IT-auditor is meer dan controleur van informatietechnologie

Rob Fijneman

SAMENVATTING Een IT-auditor beoordeelt de informatietechnologie (IT) van een organisatie. Toch is niet duidelijk of de IT-auditor nu vooral een controleur of een adviseur is. Als een Chief Information Officer (CIO) een IT-auditor inschakelt, zoekt hij meer een adviseur dan een controleur. Een accountant daarentegen schakelt eerder een IT-auditor in als controleur. Is de IT-auditor nu vooral een accountant op IT-gebied of een IT-consultant met auditkennis? Antwoorden op deze vraag worden gezocht. Daarbij wordt gesteld dat IT-auditors niet slechts als uitvoerder regels moeten verifiëren, maar dat ze kritisch moeten blijven handelen en denken en actief verbeteringen moeten aandragen. Hiermee wordt stelling genomen tegen de opvatting dat een IT-auditor controle- en advieswerk niet mag combineren om belangenverstrengeling te voorkomen.

1 Inleiding

IT-auditing is een vakgebied dat een stormachtige ontwikkeling heeft doorgemaakt. Intussen is er sprake van een werktein van dat zich al meer dan veertig jaar manifesteert, dit duidt op een volwassen vakgebied dat nog volop energie heeft om zich verder te ontplooiën (Fijneman, 2005b)¹.

Prof. Dr. R.G.A. Fijneman RE RA is als partner verbonden aan KPMG en voorzitter van Information Risk Management in Nederland. Sinds 1986 is hij werkzaam in het IT-auditvakgebied. Per 1 september 2004 is hij als deeltijdhoogleraar EDP-auditing verbonden aan de Universiteit van Tilburg en de TIAS Business School.

Dit artikel is een bewerking van de rede 'IT-auditing, grenzeloos of gelimiteerd?' uitgesproken op 22 april 2005 door prof.dr. R.G.A. Fijneman RE RA bij de aanvaarding van het ambt van hoogleraar IT-auditing aan de Universiteit van Tilburg.

Het zal velen niet ontgaan zijn dat er in Auditingland de nodige discussies zijn ontstaan en deels nog gaande zijn over het combineren van audit- en advieswerkzaamheden (Fijneman, 2005a). Het accountantsberoep heeft zich jarenlang (vooral in de jaren negentig van de vorige eeuw) ontwikkeld op basis van een 'one-stop-shopping'-concept, waarbij opdrachtgevers met al hun veelal financieel gerichte vragen bij de accountant terecht konden. Dit geldt naar analogie ook voor de IT-auditor, opdrachtgevers kunnen met al hun informatietechnologiegerichte vragen terecht bij de IT-auditor. De aanduiding van Information Risk Management als werktein van de IT-auditor maakt dit ook duidelijk. IT-auditors brengen de risico's in kaart die een organisatie loopt voor wat betreft informatietechnologie en informatievoorziening en dragen hiervoor actief oplossingen aan.

Intussen heeft in het accountantsberoep de wal het schip gekeerd. Als gevolg van een aantal boekhoudschandalen, zowel nationaal als internationaal, is het werktein van de accountant stringenter afgebakend en is het toezicht aangescherpt. Ook in de Wet Toezicht Accountants komt dit tot uitdrukking. De perceptie is minimaal gerechtvaardigd dat de accountants terug bij hun 'roots' zijn; vervelend is alleen dat dit ogenschijnlijk reactief tot stand is gekomen. Daarnaast bestaat de indruk dat de limiteringen wel erg sterk zijn gedefinieerd, en vanuit de optiek van sommige opdrachtgevers wellicht zelfs te beperkend.

De toegevoegde waarde van de accountantsfunctie komt daarmee in het gedrang en kan blijven steken in de uitkomst van een wettelijk verplichte exercitie. Ook in de IT-auditing is een 'back-to-the-roots'-trend waar te nemen. IT-auditing zou zich ogenschijnlijk weer primair moeten richten op de beoordeling van de kwaliteit van de aanwezige informatietechnologie.

