapporten, verslagen, bevragingen, uittreksels, e.d.. Zodra er voldoende auditbewijs is verzameld om een opinie te formuleren, wordt deze opgenomen in het auditrapport tezamen met eventuele aanbevelingen. In een vierde en laatste fase dient de auditor na te gaan of zijn aanbevelingen ook werkelijk werden doorgevoerd (Mercken, 2010).

2.2. Verschil tussen de interne en externe auditor

Zowel interne als externe auditors hanteren professionele standaarden en ethische codes die zijn opgesteld door hun respectievelijke beroepsorganisaties. Voor België is dit het 'Institute Of Internal Auditors Belgium' voor de interne auditors en het 'Instituut voor bedrijfsrevisoren' voor externe auditors. Ondanks enkele overeenkomende doelstellingen, zoals het verzekeren van betrouwbare financiële resultaten en een efficiënt intern controlesysteem, zijn er toch nog grote verschillen in de reikwijdte van de audit en de afstand van de auditor tot de onderneming[3].

Interne auditors maken deel uit van de organisatie zelf. Hun doelstellingen worden bepaald door het management en de raad van bestuur. Externe auditors werken daarentegen onafhankelijk van de onderneming. Hun doelstellingen worden grotendeels bepaald door de professionele

[3] Een uitgebreide vergelijking wordt gegeven in bijlage 9.

standaarden, in overleg met de raad van bestuur en/of het audit comité (IIABEL, 2005). Dit verschil wordt ook aangegeven in SAS 65 – "Considering the work of internal audit":

"The role of internal auditing is determined by management, and its objectives differ from those of the external auditor who is appointed to report independently on the financial statements. The internal audit function's objectives vary according to management's requirements. The external auditor's primary concern is whether the financial statements are free of material misstatements"

De reikwijdte van een interne audit is zeer uitgebreid. Op deze manier ondersteunt het de onderneming bij de interne controle, het risicomanagement en bij het verbeteren van de operationele processen. De interne audit richt zich op zowel financiële als niet-financiële informatie. Dit in tegenstelling tot de externe auditors, die zich primair richt op het formuleren van een jaarlijkse, onafhankelijke mening omtrent de financiële organisatie van de onderneming (IIABEL, 2005).

2.3. Relatie tussen de interne en externe audit

Ook de relatie tussen de interne en de externe audit komt aan bod in SAS 65:

- The external auditor should obtain a sufficient understanding of internal audit activities to identify and assess the risks of material misstatement of the financial statements and to design and perform further audit procedures.
- The external auditor should perform an assessment of the internal audit function, when internal auditing is relevant to the external auditor's risk assessments.
- Liaison with internal auditing is more effective when meetings are held at appropriate intervals during the audit period. The external auditor would need to be advised of and have access to relevant internal auditing reports and be kept informed of any significant matter that comes to the internal auditor's attention which may affect the work of the external auditor. Similarly, the external auditor would ordinarily inform the internal auditor of any significant matters which may affect internal auditing.

Een voorbeeld hiervan is terug te vinden in de planningsfase van de externe audit. In deze fase zal het auditrisico, oftewel het risico dat er een verkeerde auditopinie wordt afgeleverd, worden vastgesteld. Aan de hand hiervan zal vervolgens de diepte en materialiteit van de audit worden bepaald. Een belangrijk element van het auditrisico is het controlerisico, oftewel het risico dat het interne controlesysteem van de onderneming er niet in slaagt om een materiële afwijking te detecteren. Indien een onderneming een slecht intern controle- of auditsysteem hanteert, zal het

controlerisico hoger liggen. Bijgevolg zal ook het auditrisico toenemen[4]. Een goed werkende interne auditafdeling zal het interne controlesysteem verbeteren en zal zo ook het auditrisico verlagen (Mercken, 2010).

SAS 65 geeft bovendien aan dat externe auditors zich mogen baseren op controles uitgevoerd door de interne auditor. Dit mogen ze echter enkel doen indien ze tevreden zijn met de graad van bekwaamheid en objectiviteit van de interne auditor (Pop et al., 2008).

Vanuit de professionele standaarden worden externe auditors dus aangezet tot samenwerking met de interne auditafdelingen. Ook het Institute of Internal Auditors (IIA) beveelt regelmatige samenkomsten aan, waarbij interne en externe auditors hun gemeenschappelijke belangen kunnen bespreken. Op deze manier kunnen zij hun complementaire vaardigheden verbeteren en wordt het begrip van elkaars werkzaamheden vergroot (IIABEL, 2005).

De sterke relatie tussen de interne en externe audit heeft tot gevolg dat vele auditmethodes, tools en technologieën binnen beide beroepen kunnen worden aangewend. In wat volgt zal er dan ook enkel een onderscheid worden gemaakt tussen het interne- en externe auditberoep, indien er een duidelijk verschil is tussen beide gebieden.

[4] Zie schema bijlage 3.

Hoofdstuk 3: Begrippen en definities

Het auditing gebied kent een grote verscheidenheid aan sterk bij elkaar aansluitende begrippen. In vele gevallen bestaat er bovendien een sterke interrelatie tussen bepaalde audit- en managementfuncties. Om eventuele verwarring tussen begrippen te vermijden, wordt er in dit hoofdstuk een uiteenzetting gegeven van de belangrijkste audit- en controlebegrippen[5].

3.1. Interne controle

Het begrip interne controle wordt vaak verward met het Engelse 'internal control', dat verwijst naar interne beheersing. Het Nederlandse interne controle verwijst naar de toetsing van de realiteit aan een vooraf vastgestelde norm. In deze definitie bevat het dus een terugkijkend en een constituerend element, gericht op het verbeteren van de oordeelsvorming en de activiteiten van anderen. Zowel bij het vastleggen van gegevens, als het verzorgen van informatie speelt IT hier een belangrijke rol (Vaassen et al., 2007). Interne controle is een managementfunctie en zal in deze verhandeling niet verder worden besproken. Indien het begrip controle wordt gebruikt, verwijst dit naar interne beheersing zoals besproken in het volgende punt.

3.2. Interne beheersing

De definitie van interne beheersing bevat naast een terugkijkend en constituerend element ook een vooruitkijkend element. Zoals reeds vermeld definieert COSO (1992) interne beheersing als een proces, gericht op het verkrijgen van een redelijke mate van zekerheid omtrent het bereiken van doelstellingen in de volgende categorieën:

- De effectiviteit en efficiëntie van bedrijfsprocessen
- De betrouwbaarheid van de financiële informatieverzorging
- De naleving van relevante wet- en regelgeving

[5] Bespreking aan de hand van de schema's opgenomen in bijlage 1 en 2.

General Accounting Office[6] voegde hier nog een vierde doelstelling aan toe, namelijk (Vaassen et al., 2007):

- Bewaking van de waarden van de organisatie

Het verschil tussen interne controle en interne beheersing bevindt zich dus in de manier waarop men afwijkingen van de norm tracht te voorkomen. Indien het management beslissingen neemt die gericht zijn op het voorkomen van afwijkingen ten opzichte van de norm, dan is dit een vooruitkijkend element en spreekt men over interne beheersing. Indien men zich enkel richt op het achteraf detecteren van afwijkingen spreekt men over interne controle. Net zoals interne controle, is ook interne beheersing een managementfunctie.

De vijf componenten waaruit interne beheersing bestaat werden reeds eerder aangehaald[7]. Van deze componenten is voornamelijk de laatste component, namelijk monitoring, belangrijk binnen het domein van auditing. De mate waarin het management zich bezig houdt met monitoring heeft immers een directe invloed op de focus van de audit activiteiten[8]. Door gebruik te maken van informatietechnologieën, kan het monitoringproces meer continu verlopen. In dat geval spreekt men van continuous monitoring.

3.3. Continuous monitoring

Continuous monitoring (CM) kan worden gedefinieerd als een proces waarin gebruik wordt gemaakt van informatiesystemen om de werking en prestaties van bedrijfsprocessen, inclusief de interne controlesystemen, op een meer real-time wijze te volgen. CM ondersteunt het management door continu significante afwijkingen van verwachte uitkomsten te signaleren en tijdig bij te sturen. Er wordt nagegaan of alle systemen en besturingselementen werken zoals die zijn ontworpen en of transacties worden verwerkt in overeenstemming met de voorgeschreven richtlijnen en procedures (Meegeren, 2008).

---

[6] De GOA is een onafhankelijke instelling die erop toeziet dat belastinggelden in de VS op de juiste manier worden aangewend (Vaassen et al., 2007).

[7] Zie 1.1. praktijkprobleem.

[8] Schema bijlage 1: de focus en intensiteit van de audit wordt bepaald aan de hand van een beoordeling van het interne monitoring systeem, oftewel de 'Assessment of continuous monitoring'. Deze component vormt een onderdeel van continuous assurance en wordt verder besproken in punt 3.5.

Continuous monitoring verzekert:

- Operationele efficiëntie en effectiviteit
- Betrouwbaarheid van de financiële rapportering
- Naleving van de regelgeving

CM fungeert zowel als preventief, als corrigerend controlesysteem. De preventieve werking komt voort uit van de invloed die wordt uitgeoefend op de personen die verantwoordelijk zijn voor het opstellen van de interne controles. Indien zij er zich bewust van zijn dat hun werk gecontroleerd zal worden, is de kans groot dat ze nauwkeuriger gaan werken. De corrigerende werking komt verder uit het feit dat CM verzekert dat alle fouten in het interne controlesysteem kunnen worden opgespoord voordat ze enige invloed kunnen hebben op de doelstellingen van de onderneming (COSO, 2009b). Net zoals interne controle en interne beheersing, is CM een managementfunctie.

3.4. Continuous auditing

De continue audit (CA) is een methode die auditors in staat stelt om een schriftelijke garantie af te leveren aan de hand van auditverslagen die gelijktijdig met, of een korte periode na het ontstaan van relevante gebeurtenissen worden opgesteld. Op deze manier kunnen fouten gemakkelijker en sneller worden opgespoord (Alles et al., 2008). Vaak wordt er onterecht aangenomen dat CA een volledig geautomatiseerd proces is, terwijl het in realiteit bestaat uit een mix van zowel automatische als handmatige systemen (Kwee, 2010).

3.4.1. Evolutie van de klassieke audit naar continuous audit

Alles et al. (2002) bekijkt continuous auditing als de volgende stap in de evolutie van een klassiek, naar een op informatiesystemen gebaseerd auditsysteem. Deze evolutie verloopt langs zeven dimensies (Vasarhelyi en Chan., 2011):

Tabel 1: Evolutie naar CA langs 7 dimensies (Vasarhelyi en Chan, 2011)

Traditionele audit →	**Continuous audit**
1. Frequentie: Periodiek	1. Frequentie: Continu of meer frequent
2. Aanpak: Reactief	2. Aanpak: Proactief
3. Procedure: Manueel	3. Procedure: Geautomatiseerd
4. Werk en rol van de auditor: • Het merendeel van het werk is geconcentreerd rond arbeidsintensieve auditprocedures • Interne en externe auditor werken onafhankelijk van elkaar	4. Werk en rol van de auditor: • Het merendeel van het werk is geconcentreerd rond uitzonderingen en niet automatiseerbare auditprocedures • Externe auditor certificeert het CA systeem
5. De aard en de omvang: • Analytische controles en uitgebreide gedetailleerde controles • Monitoring en gedetailleerde controles worden onafhankelijk van elkaar uitgevoerd • Controle door middel van sampling	5. De aard en de omvang: • Continuous control monitoring en continuous risk assessment (IIA)/ continuous control monitoring en continuous data assurance (Alles et al.) • Simultaan uitgevoerd • De hele populatie wordt getest
6. Controles: Uitgevoerd door mensen	6. Controles: Data modellering en data-analyse
7. Rapportering: Periodiek	7. Rapportering: Continu of meer frequent

- Continue of meer frequente audit

Een traditionele audit zal op periodieke basis, meestal eenmaal per jaar, worden uitgevoerd. CA kan daarentegen in real-time verlopen. In de praktijk is dit echter niet steeds aan te raden. Een real-time audit zal immers een grote impact hebben op de werking van de ondernemingssystemen en zal niet steeds kostenefficiënt zijn. Een audit wordt dan ook enkel in real-time uitgevoerd in gebieden met een hoog risiconiveau. Binnen gebieden met een lager risiconiveau volstaat het om te werken met periodieke of frequente cycli. Een cycli wordt dan gestart wanneer de auditor verbinding maakt, of zal automatisch starten na een vooraf bepaald aantal transacties.

Figuur 1: CA cycli - starten van een cycli na een vast aantal transacties (Vasarhelyi et al., 2011)

- Proactieve audit

Doordat de traditionele audit slechts op periodieke basis wordt uitgevoerd, kan het enkele maanden duren vooraleer materiële fouten en/of fraude gedetecteerd wordt. Het continu monitoren van de interne controlesystemen en het testen van transacties op het moment dat ze worden ingevoerd staat de auditor toe om actief op zoek te gaan naar uitzonderingen.

- Automatisatie van auditprocedures

Het traditionele auditproces is arbeids- en tijdsintensief. De automatisatie van auditprocedures kan deze beperkingen opheffen. De reeds bestaande manuele procedures kunnen hierbij gebruikt worden als basis. Er dient dan bepaald te worden welke processen automatiseerbaar zijn en welke een manuele controle zullen blijven vereisen.

- Werk en rol van de auditor

Vasarhelyi et al. (2004) stelde vier niveaus van audit doelstellingen voorop:

Niveau één - Verifiëren van transacties: controleren van transacties op onregelmatigheden.
Niveau twee - Nagaan of aan alle wettelijke voorschriften voldaan is: verifiëren of de boekhouding voldoet aan alle wettelijke voorschriften. Bijvoorbeeld: Generally Accepted Accounting Principles (GAAP), International Financial Reporting Standards (IFRS), e.d..
Niveau drie - verifiëren van gemaakte schattingen: nagaan van de redelijkheid van door het management gemaakte schattingen.
Niveau vier - Beoordelingen op hoog niveau: verminderen van het auditrisico door het toepassen van complexe beoordelingsmethoden.

CA zal voornamelijk worden toegepast binnen niveau één en twee, waar auditfuncties eenvoudig kunnen worden geautomatiseerd. De rol van de auditor binnen CA verschuift dan ook het onderzoeken van de uitzonderingen die werden gegenereerd door het CA systeem en het uitvoeren van niet-automatiseerbare auditprocedures. Deze laatste bevinden zich voornamelijk binnen niveau drie en vier, waar expertinschattingen een belangrijke rol spelen.

- De aard en de omvang van de audit

De manuele aard van de traditionele audit heeft tot gevolg dat slechts een gedeelte van de populatie zal worden getest. Binnen CA wordt met behulp van continuous control assessment (CCA) en continuous risk assessment (CRA) oftewel continuous control monitoring (CCM) en continuous data assurance (CDA) controles uitgevoerd op de hele populatie. Deze onderdelen worden later nog verder besproken.

- Gegevens modellering en analyse

Binnen CA wordt er gebruik gemaakt van gegevens modellering en geavanceerde analysetechnieken zoals ratio-, trend- en regressieanalyses. Gegevens modellering betreft het gebruik van historische gegevens voor het opstellen van benchmarks. Deze benchmarks worden vervolgens gebruikt ter controle van de huidige transacties. De assumptie die hier wordt gemaakt is dat toekomstige transactiegegevens dezelfde kenmerken zullen vertonen als historische.

- Audit rapportering

Door de meer continue controle wordt ook een meer continue rapportering mogelijk gemaakt. Een uitzonderingsrapport zal gegenereerd worden vlak na het optreden van een materiële fout, waardoor fouten sneller kunnen worden verholpen (Vasarhelyi en Chan, 2011).

3.4.2. Onderdelen van een CA systeem

De literatuur onderscheidt twee dominante theorieën omtrent de onderdelen van een effectief CA systeem. Alles et al. (2006) beschouwt CA als de som van continuous control monitoring (CCM) en continuous data assurance (CDA). Hoewel zowel CCM als CDA in principe managementfuncties zijn, kunnen ook auditors dezelfde technieken toepassen ter beoordeling van de interne controlesystemen. Een tweede definitie wordt gegeven door het Institute of Internal Auditors (IIA) en luidt als volgt:

"Continuous Auditing is any method used by auditors to perform audit-related activities on a more continuous or continual basis. It is the continuum of activities ranging from continuous control assessment to continuous risk assessment — all activities on the control-risk continuum (IIA,2005)."

CA wordt hier dus beschouwd als alle activiteiten gaande van continuous control assessment tot continuous risk assessment[9].

Eerstgenoemde definitie sluit aan bij CA vanuit het perspectief van de externe audit. De focus ligt op het voorkomen van materiële afwijkingen in de financiële staten en het nagaan van de managementbeweringen omtrent het interne controlesysteem. De definitie van het IIA besteedt meer aandacht aan het identificeren van ondernemingsrisico's en het verbeteren van de operationele processen. Hierdoor sluit deze beter aan bij de doelstellingen van een interne audit zoals aangegeven in hoofdstuk twee.

- Continuous data assurance

Binnen CDA worden transactiegegevens continu gecontroleerd op onregelmatigheden en uitschieters. Op deze manier wordt verzekerd dat de financiële informatie correct is (Vasarhelyi, 2011).

- Continuous control monitoring en continuous control assessment

Vasarhelyi en Chan (2011) definieert CCM als het continu monitoren van de effectiviteit van de interne controlesystemen. CCA verwijst naar alle activiteiten, uitgevoerd door de auditor, met betrekking tot de beoordeling van het interne controlesysteem. Door gebruik te maken van CCA kan de auditor garanties leveren aan het management en het auditcomité voor wat betreft de efficiëntie en effectiviteit van deze systemen (IIA, 2005). In vergelijking met CCM, zal CCA een grotere focus leggen op de geschiktheid van het interne beheersingssysteem in verhouding tot de sleutel risico- en succesfactoren. Het verschil tussen CCM en CCA is dus. Het primaire doel van beide is het verzekeren van de effectiviteit van de interne controlesystemen.

[9] Een overzicht van alle functies tussen CCM en CRA wordt gegeven in bijlage 4.

- Continuous risk assessment

CRA verwijst naar alle activiteiten uitgevoerd door de auditor met betrekking tot het identificeren en inschatten van risico's. Door gebruik te maken van trend- en tijdanalyses kan bepaald worden welke systemen of bedrijfsprocessen een hoger risico inhouden dan andere. Hier kan vervolgens op ingespeeld worden bij het opstellen van het auditplan en bij het uitvoeren van CCA (IIA, 2005). Deze definitie sluit nauw aan bij deze van ondernemingsrisicomanagement (Enterprise Risk Management, ERM). CRA kan dan ook beschouwd worden als de auditcontrole op deze managementfunctie:

ERM is een proces dat bewerkstelligd wordt door het bestuur van de onderneming, het management en ander personeel. Het wordt toegepast bij het formuleren van de strategie en is ontworpen om potentiële gebeurtenissen die een invloed zouden kunnen uitoefenen op de onderneming te identificeren en om risico's te managen zodat deze binnen de risicoacceptatiegraad vallen. Op deze manier wordt een redelijke zekerheid geboden ten aanzien van het behalen van de ondernemingsdoelstellingen (COSO, 2004).

- Relatie tussen continuous control assessment en continuous risk assessment

Er bestaat een directe link tussen CCA en CRA. Auditors die zich bezig houden met risk assessment dienen niet alleen het ERM systeem te ondersteunen, maar ook het proces van control assessment. Gebieden die binnen CRA worden geïdentificeerd als sleutel succes- of risicofactor, vereisen een grondigere en meer continue analyse binnen CCA. Een verhoogd risiconiveau kan bovendien ook wijzen op een gebrekkig of niet bestaand controlesysteem.

Omgekeerd dienen ook de resultaten van CCA te worden opgenomen in de CRA. Indien uit de control assessment bijvoorbeeld blijkt dat de onderneming een gebrekkig intern controlesysteem hanteert, of dat het interne controlesysteem niet in staat is om in te spelen op recente ontwikkelingen in de bedrijfsomgeving, zal dit een verhoogd risiconiveau tot gevolg hebben (IIA, 2005).

3.5. Continuous assurance

Het American Institute of Certified Public Accountants definieert continuous assurance als alle onafhankelijke professionele diensten die gericht zijn op het verbeteren van de kwaliteit van informatie waarop beslissingen worden gebaseerd. Assurance diensten zijn gericht op het verbeteren van beslissingen door het vergroten van het vertrouwen in informatie, de manier waarop deze informatie verzameld wordt en de manier waarop deze gepresenteerd wordt. Het gebied van continuous assurance is dus veel breder dan dit van de continue audit. Meer specifiek omvat het:

- Een breder aanbod van diensten (bv. risicobeoordeling, analyse van bedrijfsprestaties,…)
- Een meer gediversifieerde groep van gebruikers
- Gebruikers met bredere verwachtingen dan de betrouwbaarheid van financiële gegevens

Door de grote nadruk op de financiële audit binnen de SOX- en andere wetgevingen, verloopt de ontwikkeling van deze uitgebreidere diensten zeer traag (Rittenberg et al., 2010).

Een belangrijke vorm van continuous assurance binnen het continu auditproces is 'assessment of continuous monitoring', oftewel de beoordeling van het continue monitoring systeem van de onderneming. Het grote belang komt voort uit de relatie die bestaat tussen deze beoordeling en de auditfocus. Als de auditor concludeert dat de interne controlesystemen reeds voldoende getest worden, kan hij de auditfocus verschuiven naar het identificeren en inschatten van ondernemingsrisico's - CRA. Indien dit systeem onvoldoende is ontwikkeld, dient de auditor meer aandacht te besteden aan het beoordelen van de interne controlesystemen – CCA. Assessment of continuous monitoring vormt dus de brug tussen CM en CA (IIA,2005).

Hoofdstuk 4: Audit ondersteunende informatietechnologie

In voorgaande hoofdstukken werd een overzicht gegeven van enkele auditprocedures- en methodes die mogelijk worden gemaakt door de toepassing van IS. De ontwikkeling van dit soort geavanceerde technieken was noodzakelijk ten gevolge van ontwikkelingen in de bedrijfsomgeving. Over de jaren heen evolueerde deze immers van een overwegend manueel gebeuren, naar een volledig geautomatiseerd systeem. Vermits een audit vanuit zijn definitie verder gaat op de onderliggende bedrijfssystemen, drong ook een nieuwe auditaanpak zich op. Het traditionele auditproces evolueerde naar een meer continu gebeuren, ondersteund door informatiesystemen. In dit hoofdstuk wordt een overzicht gegeven van de informatiesystemen en technologieën die interne en externe auditors ter beschikking hebben en de evolutie van deze technologieën.

4.1. Technologische evoluties

Onderstaande tabel geeft een overzicht van de ontwikkelingen die hebben plaatsgevonden binnen bedrijven, de auditproblemen die ontstonden ten gevolge van deze ontwikkelingen en de manier waarop de auditsector heeft gereageerd op deze uitdagingen.

Tabel 2: Technologische evoluties met een invloed op de audit (Vasarhelyi en Halper, 1990)

Periode	Ontwikkeling IT binnen ondernemingen	Audit probleem	Ontwikkeling auditfunctie
1945 – 1955	• Ponskaarten	• Gegevens transcriptie • Repetitieve verwerking	• Auditors "audit around the computer"
1955 – 1965	• Magneetbanden	• Data niet visueel leesbaar • Data kan worden aangepast zonder bewijs	• Ontwikkeling van steekproefapplicaties. • Primitieve "auditing with and through the computer"
1965 – 1975	• Time-sharing systemen[10] • Gegevensopslag op optische schijven • Uitgebreide operationele ondersteuning	• Geen fysieke toegang tot gegevens	• Uitgifte van een IT handleiding door het IIA

[10] Time-sharing is het delen van computersystemen met een groot aantal gebruikers, met als doel multitasking en multiprogrammering.

1975 – 1985	• Geïntegreerde databases • Decision support systems (aids) • Ondernemingsbrede applicaties	• Geen verband tussen de fysieke en logische data lay-out • Nieuwe complexe gegevens laag • Beslissingen opgenomen in software	• Auditors experimenteren met IT toepassingen
1986 – 1991	• Netwerken • Decision support systems (non-expert) • Massa optische opslag	• Grote hoeveelheid gedecentraliseerde gegevens • Onderling verbonden systemen	• Verdere adoptie van generalized audit software zoals ACL en IDEA
1991 – Nu	• Decision support systems (expert)	• Stochastische beslissingen opgenomen in management informatie systemen	• Audit focust op het voldoen aan de SOX wetgeving (interne controle management en real-time reporting)

De introductie van technologie in het productieproces maakte het voor de auditor in eerste instantie onmogelijk om gegevens direct van zijn bron te lezen en gaf het management de mogelijkheid om gegevens te wijzigen zonder hier enig spoor van na te laten. Het "paper-trail" werd vervangen door moeilijk controleerbare elektronisch opgeslagen documenten. Time-sharing en data communicatiesystemen maakten daarenboven een continue toegang tot alle gegevens mogelijk vanop verschillende locaties. Hierdoor werd het systeem nog sterker blootgesteld aan mogelijk onterechte manipulaties of fouten. Database systemen leidde er ten slotte toe dat er geen duidelijk verband meer bestond tussen de fysieke en logische organisatie van gegevens (1945 – 1985).