Het IT-auditberoep, bestaande uit de professionals en de beroepsorganisatie Nederlandse Orde voor Register

EDP-auditors (NOREA), kan proactief sturing geven aan de discussie over zijn taken en verantwoordelijkheden. De behoefte daaraan wordt gevoeld. Er bestaan onduidelijkheden. Is de IT-auditor nu vooral een accountant op IT-gebied, of is hij bovenal een IT-consultant met ook auditkennis? Of moeten we het omdraaien: een IT-auditor heeft als kerncompetentie auditing, maar daarnaast ook adviesvaardigheden. Reden genoeg om de zaken verder te verkennen. Als uitgangspunt daarbij is vooral de Nederlandse situatie genomen. Dit heeft te maken met de gekozen invalshoek door Fijneman (2005a). Belangrijk daarbij is dat Nederland mede trendsettend is voor de breedte en diepte van het IT-auditvakgebied.

De afbakening van IT-auditing van de Internationale IT-auditberoepsorganisatie, de Information Systems Audit and Control Association (ISACA), is veelal een subset van de Nederlandse discussie. Natuurlijk is wel rekening gehouden met de buitenlandse invloeden bij een aantal grote auditororganisaties.

In paragraaf 2 wordt gestart met een aantal definities van IT-auditing die een beeld geven van het werkkterrein. In paragraaf 3 wordt dit verder uitgediept. De visies van opdrachtgevers, als belangrijke leidraad voor de verdere vorming van het vakgebied, staan centraal in paragraaf 4. Niet alleen het heden is relevant bij de positionering van de IT-auditor, maar ook een toekomstverkenning kan helpen. Enkele uitgangspunten zijn in paragraaf 5 opgenomen. Paragraaf 6 bevat ten slotte een aantal conclusies.

2 Definities van IT-auditing

De definities worden vanuit een aantal invalshoeken gegeven, zodat een beeld ontstaat van het vakgebied.

2.1 Definities van hoogleraren

Vanuit de Nederlandse invalshoek lijkt het logisch om te starten met het bekijken van een aantal definities van het vakgebied vanuit de positie van enkele hoogleraren IT-auditing. Moonen (1991) definieerde IT- of EDP-auditing als volgt: 'het vakgebied dat zich bezighoudt met het beoordelen van de kwaliteit van de informatievoorziening in een omgeving waar sprake is van het gebruik van informatietechnologie en van elektronische gegevensverwerking'.

Duidelijk is dat Moonen in zijn definitie het beoordelen zeer centraal stelde. Toch was ook duidelijk dat het beoordelen diende te leiden tot zinvolle adviezen. Men zou kunnen stellen: zonder oplossingen ter verbetering kan er geen sprake zijn van een zinvolle audit.

Deze invulling werd in dezelfde tijd ook zichtbaar in de rede van Kocks (1991), die refererend aan de definitie van EDP-auditing aan de Erasmus Universiteit stelde: 'EDP-auditing is het vakgebied dat zich bezighoudt met het beoordelen alsmede het (richtinggevend) adviseren met betrekking tot kwaliteitsaspecten van objecten in een omgeving waar gebruik wordt gemaakt van automatisering/informatietechnologie'.

De definities bewegen tussen audit en advies. Recenter hebben Van der Pijl (2000) en Roos Lindgreen (2002) ook het werkkterrein van IT-auditing verkend.

Van der Pijl definieerde IT-auditing als het werkkterrein dat betrokken is bij het beoordelen van en adviseren over het gebruik van IT in organisaties. Het werkkterrein wordt volgens Van der Pijl gevormd door ontwikkelingen in IT, ontwikkelingen in organisaties en ontwikkelingen in auditing. De ontwikkelingen in IT zijn daarbij velerlei; alles wordt sneller en transparanter. Organisaties ontwikkelen zich tot netwerkorganisaties, de procesfocus staat voorop. De kwaliteit van de processen dient continu te worden gewaarborgd inclusief de daarbij ingezette IT. Van der Pijl stelt dat als gevolg van deze veranderingen de IT-auditor steeds vaker als sparringpartner optreedt voor het management, aangezien het management onzeker is over het beheer van de IT-functie. Daarbij onderstreept hij de door Mollema (1999) verwoorde visie dat ook de IT-auditor managementbesluitvorming op alle niveaus in de organisatie dient te ondersteunen. De IT-auditor ontwikkelt zich, volgens Mollema, zoals vele andere soorten auditors. Wezenlijk is dat Van der Pijl stelt dat de audit- en de adviesfunctie van de IT-auditor steeds meer verbonden zijn, een statement dat we vandaag de dag met de nodige voorzichtigheid bezien. In de tijdgeest van 2000 klopte het beeld echter heel aardig, ook de opdrachtgevers wilden de expertise van de IT-auditor voluit benutten.