Auditors speelden in op deze veranderingen door computerprogramma's te ontwikkelen ter automatisatie van standaard auditfuncties, generalized audit software om informatie in gegevensbestanden te raadplegen en gespecialiseerde audit software om tegemoet te komen aan de nieuwe database omgeving. Naast deze tools werden er ook vereisten vastgelegd omtrent toegang tot gegevens en gegevensbeveiliging. Auditors schakelden over van een "auditing around the computer", naar een "auditing with the computer" en "auditing through the computer" benadering

In eerstgenoemde benadering, auditing around the computer, wordt de betrouwbaarheid van computer gegenereerde informatie gecontroleerd door een willekeurige selectie van documenten en transacties te vergelijken met de gegenereerde output. Indien er geen onregelmatigheden worden gedetecteerd, wordt aangenomen dat het controlesysteem effectief en efficiënt werkt. Deze benadering is enkel bruikbaar indien de geautomatiseerde systemen relatief eenvoudig zijn.

.

Binnen sterk geautomatiseerde omgevingen dient een "auditing with the computer" en "auditing through the computer" benadering worden toegepast. "Auditing with the computer" verwijst naar het gebruik van computer-assisted audit tools and techniques (CAATTs) bij het uitvoeren van detail- en transactiecontroles. "Auditing through the computer" voegt hier nog de controle van het transactieverwerkingssysteem en het beheersingssysteem aan toe.

De bedrijfsomgeving evolueerde verder naar een gedecentraliseerd geheel waarin gebruik wordt gemaakt van online systemen, netwerken, massaopslag en expertsystemen ter ondersteuning van het beslissingsproces (1986 – nu). Ondernemingen werden omgevormd naar een meer real-time gebeuren, waarin informatie onmiddellijk beschikbaar en sterk verspreid is (Vasarhelyi en Chan, 2011).

Om aan deze uitdagingen te voldoen is, naast de verdere implementatie van CAATTs, een nieuwe auditaanpak essentieel. Deze is te vinden in het concept van continuous audit en zal verder worden besproken in hoofdstuk vijf.

Een belangrijke ontwikkeling verantwoordelijk voor het stimuleren van het gebruik van CAATTs en de overgang van de traditionele audit naar een continue audit, was XBRL oftewel eXtensible Business Reporting Language. XBRL is gebaseerd op eXtensible Markup Language (XML) en voegt informatie met betrekking tot de inhoud van financiële documenten toe in tags. Op deze manier staat het computers toe om gegevens te "begrijpen" en op een eenvoudige manier te verspreiden tussen verschillende software applicaties. Het is ook door deze software-onafhankelijkheid dat XBRL een drijfveer vormt achter CA (Vasarhelyi et al., 2004).

4.1.1. Technologie in de huidige bedrijfsomgeving

Vele grote ondernemingen maken gebruik van één type Database Management System (DBMS), bestaande uit verschillende kleinere databases die telkens worden gekoppeld aan een specifiek deel van het productieproces. In de meeste gevallen gaat het om gerelateerde databases zoals de master database, een transactie database, een controle database en een administratieve database. De gegevens worden verwerkt binnen de individuele database, of binnen een centraal verwerkingssysteem.

De onderliggende bedrijfssystemen bestaan vaak uit een mengeling van technologieën en programmeertalen. Door gebruik te maken van bridges worden deze systemen vervolgens aan elkaar en aan het DBMS gekoppeld. Een audit van het volledige systeem vereist dan ook een analyse van de verschillende systemen op zich, de gebruikte bridges en een analyse van het systeem als geheel (Vasarhelyi et al., 2004).

Op basis van het DBMS kunnen enkele hedendaags belangrijke softwarepakketten worden geprogrammeerd. Een eerste voorbeeld hiervan is een enterprise resource planning (ERP) systeem. ERP wordt gedefinieerd als een softwarepakket waarin gebruik wordt gemaakt van relationele databasetechnieken om informatie uit verschillende ondernemingseenheden te integreren. Op deze manier wordt een ondernemingsbreed beslissingsproces ondersteund (Bae en Ashcroft, 2004).

Een tweede softwaretool zijn de zogenaamde expertsystemen: "An expert system is an interactive computer-based decision tool that uses both facts and heuristics to solve difficult decision problems based on knowledge acquired from an expert". Op basis van gegevens, aangeleverd door een expert ter zake en een relationele database, kan een expertsysteem het beslissingsgedrag van een menselijke expert simuleren. Dit systeem kan vervolgens worden gebruikt door werknemers met minder ervaring.

Het belangrijkste kenmerk van al deze bedrijfs- en beslissingsondersteunende systemen, is dat het merendeel in real-time of near real-time opereert (Vasarhelyi et al., 2004).

4.1.2. Technologie in de huidige auditomgeving

De technologische oplossingen die het meest worden gebruikt bij het uitvoeren van een audit omvatten volgens PwC (2009):

- Geïntegreerde audit software om de opstelling van werkdocumenten, papers, risicoanalyses en auditrapporten te stroomlijnen. Alsook het automatiseren van monitoring en administratieve processen.
- Data retrieval software ter automatisatie van controles. Vaardigheid met dergelijke software moet worden beschouwd als een kerncompetentie voor het interne en externe audit personeel.
- Datamining/analyse software voor voorspellende analyses en modelleringen.
- Kennistools- en databases om 'best-practice' inzichten te verkrijgen.

Het aantal audit tools ter beschikking van de auditor is breed genoeg om elk type audit te ondersteunen. Er wordt een onderscheid gemaakt tussen vier soorten software tools (ICAI, 2004):

1. Package programs: zijn ontwikkeld om data verwerkingsfuncties uit te voeren zoals het uitlezen, selecteren, analyseren van gegevens en het opstellen van rapporten in een op voorhand bepaald formaat.
2. Purpose-written programs: programma's ontwikkeld voor het uitvoeren van specifieke audittaken in specifieke omstandigheden. Dit soort programma's kan worden ontwikkeld door de auditor zelf, of door het bedrijf waarin de audit wordt uitgevoerd.
3. Utility programs: worden gebruikt om standaard verwerkingsfuncties zoals het sorteren, opmaken en printen van documenten uit te voeren. Dit soort programma's is in eerste instantie niet ontwikkeld ter ondersteuning van het auditproces, maar kunnen het auditproces wel ondersteunen.
4. System management programs: zijn verbeterde en meer geavanceerde audit productiviteittools. Hieronder vallen bijvoorbeeld data selectie software en code vergelijkings software.

Deze tools kunnen nogmaals verder worden onderverdeeld in 'computer assissted auditing tools and techniques' (CAATTs) en 'audit productiviteittools'. In vele onderzoeken wordt een brede definitie van CAATTs toegepast zijnde 'any use of technology to assist in the completion of the audit'. In wat volgt wordt het begrip echter beperkt tot software tools die worden gebruikt om gegevens te extraheren, sorteren en analyseren. Overige tools die het auditproces kunnen ondersteunen, worden geplaatst onder de noemer audit productiviteit tools (Janvrin et al., 2008).

4.2. Computer-assisted audit tools and techniques

Computer-assisted audit tools and techniques (CAATTs) ondersteunen het auditproces door auditors te helpen bij het selecteren en analyseren van gegevens. Indien er binnen de onderneming controlesystemen zijn opgezet, dient de auditor de efficiëntie en effectiviteit van deze systemen te controleren. Als er geen controlesystemen zijn geïmplementeerd, dient de auditor meer extensieve tests uit te voeren om de integriteit van alle gebruikte gegevens te verzekeren. Binnen beide activiteiten kunnen auditors gebruik maken van CAATTs om de controle efficiëntie te verbeteren.

Het gebruik van CAATTs wordt sterk aangeraden door de meer recente auditstandaarden. SAS nr. 99 moedigt auditors bijvoorbeeld aan om CAATTs te gebruiken om risico's in te schatten, belangrijke journaalposten te identificeren en om het bestaan en de correctheid van de voorraad te

bepalen (2002b). De nieuwe risicostandaarden, zijnde SAS nr. 104-111, promoten het gebruik van CAATTs daarenboven ook om gegevens te selecteren vanuit elektronische documenten, voor het sorteren van transacties met specifieke karakteristieken, het uitvoeren van audittests op een hele populatie in de plaats van een gedeelte en het bekomen van audit bewijs betreffende de controle efficiëntie (AICPA, 2006). Ten slotte kunnen CAATTs ook worden aangewend om de accuraatheid van elektronische werkdocumenten te verifiëren (AICPA, 2001). Ook de interne auditstandaarden raden het gebruik van technologie aan om de efficiëntie en effectiviteit van de interne audit te vergroten. Bijvoorbeeld IIA standaard 1220.A2: "In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques**."**

4.2.1. Gebruik van CAATTs in de externe audit

Een onderzoek omtrent het gebruik van CAATTs in de externe audit, werd uitgevoerd door Cushing en Loebbecke (1983). Hier werd onderzocht op welke manier externe auditkantoren gebruik maken van CAATTs. Hun conclusies zijn gebaseerd op een enquête die werd verzonden naar 744 kantoren van "the Big Eight[11]". Uit de resultaten kwam naar voren dat op dat moment de beschikbare CAATTs nog niet ten volle werden benut. Ook in meer recent onderzoek van Janvrin et al. (2008) wordt nagegaan in welke mate auditors gebruik maken van de hen ter beschikking staande CAATTs. Het onderzoek werd uitgevoerd bij 109 auditors actief in een lokaal, regionaal of globaal auditkantoor. Opnieuw werd vastgesteld dat CAATTs slechts in beperkte mate werden gebruikt.

Aan de hand van deze standaarden en de voordelen verbonden aan het gebruik van CAATTs, kunnen vier redenen geformuleerd worden om CAATTs in gebruik te nemen, namelijk 'performance expectancy', 'effort expectancy', 'social influence' en 'facilitating conditions'. Performance expectancy verwijst naar de mate waarin gebruikers geloven dat de tool hen zal helpen om een beter resultaat te bereiken. Effort expectancy is het gemak waarmee de tool kan worden toegepast. Social influence verwijst naar de mate waarin iemand gelooft dat hoger geplaatsten rondom hen verwachten dat de tool wordt toegepast. Facilitating conditions verwijst ten slotte naar de mate waarin gebruikers het gevoel hebben dat een organisationele en technische infrastructuur bestaat ter ondersteuning van CAATTs. De respondenten werd gevraagd de verschillende redenen te beoordelen op een schaal van één tot zeven. Waar één = niet belangrijk en zeven = belangrijk. De belangrijkste reden voor het invoeren van CAATTs bleek de verhoogde prestatieverwachtingen en de onderliggende infrastructuur. Het eenvoudig kunnen gebruiken van de tools en de verwachtingen van de sociale omgeving bleken minder belangrijk te zijn[12].

[11] Op dat moment bestaande uit: Arthur Andersen, Arthur Young & Co., Coopers & Lybrand, Ernst & Whinney, Deloitte Haskins & Sells, Peat Marwick Mitchell, Price Waterhouse, Touche Ross.

[12] Resultaten in bijlage 8.

CAATTs worden voornamelijk gebruikt voor het selecteren van gegevens, het sorteren van transacties en het controleren van elektronische documenten. Het belang van CAATTs wordt geschat tussen de 3.10 en 3.81. Uit de resultaten komt bovendien naar voren dat auditors tewerkgesteld in één van de Big Four auditkantoren sneller geneigd zullen zijn om CAATTs aan te wenden. Hiervoor worden twee oorzaken gegeven. Allereerst zullen deze auditkantoren vaak audits uitvoeren in grote bedrijven met complexere IT systemen. Ten tweede hebben ze meer bronnen ter hunner beschikking om te kunnen reageren op de ontwikkelingen in hun omgeving.

Tabel 3: Resultaten studie in verband met het gebruik van CAATTs (Janvrin et al., 2008)

Functie CAAT	Gebaseerd op standaard	Gebruik	Procentueel gebruik	Belang van het systeem
Evalueren van fraude risico's	AU 316.52	Ja = 36 Neen= 93	27.91	3.18
Identificeren van journaalposten voor verdere analyse	AU 316.64	Ja = 46 Neen = 83	35.66	3.43
Controleren accuraatheid van elektronische documenten	AU 308.33	Ja = 59 Neen = 69	46.09	3.79
Opnieuw controleren van transacties	AU 308.34	Ja = 46 Neen = 82	35.94	3.40
Selecteren van steekproeven	AU 327.19	Ja = 63 Neen = 65	49.22	3.81
Sorteren van transacties met specifieke karakteristieken	AU 327.19	Ja = 59 Neen = 69	46.09	3.80
Testen van de hele populatie in de plaats van een steekproef	AU 327.19; AU 327.61	Ja = 39 Neen = 88	30.71	3.10
Bekomen van bewijslast omtrent de werking van het interne controlesysteem	AU 327.27	Ja = 39 Neen = 90	30.23	3.18
Evalueren van voorraad waardering en correctheid	AU 316.54	Ja = 47 Neen = 80	37.01	3.47

In een studie van Dowling en leech (2007) worden de gebruikte CAATTs binnen de Big Four en een vijfde internationale auditfirma onderzocht. De gebruikte systemen worden vergeleken op gebied van ontwikkeling, beleid, gebruik, integratie en rol. Uit het onderzoek kwamen significante verschillen naar voren binnen elk van deze gebieden.

- Ontwikkeling en gebruik

In alle vijf de ondernemingen worden de audit ondersteunende informatiesystemen (Audit Support Systems, ASS)[13] globaal ontwikkeld en vervolgens aangepast aan de specifieke eisen van het land waarin de onderneming actief is. In twee gevallen worden de systemen nog verder aangevuld met standalone tools. Het gebruik van ASS wordt steeds verplicht, tenzij het gaat om een zeer kleine cliënt waar een handmatige audit nog mogelijk is. De auditor dient een vooraf opgesteld plan te volgen om het auditprogramma af te stellen op de situatie van de cliënt.

- Automatisch versus manueel afstellen

Het afstemmen van de ASS op de specifieke behoefte van de cliënt vormt steeds de eerste stap in de planningsfase. Het afstemmen van deze systemen op de specifieke cliënt is belangrijk om te vermijden dat er tijd wordt geïnvesteerd in het onderzoeken van onbelangrijke gebeurtenissen. De vijf onderzochte bedrijven stelden pakketten ter beschikking waarin standaarden voor alle industrieën werden gespecifieerd. In twee ondernemingen werden deze standaarden automatisch toegepast aan de hand van antwoorden op enkele standaardvragen. In de overige drie auditfirma's dienden auditors manueel de ASS aan te passen aan de hand van checklists en industrievoorwaarden.

- Beslissingsondersteunende systemen

In alle vijf de ondernemingen waren beslissingsondersteunende- en expertsystemen geïntegreerd in de ASS. Het gaat om systemen die aanbevelingen maken, risico's identificeren, de effectiviteit van de controleactiviteiten nagaan en verdere audittests aanbevelen. In een auditfirma waar strenge voorschriften gelden, zullen beslissingsondersteunende systemen meer gestructureerd zijn. Dit houdt in dat auditors volledig moeten voldoen aan de door het systeem voorgestelde checklist en bijkomende controles (Dowling en leech, 2007).

[13] Als verzamelnaam voor alle gebruikte CAATTs.

4.2.2. Gebruik van CAATTs in de interne audit

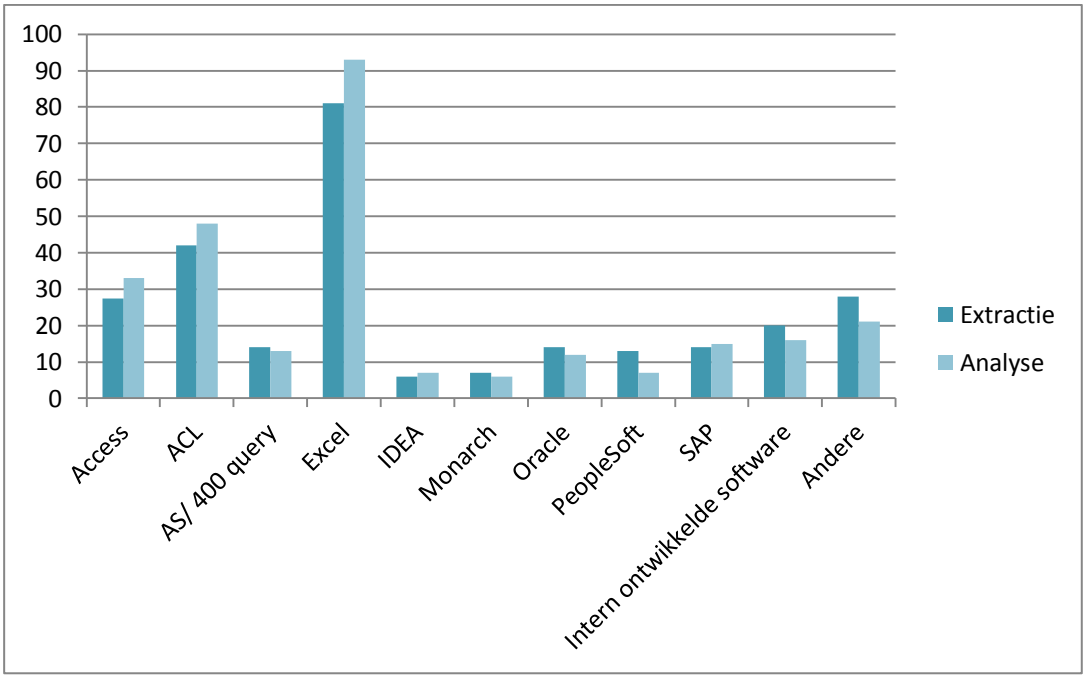
Het aantal onderzoeken naar het gebruik van CAATTs in de interne audit is eerder beperkt. De onderzoeken die wel zijn uitgevoerd, hebben meestal betrekking op een specifiek geografisch gebied. Mahzan en Lymer (2007) onderzocht het gebruik van CAATTs binnen de interne audit in Groot-Brittannië.

Net zoals in het onderzoek van Janvrin et al. (2008) worden de redenen voor het gebruiken van CAATTs onderzocht. Er wordt aangetoond dat interne auditors CAATTs beschouwen als een manier om risicoanalyses en controles te ondersteunen en de algemene audit efficiëntie te verhogen. Performance expectancy is dan ook de belangrijkste implementatiereden. De overige redenen zoals het gebruiksgemak en de sociale verwachtingen spelen slechts een beperkte rol.

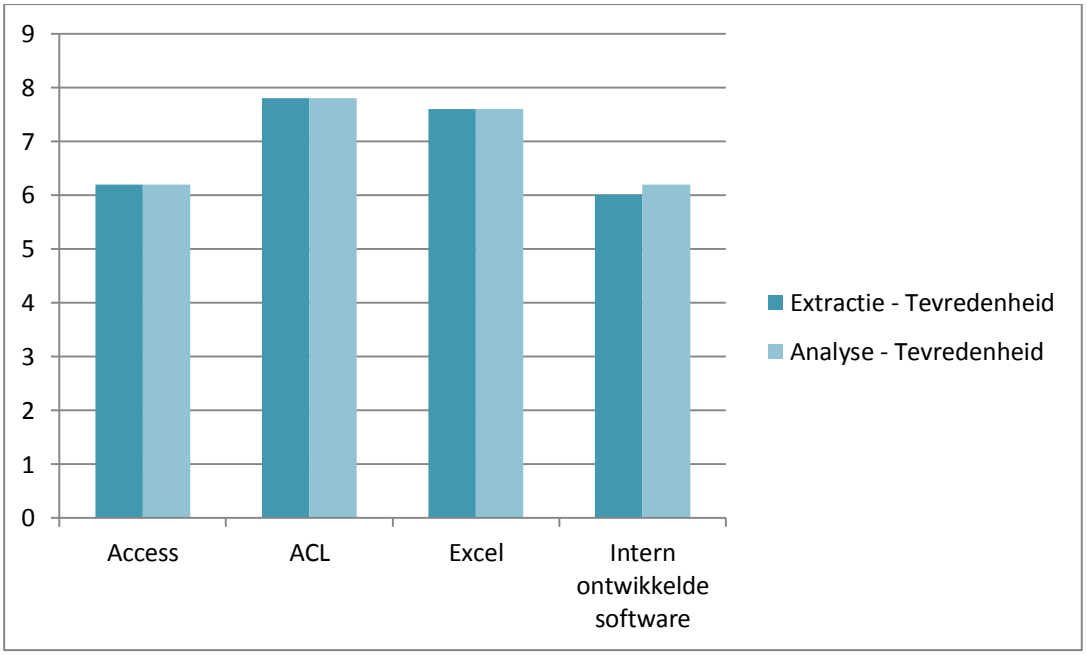
Er wordt voornamelijk gebruik gemaakt van CAATTs binnen de categorie "generalised audit software"[14] (GAS). Slechts een beperkt aantal grotere ondernemingen maakt gebruik van meer geavanceerde auditsoftware zoals audit expertsystemen en/of CA modules (Mahzan en Lymer, 2007).

Omtrent het gebruik van deze GAS werd een onderzoek verricht door het IIA (2006) in de vorm van een 'Internal Auditor Software Survey'. Hiering werd nagegaan welke software wordt gebruikt voor het uitvoeren van data extractie en analysefuncties. Uit de bevraging kwam naar voren dat voornamelijk gebruik wordt gemaakt van Excel. ACL en Access nemen respectievelijk de tweede en derde plaats in. De algemene tevredenheid over de gebruikte tool is echter wel groter bij ACL dan bij Excel en Access.

[14] Deze categorie wordt nog verder besproken in punt 4.2.4.3.



Figuur 2: Resultaten gebruikte Data Extractie en Analyse Software (IIA, 2006)



Figuur 3: Algemene tevredenheid over de gebruikte tool (Met 10 = Zeer tevreden) (IIA, 2006)

4.2.3. Voor- en nadelen van CAATTs

De voor- en nadelen van CAATTs kunnen worden aangegeven als volgt:

Tabel 4: Overzicht van de voordelen en beperkingen van CAATTs (Dowling en Leech, 2007)

Voordelen	Beperkingen
• Verbetering van de audit kwaliteit • Verbetering audit efficiëntie • Consistente audit aanpak over cliënten heen • Verbeterd risico management • Eenvoudigere documentatie • Betere controle van junior stafleden	• Overdreven vertrouwen in de aanbevelingen van het systeem. • Mechanisch gedrag • Training van personeelsleden vereist • Stabiliteit van de technologie • Niet kostenefficiënt bij kleine cliënten

CAATTs verbeteren de kwaliteit en de efficiëntie van de audit door te verzekeren dat de audit en boekhoudkundige normen worden nageleefd, door het verlagen van de beslissingstijd en het structureren van informatie zodat relevante gegevens snel kunnen worden gevonden. Door gebruik te maken van werkdocumenten en vooraf vastgestelde werkwijzen verzekert men daarenboven consistentie over alle cliënten heen. Indien deze procedures echter te sterk moeten worden nageleefd, bestaat de kans dat het auditproces enkel nog maar bestaat uit mechanisch gedrag. De auditor wordt dan in een positie geduwd dat hij enkel nog de gegevens moet ingeven, het systeem maakt vervolgens alle beslissingen. Dit kan demotiverend werken. Hiernaast dient het personeel ook steeds voldoende getraind te worden en zal het gebruik van CAATTs niet steeds kosten efficiënt zijn. Bijvoorbeeld bij zeer kleine cliënten kan een handmatige audit aan te bevelen zijn (Dowling en Leech, 2007).

4.2.4. Toepassingsgebied

De voordelen van CAATTs zijn niet beperkt tot een specifieke auditactiviteit. CAATTs kunnen immers worden gebruikt voor het uitvoeren van verschillende auditprocedures, waaronder bijvoorbeeld de volgende:

- In detail testen van transacties en saldi
- Het uitvoeren van analytische procedures zoals bijvoorbeeld het detecteren van inconsistenties en significante fluctuaties
- Testen van controlesystemen. Zowel algemene als toepassingsgerichte.
- Het selecteren van gegevens waarop een audit dient te worden uitgevoerd

- Heruitvoering van berekeningen gemaakt door accounting systemen
- Nagaan van de betrouwbaarheid van het cliëntsysteem
- Bekomen van toegang tot benodigde gegevens, zonder daarbij afhankelijk te zijn van de cliënt of het management.

Indien een onderneming dit soort systemen aanwendt, betekent dit niet dat er sprake is van CA. Het gebruik van CAATTs is wel een essentieel deel van CA, maar kan niet beschouwd worden als CA op zichzelf. Bijvoorbeeld het gebruiken van CAATTs om het bedrag handelsdebiteuren te controleren tijdens een geplande audit, wordt niet beschouwd als CA tenzij deze controle wordt uitgevoerd op een continue of bijna continue basis. Hierop wordt later nog teruggekomen.

In dit gedeelte worden de bekendste en meest gebruikte toepassingen van CAATTs zoals aangegeven door Coderre (2009) en Mercken (2010) besproken. Het gaat van software bedoeld voor het eenvoudigweg extraheren van gegevens, tot volledige expert systemen ter ondersteuning van het beslissingsproces.

Tabel 5: Overzicht van de belangrijkste CAATTs (Mercken, 2010; Coderre, 2009)

	Ex-post	**Continu**
Ondersteuning planning, dossier, beslissingen		Elektronische werkdocumenten (4.3.4.1) Expert systemen (4.3.4.2) GAS (4.3.4.3)
Datagericht (Testen van transactiegegevens)	Primaire aanwending van GAS zoals ACL of IDEA. Maar ook algemene of gespecialiseerde pakketten met een breder spectrum van gebruikers (4.3.4.3)	ACL-scripts (4.3.4.3) DBMS instructies (4.3.4.4 en 4.3.4.5) CA modules (hoofdstuk 5)
Systeemgericht (Testen van controlesystemen)	GAS (4.3.4.3) Test data generators (TDG) (4.3.4.4) Code analyse/ vergelijkingssoftware (4.3.4.6) Parallelle simulatie (4.3.4.7)	Integrated Test Facilities (4.3.4.8) Code analyse/ vergelijkingssoftware (4.3.4.6) Parallelle simulatie (4.3.4.7) CA modules (hoofdstuk 5)

4.2.4.1. Elektronische werkdocumenten

Elektronische werkdocumenten standaardiseren het formaat waarin elementen nodig voor het uitvoeren van een audit worden in weergegeven. Op deze manier maken ze een audit minder tijdsintensief.

De basis mogelijkheden van elektronische werkdocumenten bestaan onder meer uit:

- Snelle en betrouwbare replicatie van databases en documenten over meerdere servers
- Automatisch verzenden van informatie
- Ondersteuning voor ongestructureerde data types zoals spreadsheets en flow charts
- Mogelijkheid om gebruik te maken van standaard templates voor rapporten, papers,..
- Handhaving van een standaard werkwijze voor het uitvoeren van de audit
- Automatisch benoemen van documenten
- Eenzelfde verzameling van data weergeven op verschillende wijzen
- Leggen van links tussen verschillende documenten

Een deel van deze eigenschappen vinden we ook terug onder de audit productiviteit tools. Elektronische werkdocumenten bevatten echter toegangsmogelijkheden tot audit software voor gegevens toegang, analyse, screening en rapportering.

4.2.4.2. Expert systemen

Net zoals binnen ondernemingen, kan er ook binnen een audit gebruik worden gemaakt van expert systemen voor het ondersteunen van beslissingen. Uit onderzoek blijkt dat er sterke verschillen zijn voor wat betreft genomen beslissingen tussen ervaren en onervaren auditors. Expertsystemen kunnen deze kloof verkleinen. Deze systemen worden geprogrammeerd met kennis van één of meerdere experten en zijn in staat om patronen te ontdekken in een grote hoeveelheid ruwe gegevens (Vasarhelyi, 1990).

Binnen een audit kunnen expertsystemen worden aangewend ter ondersteuning van volgende functies:

- Het ontwikkelen van auditprogramma’s

Expertsystemen kunnen worden aangewend tijdens de ontwikkeling van auditprogramma’s. De software past een algemeen auditprogramma aan op basis van de specifieke kenmerken van de

audit cliënt, rekening houdend met de kennis opgenomen in de "knowledge-database". Bijvoorbeeld Expertest.

- Evalueren van het interne controlesysteem en het uitvoeren van een risicoanalyse

Zowel de evaluatie van het interne controlesysteem als het uitvoeren van een risicoanalyse is grotendeels een subjectief gebeuren. Expertsystemen zijn in staat om kennis en ervaring van experten op te slaan om op die manier ook minder ervaren auditors te ondersteunen bij deze taken. Bijvoorbeeld Internal Controls Expert.

- Andere toepassingen

Naast bovenstaande toepassingen, kunnen expertsystemen ook worden aangewend binnen enkele andere gebieden zoals belastingen, juridische vraagstukken en accounting. Elk van deze gebieden omvat een uitgebreide regelgeving, waardoor expertsystemen de ideale tool vormen om de auditor te ondersteunen. Bijvoorbeeld Expertax.

4.2.4.3. Generalized audit software

In de huidige bedrijfsomgeving worden gegevens voornamelijk opgeslagen in elektronisch formaat. Door het grote aantal documenten wordt een manuele audit hierdoor vaak bemoeilijkt. Om aan dit probleem tegemoet te komen werd een groot aantal toepassingen ontwikkeld die de auditor het vermogen geven om elektronische informatie op een mainframe, database of microcomputer te analyseren.

De meest voorkomende vorm van dit soort data extractie software staat bekend als "Generalized Audit Software" (GAS). Dit soort softwarepakketten heeft twee primaire doelstellingen (AuditNet, 2003):

1. Het faciliteren en automatiseren van tests over 100% van de populatie
2. De aandacht van de auditor vestigen op gebieden met een hoger risicogehalte

GAS werd ontwikkeld om universele datatoegang, samenvattende analyses, uitgebreidere controles en rapporten mogelijk te maken. Door het dynamische en interactieve karakter kunnen auditors verschillende hypotheses verkennen en testen. Op deze manier kan de integriteit van de data, de relaties tussen uitzonderingen, de effectieve en efficiënte werking van het accounting systeem, e.d. eenvoudiger worden onderzocht.

GAS staat de auditor toe om toegang tot gegevens te verkrijgen en hierop verschillende operaties uit te voeren. De populariteit komt voort uit het gebruiksgemak en het feit dat de auditor niet over een uitgebreide computerkennis dient te beschikken. De bekendste en meest gebruikte auditsoftware op dit gebied is "Audit Command Language" (ACL) en "Interactive Data Extraction and Analysis" (IDEA).

Gedurende de planningsfase kan GAS worden gebruikt om de audit populatie te definiëren, uitgaven en budgetten van het huidige en vorige boekjaar te onderzoeken, input en output patronen te identificeren en trendanalyses uit te voeren. Hierdoor zal de auditor nog voor het starten van de audit een beter begrip hebben van de onderneming en ondernemingsprocessen.

Tijdens de eigenlijke uitvoeringsfase kan GAS worden ingezet om:

- Testen op redelijkheid, ongeldige bewerkingen en interrelaties
- Verifiëren van controletotalen
- Berekenen van turnover ratio's voorraad en handelsdebiteuren
- Locatie gebaseerde indeling van uitgaven en inkomsten
- Selecteren van gegevens gebaseerd op risico of materialiteit (sampling)
- Ontwikkelen van uitzonderingsrapporten

Een voorbeeld hiervan is de aanwending van GAS als aanvulling op de evaluatie van een beheersingssysteem. Eenvoudige beheersingssystemen, zoals invoercontroles, kunnen worden geverifieerd door alle informatie in een specifiek veld te controleren op ongeldige waardes. In tegenstelling tot een manuele controle, waar deze test enkel kan worden uitgevoerd op een klein gedeelte van de gegevens, kan deze test door gebruik te maken van CAATTs worden uitgevoerd op alle gegevens.

4.2.4.4. Data warehouse

Een data warehouse is een grote verzameling van gegevens afkomstig uit verschillende productieprocessen. De informatie wordt voornamelijk gebruikt voor trendanalyses en projecties ter ondersteuning van lange termijn beslissingen. Hoewel een data warehouse voornamelijk is gericht op gebruik door het management, kan een data warehouse ook een toegevoegde waarde leveren tijdens het auditproces.

Indien een auditor zich moet baseren op de onderliggende productiesystemen zal een groot deel van de audittijd gespendeerd worden aan het verzamelen van gegevens. In een omgeving waar men zich kan baseren op een data warehouse, kan er daarentegen meer tijd worden gespendeerd aan de eigenlijke analyse van deze gegevens. Doordat gegevens over een langere termijn worden

bijgehouden, zal de auditor ook trend- en risicoanalyses kunnen uitvoeren. Hierdoor zal de audit meer gericht zijn op gebieden met een hoog risicogehalte met meer gerichte aanbevelingen tot gevolg.

Bij het opzetten van een DBMS dient het systeem eerst uitgebreid getest te worden. Dit kan gebeuren met behulp van test data generators. Dit soort software vult de database met willekeurige gegevens voor het uitvoeren van prestatietests, query tests, stabiliteitstests, e.d..

4.2.4.5. Data mining

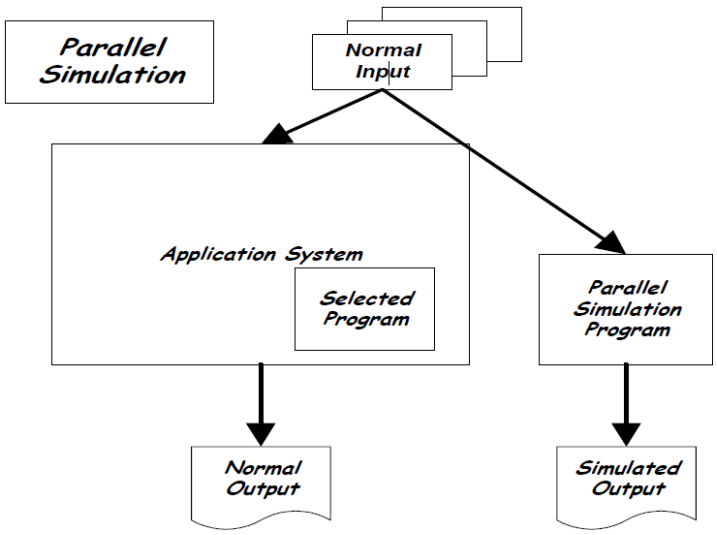
Indien gegevens worden opgeslagen in een data warehouse kunnen complexe vraagstukken worden opgelost aan de hand van data mining technieken. Binnen het auditgebied verwijst data mining naar het proces van het analyseren van gegevens vanuit verschillende invalshoeken om op die manier zeer gedetailleerde informatie te bekomen. Een meer continue audit wordt mogelijk gemaakt door DBMS instructies/ bevragingen te programmeren op specifieke tijdstippen of bij een specifieke gebeurtenis (Coderre, 2009).

4.2.4.6. Programmacode analyse/ vergelijkingssoftware

Aangezien software in deze categorie geen gegevens extractie- of analysefuncties uitvoert, kunnen deze applicaties ook worden geclassificeerd onder de noemer audit productiviteit tools. Het gaat echter om meer geavanceerde tools. Het gaat echter om zeer geavanceerde vormen van audit productiviteit tools. Programmacode vergelijkingssoftware maakt het mogelijk om twee versies van een bepaalde applicatie met elkaar te vergelijken, of om de programmacode te bestuderen.

4.2.4.7. Parallelle simulatie

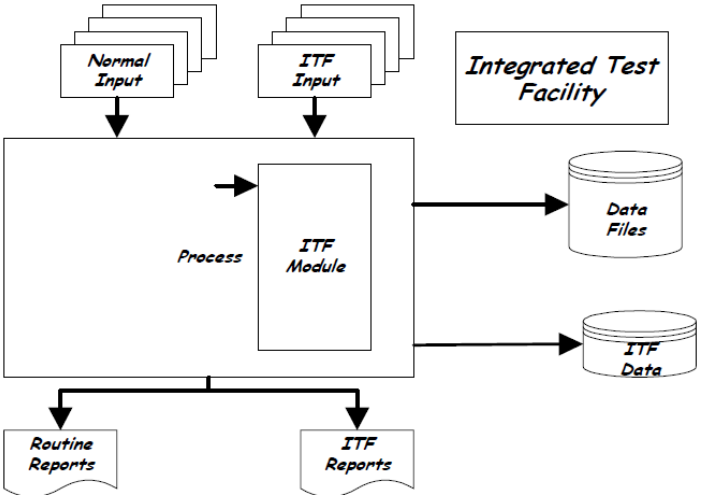
Een parallelle simulatie wordt uitgevoerd door de functionering van een systeem of een deel van een systeem te simuleren. Dit onafhankelijke systeem zal door de auditor worden geprogrammeerd met dezelfde instellingen als het originele systeem. Indien geen ongeautoriseerde toegang heeft plaatsgevonden, zouden beide systemen eenzelfde resultaat moeten geven. Het gaat bijvoorbeeld om het opnieuw uitvoeren van een bepaalde controle in ACL.



Figuur 4: Schematische voorstelling van een parallelle simulatie (Auditnet, 2002)

4.2.4.8. Integrated Test Facility

Een Integrated Test Facility (ITF) voorziet in een geïntegreerde oplossing voor het testen van controlesystemen op een continue basis. Dit zal gebeuren door de creatie van een dummy entiteit in de operationele bestanden. Simultaan met de verwerking van real-time transactiegegevens worden testgegevens ingegeven in de ITF testmodule. Hierbij is het belangrijk dat de testgegevens niet in aanraking komen met de werkelijke transactiegegevens. Indien de ITF geen fouten genereert, zou ook het originele systeem correct moeten werken (Auditnet, 2002).



Figuur 5: Schematische voorstelling van een Integrated Test Facility (Auditnet, 2002)

4.3. Audit productiviteit tools

Audit productiviteit tools staan de auditor toe om de benodigde audittijd te verminderen door de automatisatie van standaard auditfuncties en het integreren en beschikbaar maken van informatie over het hele auditproces. Ze kunnen in elke fase van het auditproces worden aangewend. Bijvoorbeeld bij het uitvoeren van volgende activiteiten (Gallegos et al., 2004):

- Audit planning en het bijhouden van het auditschema met behulp van spreadsheet, database en project management software
- Documenteren en presenteren met behulp van tekstverwerkings, flowchart en grafische software
- Communicatie en gegevens-overdracht met behulp van elektronische netwerken en/ of een centrale server
- Resource management met behulp van online werkdocumenten, e-mail en self-assessment software
- Bevorderen van teamwork met database, groupware en intranet software
- Verzekeren van audit consistentie over verschillende locaties en bedrijven heen. Door middel van elektronische formulieren en standaard audit programma's

4.3.1. Audit planning

Risicobeoordeling, auditplanning, auditopvolging en het opstellen van een begroting zijn essentiële onderdelen van het auditproces. Om deze taken te ondersteunen kunnen verschillende software tools worden ingezet. Spreadsheet en data analyse software kan worden gebruikt bij het uitvoeren van een risicoanalyse en het opstellen van het budget. Project management software kan worden gebruikt om audits te plannen en hun voortgang op te volgen. Indien deze applicaties worden geïntegreerd over het hele auditproces, kunnen de verschillende componenten bovendien op elkaar kunnen worden afgestemd. Bijvoorbeeld het afstemmen van het budget op de gemaakte planning.

4.3.2. Gestandaardiseerde extracties en rapporten

Meer accurate en consistente documenten kunnen worden verkregen door gebruik te maken van software pakketten zoals bijvoorbeeld de office suite. Dit soort software is ook in staat om gegevens te linken, waardoor eventuele aanpassingen onmiddellijk in verschillende documenten worden doorgevoerd.

In vele gevallen is bovendien eenzelfde soort informatie nodig voor het uitvoeren van diverse audits. Om hieraan tegemoet te komen werden er programma's ontwikkeld ter ondersteuning van standaardrapporten. Door gebruik te maken van scripts en macro's kunnen taken zoals het combineren van maandrapporten naar een year-to-date rapport vervolgens worden geautomatiseerd. Deze standaardrapporten kunnen worden gebruikt tijdens de planningsfase in de vorm van algemene rapporten en tijdens de uitvoeringsfase in een meer gedetailleerde vorm.

4.3.3. Communicatie en toegang tot gegevens

Een audit wordt steeds uitgevoerd door een team van auditors. Een goede communicatie en het delen van informatie tussen de verschillende teamleden is hierbij onontbeerlijk. Uitgebreide netwerkmogelijkheden, elektronische berichtgeving en online databases stellen auditors in staat om efficiënt te communiceren en alle noodzakelijke informatie te verzamelen voor het uitvoeren van een audit.

Informatietechnologie stelt auditors ook in staat om efficiënter te communiceren met hun audit cliënt. Zo kan men bijvoorbeeld een lid van het managementteam toegang geven tot de auditing database. Dit laat hen toe om aanvullingen of wijzigingen met betrekking tot risicogebieden door te voeren. Natuurlijk dienen er hier voldoende maatregelen te worden genomen om eventueel misbruik te vermijden.

4.3.4. Evaluatie en feedback

Een belangrijk deel van het auditproces is evaluatie en feedback. Om dit te ondersteunen wordt er gebruik gemaakt van zogenaamde self-assessment software. Het gaat om software die gebruikers toestaat om tijdens een evaluatiesessie, al dan niet anoniem, ideeën en beoordelingen door te geven aan de manager. Ook staat het gebruikers toe om te stemmen op bepaalde ideeën en stellingen. Op deze manier kunnen sterktes en zwaktes in het auditproces op een efficiënte wijze worden gevonden.

Auditmanagers krijgen daarenboven te maken met een groot aantal sterk verspreide werknemers. Toch moeten zij in staat zijn om richtlijnen te geven en controles uit te voeren op het uitgevoerde werk. Om dit te kunnen bereiken is het belangrijk dat informatie snel verzameld en verspreid kan worden. Door middel van e-mails, interne bedrijfsnetwerken en andere communicatiekanalen verzekert men een onmiddellijke feedback.

4.3.5. Groupware

Groupware is een gespecialiseerde tool of groep van tools die teams toelaat om een gezamenlijk doel te bereiken. Onder groupware valt bijvoorbeeld video conferentie software, co-authoring software, groep kalenders,… Al deze tools zijn erop gericht om een goede groepswerking te verzekeren en een beter eindresultaat te bekomen.

4.3.6. Elektronische formulieren en audit programma's

Een elektronische enquête kan gaan van een eenvoudig formulier gebruikt om input elektronisch vast te leggen tot een complex interactief formulier waarbij vragen gebaseerd zullen zijn op voorgaande antwoorden. Deze kunnen worden gebruikt om audit klanten te ondervragen of om gestandaardiseerde audit programma's op te stellen. De ontwikkeling van een auditprogramma in elektronisch formaat verzekert de consistentie van audits over verschillende locaties en bedrijven heen. De auditor wordt begeleid in elke stap van de audit. Bij een audit van het aantal overuren, zal bijvoorbeeld het gepaste aantal overuren automatisch worden bepaald aan de hand van de aanwezige vakbonden en de sector waarin de onderneming actief is (Gallegos et al., 2004).

Hoofdstuk 5: Informatiesystemen en de continue audit

De eerder besproken CAATTs verhogen de efficiëntie en de betrouwbaarheid van een audit door de benodigde audittijd te verlagen en de hoeveelheid geanalyseerde gegevens te vergroten op het moment van de periodieke audit. In vele gevallen zal de auditor echter ook geïnteresseerd zijn in uitzonderlijke transacties en de werking van het interne controlesysteem tussen twee auditperiodes in. Een continue audit is een methode die werd ontwikkeld om dit mogelijk te maken. (Moeller, 2009). Met behulp van de eerder genoemde continue CAATTs en de nog niet besproken audit modules, worden transacties gecontroleerd op het moment dat ze worden ingegeven. In dit hoofdstuk wordt een overzicht gegeven van de verschillende factoren die de vraag naar CA sturen, de toepassing ervan in de praktijk en de achterliggende technologieën.

5.1. Vraagfactoren

De vraag naar een meer continue audit wordt gedreven door verschillende factoren: de verhoogde complexiteit en data intensiviteit van de bedrijfsprocessen, het groeiende aandeel elektronische transacties, outsourcing, waardeketen integratie, web gebaseerde rapportering en een verhoogde vraag naar betrouwbare informatie aangestuurd vanuit een vrije markt economie. Er wordt verwacht dat accurate informatie tijdig en frequent wordt aangeleverd.

Ook binnen verschillende wetgevingen wordt een meer continue informatieverplichting vastgelegd. Bijvoorbeeld binnen sectie 409 van de SOX wetgeving, oftewel "the Real-Time Issuer Disclosures section" (Alles et al., 2008). Deze schrijft voor:

"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." (SOX, 2002).

Vanuit zijn definitie brengt CA de audit dichter bij het operationele proces, waardoor een meer continue informatiestroom verzekerd wordt (Alles et al., 2008). Ook voor wat betreft het aanleveren van externe auditbewijs kan CA een belangrijke rol spelen. Dit wordt het best uitgelegd door CA te vergelijken met het traditionele auditproces voor wat betreft de audit wachttijd en controle efficiëntie.

In een traditioneel auditproces is er een wachttijd tussen opeenvolgende audits. Na elke audit zal de efficiëntie van de controlesystemen verbeteren door de aanwezigheid en de aanbevelingen van de auditor. Ten gevolge van bijvoorbeeld veranderingen in het systeem, personeelswijzigingen en/of externe factoren kan de efficiëntie tussen twee audits in echter terug dalen[15]. Hierdoor bestaat de kans dat controlesystemen minder goed presteren dan wordt verwacht. Binnen de externe audit heeft dit een gebrek aan auditbewijs tot gevolg. Het zal immers moeilijk zijn om te bewijzen dat het controlesysteem gedurende het hele jaar op hetzelfde niveau heeft gewerkt. Het continue karakter van CA verzekert dat de controle efficiëntie stabiel zal blijven rondom de verwachtte efficiëntie en levert het benodigde auditbewijs[16] (Handscombe et al., 2007).

Op het moment dat er een mening betreffende het interne controlesysteem dient geformuleerd te worden, zullen de controleprocessen reeds zijn aangepast aan eventueel gedetecteerde uitzonderingen. Hierdoor ondersteund CA ook de voorschriften van SOX 404 betreffende de betrouwbaarheid van interne controles (Alles et al., 2008).

5.1.1. Voordelen continuous audit

Naast het feit een CA systeem beter inspeelt op veranderingen binnen de bedrijfsomgeving, zijn er ook nog een hele reeks andere voordelen verbonden aan het gebruik ervan. Deze voordelen zullen echter deels afhankelijk zijn van de specifieke bedrijfskenmerken. De voordelen van een CA systeem zullen immers groter zijn binnen een onderneming met een uitgebreid ERP-systeem en een grote hoeveelheid gegevens, dan binnen een kleine onderneming. Handscombe et al. (2007) vermeldt volgende algemeen geldende voordelen:

- Verminderde informatiewachttijd: door het bestaan van uitgebreide informatiesystemen beschikt een auditor op elk moment over alle benodigde gegevens. Hierdoor vervallen de wachttijden die normaal bestaan tussen het moment dat de auditor een informatieaanvraag indient en het moment dat de gegevens worden aangeleverd door de klant.
- Audit van uitzonderingen: auditors kunnen zich richten op uitzonderingen binnen het interne controlesysteem. Hierdoor zullen fouten in dit systeem sneller worden opgespoord.
- Grotere auditdiepte voor dezelfde kost: in tegenstelling tot het klassieke auditproces, waar men zich baseert op deelwaarnemingen, kan er binnen CA gewerkt worden met meer gedetailleerde gegevens.
- Nieuwe audit alternatieven: in een klassieke auditproces wordt er geen rekening gehouden met preventieve controlesystemen. Het was immers niet mogelijk om na te gaan of deze systemen gedurende het hele jaar op dezelfde wijze hadden gewerkt, waardoor er te

[15] Grafische voorstelling in bijlage 5.
[16] Grafische voorstelling in bijlage 6.

weinig audit bewijs beschikbaar was. Deze problemen doen zich echter niet voor binnen CA, waardoor preventieve controles aantrekkelijker worden. Dit voordeel werd ook besproken in punt 5.1.

- Proactieve aanpak: voor een audit cliënt zijn oplossingen waardevoller op het moment dat een probleem zich voordoet, dan ex-post. Op het moment dat men een uitspraak dient te doen over de kwaliteit van het systeem, zijn de fouten reeds gedetecteerd en gecorrigeerd.
- Grotere zichtbaarheid: doordat de audit beter inspeelt op de huidige economische werkelijkheid en problemen, wordt de zichtbaarheid van de audit vergroot.

Ook Masli et al. (2009) voerde een onderzoek naar de voordelen van continuous audit en meer specifiek naar continuous control monitoring zoals gedefinieerd door Alles et al. (2006). Hier werden drie mogelijke voordelen voorop gesteld, namelijk:

1. Efficiëntere interne controlesystemen

Het opzet van CCM omvat processen voor het bepalen van beveiligingsprotocollen, protocollen om de integriteit van informatie te verzekeren, monitoring tools voor het managen van bedrijfssystemen en risico's, e.d.. Al deze maatregelen hebben eenzelfde doelstelling, namelijk het verminderen van de kans op materiële fouten binnen het interne controlesysteem. Bijgevolg zullen ze leiden tot een efficiënter controlesysteem.

2. Voldoen aan SOX en extern audit bewijs

Verschillende functies van CCM technologie zijn gericht op de rol van externe auditors en het voldoen aan de voorschriften van SOX. CCM kan voorzien in de documentatie van monitoring en assessment activiteiten van het management (Masli et al., 2009). Dit principe vinden we ook terug in COSO (2009b):

"A properly designed and executed monitoring program helps support external certifications…because it provides persuasive information that internal control operated affectively at a point in time during a specific period."

Externe auditors kunnen verdergaan op documenten die voortkomen uit een intern controlesysteem met goede CCM. Hierdoor zal de audit efficiëntie stijgen en zullen de externe auditkosten dalen.

3. Tijdige audit rapportering

Zoals ook aangehaald door Handscombe et al. (2007), zal een uitgebreid CCM systeem een constante informatiestroom verzekeren, waardoor een tijdige en meer efficiënte rapportering mogelijk wordt.

5.2. Continue audit in de praktijk

5.2.1. Toepasbaarheid continuous auditing in de interne audit

Nu de vraagfactoren voor een CA vaststaan, kan er worden nagegaan hoe CA in de praktijk ook kan worden toegepast. In dit onderdeel worden CA toepassingen binnen het interne auditgebied van naderbij bekeken.

Een continu auditproces staat interne auditors toe om (IIA, 2005):

- Kritieke controlepunten, regels en uitzonderingen ten volle te begrijpen
- Controle en risicobeoordelingen uit te voeren in real-time
- Uitzonderingen te detecteren op het transactieniveau
- Analyseresultaten te integreren in alle aspecten van het auditproces

Een continue audit kan worden opgezet om de interne controle van een bedrijf te testen, of om de risico's waarmee het bedrijf in aanraking komt of kan komen te identificeren en analyseren. Er wordt dan respectievelijk gesproken over continuous control assessment en continuous risk assessment, zoals aangegeven in de definitie van het IIA (2005).