Roos Lindgreen (2002) definieerde IT-auditing niet specifiek aangezien zijn inaugurele rede zich vooral richtte op de accountantsfunctie en informatiebeveiliging. Echter, uit zijn opsomming van mogelijke IT-audits blijkt wel een breed werkkterrein.

2.2 Definitie van de beroepsorganisatie

Ook de beroepsorganisatie NOREA hanteert een definitie voor het werkveld van IT-auditing. NOREA stelt (NOREA, 2004b) dat een IT-auditor de informatietechnologie in een organisatie beoordeelt. Een gekwalificeerde IT-auditor geeft volgens de NOREA

onpartijdige oordelen en adviezen over de kwaliteitsaspecten van IT.

Deze definitie is ook herkenbaar in de uitingen van ISACA. Ook de internationale definitie stelt het onafhankelijk en onpartijdig beoordelen van de kwaliteit van IT centraal.

2.3 Definities van enkele auditkantoren

Het beeld ontstaat dat de hiervoor besproken definities veelal redeneren vanuit de positie van de IT-auditor c.q. het vakgebied zelf. Ze zijn daarmee aanbodgedreven. Het is interessant om kennis te nemen van de definities van enkele grote IT-auditkantoren om te zien of de vraagkant dan zichtbaarder wordt.

KPMG Information Risk Management (IRM) stelt in haar internationale serviceportfolio (KPMG, 2004) het volgende:

'IRM focusses on the risk inherent in the technology systems and processes used to support an organizations business objectives. IRM is dedicated to assist clients in the identification, understanding, measurement and management of business risks resulting from the dependence on information and technology to manage and evolve their businesses.'

Dit brengt een verbreding aan in het begrip auditing en werkt het adviserend element veel verder uit. Vereenvoudigd wordt wel gesteld dat de IT-auditor zich bezighoudt met pakketten, projecten, beheersing, beveiliging en de ondersteuning van de accountant. Indien we de websites van de overige grote auditkantoren bekijken komen we ook bij de relatief brede definities uit. Zo spreekt PWC vooral over riskmanagement, het helpen de materiële en immateriële waarden van een organisatie te beschermen en te benutten. Deloitte definieert haar dienstverlening als breed pakket aan diensten op het gebied van risicomangement en controle. IT-risico's worden geïdentificeerd en beheerst. Ernst & Young stelt dat haar onafhankelijke specialisten concrete oplossingen bieden voor allerlei vraagstukken die zich voordoen in een geautomatiseerde en virtuele bedrijfsomgeving (websites genoemde kantoren).

Een voorlopige conclusie is dat in de praktijk het begrip IT-auditing is verbreed. Niet alleen wordt de IT-auditor herkend als beoordelaar van IT-risico's en IT-beheersing, maar ook als sparringpartner c.q. adviseur van het (IT-)management op IT-beheersingsgebied speelt hij zijn rol. IT-auditing of, zoals sommi-

gen zeggen, Information Risk Management heeft daarmee een grotere reikwijdte verkregen.

Daarbij moet worden opgemerkt dat de grote kantoren aan grensverkenning doen. Zoals eerder vermeld is deze grensverkenning voor het accountantsberoep ontvaard in een 'back-to-the-roots'. Voor IT-auditors lijken op het eerste oog nog geen begrenzingen te zijn aangebracht. Toch zijn deze er wel. Bij een jaarrekeningcontroleklant is de IT-auditor gehouden aan strikte spelregels zoals deze ook gelden voor de controlerend accountant. Dit verklaart ook de aandacht voor het ontwikkelen van zogeheten 'non-auditklanten', waar de expertise van de IT-auditor in de volle adviesomvang kan worden ingezet.

De vraagkant (wat vinden de opdrachtgevers) is nog niet geheel in beeld. Hierop wordt in paragraaf 4 nader ingegaan.

3 Werkerterrein van IT-auditing

Het verkennen van definities heeft ons een eerste indruk gegeven van het werkerterrein van IT-auditing. Het werkerterrein valt op basis van andere kenmerken nog verder in te delen.