5.2.1.1. Doelstelling continuous control assessment

Door gebruik te maken van door technologie ondersteunde analytische methoden, kan een auditor op continue basis beoordelen of het interne controlekader voldoende toereikend is. De frequentie van deze analyse dient afhankelijk te zijn van het risico waaraan het bedrijf wordt blootgesteld en van de mate waarin het management toezicht houdt op de interne controlesystemen[17].

- Opsporen van gebreken in het interne controlesysteem

Over het algemeen wordt aangenomen dat het management verantwoordelijk is voor het ontwerpen van, het toezicht houden op en het onderhouden van interne controleprocessen. Desondanks vermelden de voorschriften van het Institute of Internal Auditors Standard 2120.A1:

[17] Schema bijlage 1 – De resultaten van CRA worden gebruikt voor het bepalen van de frequentie en diepgang van CCA. Gebieden met een hoger risiconiveau, worden vaker en uitgebreider gecontroleerd. Ook dient er rekening te worden gehouden met de monitoring activiteiten uitgevoerd door het management.

"The auditor should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvements."

Zoals reeds eerder vermeld zullen auditors de grondigheid van hun analyse laten afhangen van de mate waarin het management zich bezighoudt met continuous monitoring. Indien het management een uitgebreid en betrouwbaar continuous monitoring systeem heeft opgezet, zal er minder aandacht worden besteed aan continuous control assessment en omgekeerd (IIA, 2005).

- Ontdekken van fraude, verkwisting en misbruik

Technologieën die continuous control assessment ondersteunen kunnen de auditor helpen bij het onderzoeken van transacties en bij het analyseren van databases om anomalieën te detecteren die kunnen wijzen op fraude, verkwisting of misbruik (IIA, 2005).

5.2.1.2. Doelstelling continuous risk assessment

Auditors zijn verantwoordelijk voor het identificeren en evalueren van de risico's waaraan een bedrijf wordt blootgesteld en voor het verbeteren van het risicomanagement. Continuous risk assessment kan worden ingezet om risico gebaseerde plannen op te stellen en om de prioriteiten van de interne audit af te stellen op de bedrijfsdoelstellingen. Zowel interne als externe risico's moeten continu worden beoordeeld, zodat er op een tijdige en gepaste wijze kan worden ingespeeld op potentiële risico's (IIA, 2005).

- Ontwikkeling audit plan

Continuous risk assessment staat de auditor toe om een meer strategische context te geven aan het audit plan. Nadat de kritieke succesfactoren voor de bedrijfsstrategie zijn geïdentificeerd, kunnen deze worden verwerkt in het audit plan. Op deze manier worden de schaarse audit middelen toegewezen aan de belangrijkste posten.

- Individuele audit ondersteuning

De schaal en gedetailleerdheid van een conventionele audit wordt sterk beperkt door het type en de hoeveelheid data die kan worden verzameld door gebruik te maken van traditionele technieken. Continuous audit heeft het potentieel om de hoeveelheid gegevens waarover de auditor kan beschikken sterk te vergroten.

Een grotere hoeveelheid data staat de auditor toe om de schaal waarop de audit wordt uitgevoerd te verkleinen. Een ondernemingsbrede audit kan zo worden aangevuld met een meer specifieke audit gericht op één bepaald bedrijfsonderdeel, bedrijfsproces of locatie.

- Opvolging aanbevelingen audit

Na het uitvoeren van een audit en het geven van aanbevelingen, kan de auditor CRA aanwenden om na te gaan of zijn aanbevelingen zijn geïmplementeerd en om te bepalen of deze het gewenste effect hebben gehad. Indien dit niet het geval is, kan er nog worden bijgestuurd (IIA, 2005).

5.2.2. Toepasbaarheid continuous auditing in de externe audit

Ook bij het uitvoeren van een externe audit kunnen continuous audit systemen worden toegepast. De mogelijke toepassingen hiervan komen dan grotendeels overeen met deze binnen de interne audit. De focus zal hier echter meer liggen op het verzekeren van de betrouwbaarheid van de financiële gegevens en het interne beheersingssysteem. Binnen de externe audit wordt er dan ook geopteerd voor een opsplitsing van CA naar CDA en CCM, zoals aangegeven door Alles et al. (2006).

Binnen de externe audit dient er bovendien ook rekening te worden gehouden met de geldende gedrags– en onafhankelijkheidsvoorschriften. Het gebruik van een geïntegreerd CA systeem kan immers leiden tot een onafhankelijkheidsprobleem. De problemen die zich voordoen bij het gebruik van CA binnen de externe audit worden verder uitgediept in hoofdstuk acht.

5.3. Voorwaarden continuous audit

De voordelen en mogelijke toepassingen van CA zijn talrijk. Het opzetten van een dergelijk systeem is echter geen sinecure. Er zijn verschillende voorwaarden waaraan een onderneming en een auditor moet voldoen om een succesvol en effectief CA systeem op te zetten. Deze zijn volgens Handscombe et al. (2007):

- Technologie: het is noodzakelijk om audit tests te automatiseren om zodoende de kosten te kunnen onderdrukken. Indien men gebruik zou maken van klassieke audit technologieën zouden de auditkosten te snel stijgen. Ook dient er voldoende aandacht besteed te worden

aan het opzetten van communicatietechnologieën, zodat gevonden fouten snel kunnen worden gecommuniceerd.

- Goede controleomgeving[18]: de controleomgeving dient te verzekeren dat het aantal uitzonderingen op een aanvaardbaar niveau wordt gehouden. Continuous monitoring speelt hier een belangrijke rol in.
- Georganiseerde audit aanpak: auditors moeten zich bewust zijn van de belangrijkste risico- en succesfactoren van de onderneming. De regels voor het detecteren van uitzonderingen, dienen hierop gebaseerd te zijn.
- Flexibel audit team: de nieuwe aanpak van CA vertegenwoordigt een nieuwe audit aanpak waarin auditors simultaan verantwoordelijk zullen zijn voor meerdere bedrijven, in de plaats van één bedrijf tegelijk. Een flexibel auditteam is bijgevolg onontbeerlijk.
- Uitgebreide systeemkennis: om controlesystemen waarheidsgetrouw te kunnen beoordelen, dienen auditors over een uitgebreide kennis over deze systemen te beschikken.
- Ondersteuning van het management: management ondersteuning is nodig om te verzekeren dat auditors toegang hebben tot de benodigde systemen en data. Ook dienen ze een gepaste reactie te voorzien op de auditrapporten.
- Toegang tot alle gegevens: auditors dienen toegang te hebben tot alle benodigde gegevens op een continue basis.

GTAG 3 (2005) - Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment - vermeldt hiernaast ook het belang van een competent auditteam, het stimuleren van het management om een monitoring systeem op te zetten en de opvolging van auditaanbevelingen.

Ook de externe auditor dient betrokken te worden bij het opzetten van CA. Betrokkenheid van de externe auditor zorgt immers voor een optimale auditdekking. Deze betrokkenheid zal daarenboven ook buitenstaanders meer comfort geven over het niveau van continuous assurance.

5.3.1. Voorwaarden onderliggende informatietechnologie

De belangrijkste factor bij de implementatie van CA is de onderliggende informatietechnologie. Opdat technologie kan bijdragen aan het proces van interne beheersing dient het te voldoen aan volgende criteria (Handscombe et al., 2007):

- Geautomatiseerde aanvang: het systeem dient de audittests automatisch te starten aan de hand van een vooraf opgestelde planning.

[18] Als onderdeel van de interne controleomgeving zoals aangegeven door COSO (2004).

- Onopvallend: de audit tools dienen onopvallend verwerkt te worden in het bestaande systeem. Dit is bijvoorbeeld niet het geval indien het auditproces een negatieve invloed heeft op de systeemprestaties of een extra administratieve werklast tot gevolg heeft. In dat geval zullen audit systemen als eerste worden uitgeschakeld door gebruikers om de systeemprestaties te verbeteren.
- Onafhankelijke analyse van de brongegevens: er dient een minimale manipulatie plaats te vinden van de gegevens die worden gemonitord. Dit kan enkel worden verzekerd indien het systeem de brongegevens analyseert, zonder enige vorm van selectie bias of invloed.
- Automatische distributie: zoals reeds aangehaald is een vroegtijdige detectie van uitzonderingen enkel nuttig indien deze ook snel worden gecommuniceerd aan de betrokken partijen. Hiervoor dient de benodigde communicatietechnologie te worden voor voorzien.
- Platform onafhankelijk: een platform onafhankelijk[19] controlesysteem zou tot gevolg hebben dat een auditor slechts één systeem moet leren kennen.
- Intuïtief: De audittool dient relatief eenvoudig in gebruik te zijn om algemeen gebruik te bevorderen.
- Audit systeemcontroles: een onderdeel van het CA systeem dient na te gaan of de interne controlesystemen effectief werken. Indien er geen of slechts een beperkt aantal uitzonderingen worden gedetecteerd, is dit namelijk geen garantie dat de controlesystemen werken.

5.4. Een continuous audit model

Een continuous auditproces bestaat uit vier fasen[20]. In een eerste fase wordt nagegaan voor welke bestaande auditprocedures CA technieken kunnen worden toegepast. In een tweede fase worden data modellerings technieken aangewend voor het ontwikkelen van benchmarks. De impliciete assumptie die hier wordt gemaakt is dat toekomstige transacties dezelfde kenmerken zullen vertonen als historische transacties. Deze fasen maken deel uit van het implementatieproces en worden nog verder besproken in punt 5.5. In een derde fase worden alle transacties en interne beheersingssystemen gecontroleerd op basis van de eerder opgestelde benchmarks. In de vierde en laatste fase worden de resultaten van deze analyse verspreid (Vasarhelyi et al., 2004). Rekening houdend met de verschillende doelstellingen van CA en met bovenstaande voorwaarden, kan volgend "ideaal" auditmodel worden opgesteld.

[19] Zijnde hardware, operating system en applicatie onafhankelijk.

[20] Zie schematische voorstelling in bijlage 7.

In een eerste stap wordt de monitoring tool geïnstalleerd op een computer binnen het netwerk van de cliënt of de auditor. Dit dient te gebeuren op een manier die verzekert dat de tool geen negatieve invloed uitoefent op de bedrijfsprestaties. De tool wordt ingesteld om op vooraf geplande tijdstippen specifieke auditcontroles uit te voeren (Handscombe et al., 2007). In deze fase dient de auditor na te gaan binnen welke procedures CA kan worden toegepast. Een deel van de controles zal immers niet kunnen worden uitgevoerd met behulp van automatische systemen. Zoals reeds aangegeven, vormt CA dan ook een combinatie van automatische en handmatige processen (Vasarhelyi et al., 2004). De frequentie van de verschillende controles zal afhankelijk zijn van het belang van de uitgevoerde test. Een test met betrekking tot een succesfactor zal bijvoorbeeld continu worden uitgevoerd. De meest voorkomende controles zijn transactiecontroles, detailanalyses van willekeurig gekozen samples, waarschuwingen bij wijzigingen binnen het controlesysteem, key performance indicators, ratioanalyses,… (Handscombe et al., 2007).

In een tweede fase verkrijgt de audit tool read only toegang tot de brongegevens opgeslagen in de verschillende (ERP) databases (Handscombe et al., 2007). De toegang tot de gegevens zal gebeuren aan de hand van een embedded audit module (EAM) of een monitoring & control layer (M&C layer). Deze architecturen worden later nog verder besproken (Vasarhelyi et al., 2004). Zowel financiële als niet-financiële informatie kan worden geraadpleegd, waardoor het verzamelen van audit bewijs eenvoudiger wordt. Door gebruik te maken van virtual private network[21] technieken, wordt het auditproces daarenboven gedecentraliseerd. De auditor is in staat om vanop elke locatie de gegevens te raadplegen (Handscombe et al., 2007).

Aan de hand van historische, reeds gecontroleerde gegevens en data modelleringstechnieken worden benchmarks opgesteld die gebruikt kunnen worden als referentiekader voor toekomstige transacties. Deze benchmarks worden gebruikt binnen de analytische fase voor het evalueren van transacties en het interne beheersingssystemen (Vasarhelyi et al., 2004).

Na het uitvoeren van de geplande auditcontroles zullen de rapporten worden verzonden via email naar de betrokken partijen of worden verspreid via een exception database en bijhorend audit dashboard. Auditteams kunnen deze rapporten vervolgens verwerken in hun analyses en resultaten. In overleg met het management kunnen oplossingen worden geformuleerd voor gedetecteerde problemen (Handscombe et al., 2007). Indien het CA systeem geen uitzonderingen detecteert, zou het onderliggende accounting systeem vrij moeten zijn van materiële fouten (Vasarhelyi et al., 2004).

[21] Een virtueel privaat netwerk (VPN) is een uitbreiding van het privénetwerk van de organisatie en staat gebruikers toe om vanop afstand met behulp van een publiek netwerk te verbinden (Cisco).

5.4.1. CA architectuur

Een CA systeem kan worden opgezet als subsysteem van het bestaande informatiesysteem of als een onafhankelijk systeem. In het eerste geval spreekt men van een embedded audit module, in het tweede van een monitoring and control layer.

Groomer en Murthy (1989) en Vasarhelyi en Harper (1990) introduceerde de "embedded audit module" (EAM). Deze module wordt verwerkt in het operationeel systeem van de cliënt en controleert transacties op het moment dat ze worden ingevoerd. Indien transacties bepaalde vooraf vastgestelde criteria overschrijden, wordt een alarm gegenereerd en zal de transactie worden gekopieerd naar een auditbestand voor verdere analyse. Op het moment van de audit zal de auditor bijgevolg minder tijd dienen te besteden aan het identificeren van significante transacties.

In tegenstelling tot de initiële verwachtingen, wordt er echter maar weinig gebruik gemaakt van de EAM architectuur. Het feit dat een EAM in het bestaande systeem wordt geïmplementeerd heeft immers tot gevolg dat er een invloed op de brongegevens kan worden uitgeoefend. Dit risico neemt nog toe indien de read-only toegang van het auditsysteem tot de bedrijfsinformatie niet overal consistent wordt doorgedreven (Alles, 2008, 2006). Om aan dit nadeel tegemoet te komen, werd EAM ghosting ontwikkeld.

EAM ghosting houdt in dat men gebruik maakt van een exacte kopie van het originele bedrijfssysteem en is in deze zin te vergelijken met het systeem van een parallelle simulatie. Zowel gegevens als instellingen worden in real-time overgenomen. De controles zullen vervolgens worden uitgevoerd op dit ghost systeem. Op deze manier is er geen risico dat het controlesysteem een invloed uitoefent op de originele transactiegegevens (Kuhn en Sutton, 2010).

Naast de invloed die een EAM kan uitoefenen op de originele gegevens, zijn er echter ook nog verschillende andere beperkingen. Debreceny et al. (2005) en Alles et al. (2002) vermelden de volgende:

1. Technische behoefte

Het opzetten en opereren van een ERP systeem vereist een grote hoeveelheid informatiesystemen. De extra berekeningen en controles die worden uitgevoerd door een EAM, of de extra processorkracht die nodig is om gegevens door te sturen naar het ghost systeem, kunnen het ERP systeem en daardoor ook alle gerelateerde processen drastisch vertragen. Om deze vertragingen te voorkomen is een significante investering in bijkomende hardware vereist. Toch vormt een extra investering in hardware nog geen zekerheid dat alle vertragingen kunnen worden weggewerkt. Een deel van deze vertragingen kan immers te wijten zijn aan 'non-native code'. EAM maakt immers

slechts zelden deel uit van een standaard ERP pakket, waardoor dit er steeds op een later tijdstip moet worden in geprogrammeerd. Zelfs indien dit gebeurt in de scripttaal van het originele pakket, zijn vertragingen onvermijdelijk. Binnen een ghost systeem hebben deze vertragingen geen invloed op de bedrijfsprocessen, maar een onstabiel systeem kan wel leiden tot slecht of niet uitgevoerde controles.

2. Implementatieproblemen in grote ondernemingen

In grotere organisaties wordt vaak gebruik gemaakt van meerdere ERP systemen. Aangezien EAM geïntegreerd dient te worden in de programmacode van het onderliggende systeem, moet bijgevolg voor elk ERP systeem een individuele EAM worden ontwikkeld. Elk van deze systemen dient daarenboven afzonderlijk te worden afgesteld en onderhouden. Het uitvoeren van een algemene audit over alle ERP systemen heen wordt hierdoor bemoeilijkt.

In 2004 introduceerde Vasarhelyi et al. een alternatieve CA architectuur, namelijk een "monitoring and control layer" (M&C layer). Deze architectuur wordt geïmplementeerd op een onafhankelijk systeem dat meestal eigendom is van de auditor. In tegenstelling tot EAM kan een M&C layer enkel gegevens uitlezen, waardoor de originele gegevens niet kunnen worden beïnvloed door het controlesysteem (Alles et al., 2008, 2006).

De hoofdbestandsdelen van een M&C layer zijn:

1. Gegevens verzameling
2. Gegevensfilter
3. Relationele opslag
4. Meetstandaarden
5. Relatiecontroles
6. Analytische laag
7. Alarmen en waarschuwingen
8. Rapporteringsplatform

Op periodieke tijdstippen, gespecifieerd door de auditor, ontvangt het CA systeem gegevens die vervolgens worden vergeleken met vooraf opgestelde criteria. Net zoals bij een EAM zullen transacties die bepaalde criteria overschrijden een alarm genereren en worden opgeslagen in een audit database. Deze database staat onder controle van de auditor en kan niet worden aangepast door het management. Dit in tegenstelling tot de EAM architectuur, waar uitzonderingen worden opgeslagen in de ERP database die wordt beheerd door het management (Kuhn en Sutton, 2010).

Desondanks de grotere populariteit van de M&C layer, heeft ook deze architectuur nog enkele nadelen. De gegevens die worden geëxtraheerd uit de database van de cliënt dienen immers even

sterk beveiligd te worden als in het originele systeem. Ook dient er voldoende opslag te worden voorzien. De kosten van een M&C layer zijn dus aanzienlijk (Alles et al., 2008, 2006).

5.5. Implementatie continu auditsysteem

Nu de voordelen, doelstellingen en voorwaarden van een CA systeem bekend zijn, kan er worden overgegaan tot het bespreken van de implementatie ervan. De vorm en werking van een CA systeem is sterk afhankelijk van de situatie en de interne bedrijfsomgeving. Het systeem dient immers steeds te worden afgestemd op de specifieke bedrijfseigenschappen, succesfactoren en risicofactoren.

Wat betreft de te volgen stappen voor de implementatie van CA kan er worden verder gegaan op meerdere kaders. In wat volgt wordt een algemeen kader besproken opgesteld door het IIA (2005), aangevuld met implementatierichtlijnen van Vasarhelyi et al. (2009). Er wordt geopteerd voor de richtlijnen van het IIA omwille van de grotere rol die CA speelt binnen de interne auditomgeving in vergelijking met de externe audit. Volgens deze richtlijnen verloopt een implementatie in 9 stappen:

5.5.1. Vaststellen van de audit doelstellingen en vereisten

In een eerste stap dient de auditor de huidige en toekomstige doelstellingen van het CA systeem te begrijpen. Rekening houdend met input van het management en externe auditors, dient bepaald te worden aan welke vereisten het systeem moet voldoen. De auditor zal hiervoor over voldoende kennis moeten beschikken met betrekking tot de industrie, de organisatie, de ondernemingsprocessen, de controleprocessen en technologie gebaseerde oplossingen (IIA, 2005). Er dient ook te worden nagegaan of er voldoende gegevens beschikbaar zijn om een CA systeem op te baseren en of de voordelen ervan opwegen tegen de implementatiekosten (Vasarhelyi et al., 2009).

5.5.2. Verkrijgen van management ondersteuning

Om een succesvolle ondernemingsbrede implementatie te kunnen verzekeren, moet zowel het management als het auditcomité het opzet ondersteunen. Beide dienen op de hoogte te zijn van het auditproces en de manier waarop de resultaten zullen gecommuniceerd worden. Hierdoor wordt ook de legitimiteit van de audit vergroot.

5.5.3. Bepalen van de auditscope

In deze stap dient bepaald te worden in welke mate van detail de controlesystemen en risico's getest zullen worden. De mate waarin het management zich bezig houdt met continuous monitoring zal hier van groot belang zijn. Indien het management een sterk CM systeem in gebruik heeft, zal de auditor zijn inspanningen op dit gebied kunnen verminderen en vice versa.

5.5.4. Identificeren van informatiebronnen en bekomen van toegang

Aan de hand van de doelstellingen en schaal van de audit, kan er bepaald worden welke informatie nodig is om een betrouwbare audit te bereiken. Vervolgens moet ook de toegang tot deze gegevens worden bekomen. Een goede relatie met IT management is hier onontbeerlijk. Door de ontwikkelingen die hebben plaatsgevonden op het gebied van IT, is het verkrijgen van deze informatie eenvoudiger geworden dan voorheen. Er dient bijzondere aandacht te worden besteed aan de selectie van deze technologieën.

Toegang tot deze informatiebronnen kan worden verkregen door gebruik te maken van één of meerdere van volgende methoden:

- Het verwerken van CA software in het systeem van de onderneming.
- Verkrijgen van onafhankelijke toegang tot de database, zonder gebruik te maken van de software opgesteld door de onderneming.
- Kopiëren van standaard rapporten en opslaan in elektronisch formaat voor verdere analyse
- Uitvoeren van query's.
- Verkrijgen van fysieke en logische toegang tot het systeem van de cliënt met read-only access.

5.5.5. Begrijpen van de ondernemingsprocessen

Om een efficiënt auditproces op te zetten moet een goed begrip van de verschillende ondernemingsprocessen worden verkregen. Dit kan onder andere worden bekomen door het inkijken van documentatie, het afnemen van interviews, het analyseren van het systeem en data stroommodellen, e.d.. Aan de hand van de belangrijkste risicofactoren kunnen vervolgens de controles worden geselecteerd die onderdeel zullen uitmaken van de audit.

5.5.6. Opbouwen technische audit vaardigheden en kennis

IIA standaard 1210 vereist dat interne auditors over de benodigde vaardigheden en technische kennis beschikken om aan hun verantwoordelijkheden te voldoen. GTAG-1 (2005) vermeldt:

"Varying levels of IT knowledge are needed throughout the organization to provide systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes. Knowledge of how IT is used, the related risks, and the ability to use IT as a resource in the performance of audit work is essential for auditor effectiveness at all levels." (GTAG-1).

5.5.7. Opzetten van continuous control assessment

Het opzetten van CCA gebeurt aan de hand van het COSO of CoBIT raamwerk. De controledoelstellingen kunnen worden onderverdeeld in: autorisatie, accuraatheid, volledigheid, geldigheid, efficiëntie en effectiviteit. Hieruit worden vervolgens de belangrijkste controlesystemen geselecteerd en gerangschikt naar de invloed die ze uitoefenen op het bereiken van de ondernemingsdoelstellingen (IIA, 2005). Voor elk van deze systemen dienen regels en analytische methodes te worden ontwikkeld die gebruikt zullen worden als toetsingscriteriums. Bijvoorbeeld een regel die aangeeft vanaf welk bedrag een transactie als uitzonderlijk zal worden beschouwd. Deze regels zullen verschillen per transactie en dienen dus in samenwerking met het management te worden opgesteld en dienen aangepast te worden aan interne of externe veranderingen (Vasarhelyi et al., 2009).

5.5.8. Opzetten van continuous risk assessment

Het doel van een risk assessment is het afstemmen van de organisatiestrategie op de organisatieprocessen, technologie en aanwezige kennis ter evaluatie van de mogelijke risico's die een invloed kunnen hebben op het bereiken van de doelstellingen. Indien aanwezig, kan de auditor zich baseren op het ERM systeem.

In een volgende fase zullen de verschillende risico categorieën worden geïdentificeerd. Zo wordt er een onderscheid gemaakt tussen externe, juridische, overheid, strategische, operationele, e.d. risico's. Deze categorieën kunnen helpen om de verschillende risico's te bepalen en in te schatten. Voor elk van deze risico's dient bepaald te worden wat de kans is dat het risico zich voordoet en wat de gevolgen hiervan zouden zijn (IIA, 2005). Het opzetten van een CRA functie zal binnen het gebied van de externe audit een kleinere rol spelen. Het voornaamste doel van CRA is immers het

ondersteunen van de operationele processen en het tijdig inspelen op veranderingen in de omgeving. Deze doelstelling sluit niet aan bij de definitie van de externe audit.

5.5.9. Managen en rapporteren van de resultaten

In een laatste stap dient de auditfrequentie te worden bepaald. Auditors moeten rekening houden met het natuurlijke ritme van de bedrijfsprocessen en met de cost-benefit ratio. Indien auditcontroles worden uitgevoerd met een grotere frequentie, zullen de auditkosten immers stijgen. Enkel indien de voordelen van een verhoogde frequentie groter zijn dan de kosten dient de frequentie te worden verhoogd (Vasarhelyi et al., 2009). De tests kunnen worden uitgevoerd in real-time, near real-time of op periodieke tijdstippen. Daarnaast dient de wijze bepaald te worden waarop de resultaten gecommuniceerd zullen worden naar de betrokken partijen (IIA, 2005).