3.1 Kwaliteitsaspecten

Een startpunt daarbij vormt een indeling in kwaliteitsaspecten. NOREA (1997, 1998, 2004b) onderkent de aspecten: efficiency, effectiviteit, exclusiviteit, integriteit, controleerbaarheid, continuïteit en beheersbaarheid. Aan de TIAS Business School wordt gesproken over beveiliging, efficiency, effectiviteit en controleerbaarheid (Moonen, 1991). Hoewel de IT-auditor juist ook zijn expertise wil laten gelden op efficiency- en effectiviteitsgebied, is hij hiervoor nog niet altijd de logische sparringpartner van het topmanagement. Bijvoorbeeld bij het nemen van investeringsbeslissingen, het aangaan van uitbestedingscontracten en het meten van het rendement van IT wordt niet primair gedacht aan het inschakelen van de IT-auditor. Wellicht dat er toch iets schort aan het advies c.q. het managementprofiel van de IT-auditor.

3.2 Objecten

In het NOREA-geschrift no. 1 (NOREA, 1998) wordt het werkerterrein van de IT-auditor primair benaderd vanuit de attestfunctie en als volgt ingedeeld:

- informatiestrategie;
- IT-management;
- informatiesystemen;

- technische systemen;
- processystemen;
- operationele automatiseringsondersteuning.

Dit duidt op een werkterrein dat verder voert dan het ondersteunen van de accountant, en juist is gericht op het management van organisaties.

De indeling in objecten of, zoals in het NOREA-geschrift aangeduid, in domeinen, is in 2003 door NOREA in samenwerking met de Universiteiten die opleidingen tot EDP-auditing verzorgen ook vertaald in een set van minimale normen (ook wel aangeduid als eindtermen) voor de opleiding tot IT-auditor.

3.3 Overige indelingen

In de praktijk worden talloze andere indelingen van het werkterrein gehanteerd.

Een van de grote auditkantoren stelt als afgeleide van de eerder vermelde definitie dat 'business and technology risks can result from the need for better governance and information management performance, partnering with third parties, management of change and the implementation of controls at the technology layer'. Dit resulteert bij dit kantoor in een werkterrein bestaande uit:

- Governance and Performance; beheersen we de IT-functie en levert de inzet van IT het verwachte rendement op?
- Sourcing Risk Management; hebben we de IT-functie goed georganiseerd of dienen we delen uit te besteden?
- Business Systems Controls; zijn de geïntegreerde Enterprise Resource Planning (ERP)-systemen goed ingericht en kunnen we verantwoordingsinformatie daaraan ontleen?
- Security, privacy, continuity; is de beveiliging op orde?
- IT Internal Audit services; kunnen we samen met Internal Audit de taakstelling op IT-auditgebied invullen?
- IT attestation (Statement on Auditing Standards 70, Webtrust); kunnen de IT-processen en -producten voorzien worden van een certificaat?
- IRM in the External Audit; kunnen we de betrouwbaarheid en continuïteit van de IT voorzover relevant voor de financiële verslaglegging beoordelen?

Natuurlijk staat niet de hiervoor gemelde indeling centraal – de diverse kantoren hanteren allemaal net iets andere begrippen – echter wel de richting die hieruit blijkt.

Het werkterrein en de te beantwoorden management-vragen geven aan dat de IT-auditor of Information Risk Manager zich bezighoudt met Audit, Control, Protections of management support. Ook Mollema stelde – zoals eerder vermeld – dat de IT-auditor zich op alle niveaus in een organisatie beweegt. Niet alleen houdt de IT-auditor zich bezig met het beoordelen van operationele systemen, maar juist ook op tactisch en strategisch IT-niveau probeert de IT-auditor zijn bijdrage te leveren.

3.4 Audit versus advies

Al met al een breed en omvangrijk werkterrein, ogenschijnlijk breder dan de definities van IT-auditing zoals gehanteerd in 1991. Het lijkt of 'the sky the limit' is.

In de jaren negentig is dit ook herkenbaar als we de resultaten van de grote auditkantoren analyseren. Het aandeel van adviesopdrachten ten opzichte van auditopdrachten stijgt enorm. Het door de IT-auditor leveren van ondersteuning aan de accountant bij de jaarrekeningcontrole is nog slechts een marginaal deel van de IT-auditwerkzaamheden. Het onderscheid tussen audit en advies is soms kunstmatig. Een audit zonder enig advies lijkt nauwelijks zinvol. De opdrachtgever zal een oplossing willen hebben voor zijn probleem. Een audit vergt echter wel een duidelijke normenstelling op basis waarvan getoetst kan worden; een adviesaanpak heeft meer vrijheden.

Het hier genoemde advies bevindt zich veelal op een bepaald terrein van de IT. De IT-auditor is vooral deskundige ten aanzien van IT-risico's en IT-beheersing. Dit maakt hem nog geen IT-consultant in de volle breedte.

Van Kessel (2005) merkt dit terecht op. Dit verklaart wellicht dat een IT-auditor en een IT-consultant in de praktijk ook goed naast elkaar kunnen functioneren.

In 2003 tekent zich een kentering af, in belangrijke mate veroorzaakt door enkele boekhoudschandalen. De IT-auditor lijkt deels terug bij af. Dit klinkt negatiever dan het is. De IT-auditor dient onder invloed van wet- en regelgeving, zoals Sarbanes-Oxley en Tabaksblat, weer volop als auditor actief te zijn. De betrouwbaarheid en continuïteit van de IT-functie en -toepassingen dienen te worden beoordeeld aangezien vele IT-controls relevantie blijken te hebben voor de kwaliteit van de financiële verslaglegging. Dit geeft een enorme stimulans aan de samenwerking tussen de IT-auditor en de accountant. In 2004 besteedden bepaalde IT-auditkantoren, vooral in Amerika, weer 70% van hun tijd aan IT-auditsupport ten behoeve van accountants. Een voorlopige conclusie is dat ook

de IT-auditor 'back-to-the-roots' is; roots die sommige IT-auditors vergeten waren. Het stellen van de deskundigheidsvraag voor het uitvoeren van audits is daarbij volop legitiem. Is de IT-auditor in staat te leveren op een terrein dat vanouds als startpunt van het IT-auditberoep wordt gezien?

4 Verwachtingen van opdrachtgevers

4.1 Helderheid en duidelijkheid

Hopelijk blijkt uit al hetgeen tot op heden is gezegd dat het IT-auditberoep met de nodige nuanceringen zijn werkteerrein definieert. Het valt op dat het al snel ingewikkeld wordt. Wellicht is het een kenmerk van professionals dat relatief veel woorden nodig zijn om iets uit te leggen. Opdrachtgevers zijn meestal korter van stof. Zij ervaren een probleem op IT-gebied en willen dat het wordt opgelost. Enkele vragen die zij stellen luiden als volgt:

- Is de geselecteerde IT-leverancier betrouwbaar?
- Levert het geld op als we deze IT-investeringen verrichten?
- Kan ik op verantwoorde wijze werken met de output uit dit systeem?
- Is mijn IT-manager geschikt en beschik ik over een capabele IT-organisatie?

In de ICT-assessmentmethodiek, onder andere gebaseerd op de Nolan Norton-aanpak zoals door Van der Zee (2002) beschreven, zijn deze managementvragen nog verder uitgediept. Het management vraagt niet om IT-auditproducten, maar om zekerheid en oplossingen. Korte en bondige meningen worden op prijs gesteld. Dit geldt eens te meer als de IT-auditor zich beweegt in de richting van het C-level-management. Van Biene-Hershey (2004) stelt dat de IT-auditor de effectiviteit en efficiëntie van een organisatie dient te dienen. Probleem is dat de IT-auditor met vele opdrachtgevers te maken heeft. De vraagstelling van een CIO bij een groot concern is anders dan de vraagstelling van de Chief Financial Officer (CFO). De accountant heeft daarnaast weer heel andere vragen aan de IT-auditor. Hierna wordt kort ingegaan op de vragen van enkele opdrachtgevers, waarbij ook drie dilemma's worden verwoord.

4.2 Vragen van de CIO

Het loont naar mijn mening de moeite of – nog sterker – het is absoluut noodzakelijk om meer tijd te spenderen aan het verkennen van de vraagkant in plaats van de aanbodgedreven houding van diverse

IT-auditors. Gelet op de fase van volwassenheid – veertig jaar is een mooi omslagpunt – is het moment daar om met open vizier de vraagzijde tegemoet te treden. De vraagzijde van IT-auditdiensten heeft daarvoor ook materiaal beschikbaar. Zo wordt periodiek over de agenda van de CIO gepubliceerd (Gartner Group, 2004). Aanvang 2004 werd gesteld dat 'An economic recovery is underway and enterprises are looking to grow. IT is a catalyst for growth, enhancing business effectiveness, business efficiency and operational integrity'. Vooral het laatste punt refereert aan het voldoen aan wet- en regelgeving, beveiliging, en dergelijke.