5.6. Praktijkvoorbeelden uit de literatuur

Zoals reeds eerder aangehaald kan naar analogie met de traditionele audit en de definitie gegeven door Alles et al. (2002), CA worden ingericht ter controle van de interne controlesystemen – CCM - of om substantiële testen uit te voeren op operationele data - CDA (Alles et al., 2008). Van beide wordt in dit hoofdstuk een pilootimplementatie besproken.

5.6.1. Continuous control monitoring

Een pilootimplementatie van CCM vond plaats bij Siemens onder toezicht van M. Alles, A. Kogan en M. Vasarhelyi. De drijfveer voor het opzetten van een CA systeem waren hier, naast een verhoogde efficiëntie, voornamelijk de verplichtingen opgelegd door SOX 404. CA werd bekeken als een hulpmiddel om de werklast voor de interne auditors te verminderen, zodat er tijd vrijkwam om aan de verplichtingen van de SOX wetgeving te voldoen.

Volgens Vasarhelyi et al. (2004) worden in een eerste fase van een CA implementatie de reeds bestaande auditprocedures geautomatiseerd. Zodra de toegevoegde waarde hiervan vaststaat, kan er worden overgegaan naar het herontwerpen van de auditprocedures zodat deze de onderliggende technische mogelijkheden ten volle kunnen benutten. Om dit stadium te bereiken zullen auditors hun eigen werkwijze moeten onderzoeken om na te gaan of en waar deze nog kan worden verbeterd.

Bij de pilootimplementatie bij Siemens volgde men zes stappen gebaseerd op Vasarhelyi et al. (2004):

Stap één: in deze eerste stap wordt er bepaald op welke manier de interne audit wordt uitgevoerd en welke interne monitoring systemen actief zijn. We onderscheiden drie mogelijke manieren waarop de effectiviteit van de interne systemen kan worden bepaald:

1. Nagaan of data wordt onderworpen aan controles en of deze controles bestaan, correct zijn opgesteld en correct functioneren.
2. Uitvoeren van een verboden transactie en nagaan of deze wordt gedetecteerd.
3. De instellingen van het opgezette controlesysteem vergelijken met vooraf opgestelde standaarden.

Het merendeel van de auditcontroles uitgevoerd binnen Siemens viel onder de derde categorie. Bij de CA implementatie diende men dus te bepalen welke van de controles geautomatiseerd konden worden.

Stap twee: ontwikkelen van een systeemarchitectuur voor het uitvoeren van de controles. Zijnde met behulp van een monitoring & control layer of een embedded audit module. Om de invloed van het systeem zo minimaal mogelijk te houden, werd er hier geopteerd voor een M&C layer.

Stap drie: bepalen van de interactie tussen het CA-mechanisme en het ERP systeem en de mate van integratie. In een klassiek auditproces kijkt men enkele keren per jaar terug op de gebeurtenissen van de voorbije periode. Binnen een M&C layer is dit niet het geval en dient men enkel te bepalen in welke mate men deze wenst te integreren met het bestaande ERP systeem.

Stap vier: ontwikkelen van richtlijnen voor de formalisatie en automatisatie van auditprocedures. Dit vereist dat men nagaat welke procedures onmiddellijk geautomatiseerd kunnen worden en tracht om niet automatiseerbare procedures te herontwerpen.

Stap vijf: creëren van processen voor het managen van de waarschuwingen die worden gegenereerd door het geautomatiseerde auditsysteem. Een controlesysteem wordt ingesteld om de auditor te verwittigen door middel van sms, email,… Het risico bestaat dat er teveel waarschuwingen worden gegenereerd, waardoor er te weinig aandacht wordt besteed aan elke fout.

Stap zes: formuleren van een veranderingsplan ter implementatie van de geautomatiseerde systemen.

Uit de pilootimplementatie bij Siemens bleek dat, in een bedrijfsomgeving gekenmerkt door een hoge mate van automatisatie, CA gedefinieerd kan worden als een proces gericht op het continu testen van controlesystemen. Deze controles zijn gebaseerd op criteria voorgeschreven door de auditor met de bedoeling uitzonderingen te detecteren die nader onderzoek vereisen.

5.6.2. Continuous data assurance

Een pilootimplementatie van een continuous data assurance systeem vond plaats bij een Amerikaanse health service provider (HSP). Eén van de belangrijkste strategische drijvers binnen hun bedrijfsproces was de mogelijkheid om hun aanbodketen efficiënter te managen. Deze bestond immers uit een groot aantal magazijnen verspreid over het hele land.

In tegenstelling tot Siemens maakte HSP nog voornamelijk gebruik van legacy systemen die slechts in beperkte mate met elkaar verbonden waren. Wel werd er gebruik gemaakt van een moderne database waarheen alle ruwe gegevens werden geüpload. Omwille van deze redenen werd er geopteerd voor een systeem van continuous data assurance in de plaats van continuous control monitoring.

Binnen een CDA systeem worden in een eerste fase verschillende geautomatiseerde tests uitgevoerd op individuele transacties. Nadien wordt de ruwe data getest door middel van 'continuity equations'. Aan elk bedrijfsproces wordt een controlevolume gekoppeld dat afkomstig is van een analoog bedrijfsproces. Bijvoorbeeld het aantal ontvangen leveringen zou moeten overeen komen met het aantal geplaatste bestellingen.

In tegenstelling tot de moderne ERP systemen binnen Siemens, werden er door de legacy systemen geen controles uitgevoerd op de gegevens vooraleer deze werden verzonden naar de centrale database. Niet verwonderlijk bleek het aantal onregelmatigheden in de dataset dan ook vrij hoog te zijn (Alles et al., 2008).

Hoofdstuk 6: Kloof tussen intern en extern gebruik van CA systemen

In tegenstelling tot de verwachtingen voor de eigenlijke invoering van de SOX wetgeving (2002) waren het niet de externe, maar wel de interne auditors die gebruik gingen maken van CA-systemen (Alles et al., 2008). De redenen hiervoor zijn tweeledig:

1. De verplichtingen vooropgesteld door SOX 404 leidde tot extra werk voor de externe auditor. Naast hun gebruikelijke taak dienden zij nu immers ook een uitspraak te doen over de efficiëntie en betrouwbaarheid van de interne controles die in het bedrijf worden gehanteerd. Hierdoor bleef er weinig tijd over om nieuwe CA methodologieën te ontwikkelen. Interne auditors zagen in CA daarentegen een manier om de extra werklast, veroorzaakt door SOX 404, te verminderen. Bij de pilootimplementatie bij Siemens was het voldoen aan de SOX 404 voorschriften bijvoorbeeld een belangrijke implementatiereden.

2. Een tweede factor waren de onafhankelijkheidsvoorwaarden die werden opgelegd in SOX 201[22]. Door deze voorwaarden werd de bewegingsvrijheid van de externe auditor enigszins beperkt. Het geïntegreerde ontwerp van een CA systeem zou immers een inbreuk kunnen vormen op de SOX 201 consultancy en/of interne audit onafhankelijkheid voorschriften. De auditor bevindt zich dan in een positie waarin hij een uitsprak moet doet over een systeem dat hij zelf (deels) heeft ontworpen. De interne auditor diende daarentegen niet te voldoen aan dit soort onafhankelijkheidsvoorschriften (Alles et al., 2008).

Voor wat betreft de onafhankelijkheid van de externe auditor, speelt ook de gekozen CA architectuur een belangrijke rol. Deze zal immers een grote invloed uitoefenen op de mate waarin de auditor betrokken is in de interne controleactiviteiten van de onderneming.

6.1. EAM en M&C Layer

Het volledig geïntegreerde ontwerp van een EAM stelt enkele problemen voor het gebruik ervan binnen het gebied van de externe audit. De meest kritieke bevinden zich op het gebied van

[22] SOX 201: elke audit en niet-auditdienst dient vooraf te worden goedgekeurd door het audit comité. Gericht op het behoud van onafhankelijkheid en het voorkomen van controle van eigen werk.

systeem ontwerp en onderhoud, auditor aansprakelijkheid en de reeds eerder vermelde onafhankelijkheid. Op deze gebieden heeft een M&C layer een duidelijk voordeel ten opzichte van EAM en EAM ghosting.

- Systeem ontwerp en onderhoud

Zoals voorgesteld door Debreceny et al. (2005) en naar de CA implementatierichtlijnen van Vasarhelyi et al. (2009) dient de externe auditor betrokken te worden bij het ontwerp en de implementatie van een EAM. Op deze manier heeft de externe auditor meer zekerheid over de efficiëntie en effectiviteit van het systeem en voorkomt men dat de cliënt over een te grote kennis van de auditprocessen beschikt. Hieruit ontstaan echter enkele praktische problemen. Om dit mogelijk te maken zal de auditor immers over onbeperkte toegang moeten beschikken tot de IS van de cliënt. Hij moet in staat zijn om op zelfstandige basis aanpassing door te voeren aan het systeem. Indien dit niet op een correcte manier gebeurt, bestaat er een kans op gegevensverlies, een systeemcrash, een slecht werkend systeem, e.d.. Omwille van deze risico's zullen bedrijven nooit de volledige controle uit handen willen geven.

De implementatie van een EAM vereist een grondige kennis van ERP programmeertaal. Indien een externe auditfirma ervoor kiest om EAM als onderliggende architectuur te gebruiken, dienen auditors niet alleen te trainen in het uitvoeren van een audit, maar ook in de diverse ERP systemen en talen. Het aantrekken van IT auditors vormt hier een grote uitdaging.

- Auditor onafhankelijkheid

Er bestaat een onweerlegbare technische relatie tussen het informatiesysteem van de onderneming en de EAM. De verantwoordelijkheid en toegang die de auditor door deze relatie krijgt over het IS van de cliënt kan een inbreuk vormen op de onafhankelijkheidsvoorwaarden vooropgesteld in de SOX wetgeving en de SAS. Dan wel in feite of in schijn.

- Cliënt onafhankelijkheid

Zoals reeds eerder vermeld zullen ondernemingen de auditor nooit volledige toegang tot hun systemen verschaffen. Ook langs de andere kant zullen systeembeheerders nooit toestaan dat zij geen toegangsrechten hebben tot het audit systeem in het geval van systeemproblemen.

De cliënt toegang geven tot en inzicht geven in het audit systeem tijdens de ontwikkelings- en de implementatiefase of na de implementatie, kan een cliënt onafhankelijkheidsprobleem tot gevolg

hebben. Een te grote kennis van het systeem kan immers leiden tot manipulatie ervan door de cliënt. Deze kan zijn kennis aanwenden om bijvoorbeeld frauduleuze activiteiten zo te plannen dat ze niet aan een controle onderhevig zullen zijn of zo configureren dat er geen alarm zal worden gegenereerd.

- Juridische aansprakelijkheid

Informatiesystemen vormen vaak de kern van een onderneming. Ze zijn belangrijk voor het verderzetten van operationele activiteiten en het bekomen van een competitief voordeel. Het doorvoeren van aanpassingen in dit systeem draagt dan ook een groot risicogehalte. De onderneming zal dit risico willen verminderen door de auditor juridisch aansprakelijk te stellen indien hun IS wordt beschadigd. De dreiging van dit soort juridische acties zal veel ondernemingen aanzetten om geen gebruik te maken van een EAM strategie.

Een externe auditor zal in de praktijk dan ook voornamelijk gebruik maken van een M&C layer. Om op deze manier zijn onafhankelijkheid te verzekeren en eventuele inmenging van het management te voorkomen. Dit systeem heeft, zoals ook eerder werd vermeld, ook zijn nadelen. Zo zal de externe auditmaatschappij over een grote hoeveelheid IS dienen te beschikken om alle controles te kunnen uitvoeren zonder te steunen op de bedrijfssystemen. Ook dient de informatie voldoende te worden beveiligd om verspreiding naar derden te voorkomen (Kuhn en Sutton, 2010).

Hoofdstuk 7: Empirisch onderzoek

Het empirisch onderzoek is gericht op het bevestigen of weerleggen van de bevindingen uit de literatuurstudie. Om dit te kunnen bereiken wordt het gebruik van IS binnen een combinatie van interne en externe auditafdelingen bestudeerd. Er wordt aangenomen dat enkel grote bedrijven een door IS ondersteund auditsysteem opzetten. Dit onderzoek wordt daarom ook uitgevoerd binnen een beursgenoteerde onderneming, zijnde Telenet. Om vervolgens ook informatie te verkrijgen betreffende het algemene gebruik van IS, wordt er een beroep gedaan op interne audit consultancy kantoren. Deze zullen immers een goed overzicht hebben over de huidige auditomgeving. Binnen de externe audit wordt een opsplitsing gemaakt tussen Big Four revisoren en kleinere revisoren.

Tabel 6: Uitwerking empirisch onderzoek

Interne audit	Externe audit
Onderneming	**Auditkantoor**
Telenet - Jan Borzée	Deloitte – Peter Leyman
	PwC - Jeroen Decroos
Consultancy	
PwC - Jeroen Decroos	
BDO - Koen Claessens	

Deze specifieke opsplitsing is gericht op het verifiëren van volgende hypothesen die voortkomen uit de literatuurstudie:

- H_1: Het gebruik van door CAATTs ondersteunde interne auditsystemen is beperkt tot grote ondernemingen. Binnen kleine ondernemingen wegen de bekomen voordelen niet op tegen de implementatie- en onderhoudskosten.
- H_2: Zowel binnen interne als externe auditafdelingen wordt geen gebruik gemaakt van alle mogelijke toepassingen van CAATTs.
- H_3: CA modules worden niet toegepast binnen de externe audit ten gevolge van onafhankelijkheidsproblemen.

De bevindingen uit deze interviews worden in hoofdstuk acht ook gebruikt om voorspellingen te maken voor wat betreft de toekomst van interne- en externe audits op het gebied van IT gebruik.

7.1. Interne audit

7.1.1. Telenet

Telenet is actief als breedbandleverancier sinds 1996 en beursgenoteerd op Euronext Brussels sinds 2005. Op 31 december 2010 telde Telenet 1.226.600 abonnees voor breedbandinternet 814.600 voor vaste telefonie en 1.241.900 voor digitale televisie. De groei ten opzichte van boekjaar 2009 bedroeg respectievelijk 10%, 10% en 24%. Het managen van een dergelijk groot klantenbestand en een dergelijke grote groei vereist, naast een goede strategie en operationeel systeem, een efficiënt intern controle- en auditsysteem. De interne audit van Telenet is uitbesteed aan de externe auditfirma PwC, die optreedt als interne auditor van de vennootschap.

Als dochteronderneming van het Liberty Global Consortium (LGI), is Telenet sinds 2008 onderworpen aan de Amerikaanse SOX wetgeving. Hoewel de SOX wetgeving in hoofdzaak risico's bewaakt die relevant zijn voor de financiële rapportering, is het toepassingsgebied voor de interne audit ruimer en beoogt het ook andere doelstellingen in het COSO raamwerk, zoals het voldoen aan regels en wetgevingen en het verzekeren van de efficiëntie en effectiviteit van alle activiteiten (Telenet jaarverslag, 2010).

7.1.1.1. Contactpersoon

Jan Borzée is director van 'change en internal control' bij Telenet. Hij is verantwoordelijk voor het beheer van de interne controle- en monitoringactiviteiten en dient te verzekeren dat Telenet voldoet aan de SOX regelgevingen. Dit door onder andere de verantwoordelijkheden hieromtrent vast te leggen en door het opzetten van inkomsten- en fraudecontroles. Bij specifieke projecten voert hij project risk assessments uit. Het 'change' gedeelte verwijst naar het continue aanpassen van de interne controlesystemen om kunnen in te spelen op veranderingen in de markt en op de snelle groei van de onderneming.

7.1.1.2. Bedrijfsomgeving en interne beheersing

Telenet maakt gebruik van een ERP systeem gebaseerd op een data warehouse. Hierin worden alle relevante bedrijfsgegevens verzameld. Het 'business intelligence competence center' van de Telenet Groep voorziet het executive team vervolgens van periodieke en ad hoc operationele en management rapporteringen op basis van deze informatie.

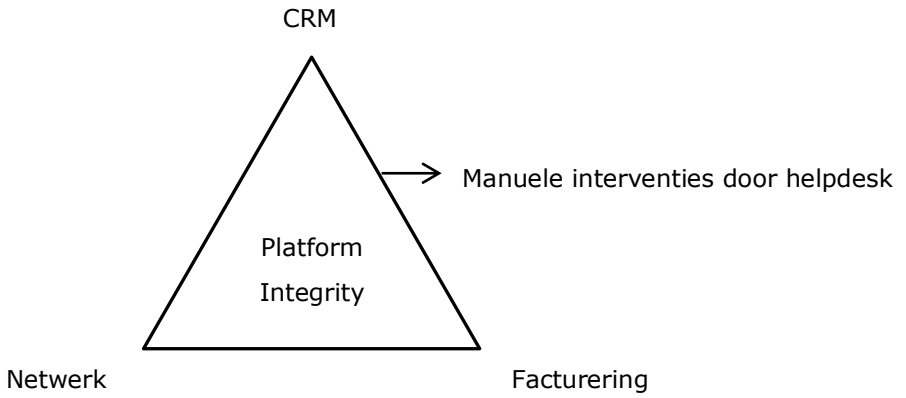
Hiernaast wordt gebruik gemaakt van een centrale 'interne controle' databank. Hierin bevindt zich een beschrijving van alle tekortkomingen van het interne controlesysteem en de actieplannen die zijn opgesteld om een tijdige oplossing te verzekeren.

Dit systeem werd ingevoerd nadat werd vastgesteld dat aan auditrapporten, die werden afgeleverd in papieren of digitale vorm, in vele gevallen geen gevolg werd gegeven. Tijdens de volgende audit kwamen opnieuw dezelfde fouten naar voren. Om dit te voorkomen werd de interne controle databank ingevoerd. Alle interne problemen, die worden vastgesteld binnen de audit of erbuiten, worden hierin opgenomen tezamen met een actieplan om deze problemen te verhelpen. Op deze manier wordt verzekerd dat interne problemen zo snel mogelijk worden opgelost. Hierover wordt bovendien maandelijks en op kwartaalbasis gerapporteerd aan het management. In de kwartaalrapporten worden telkens twee key performance indicators besproken, zijnde de tijdigheid en volledigheid van de oplossing. Tijdigheid beoordeelt of het probleem tijdig werd verholpen en volledigheid beoordeelt of het probleem volledig werd verholpen.

Binnen Telenet wordt gebruik gemaakt van de governance risk and compliance software tool 'OpenPages':

"OpenPages provides software that helps companies more easily identify and manage risk and compliance activities across the enterprise, enabling them to increase insight and focus on business performance while avoiding unexpected outcomes." (Website OpenPages)

In deze tool is het interne controle raamwerk opgenomen dat werd opgesteld door LGI, aangepast naar de specifieke eigenschappen van Telenet. Openpages wordt voornamelijk gebruikt als communicatiemiddel naar de moedermaatschappij toe. De eigenlijke controles worden uitgevoerd in een zelf ontwikkeld intern controlesysteem opgenomen in de ERP- en datawarehouse omgeving. Een belangrijk element hierin is het 'platform integrity' systeem. Dit systeem is gebaseerd op de relatie tussen drie elementen, zijnde Customer Relationship Management (CRM), facturering en netwerk.



Elke dag wordt nagegaan of alle drie de elementen zijn gesynchroniseerd. Bijvoorbeeld of niemand is aangesloten op het netwerk, zonder dat hiervoor een factuur wordt aangemaakt of opdat er niemand wordt gefactureerd voor niet verkregen diensten. Ook is er een mogelijkheid om aankopen te traceren van de aankoop tot de facturering (Usage to Bill). Indien een klant een fout opmerkt op zijn factuur en dit doorgeeft aan de helpdesk, kan dit eenvoudig worden geverifieerd en indien nodig worden gecorrigeerd. Elke interventie met betrekking tot een factuur zal worden verzameld in een aparte database en nogmaals worden gecontroleerd door een verantwoordelijke om eventuele fouten of misbruik door helpdeskpersoneel uit te sluiten.

Ook de correcte werking van het verwerkingssysteem wordt gecontroleerd doordat er, onder andere, elk uur testgesprekken worden uitgevoerd door een test call generator. Vervolgens wordt nagegaan of elk testgesprek ook correct werd geregistreerd en aangerekend. Op deze manier wordt verzekerd dat voor elk gesprek ook een data entry wordt aangemaakt.

Uit deze uiteenzetting valt duidelijk af te leiden dat Telenet zowel een continuous control als monitoring systeem heeft opgezet. Dit systeem is daarenboven sterk gebaseerd op informatietechnologieën zoals het data warehouse en ERP-systeem.

7.1.1.3. Interne audit

Telenet heeft ervoor gekozen om zijn interne auditafdeling uit te besteden aan PwC. De redenen hiervoor zijn drieledig:

- Gerichte expertise en flexibele kennis: om alle kennis te verzamelen benodigd voor het uitvoeren van variërende projecten, zou een zeer uitgebreide interne auditafdeling moeten worden opgezet. Dit wordt vermeden door beroep te doen op de kennis van PwC.
- Onafhankelijk/ objectieve input: de onafhankelijkheid van PwC verzekert correcte controles.
- Ad hoc resources: indien voor een bepaalde controle meer personeel vereist is, kan PwC hier eenvoudig aan voldoen. Het personeelsbeleid wordt hierdoor vereenvoudigd.

PwC is verantwoordelijk voor het opstellen van een risico gebaseerd auditplan. Risico's worden gekwantificeerd op de kans dat ze zich voordoen en de impact die ze hebben indien ze zich voordoen. Hierop wordt vervolgens het auditplan en bijhorende auditcontroles gebaseerd. Indien uit de risicoanalyse bijvoorbeeld blijkt dat er een verhoogd risico is op misbruik door interne dealers, dan zullen er extra controles worden uitgevoerd op de betreffende transacties en de interne controles hierop.

Het testen van de interne controlesystemen zal gebeuren op één of meerdere van de volgende manieren:

- Inquiry (gesprekken met verantwoordelijke personen)
- Inspection/ observation (nagaan of de controle is uitgevoerd, op welke manier,..)
- Reperformance (controle of deelcontrole opnieuw uitvoeren)

Audit software wordt voornamelijk gebruikt binnen reperformance. Bijvoorbeeld bij het uitvoeren van een parallelle simulatie in ACL. Een specifieke controle, uitgevoerd binnen het integrity platform van Telenet, zal dan opnieuw worden uitgevoerd binnen ACL. De gegevens benodigd hiervoor worden bekomen door fysieke overdracht op een geëncrypteerde schijf. Deze overdrachtsmethode verzekert dat de kans op gegevensverlies en diefstal wordt beperkt.

Elk van deze controles wordt uitgevoerd op kwartaalbasis. Indien er tijdens de audit een probleem wordt gedetecteerd, wordt hiervoor een herstelplan geformuleerd. Dit plan zal vervolgens periodiek tot continu worden opgevolgd. Er is hier dus geen sprake van CA, maar wel van een continue opvolging.

7.1.2. PwC

PwC behoort tot de Big Four auditkantoren en is zodus één van 's werelds grootste dienstverleners op het vlak van audit, fiscaliteit en adviesverlening aan bedrijven. Wereldwijd zijn ze actief in 154 landen met meer dan 161.000 werknemers. In België telt PwC meer dan 1.400 medewerkers in 4 kantoren gelegen te Brussel, Antwerpen, Gent en Luik.

7.1.2.1. Visie op interne audit

In de auditomgeving is de focus aan het verschuiven van in het verleden behaalde resultaten, naar toekomstige groei. Dit betekend echter niet dat het controleproces ook meer continu zal worden uitgevoerd, maar wel dat de auditfocus zal verschuiven naar een meer risico gebaseerde benadering. Interne auditors kunnen op deze manier een strategische meerwaarde leveren aan de onderneming.

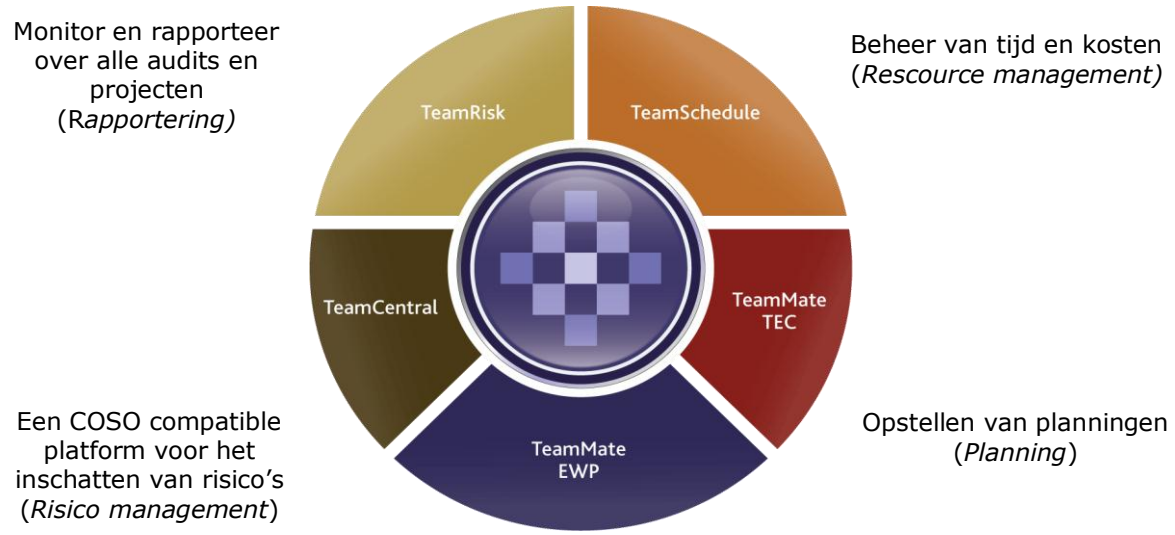
7.1.2.2. Contactpersoon

Jeroen Decroos is manager bij PwC binnen de afdeling Risk and Assurance Services. Hiernaast is hij subject-matter expert voor het gebruik van auditsoftware binnen heel PwC. Op jaarlijkse basis geeft hij infosessies aan de Solvay Brussels School en verzorgt hij de Eurofirm trainingen op dit

gebied. De Eurofirm structuur is een samenwerking van PwC kantoren verspreid over 12 EU landen gericht op het verbeteren van de samenwerking en het elimineren van interne hindernissen. Het verspreiden van kennis omtrent auditsoftware kan hier een grote rol in spelen.

7.1.2.3. Informatietechnologieën

Binnen PwC wordt gebruik gemaakt van audit management software en audit analyse software. De gebruikte audit management software is Teammate. De verschillende componenten van Teammate zijn gericht op het ondersteunen van de verschillende auditfasen en het verzekeren van audit consistentie. Het gaat om een verzameling van audit productiviteit tools en enkele minder geavanceerde CAATTs die zijn geprogrammeerd om samen te werken met elkaar en met populaire software zoals de Microsoft Office Suite.



Figuur 6: Overzicht softwarepakket Teammate

Als auditanalysetool wordt gebruik gemaakt van ACL. De voordelen van ACL ten opzichte van eenvoudigere spreadsheet software zoals Excel zijn, binnen grote ondernemingen, voldoende groot om de meerkost te verantwoorden. De voordelen van ACL ten opzichte van spreadsheet software zijn als volgt:

- Automatisch logboek dat gebruikt kan worden bij het opstellen van een audit trail. Het aanleggen van dit trail kost, zelfs met een logboek functie, zeer veel tijd. Elk uur gespendeerd aan het uitvoeren van controles, vereist twee uren voor het verzamelen van het benodigde bewijs.

- Eenmaal de gegevens zijn geïmporteerd, kunnen deze niet meer worden gewijzigd. Hiermee wordt verzekerd dat de gegevens niet, per ongeluk, worden gewijzigd.
- Door gebruik te maken van scripts kunnen auditcontroles eenvoudig worden geautomatiseerd. Binnen PwC wordt gebruik gemaakt van ACL scripting. Deze scripts worden buiten de kantooruren doorgevoerd.

Tabel 7: Mogelijkheden van de verschillende mogelijke auditsoftware

	Excel	**Access**	**ACL**
Data Analyse	Ja	Ja	Ja
Voorkomen van data manipulatie	Neen	Neen	Ja
Audit Trail	Neen	Neen	Ja
Linken van tabellen	Neen	Ja	Ja
Geautomatiseerde processen	Deels	Deels	Ja

Volgens SAS 65 mogen externe auditors steunen op het werk van interne auditors indien ze overtuigd zijn van de betrouwbaarheid en onafhankelijkheid van de interne auditor. In een Excel omgeving daalt het vertrouwen in de interne auditactiviteiten. De betrouwbaarheid zal dan afhankelijk zijn van de ervaring van, de kennis van en de controles uitgevoerd door de IA. Indien er gebruik wordt gemaakt van ACL, met een goed bijgehouden audit trail, is de betrouwbaarheid bijna 100%.

Naast de voordelen, heeft ACL echter ook enkele nadelen. Het gaat om:

- Duur in aankoop.
- Training van personeel is een vereiste.
- Kennis is moeilijk te onderhouden indien er enkele weken geen gebruik wordt gemaakt van ACL.
- Binnen kleine bedrijven wegen de aankoopkosten niet op tegen de bekomen voordelen.
- Importeren van gegevens gaat trager.

Een meer continue audit of CA wordt beschouwd als een hype die om de twee tal jaren terug onder de aandacht komt. De praktische implementatie ervan is echter zeer moeilijk. Een bedrijf en zijn interne audit afdeling dient zeer sterk ontwikkeld te zijn vooraleer CA succesvol kan worden geïmplementeerd. Een voorbeeld van één van de weinige ondernemingen waar CA wordt toegepast is Fortis. Hier wordt gebruik gemaakt van een hele reeks van continue controles en alarmsystemen, maar zelfs na vijf jaren bevindt dit project zich nog steeds in de implementatiefase.

Het is dan ook tijdens de implementatiefase dat de moeilijkheden omtrent CA naar voren komen. Een gerelateerd praktijkvoorbeeld is een retailer met verschillende sterk verspreide kantoren. Mits een auditor steeds elke locatie diende te bezoeken, werd het idee geopperd om alle gegevens te centraliseren binnen het hoofdkantoor. Op deze manier zou de reistijd en bijgevolg de benodigde audittijd sterk verminderen. De implementatie hiervan bleek echter moeilijker te zijn dan initieel werd aangenomen. Het verzekeren van data consistentie en het opzetten van een data feed tussen de verschillende locaties was immers geen eenvoudige opdracht. Zo is het bijvoorbeeld mogelijk dat indien er een fout wordt gemaakt, deze nog moet worden teruggedraaid terwijl de gegevens al zijn doorgestuurd. Daarenboven kregen de verschillende managers een big brother gevoel, met een lagere motivatie tot gevolg. De voordelen van een dergelijk systeem bleken dan ook niet op te wegen tegen de nadelen. Hoewel het opzet van dit project niet het bereiken van een CA systeem was, kunnen hier wel al enkele implementatieproblemen voor een CA systeem worden uit afgeleid. Het centraliseren van gegevens zou immers slechts een eerste fase zijn in een CA implementatie.

Een bijkomend nadeel van CA is het feit dat indien één controlesysteem of controleregel wijzigt, alle systemen moeten worden aangepast. Bovendien kunnen de controles het bedrijfssysteem vertragen. Een periodiek uitgevoerde, zoals bijvoorbeeld maandelijks, controle op basis van een M&C layer is wel mogelijk, maar vereist ook een continu onderhoud. CA op zich is dan ook te ambitieus. Vele bedrijven hebben daarenboven al een uitgebreid CM systeem opgezet waardoor het nut ervan afneemt. CRA kan daarentegen wel worden bereikt. Bijvoorbeeld op maandelijkse basis nagaan wat er gebeurt met de risk drivers.

7.1.3. BDO

BDO maakt deel uit van het internationaal BDO-netwerk, dat werd opgericht in 1963 en wereldwijd nummer vijf is op de markt van accountancy, audit en adviesverlening. Binnen België is BDO actief sinds 1976 met meer dan 400 partners en personeelsleden verspreid over negen vestigingen bestaande uit auditors, accountants, fiscale en juridische raadgevers en adviseurs openbare sector.

7.1.3.1. Visie op de interne audit

BDO erkent het feit dat organisaties vandaag de dag worden geconfronteerd met nieuwe vereisten op het vlak van deugdelijk bestuur. Een reactieve aanpak van interne audit is niet langer aanvaardbaar. Verrassingen moeten vermeden worden als het aankomt op het beheersen van risico's.

Om dit te bereiken biedt BDO een waaier van diensten aan die bedrijven kunnen helpen om een compliance-georiënteerde interne audit functie te transformeren naar een proactieve en risico-georiënteerde functie. Deze diensten omvatten:

- Opzetten van een effectieve Interne Audit functie
- Risicobeoordeling en Interne Audit planning
- Specifieke interne audit opdrachten, zoals IT Audit voor Interne Audit
- Interne Audit co-sourcing en outsourcing
- Corporate Governance

Het is duidelijk dat hun visie en bijhorende diensten sterk aansturen op een meer continu gerichte audit, waarin CAATTs zoals CA modules een belangrijke rol in kunnen spelen (Website BDO).

7.1.3.2. Contactpersoon

Koen Claessens is senior manager bij BDO binnen de afdeling Risk and Assurance Services (RAS). In deze functie en binnen zijn vorige functie als IT audit manager bij Deloitte, heeft hij reeds jaren ervaring met het opzetten van interne controle- en auditsystemen.

7.1.3.3. Informatietechnologieën

Desondanks de visie van BDO op de interne audit als proactieve en risico-georiënteerde functie, wordt er slechts beperkt gebruik gemaakt van CAATTs. Indien het Risk and Assurance team van BDO een interne audit afdeling ondersteunt of opzet, worden voornamelijk eenvoudige audit productiviteit tools zoals Word en Excel toegepast.

Enkel binnen sommige grote ondernemingen worden CAATTs gebruikt ter ondersteuning van zowel de interne controle- als auditsystemen. De belangrijkste implementatieredenen van deze tools zijn dan de verhoogde audit efficiëntie en de lagere arbeidsintensiviteit. De vraag naar een verhoogde audit efficiëntie wordt gedreven door het extra werk dat voortkomt uit de verschillende governance regelgevingen. De strenge voorschriften en verplichtingen opgelegd door de SOX wetgeving (2002) brachten een grote administratieve kost met zich mee. CAATTs werden, onder andere, beschouwd als een manier om deze kosten te verlagen.

Er dient rekening te worden gehouden met het feit dat deze efficiëntieverhoging zich enkel zal voordoen indien de informatisering goed wordt beheerst. Voorbeelden van een slechte beheersing zijn:

- Systemen die niet zijn aangepast aan de bedrijfsprocessen.
- Processen zijn te complex of inefficiënt.
- Genereren van slechte financiële- en/of beleidsinformatie.

Het feit dat CAATTs binnen kleinere ondernemingen in mindere mate worden toegepast, is toe te schrijven aan onder andere:

- Het feit dat er binnen kleine ondernemingen niet steeds gebruik wordt gemaakt van sterk geïnformatiseerde systemen. Een geautomatiseerd auditsysteem is in vele gevallen dan ook niet nodig.
- De hoge kosten van audit tools in vergelijking met bijvoorbeeld spreadsheet software. De functies die kunnen worden uitgevoerd met spreadsheets zijn vaak al voldoende voor het uitvoeren van een audit.
- GAS genereert een zekere overheadkost qua opzet en administratie.
- Wanneer externe consultants een interne auditafdeling opzetten, willen ze de kost van hun ondersteuning (en dus de kost voor de klant) niet nog eens verzwaren door de implementatie van audit tools. Zeker indien deze meerkost niet opweegt tegen de verkregen voordelen.

Informatisering introduceert bovendien ook een heel aantal nieuwe risico's zoals de confidentialiteit van gegevens, toegang tot gegevens, misbruik en privacy problemen, beschikbaarheid van gegevens, systeemcrashes, e.d.. Enkel indien ook deze risico's worden beheerst, zal de audit efficiëntie toenemen.

Voor het ondersteunen van de audit zelf, is er een waaier aan keuzemogelijkheden op het gebied van interne audit management software. Een voorbeeld hiervan is 'Teammate'. Zoals besproken onder de gebruikte tools binnen PwC.

In bedrijven waar er enkel gebruik wordt gemaakt van dit soort audit management software en Excel als analysetool, is het invoeren van een CA systeem niet mogelijk. Bijvoorbeeld door het gebrek aan geautomatiseerde processen in Excel.

7.2. Externe audit

7.2.1. PwC

7.2.1.1. Informatietechnologieën

Als audit management software maakt PwC gebruik van het zelf ontwikkelde 'My Client'. Dit is enigszins vergelijkbaar met Teammate, maar dan verder gevorderd. Het bevat PwC audit programma's, werkpapieren en staat real-time uitwisseling van informatie tussen de verschillende leden van het audit team toe. Als audit analysetool wordt, net zoals binnen de interne audit, gebruik gemaakt van ACL.

Binnen PwC wordt het gebruik van CAATTs aangemoedigd door middel van trainingen en presentaties. De klant verwacht immers dat de audit zo efficiënt mogelijk wordt uitgevoerd. Het gebruiken van CAATTs is hiervoor een vereiste.

ACL kan als volgt worden gebruikt binnen de verschillende audits:

- Binnen process audits: traceren van verkopen. Volgen van een verkoop tot de facturering en betaling.
- Binnen detailcontroles: uitvoeren van een specifieke controle. Bijvoorbeeld de goedkeuring van aankopen boven een bepaald bedrag nagaan.
- Binnen revenue audits: hier bevindt zich de echte kracht van ACL en gerelateerde software. Controles kunnen zeer eenvoudig opnieuw worden uitgevoerd in de vorm van een parallelle simulatie.

Een groot deel van de controles werd geautomatiseerd door middel van scripts. Deze scripts worden uitgevoerd buiten de kantooruren. Op deze manier verliest de auditor geen tijd ten gevolge van een onbruikbaar systeem tijdens het uitvoeren van de berekeningen. In vele gevallen gaat het immers om een zeer grote hoeveelheid gegevens.

De benodigde gegevens worden steeds verkregen door middel van een geëncrypteerde schijf, zoals ook toegepast binnen telenet, of via een secure FTP connection die wordt opgezet door PwC. Deze verbinding heeft een dubbele beveiliging met een wachtwoord en een code die wordt verzonden via sms naar de auditor in kwestie. Tot voor kort werd ook gebruik gemaakt van overdracht via CD. Dit wordt echter niet meer gedaan omwille van een gevaar op verlies en gebrek aan eenvoudige encryptiemethoden.

Hoewel sommige audits meerdere malen per jaar worden opgevolgd, wordt er geen gebruik gemaakt va CA technieken. Het gebruik hiervan wordt echter niet zozeer afgeremd door onafhankelijkheidsproblemen, maar wel door het feit dat de investering in CA dient te gebeuren door de onderneming zelf. De auditor, afhankelijk van een jaarlijkse fee, zal hier immers nooit toe bereid zijn. De efficiëntiewinst zal te klein zijn om bedrijven te overtuigen om deze initiële investering te maken. Het merendeel van de voordelen zal immers voor de externe auditor zijn. Daarnaast zijn er een hele reeks van implementatieproblemen. Het gaat bijvoorbeeld om het verzekeren van data consistentie en het opzetten van gegevensdeling.

7.2.2. Deloitte

Deloitte België stelt meer dan 2.400 personen tewerk verspreid over 12 kantoren. Met zowel financiële, juridische, belastingen, management als informatietechnologie expertise, bedienen ze private en publieke ondernemingen.

7.2.2.1. Contactpersoon

Peter Leyman is senior manager bij Deloitte binnen Forensic & Dispute services. Hierbinnen wordt er intensief gebruik gemaakt van auditsoftware ter ondersteuning van de audit. Hiervoor werkte hij als consultant bij KPMG.

7.2.2.2. Informatietechnologieën

Binnen Deloitte wordt gebruik gemaakt van de dataextractie- en analysetool ACL. Dit heeft als voordeel dat de audit efficiënter verloopt en de gehele populatie kan worden onderzocht in de plaats van slecht een sample. Door gebruik te maken van ACL scripts kunnen deze controles bovendien worden geautomatiseerd. Een ACL script is een reeks van ACL commando's die worden opgeslagen. Deze kunnen vervolgens herhaaldelijk en automatisch worden uitgevoerd. De benodigde auditgegevens worden verkregen door gebruik te maken van fysieke overdracht op een externe schijf.

Daarnaast wordt gebruik gemaakt van het zelf ontwikkelde 'AS2' als audit management software. Dit platform ondersteunt de audit in de planningsfase, tijdens het maken van een risico assessment, bij het bijhouden van elektronische documenten en het aanleggen van een audit trail, e.d..

Er wordt steeds verwacht dat er gebruik wordt gemaakt van AS2. Ook het gebruik van ACL wordt sterk aangemoedigd door middel van presentaties en opleidingen. Er is echter geen specifiek infopunt aangeduid om eventuele vragen omtrent het gebruik te beantwoorden.

Bij grote klanten kan het voorkomen dat er wordt geopteerd voor een meer periodieke audit. Bijvoorbeeld een audit die wordt uitgevoerd om de drie maanden. Een echte continue audit wordt echter nooit bereikt. CA is voornamelijk een intern gebeuren. Een externe auditafdeling kan immers niet betrokken zijn bij het opzetten of de werking van het interne bedrijfssysteem. Een audit zal zich steeds dan ook steeds meer gaan baseren op technologie zoals ACL en AS2, maar een echt systeem van CA zal niet worden toegepast.

Externe auditors mogen zich daarentegen wel baseren op het interne controlesysteem. Hiervoor dient er allereerst wel een assessment van het gebruikte IT systeem te gebeuren. Indien hieruit een hoge maturiteit van het systeem blijkt, dan kan de focus van de externe audit verschuiven naar het interne controlesysteem op zich. Bij een lagere maturiteit dient er meer aandacht te worden besteed aan de correctheid van de gegevens.

7.3. Hypothesen

Voor het uitvoeren van het empirisch onderzoek werden drie hypothesen vooropgesteld. Na de bevraging van bevoorrechte getuigen kunnen volgende conclusies worden getrokken:

H_1: Het gebruik van door CAATTs ondersteunde interne auditsystemen is beperkt tot grote ondernemingen. Binnen kleine ondernemingen wegen de bekomen voordelen niet op tegen de implementatie- en onderhoudskosten.

Zowel Koen Claessens van BDO als Jeroen Decroos van PwC geeft aan dat de kost van een geavanceerd, op CAATTs gebaseerd auditsysteem aanzienlijk is. Het gaat dan voornamelijk over de aanschafkosten van de software en de opleidingskosten van het personeel. In kleine ondernemingen, waar slechts een beperkt aantal gegevens dient te worden gecontroleerd, wordt er daarom vaak geopteerd om te werken met eenvoudige spreadsheetsoftware zoals Excel. In vele gevallen zal dit reeds voldoende zijn om een goede en betrouwbare audit te bekomen.

Binnen grotere ondernemingen wordt er daarentegen wel gebruik gemaakt van meer geavanceerde GAS. De verschillende voordelen verbonden aan het gebruik van deze technieken zijn in deze omgeving voldoende groot om de meerkost te verantwoorden. Het zal echter nog enige tijd duren

vooraleer grote bedrijven ook ten volle gebruik gaan maken van GAS. In vele gevallen bevinden deze projecten zich nog in de implementatiefase.

H_2: Zowel binnen interne als externe auditafdelingen wordt geen gebruik gemaakt van alle mogelijke toepassingen van CAATTs.

Uit de verschillende interviews kwam duidelijk naar voren dat binnen de interne audit nog niet ten volle gebruik wordt gemaakt van auditsoftware. Kleine bedrijven houden vast aan oudere legacy systemen en grote bedrijven bevinden zich momenteel in de implementatiefase van meer geavanceerde software.

Binnen de externe audit wordt er daarentegen wel reeds intensief gebruik gemaakt van audit management- en analysesoftware. Controles worden daarenboven steeds meer geautomatiseerd door gebruik te maken van scripts. Het gebruik van deze technieken wordt sterk aangemoedigd door middel van presentaties en het voorzien in bijkomende opleidingen. CA modules lijken in geen van beide gebieden te worden toegepast.

H_3: CA modules worden niet toegepast binnen de externe audit ten gevolge van onafhankelijkheidsproblemen.

Zoals verwacht kwam uit de interviews naar voren dat CA modules momenteel niet worden gebruikt binnen de externe audit. De mogelijke onafhankelijkheidsproblemen lijken hier echter niet de belangrijkste oorzaak van te zijn. Belangrijker zijn de hoge implementatiekosten en implementatieproblemen zoals bijvoorbeeld data inconsistentie.

Een externe auditor zal bovendien nooit bereid zijn om te investeren in een tijdelijke audit cliënt. Dit heeft tot gevolg dat de kost van het opzetten van het CA systeem volledig door de onderneming moet worden gedragen. Omwille van de verschillende implementatieproblemen, kunnen deze kosten hoog oplopen en kan de implementatie zeer lang duren.

Hoofdstuk 8: Toekomstverwachtingen

In een jaarlijkse bevraging uitgevoerd door Protiviti (2011), de "Internal Audit Capabilities and Needs Survey", wordt onderzocht op welke gebieden binnen de interne audit er nog ruimte is voor en vraag is naar verbeteringen.

Reeds drie jaren na mekaar worden CAATTs en Continuous Auditing technieken aangeduid als de voornaamste gebieden waarbinnen nog nood is aan verbetering. Hieruit valt duidelijk af te leiden dat bedrijven zich bewust worden van de voordelen die voortkomen uit het integreren van CAATTs, CA- en CM technieken in het risicomanagement en in de interne controle activiteiten.

Tabel 8: Gebieden met nood aan verbetering (Protiviti, 2011)

Rank	2011	2010	2009
1	Continuous Auditing	CAATs	Continuous Auditing
			CAATs
2	CAATs	Data Analysis Tools – Statistical Analysis	Data Analysis Tools – Statistical Analysis
		Data Analysis Tools – Data Manipulation	Data Analysis Tools – Data Manipulation
3	Data Analysis Tools – Statistical Analysis	Continuous Auditing	Fraud Monitoring
4	Data Analysis Tools – Data Manipulation	Auditing IT – Program Development	Fraud – Fraud Detection/ Investigation
			Auditing IT – Program Development
5	Auditing IT – Program Development	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)	Fraud – Auditing
			Fraud – Fraud Risk Management/Prevention
			Auditing IT – Computer Operations
			Auditing IT – Security

Een onderzoek uitgevoerd door PwC in 2006 toonde aan dat 50% van de Amerikaanse bedrijven reeds gebruik maakt van CA-technieken. 31% van resterende bedrijven hadden daarenboven plannen om een CA systeem te implementeren. Ook uit een onderzoek van het IIA blijkt dat de interesse in CA de laatste jaren zeer sterk is toegenomen. 36% Van de respondenten had hier reeds een CA systeem en 39% had plannen om dit in de toekomst te doen (Alles et al., 2008). Van al deze projecten zal er echter slechts een klein deel het volle potentieel van CA weten te benutten.

Ongeveer 20 tot 70 procent van de grootschalige IT investeringen slaagt er niet in om een meeropbrengst voor de onderneming te genereren (Masli et al., 2009).

Uit het empirisch onderzoek komt echter een heel ander beeld naar voren. Koen Claessens, BDO, en Jeroen Decroos, PwC, gevan aan dat CA systemen op dit moment nog niet gebruikt worden binnen Belgische ondernemingen. Ook in de toekomst lijkt hier geen verandering in te komen. De voordelen van een dergelijk systeem wegen immers niet op tegen de implementatiekosten- en problemen. Het is pas wanneer de interne auditafdeling van een bedrijf voldoende ontwikkeld is, dat CA een optie wordt.

Deze ontwikkeling dient en zal vooreerst plaats vinden op het gebied van CAATTs. Binnen kleine bedrijven wordt momenteel nog gebruik gemaakt van Excel als audit analysesoftware. De bekomen voordelen uit meer gespecialiseerde auditsoftware zijn in deze omgeving niet voldoende om de hogere aanschaf- en opleidingskosten te verantwoorden. Aangezien deze kosten niet snel zullen dalen, zal ook in de toekomst geen gebruik worden gemaakt van dit soort software. Binnen grote ondernemingen is er wel reeds een overschakeling merkbaar naar GAS. In vele gevallen wordt er echter nog onvoldoende gebruik van gemaakt ten gevolge van onvoldoende opgeleid personeel of doordat de software nog niet echts is afgesteld op het bedrijfsgebeuren. Het is echter aannemelijk dat dit in de toekomst nog zal veranderen en GAS steeds sterker geïntegreerd zal worden in de bedrijfsprocessen.

In een later stadium kan er dan worden geopteerd voor CA technieken. De vraag blijft in welke mate CA op dat moment dan nog een meerwaarde kan bieden. Vele bedrijven maken immers reeds gebruik van uitgebreide CM technieken. Het opzetten van een systeem van CCM zou in deze situatie een vorm van dubbel werk zijn. Het is dan ook aannemelijk dat CA in de toekomst voornamelijk zal bestaan uit CRA, zoals ook werd aangegeven door Jeroen Decroos.

Binnen het gebied van de externe audit wordt er reeds sterk gebruik gemaakt van CAATTs. Ook in de toekomst lijkt een stijgende trend zich voort te zetten. Doordat automatische scripts vaak kunnen worden hergebruikt, zullen controles daarenboven steeds vaker worden geautomatiseerd. Het tegenovergestelde is waar voor CA systemen. Net zoals binnen de interne audit, wordt er ook binnen de externe audit geen gebruik gemaakt. De achterliggende redenen hiervoor werden besproken in hoofdstuk zes.

Om het gebruik van CA binnen het gebied van de externe audit te vergroten, dient er vooreerst een duidelijk kader te worden opgesteld waarin de onafhankelijkheidsvoorwaarden bij het opzetten en onderhouden van een CA systeem worden in vastgesteld. Op die manier zou het ook voor externe auditors mogelijk worden om zich te baseren op een CA systeem. Momenteel zijn er echter nog geen plannen voor het invoeren van een dergelijk kader. Ook dient er opnieuw rekening te

worden gehouden met het feit dat het invoeren van een CA systeem in een onderneming waarin de interne controle- of auditafdeling dit reeds heeft gedaan, een vorm van dubbel werk tot gevolg zou hebben. In alle waarschijnlijkheid zal de externe audit in de toekomst dan ook worden beperkt tot het controleren van het interne CA/ CM systeem.

Om de controle van het CA systeem te vereenvoudigen, werd het concept van black box logging[23] ingevoerd. De kern van een black box log is het creëren van een permanente aantekening van de belangrijkste auditprocedures, eventuele wijzigingen aan het audit systeem en andere economisch belangrijke gebeurtenissen. Het logboek kan niet manueel worden aangepast en zal enkel worden geopend bij het uitvoeren van een externe audit of in geval van faillissement. Een black box logboek zorgt er op die manier voor dat de auditor en de cliënt geen aanpassingen aan het CA systeem kunnen doorvoeren, zonder dat hier enig bewijs van achterblijft (Vasarhelyi en Chan, 2011).

[23] Zoals ook aangegeven door Vasarhelyi et al. (2004) – Schematische weergave in bijlage 7.

Hoofdstuk 9: Conclusie

Het grote belang van de audit sinds de invoering van de SOX wetgeving (2002) en de sterke automatisatie van bedrijfsprocessen, hebben geleid tot een groot aantal auditstandaarden waarin technologie wordt aangeraden als manier om de audit efficiëntie te verhogen. SAS nr. 99, SAS nr. 104-111, IIA standaard 1220.A2 en 1210 zijn hier slechts enkele voorbeelden van.

Audit ondersteunende informatiesystemen kunnen worden onderverdeeld in twee categorieën. Enerzijds zijn er de audit productiviteittools. Dit soort tools verhoogt de audit productiviteit door de automatisatie van standaard auditfuncties en door de integratie en het beschikbaar maken van informatie over het hele auditproces. In vele gevallen gaat het om software die in eerste instantie niet werd ontwikkeld voor gebruik binnen de audit. Anderzijds zijn er de meer data gerichte computer assissted audit tools and techniques (CAATTs). De belangrijkste CAATTs vallen onder de categorie generalized audit software. Het gaat om software zoals ACL, IDEA, e.d. die auditors de mogelijkheid geeft om geautomatiseerde analyses uit te voeren op 100% van de populatie. In combinatie met elektronische werkdocumenten en audit productiviteittools verzekert men bovendien audit consistentie over auditteams- en cliënten heen. Andere systemen zoals expertsystemen verzekeren dan weer dat ervaring en kennis op een eenvoudige wijze verspreid kan worden.

Uit een enquête afgenomen door het IIA (2006) blijkt dat er binnen interne auditafdelingen voornamelijk gebruik wordt gemaakt van Excel voor het uitvoeren van een audit. Op de tweede plaats staat de dataextractie- en analysetool ACL. Dit wordt ook bevestigd in het empirisch onderzoek ten gevolge van het verschil tussen grote en kleine ondernemingen. Koen Claessens van BDO geeft aan dat kleine- en middelgrote ondernemingen gebruik maken van Excel. De meerkost van ACL weegt in deze omgeving immers niet op tegen de bekomen voordelen. In grote ondernemingen wordt in vele gevallen geopteerd voor ACL. Slechts een beperkt aantal ondernemingen maakt gebruik van gelijksoortige auditsoftware zoals bijvoorbeeld IDEA. Dit is deels het gevolg van het feit dat de Big Four auditkantoren, uitgezonderd KPMG, gebruik maken van ACL. Indien zij een onderneming bijstaan tijdens de implementatie van een interne auditafdeling, zullen zij steeds ACL aanbevelen. Naast deze audit analysetool wordt er vaak gebruik gemaakt van audit management software zoals Teammate. Dit soort software is specifiek gericht op de interne audit en ondersteund de audit in zijn verschillende fasen (Jeroen Decroos, PwC).

Uit recent onderzoek van Janvrin et al. (2008) blijkt dat er binnen de externe audit nog niet ten volle gebruik wordt gemaakt van alle mogelijke toepassingen van CAATTs. Enkel binnen Big Four auditkantoren lijken CAATTs zich sterk te hebben ontwikkeld. Dit laatste werd bevestigd in het empirisch onderzoek. Peter Leyman van Deloitte en Jeroen Decroos van PwC gaven beiden aan dat

IS een essentieel deel vormen van het auditproces. Binnen dit gebied wordt er zowel gebruik gemaakt van GAS als van audit management software. Bij het merendeel van de auditkantoren gaat het om ACL in combinatie met een zelf ontwikkeld managementprogramma. Enkel KPMG maakt gebruik van IDEA. Het gebruik van deze tools wordt aangemoedigd door het geven van bijscholingen en presentaties.

Door gebruik te maken van meer continu of periodiek gerichte CAATTs, waarvan CA modules de belangrijkste zijn, kan een meer continue auditmethodologie worden bereikt. De CA module wordt dan verwerkt in het bedrijfssysteem zelf, in welk geval er sprake is van een embedded audit module, of er wordt een link gelegd tussen het bedrijfssysteem en een onafhankelijk auditsysteem, in dat geval is er sprake van een monitoring & control layer.

In de praktijk wordt er echter geen gebruik gemaakt van de EAM architectuur. Door het geïntegreerde ontwerp kan er immers een invloed worden uitgeoefend op de originele bedrijfsgegevens. Bovendien dienen er binnen grote ondernemingen meerdere modules te worden geprogrammeerd, oftewel één per ERP systeem. Ook binnen de externe audit stelt een EAM enkele problemen. Het gaat bijvoorbeeld om onafhankelijkheidsproblemen, de mogelijkheid tot juridische vervolging en de moeilijk te bereiken vereiste van onbeperkte toegang tot alle gegevens. Omwille van deze redenen zal een M&C layer steeds de voorkeur krijgen.

De voordelen van meer continue audit zijn aanzienlijk. Een verminderde audit wachttijd, een grotere auditdiepte, een grotere auditfocus e.d.. Om deze voordelen te kunnen bereiken dient er echter rekening te worden gehouden met enkele belangrijke voorwaarden voor wat betreft de werking van het CA systeem. Zo dient er bijvoorbeeld bijzondere aandacht te worden besteed aan de invloed die het systeem uitoefent op het bedrijfsprocessen. Indien de audit deze bijvoorbeeld vertraagt, dan bestaat de kans dat gebruikers controles gaan trachten te omzeilen of uit te schakelen. Enkel indien aan de onderliggende voorwaarden is voldaan, zal CA de audit efficiëntie verhogen. In het andere geval kan een CA systeem zelfs een negatieve invloed uitoefenen op de audit- en bedrijfsprestaties.

Binnen de interne audit kan CA worden opgezet om de interne controle van een bedrijf te testen, of om de risico’s waarmee het bedrijf in aanraking komt te identificeren en analyseren. Eerstgenoemde vormt het complement van continuous monitoringfunctie, laatstgenoemde op het risicomanagementsysteem. Binnen de externe audit kan CA op eenzelfde wijze worden aangewend. De auditfocus zal hier echter meer liggen op het verifiëren van de financiële staten en de correcte werking van het interne controlesysteem.

Het extra werk dat voortkwam uit de invoering van de SOX wetgeving en de invoering van strengere onafhankelijkheidsvoorschriften hebben er echter toe geleid dat CA niet of slechts in

beperkte mate wordt toegepast binnen het externe auditgebied. Ook in het empirisch onderzoek kon deze conclusie worden getrokken. Naast bovenstaande oorzaken, die worden aangegeven in de literatuur, worden er hier nog enkele bijkomende oorzaken aangehaald. Het gaat om problemen die ontstaan tijdens de implementatiefase zoals het opzetten van data sharing en de vraag wie de implementatie van een CA systeem zal bekostigen. Een externe auditor zal bijvoorbeeld nooit bereid zijn om te investeren in een auditklant.

In tegenstelling tot de informatie verkregen uit de literatuur, lijkt CA in de praktijk ook niet te worden toegepast binnen de interne audit. Jeroen Decroos van PwC geeft aan dat het concept van CA te ambitieus is. In vele bedrijven wordt er nog maar net gebruik gemaakt van ACL of gerelateerde audit software. De invoering van een CA systeem in een dergelijke situatie is niet realistisch. Bovendien is de toegevoegde waarde ervan in vraag te stellen. Binnen vele ondernemingen wordt immers al gebruik gemaakt van een uitgebreid CM systeem, dat is geïntegreerd in het ERP- en/ of het interne controlesysteem. In deze situatie richt een interne audit zich dan ook best op het inschatten van risico's en het opvolgen van gekende problemen in het interne systeem. CA binnen de interne audit zal in de toekomst dan ook voornamelijk bestaan uit CRA.

Het feit dat CAATTs nog niet ten volle worden benut en CA technieken nog niet worden gebruikt binnen zowel de interne als de externe audit, geven aan dat er nog veel ruimte is voor verbeteringen in de toekomst. Dit blijkt ook uit een bevraging van Proviti (2009), waar ondernemingen CAATTs en CA aanduiden als gebieden waar nog ruimte is voor verbetering. Het is echter zeer moeilijk om de exacte evolutie van deze systemen voorspellen. Deze zal immers deels afhankelijk zijn van allerlei externe factoren zoals regelgevingen, auditnormen en de evolutie van de gebruikte informatietechnologieën.

Volgens de bevoorrechte getuigen zal binnen de interne audit in eerste instantie een verdere implementatie van CAATTs merkbaar zijn. Steeds meer bedrijven zullen overschakelen op meer geavanceerde tools. Het gaat echter nog niet om CA technieken. CA kan pas worden bereikt wanneer een interne auditafdeling voldoende ontwikkeld is.

Door de grote hoeveelheid problemen voor wat betreft het gebruik van CA binnen de externe audit, is het niet aannemelijk dat dit soort technieken hier zullen worden toegepast. De verschillende auditstandaarden zijn immers te beperkt om een dergelijke inmenging in het cliëntsysteem toe te staan. Ook de technische implementatieproblemen zullen niet snel een oplossing krijgen. In de toekomst zal de externe auditor zich dan ook voornamelijk bezighouden met het controleren van het interne CA of CM systeem. Ook hier zal er echter een steeds grotere focus worden gelegd op GAS en audit management software.

9.1. Mogelijkheden tot verder onderzoek

Tijdens het opstellen van deze eindverhandeling kwamen verschillende onderwerpen naar voren waarover momenteel nog onvoldoende onderzoek bestaat. Volgende onderzoeken zouden kunnen bijdragen aan het verkrijgen van een duidelijker overzicht omtrent het gebruik en de toepassingen van CAATTs:

- Hoewel er reeds heel wat onderzoeken zijn verschenen omtrent het gebruik van CAATTs, bestaat er momenteel geen onderzoek waarin de Belgische situatie word toegelicht. In deze eindverhandeling werd daarom verder gegaan op de praktijkkennis van enkele bevoorrechte getuigen. Een breder empirisch onderzoek, bijvoorbeeld in de vorm van een enquête, kan een waardevolle bijdrage leveren.
- Het grotere aantal onderzoeken naar de Amerikaanse situatie, is deels toe te schrijven aan de strengere SOX regelgeving in vergelijking met andere regelgevingen. Het is echter de vraag in welke mate deze strengere regelgeving ook een invloed uitoefent op het gebruik van CAATTs.
- Uit zowel het literatuur- als het empirisch onderzoek bleek dat de meer geavanceerde CAATTs niet worden gebruikt binnen kleine bedrijven. De voornaamste reden hierachter zou de grote aanschafkost zijn. Het is aan te bevelen om deze oorzaken verder te onderzoeken en na te gaan welke wijzigingen kunnen worden doorgevoerd om het gebruik aan te moedigen. Bijvoorbeeld de ontwikkeling van iets minder geavanceerde software.
- In het empirisch onderzoek werd er geen aandacht besteed aan het gebruik van CAATTs door kleinere, onafhankelijke auditors. Ook in de literatuur wordt vaak geopteerd voor de Big Fout auditkantoren. Desondanks vormen kleinere auditors een interessante onderzoekseenheid.
- Uit het empirisch onderzoek kwamen enkele implementatieproblemen naar voren voor wat betreft CA. Verder onderzoek omtrent de invoering van een CA systeem, met specifieke aandacht voor data sharing en de implementatie van technologieën, lijkt een vereiste om de implementatiekosten te kunnen verminderen en het gebruik van CA technieken te bevorderen. De huidige kaders besteden hier onvoldoende aandacht aan.
- Naast implementatieproblemen stelt CA binnen de externe audit nog enkele bijkomende problemen. Om het gebruik van CA binnen dit gebied mogelijk te maken, dienen er duidelijkere normen te worden opgesteld met betrekking tot deze functies. Bijvoorbeeld het opstellen van onafhankelijkheidsvoorschriften.

Lijst van geraadpleegde werken

Agrawal, R., Gunopulos, D., Leymann, F. (1998) "*Mining Process Models from Workow Logs.*", *Advances in Database Technology – EDBT'98*, vol. 1377, p467-483.

Alles, M. G., Kogan, A., Vasarhelyi, M.A. (2008) "*Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations.*", *Journal of information systems*, vol. 22, nr. 2, p195-214.

Alles, M. G., Brennan, G., Kogan, A., Vasarhelyi, M.A. (2006) *"Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens.", International Journal of* Accounting Information Systems, vol. 7, nr. 2, p137-161.

Alles, M. G., Kogan, A., Vasarhelyi, M.A. (2002) *"Feasibility and Economics of Continuous Assurance.*", Auditing:A Journal of Practice& Theory, vol.21, nr. 1.

AuditNet (2003) "*The AuditNet Monograph Series – Principles of Computer Assisted Audit Techniques*".

Bae, B. en Ashcroft, P. (2004) "*Implentation of ERP Systems: Accounting and Auditing Implications*", Information Systems Control Journal.

Commissie Corporate Governance (2009) *"Belgische Corporate Governance Code*".

Cushing, B and J.K. Loebbecke (1983) *"Analytical Approaches to Audit Risk: A Survey and Analysis"*, Auditing: A Journal of Practice & Theory 3, 23-48.

Brown, C. E. en D. S. Murphy (1990) "*The Use of Auditing Expert Systems in Public Accounting.*", Journal of Information Systems, vol. 4, nr. 3, p63-72.

Coderre, D.G. (1993) "*Computer assisted audit tools and techniques*", Internal Audit.

Coderre, D.G. (2009) "*Internal audit : efficiency through automation*", Internal Audit.

COSO (2004) "*Risico management van de onderneming: Geïntegreerd raamwerk*".

COSO (2009a) "*Guidance on Monitoring Internal Control Systems*".

Debreceny, R. S., Gray, G.L., Jun-Jin, J., Lee, K., Yau, W-F (2005) "*Embedded Audit Modules in Enterprise Resource Planning Systems:Implementation and Functionality*.", Journal of information systems, vol. 19, nr. 2, p7-27.

Dowling, C. en S. Leech (2007) "*Audit support systems and decision aids: Current practice and opportunities for future research*.", International Journal of Accounting Information Systems, vol. 8, nr. 2, p92-116.

Dumortier J. (2005) "*Over instant messaging en Sarbanes-Oxley*", Trends Business ICT.

Flowerday, S., Blundell, A.W., Von Solms, R. (2006), "*Continuous auditing technologies and models: a discussion.*", Computers & Security, vol. 25, p325-331.

Gallegos, F., Gonzales, C. , Senft, S., Manson, D.P. (2004) "*Information Technology Control and Audit*", Auerbach Publications, Second Edition.

Groomer, S.M. and U.S. Murthy. (1989) "*Continuous Auditing of Database Applications: An Embedded Audit Module Approach*", Journal of Information Systems, p53-69.

Handscombe, K., CISA, ACA (2007) "*Continuous auditing from a practical perspective*", Information Systems Control Journal, vol. 2.

Hermanson, D. R., Hill, M. C., Ivancevich, D.M. (2000) "*Information Technology-Related Activities of Internal Auditors*.", Journal of information systems, vol. 14, p39-53.

ICAI (2004), "*Guidance note on computer assisted audit techniques*", The chartered accountant.

IIA (2005) "*Global Technology Audit Guide (GTAG) 1: Information Technology Controls*".

IIA (2005) "*Global Technology Audit Guide (GTAG) 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*".

IIA (2006) "*The 2006 Internal Auditor Software Survey Results*".

IIABEL (2005) "*Heeft u alles onder controle? – Richtlijn: De Belgische Corporate Governance Code*".

Janvrin, D., Lowe, D.J., Bierstaker, J. (2008) "*Auditor acceptance of computer-assisted audit techniques*".

Jaarverslag Telenet 2010. Geraadpleegd op 10 april 2011, http://jaarverslag2010.telenet.be/nl/jaarverslag-2010.aspx

Kuhn, J. R. Jr. en S. G. Sutton (2010) "*Continuous Auditing in ERP System Environments: The Current State and Future Directions*.", Journal of information systems, vol. 24, nr. 1, p91-112.

Kwee, A. (2008) "*Continuous Auditing in relatie tot de (toekomstige) interne audit praktijk*".

Laudon C.K. en J. P. Laudon (2006) "*Bedrijfsinformatiesystemen*". Amsterdam, Pearson Education.

Ling-yu Chou, C., Du, T., Lai, V.S. (2007) "*Continuous auditing with a multi-agent system*", Decision Support Systems, vol. 42; nr. 4, p2274-2292.

Lovata M. L. (1990) "*Audit technology and the use of computer assisted audit techniques*.", Journal of Information Systems, vol. 4, nr. 2, p60-68, 9p.

Lynch, A. en M. Gomaa (2003) "*Understanding the potential impact of information technology on the susceptibility of organizations to fraudulent employee behavior*.", International Journal of Accounting Information Systems, vol. 4, nr. 4, p295-308.

Mahzan, N. en A. Lymer (2007) "*Adoption of Computer Assisted Audit Tools and Techniques (CAATTs) by Internal Auditors: Current issues in the UK*", Birmingham Business School.

Marks, N. en R. Jay (2009) "The Current State of Internal Auditing – A personal perspective and assessment".

Masli, A., Peters, G.F., Richardson, V.J., Sanchez, J.M. (2009) "*Examining the Potential Benefits of Internal Control Monitoring Technology.*", The Accounting Review, vol. 85, nr. 3.

Meegeren, B.F. (2008) "*Continuous auditing en de (veranderde) rol van de IAD*", Audit magzine, nr 5, p6-9.

Mercken, R. (2010) "*Syllabus Externe Controle*".

Mock, T. J. en J. L. Turner (2005) "*Auditor Identification of Fraud Risk Factors and their Impact on Audit Programs.*", International Journal of Accounting Information Systems, vol. 9, nr. 1, p59-77.

Moeller, R.R. (2009) "*Brink's Modern Internal Auditing – A common body of knowledge*", John Wiley and Sons, Zevende editie.

Pop, A., Boţa-Avram, C., Boţa-Avram, F. (2008) "*The Relationship Between Internal and External Audit*".

Proviti (2011) *"Internal Audit Capabilities and Needs Survey"*.

PriceWaterhouseCoopers, PwC (2006) "State of the internal audit profession study: Continuous auditing gains momentum".

PriceWaterhouseCoopers, PwC (2009) "*State of the internal audit profession*".

Ramamoorti, S. (2003) *"Internal auditing: History, evolution, and prospects*.", Research Opportunities in Internal Auditing, FL: The Institute of Internal Auditors Research Foundation, pp. 1–23.

Rezaee, Z., Elam, R., Sharbatoghlie (2001) "*Continuous auditing; the audit of the furute*", Managerial Auditing Journal, vol 16, nr 3, p150-158.

Rittenberg, L.E., Gramling, A.A., Johnstone, M.K. (2010), "*Auditing*", South-Western, 7th edition.

Steegers M. (2008) "*ISO 9001 en interne beheersing.",* Referaat EDP audit opleiding, p1-45.

Vaassen E.H.J., Meuwissen, R.G.H., Beek, A. (2007) "*Hoofdlijnen bestuurlijke informatiebezorging*". Groningen, Wolters-Noordhof.

Vaserhelyi, M. A., Alles, M.G., Kogan, A. (2004) "Principles of Analytic Monitoring for Continuous Assurance.", Journal of Emerging Technologies in Accounting, vol. 1, nr. 1, p1-21.

Vasarhelyi, M.A. (1990) "Artificial Intelligence in Accounting and Auditing: Using Expert Systems", Vol. I, Markus Werner Publishers.

Vaserhelyi, M. A. en F. B. Halper (1991) "The Continuous Audit of Online Systems.", Auditing: A Journal of Practice and Theory, vol. 10, nr. 1, p110-125.

Vasarhelyi, M.A., Elder da Aquino, C., Lopes da Silva, W., Sigolo, N. (2009) "Six steps to an effective continuous audit process", uitgave onbekend.

Vaserhelyi, M. A. en D.Y. Chan (2011) "*Innovation and practice of continuous auditing*.", International Journal of Accounting Information Systems.

Website BDO. "*Internal audit services*". Geraadpleegd op 10 april 2011, http://www.bdo.be/interne%20audit.

Website Openpages. "*About Openpages*". Geraadpleegd op 10 april 2011, http://www.openpages.com/about_us.

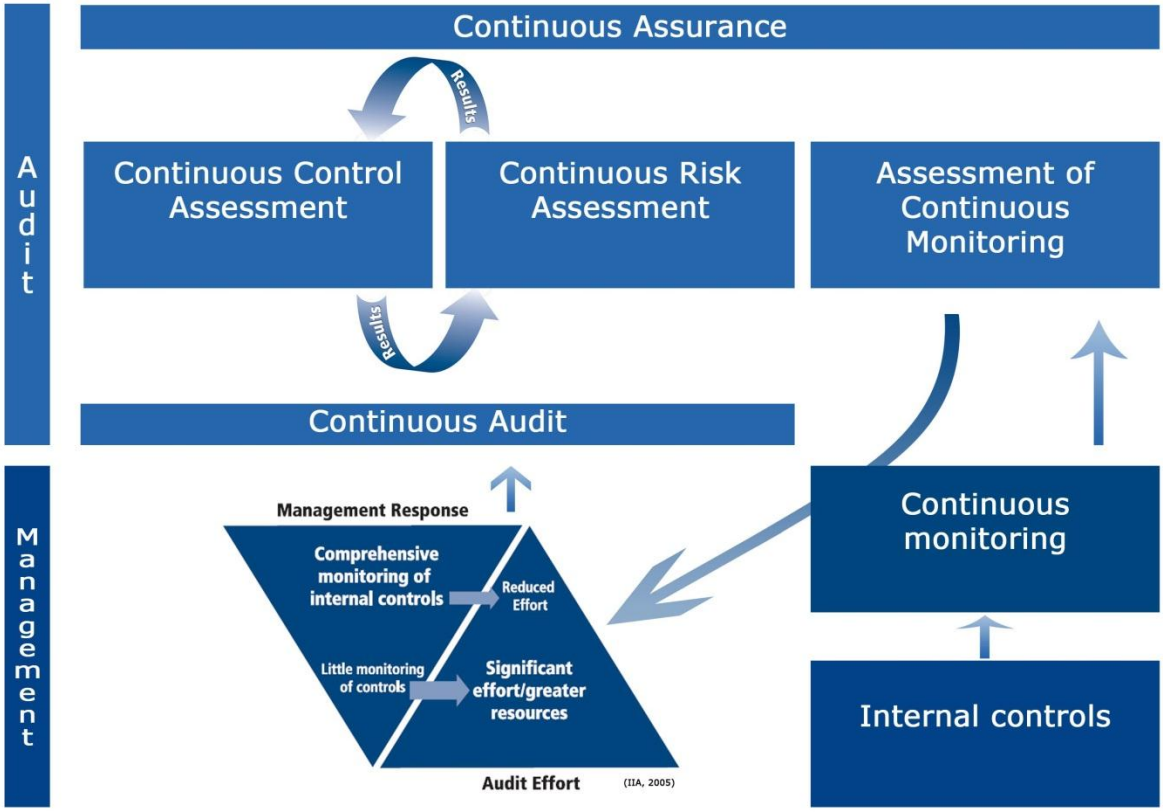
Weidenmier, M. L. en S. Ramamoorti (2006) *"Research Opportunities in Information Technology and Internal Auditing."*, Journal of information systems, vol. 20, nr. 1, p205-219.

Yang, D.C. en M. A. Vasarhelyi (z.d.) "*The Application Of Expert Systems In Accounting*", uitgave onbekend.

Bijlagen

Bijlage 1: Schema Continuous Assurance

Onderstaand schema geeft de verschillende begrippen omtrent Continuous Assurance weer gebaseerd op IIA – GTAG 3 (2005). Er wordt een onderscheid gemaakt tussen management- en auditfuncties.



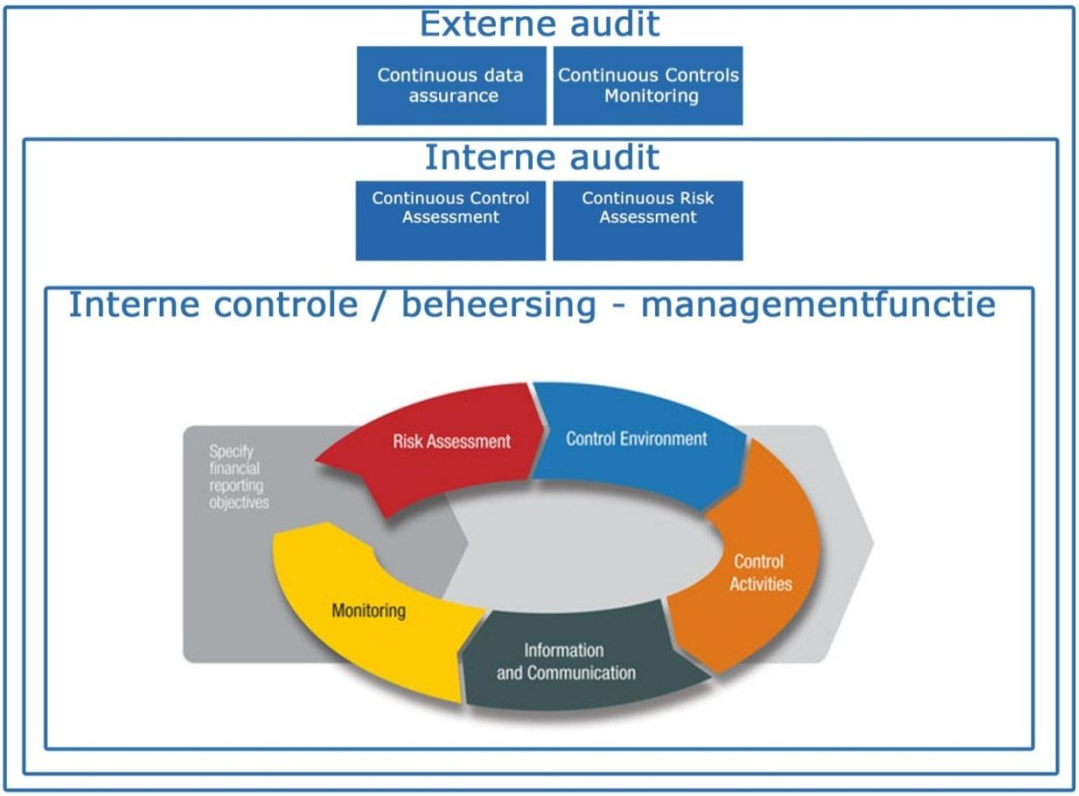
Grafische voorstelling van de verschillende interne beheersings- en auditbegrippen

De belangrijkste onderdelen van Continuous Assurance binnen het auditgebied zijn Continuous Control Assessment (CCA), Continuous Risk Assessment (CRA) en Assessment of Continuous Monitoring. Tussen elk van deze componenten bestaat bovendien een onderling verband. CCA en CRA vormen tezamen Continuous Audit. De resultaten van de CRA kunnen worden gebruikt binnen CRA en omgekeerd. De voornaamste managementfunctie is het opzetten van een intern beheersingssysteem. Naarmate dit systeem beter is uitgewerkt en beter wordt gemonitord, zal de

focus van de CA verschuiven van CCA naar CRA. Hiertoe dient het interne beheersingssysteem te worden beoordeeld binnen een Assessment of Continuous Monitoring.

Bijlage 2: Hiërarchie controlegebieden

Er bestaat een hiërarchie tussen de verschillende controlegebieden. Helemaal onderaan bevinden zich de interne beheersingssystemen. Deze worden opgezet door het management en zullen in eerste instantie worden gecontroleerd door het management zelf (eersterangs controle). Deze systemen worden vervolgens gecontroleerd door de interne auditafdeling (tweederangs controle). In een CA systeem zal dit gebeuren met behulp van Continuous Control Assessment en Continuous Risk Assessment. Deze functies zijn breed genoeg om zowel de efficiëntie en betrouwbaarheid van de financiële gegevens en de interne controlesystemen te verzekeren, als het operationele proces te ondersteunen. Het interne beheersingssysteem zal nadien nogmaals worden gecontroleerd door de externe auditor (derderangs controle). Indien hij de interne audit als betrouwbaar beschouwt, kan hij zijn werk hier deels op baseren. Extern wordt CA uitgevoerd met behulp van Continuous Data Assurance en Continuous Control Monitoring. Tezamen verzekeren ze de betrouwbaarheid van de interne controlesystemen en de financiële gegevens.



Grafische voorstelling controlehiërarchie (IIA, 2005; Vasarhelyi, 2004)

Bijlage 3: Bepalen van het auditrisico

Bij het opstarten van een audit zal vooreerst het auditrisico, oftewel het risico dat er een verkeerde auditopinie wordt afgeleverd, worden bepaald. Dit risico bestaat uit drie componenten, namelijk het inherent risico, het controle risico en het detectie risico.

- Inherent risico: het initiële risico van een transactie dat deze fout of niet zal worden opgenomen in de financiële staten.
- Controle risico: het risico dat het interne beheersingssysteem van de cliënt er niet in slaagt om eventuele fouten te detecteren of te voorkomen.
- Detectie risico: het risico dat de auditor er niet in slaagt om eventuele fouten te detecteren.

Aan de hand van het auditrisico zal de materialiteit worden vastgesteld. Een hoger auditrisico zal leiden tot een lagere materialiteitsnorm. De materialiteit geeft aan vanaf wanneer een afwijking een invloed zal uitoefenen op het beslissingsproces van derden.

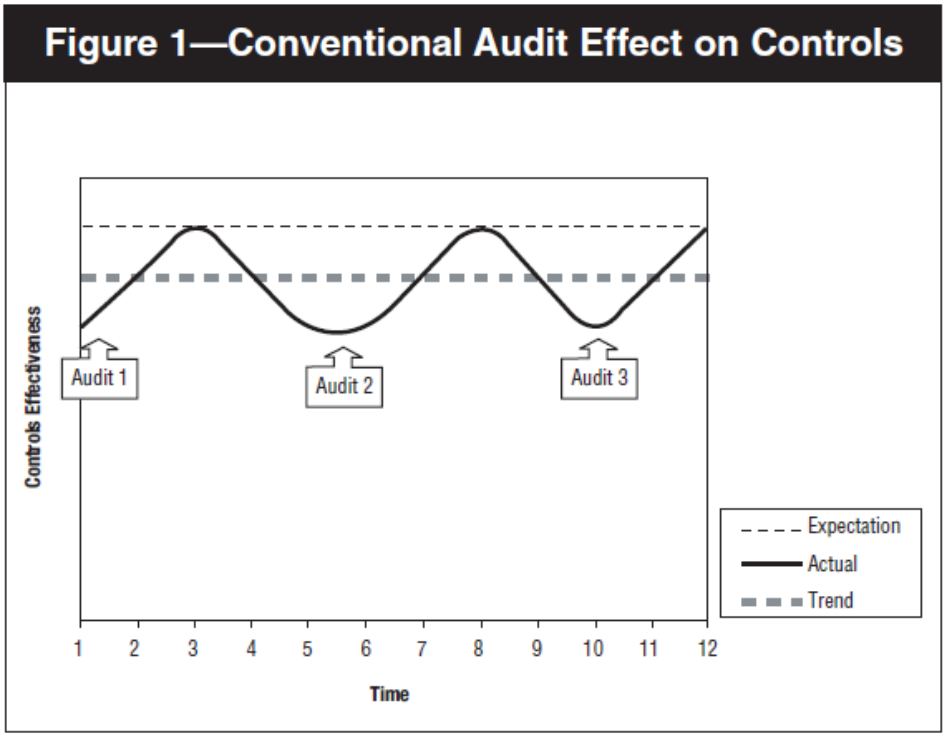
Grafische voorstelling materialiteitsberekening (Mercken, 2010)

Bijlage 4: Activiteiten tussen CCA en CRA

Continuous Auditing						
Continuous Controls Assessment	←				→ Continuous Risk Assessment	Approach
Control-based (Assurance controls are working) Financial Controls	←				→ Risk-based (Identification/Assessment of risk) Financial/Operational Controls	Focus
Real-time/Detailed transaction testing (Financial data)	←				→ Trend/Comparison (Financial/Operational data)	Analysis Techniques
Control Assurance	Financial Attest	Fraud/Waste/Abuse	Audit Scope and Objectives	Follow-up on Audit Recs	Annual Audit Plan	Related Audit Activities
Control Monitoring	Performance Monitoring		Balanced Scorecard	TQM	ERM	Related Management Activities

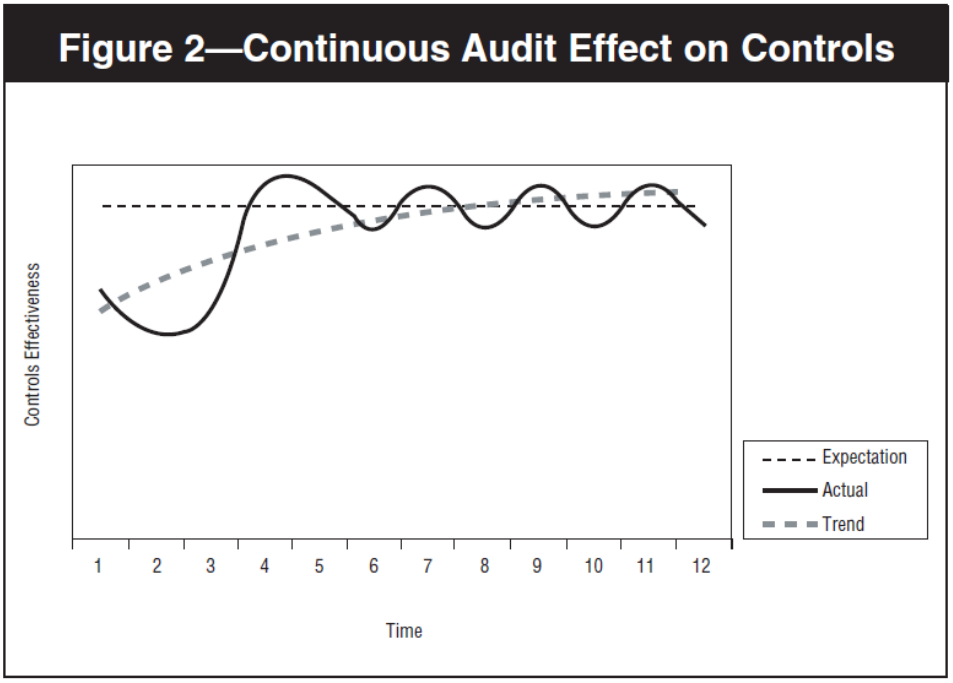
Overzicht van alle activiteiten tussen CCA en CRA (IIA, 2005)

Bijlage 5: Verwachte auditprestaties conventionele audit



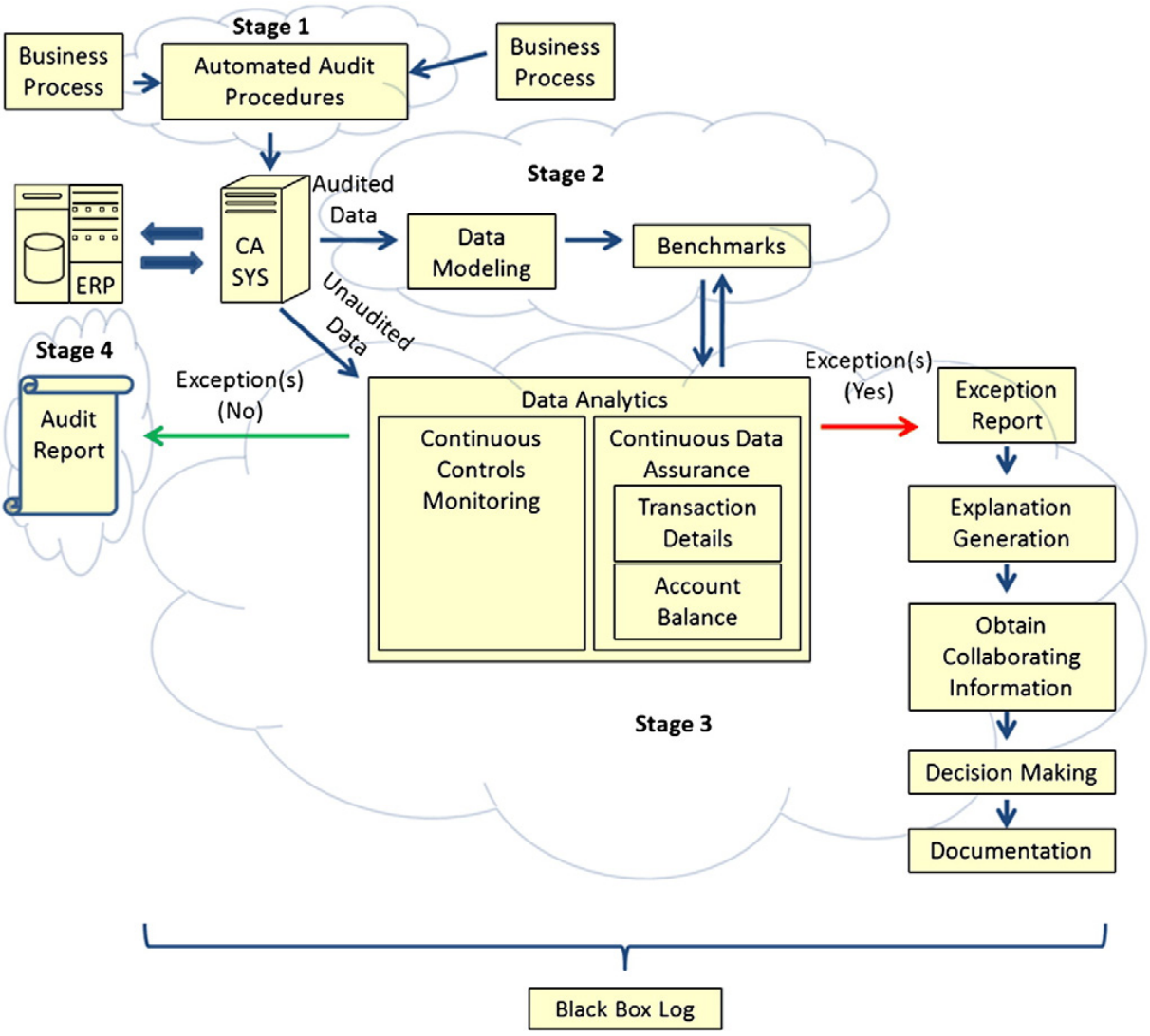
Verwachtte versus werkelijke auditprestaties – klassieke audit (Handscombe et al., 2007)

Bijlage 6: Verwachte auditprestaties continue audit



Verwachtte versus werkelijke auditprestaties – continue audit (Handscombe et al., 2007)

Bijlage 7: CA-model



Werking continu auditsysteem (Vasarhelyi et al., 2004)

Bijlage 8: Resultaten gebruik van CAATTs

Use of CAAT: Regression Results

			Model 1 TotalCAATUsage			Model 2 AverageCAATImportance		
Variables	**Coef**	**Expected Sign**	**β**	**p- value**	**Sig**	**β**	**p- value**	**Sig**
Intercept	β_0		-0.18			0.93		
Performance Expectancy (PE)	β_1	+	0.05	2.00	*	0.34	2.22	*
Effort Expectancy (EE)	β_2	+	-0.01	-0.40		-0.03	-0.18	
Social Influence (SI)	β_3	+	0.03	1.51		0.11	0.92	
Facilitating Conditions (FC)	β_4	+	0.07	3.43	**	0.30	2.52	*
F-value				24.59			17.66	
p-value				< 0.0001			< 0.0001	
Adjusted R^2 (%)				37.9			42.9	

Model specifications:

Model 1: TotalCAATUsage $= \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \beta_4 FC$

Model 2: AverageCAATImportance $= \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \beta_4 FC$

Significance:

* Significant at p-value < 0.05

** Significant at p-value < 0.01

(Janvrin et al., 2008)

Uit de regressieresultaten valt af te leiden dat CAATTs voornamelijk gebruikt worden omwille van verwachte prestatietoenames. Ook de ondersteunende voorwaarden spelen een belangrijke rol. Met een p-waarde van respectievelijk 2 en 3,43 zijn ze significant op 5% significantieniveau. Het gebruiksgemak en sociale verwachtingen zijn niet significant.

Bijlage 9: Vergelijking tussen de interne en externe audit

No.	Criterions	Internal Audit	External Audit
1	**Position inside the organization**	The internal auditors' are part of the organization. Their objectives are determined by professional standards, the board, and management. Their primary clients are management and the board.	External auditors are not part of the organization, but are engaged by it. Their objectives are set primarily by statute and their primary client - the board of directors.
2	**Objectives**	The internal auditor's scope of work is comprehensive. It serves the organization by helping it accomplish its objectives, and improving operations, risk management, internal controls, and governance processes. Concerned with all aspects of the organization - both financial and nonfinancial - the internal auditors focus on future events as a result of their continuous review and evaluation of controls and processes.	The primary mission of the external auditors is to provide an independent opinion on the organization's financial statements, annually.
3	**Independence**	Internal audit must be independent from the audited activities.	External audit is independent from its client, the organization, its independence being specific to liberal professions.
4	**Approach of internal control**	Internal audit regards all the aspects regarding the organization's internal control system.	External audit regards the internal control system only from the materiality perspective, which permits them to eliminate those errors that aren't significant, because they don't have influences over the financial results.
5	**Applying of the audit**	Internal audit covers all the organization' transactions.	External audit covers only those operations that have a contribution at the financial results and the performances of the organization.
6	**Frequency of the audit**	year, having specific missions established in according with the level of risks identified for each auditable entity.	External audit is an activity with a yearly frequency, as a rule, at the end of the year.
7	**Approach of risk**	The importance of risk for the planning of internal audit activity is very high, the assessment of risk being combined with other types of information like financial and operational.	External audit uses the information of risks for the determination of nature, period of time and necessary audit procedures that should be performed in the auditable area, taking into consideration only financial aspects.
8	**Consideration of risk factors**	Internal audit takes into consideration at least next *risk factors*: ☐ Ethical climate and pressure on management to meet objectives; ☐ Competency, adequacy, and	External audit takes into consideration next *risk factors*: ☐ Management operating and financial decisions are dominated by a single person;

		integrity of personnel; ☐ Asset size, liquidity, or transaction volume; ☐ Financial and economic conditions; ☐ Competitive conditions; ☐ Impact of customers, suppliers, and government regulations; ☐ Date and result of previous audits; ☐ Degree of computerization; ☐ Geographic dispersion of operations; ☐ Adequacy and effectiveness of the system of internal control; ☐ Organizational, operational, technological, or economic changes; ☐ Management judgments and accounting estimates; ☐ Acceptance of audit findings and corrective action taken;	☐ Management's attitude toward financial reporting is unduly aggressive; ☐ Management, particularly senior accounting personnel, turnover is high; ☐ Management places undue emphasis on meeting earnings projections; ☐ Management's reputation in the business community is poor; ☐ Profitability of entity relative to its industry is inadequate or inconsistent; ☐ Sensitivity of operating results to economic factors is high; ☐ Rate of change in entity's industry is rapid; ☐ Entity's industry is declining with many business failures; ☐ Organization is decentralized without adequate monitoring; ☐ Internal or external matter raises substantial doubt about the entity's ability to continue as a going concern; ☐ Contentious or difficult accounting issues are prevalent; ☐ There are significant and unusual related party transactions not in the ordinary course business; ☐ The nature, cause (if known), or amount of known and likely misstatements detected in the audit of prior period's financial statements is significant; ☐ Client is new with no prior audit history or sufficient information is not available from the predecessor auditor.
9	**Approach of fraud**	Internal audit is concerned about the frauds from all activities from the organization.	External audit is concerned only about the fraud from financial areas.

Vergelijking interne en externe auditors (Pop et al., 2008)

Bijlage 10: Vragenlijst empirisch onderzoek – interne audit

Zoals aangegeven in hoofdstuk zeven is het empirisch onderzoek gericht op het bevestigen of weerleggen van de bevindingen uit de literatuurstudie. De interviews binnen interne auditafdelingen zijn gericht op het bekomen van informatie omtrent:

- De opbouw van de interne controlesystemen in sterk geautomatiseerde omgevingen.
- Het verloop van de samenwerking tussen een onderneming, zijn management en de interne auditafdeling. Het gaat om de opdracht en de focus van de auditactiviteiten, de manier waarop er wordt gecommuniceerd en de manier waarop gegevens worden verkregen en de resultaten worden gerapporteerd.
- De opbouw van de interne audit: overzicht van de software audit tools die worden gebruikt en de voordelen/ beperkingen die aan dit soort tools verbonden zijn. Het belang van dit soort tools en een vergelijking van continue audittests met periodieke.
- Toekomstplannen: bespreking van de (mogelijke) veranderingen die zullen plaatsvinden binnen de interne audit op het gebied van gebruikte informatiesystemen.

Vragenlijst

1. Wat is uw huidige functie binnen de interne audit?
2. Waar ligt de focus van de interne auditactiviteiten en hoe sluit deze aan bij de auditopdracht?
3. Op welke manier zijn de interne controles opgesteld en hoe wordt hier gebruik gemaakt van informatietechnologie?
4. Op welke manier verloopt de communicatie tussen de interne auditafdeling en de onderneming?
5. Hoe worden de benodigde auditgegevens verkregen?
    a. Is er een permanente link tussen het bedrijfs- en auditsysteem?
    b. Op welke manier wordt verzekerd dat de originele gegevens niet worden beïnvloed?
    c. Op welke manier wordt verzekerd dat de ontvangen gegevens voldoende zijn beveiligd?
6. Welke op informatiesystemen gebaseerde tools worden momenteel gebruikt binnen het auditproces?
7. Welk belang zou u toewijzen aan deze tools?
8. Binnen welke auditactiviteiten wordt er gebruik gemaakt van computer assissted audit tools and techniques (CAATTs)?
    - Evalueren van fraude risico's
    - Identificeren van journaalposten die verdere controle vereisen

- Controleren van de accuraatheid van elektronische documenten
- Opnieuw uitvoeren van (interne controle) procedures
- Selecteren van steekproeven
- Sorteren van transacties met specifieke karakteristieken
- Testen van de gehele populatie in de plaats van een deel
- Verzamelen van informatie omtrent de controle effectiviteit
- Nagaan van het bestaan en de correctheid van voorraden

9. Worden de controles uitgevoerd op periodieke of op continue basis?
    a. Voor het verifiëren van interne controlesystemen?
    b. Voor het inschatten van risico's?
10. Welke zijn de voordelen verbonden aan het gebruik van CAATTs?
11. Welke zijn de nadelen verbonden aan het gebruik van CAATTs?
12. Welke redenen zijn de belangrijkste gebruiksredenen van CAATTs?
13. Hoe gaan deze systemen in de toekomst nog evolueren?

Bijlage 11: Vragenlijst empirisch onderzoek – externe audit

Ook de interviews binnen externe auditafdelingen zijn gericht op het bekomen van informatie omtrent de conclusies uit het literatuuronderzoek. Er kan een opsplitsing worden gemaakt naar twee delen.

Het eerste deel richt zich op het gebruik van audit productiviteit tools en CAATTs. Er wordt nagegaan voor welke functies en controles deze worden toegepast en wat de voordelen en beperkingen ervan zijn. Er wordt bepaald of ze ook worden toegepast bij de audit van kleinere ondernemingen, of opdat er daar nog manueel wordt gewerkt.

Het tweede deel richt zich op de continue audit en de mogelijkheden hiervan binnen de externe audit. Uit de literatuurstudie bleek immers dat het voor externe auditors, ten gevolge van onder andere onafhankelijkheidsproblemen, moeilijk is om gebruik te maken van geïntegreerde continue audit oplossingen. Het is de bedoeling dit te verifiëren en om na te gaan of dit in de toekomst nog kan veranderen.

Vragenlijst

1. Wat is uw huidige functie binnen de externe audit?
2. Op welke manier zijn de externe controles opgesteld en hoe wordt hier gebruik gemaakt van informatietechnologie?
3. Op welke manier verloopt de communicatie met de interne afdelingen?
4. Hoe worden de benodigde auditgegevens verkregen?
    a. Is er een permanente link tussen het bedrijfs- en auditsysteem?
    b. Op welke manier wordt verzekerd dat de originele gegevens niet worden beïnvloed?
    c. Op welke manier wordt verzekerd dat de ontvangen gegevens voldoende zijn beveiligd?
5. Welke op informatiesystemen gebaseerde tools worden momenteel gebruikt binnen het auditproces?
6. Welk belang zou u toewijzen aan deze tools?
7. Is dit belang even groot binnen grote als kleine ondernemingen?
8. Binnen welke auditactiviteiten wordt er gebruik gemaakt van computer assissted audit tools and techniques (CAATTs)?
    - Evalueren van fraude risico's
    - Identificeren van journaalposten die verdere controle vereisen
    - Controleren van de accuraatheid van elektronische documenten
    - Opnieuw uitvoeren van (interne controle) procedures
    - Selecteren van steekproeven
    - Sorteren van transacties met specifieke karakteristieken
    - Testen van de gehele populatie in de plaats van een deel
    - Verzamelen van informatie omtrent de controle effectiviteit
    - Nagaan van het bestaan en de correctheid van voorraden
9. Worden de controles uitgevoerd op periodieke of op continue basis?
10. Welke problemen doen zich voor bij het gebruik van continue CAATTS?
11. Welke zijn de voordelen verbonden aan het gebruik van CAATTs?
12. Welke zijn de nadelen verbonden aan het gebruik van CAATTs?
13. Welke redenen zijn de belangrijkste gebruiksredenen van CAATTs?
14. Hoe wordt er omgegaan met de interne informatiesystemen?
15. Hoe gaan deze systemen in de toekomst nog evolueren?

Auteursrechtelijke overeenkomst

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
Informatiesystemen binnen het auditproces

Richting: **master in de toegepaste economische wetenschappen-accountancy en financiering**
Jaar: **2011**

in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Niet tegenstaand deze toekenning van het auteursrecht aan de Universiteit Hasselt behoud ik als auteur het recht om de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij te reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

Ik bevestig dat de eindverhandeling mijn origineel werk is, en dat ik het recht heb om de rechten te verlenen die in deze overeenkomst worden beschreven. Ik verklaar tevens dat de eindverhandeling, naar mijn weten, het auteursrecht van anderen niet overtreedt.

Ik verklaar tevens dat ik voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen heb verkregen zodat ik deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal mij als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze overeenkomst.

Voor akkoord,

Bervoets, Kevin

Datum: **1/06/2011**