Eind 2004 stellen Gartner-analisten dat IT-professionals meer betrokken zullen raken bij de business-operatie en dat IT-beslissingen aansluiting moeten hebben met de businessstrategie en de financiële doelstellingen van de onderneming (Gartner Group, 2005). Kernpunt is dat het algemeen management vraagt om vereenvoudiging van IT-oplossingen, en dat de CIO hierop zal dienen in te spelen. Verder lijkt het aannemelijk dat veel organisaties met meerdere IT-leveranciers te maken krijgen, 'best-of-breed'-oplossingen worden geprefereerd. De eerder vermelde korte en bondige managementvragen dienen in het veranderende IT-speelveld te worden beantwoord.

Dilemma 1:

De CIO wil een IT-organisatie laten doorlichten op efficiency en effectiviteit. Het gevoel bestaat dat de IT-kosten te hoog zijn en ook op basis van externe benchmarks is dit al enigszins onderbouwd. Een IT-auditor voert een intakegesprek bij deze organisatie. Gaandeweg het gesprek wordt duidelijk dat de CIO vooral een probleem heeft met de IT-manager en de uitkomsten van de audit lijkt te willen gebruiken om de positie van de IT-manager te ondergraven. De IT-auditor dient nu kritisch te zijn en na te gaan of hij de aanleiding van de audit kan objectiveren en ook of hij zinvol op deze vraag kan inspelen. Dit refereert aan het begrip 'rationaliteit' van een opdracht. De 'klant is koning' is een belangrijk uitgangspunt, echter soms bevindt de klant zich buiten de gestelde grenzen. Het dilemma is of deze vraag wel passend te beantwoorden is volgens de Gedrags- en Beroepsregels (GBRE).

Het is niet op voorhand duidelijk of het eenvoudiger of complexer wordt om deze vragen te beantwoorden, maar minimaal is wel duidelijk dat er de nodige uitdagingen zijn voor een IT-auditor. De Amerikaanse Accountantorganisatie publiceerde aanvang 2005 dat het belangrijkste technologie-issue voor 2005 informa-

tiebeveiliging is (American Institute of Certified Public Accountants, 2005). Hiermee zijn we aanbeland bij één van de pijlers van het werkkterrein van IT-auditors. Vraag en aanbod van IT-auditdiensten kunnen op dit gebied dus relatief gemakkelijk 'op elkaar' worden gelegd.

4.3 Accountantsvragen

Er wordt volop gepubliceerd over IT-trends in relatie tot managementverantwoordelijkheden, maar ook het accountantsberoep publiceert over de door hem te beantwoorden IT-vragen. In het promotieonderzoek van Fijneman (1999) en meer recent door Roos Lindgreen (2002) is over dit laatste het nodige gezegd. In een in 2004 gehouden enquête onder register-accountants is nog eens onderkend dat de IT-kennis bij accountants nog moet toenemen om de invloed van IT op de controle te kunnen bepalen (Nederlands Instituut voor register EDP-Accountants, 2004). De IT-auditor kan hier een goede taak vervullen, hij moet optimaal inspelen op de accountant als opdrachtgever. De accountantsvraag inzake IT spitst zich toe op de zekerheden die kunnen worden ontleend aan interne controles die in en rondom IT-systemen en -infrastructuur zijn opgenomen. Daarbij is de primaire insteek de betrouwbaarheid en continuïteit van de financiële verslaglegging en de daarvoor relevante processen en IT-oplossingen. De IT-auditor dient in samenspraak met de accountant tot een goede afbakening van de te beoordelen IT te komen en aansluitend een auditprogramma uit te voeren. De te beantwoorden vraag is zo oud als het IT-auditberoep zelf, maar bezorgt toch nog hoofdbrekens. In de praktijk zijn al goede oplossingen zichtbaar, vraag en aanbod moeten elkaar echter nog optimaler gaan vinden.

Dilemma 2:

Een IT-auditor wordt ingeschakeld bij de uitvoering van de jaarrekeningcontrole van een organisatie. De accountant treedt op als opdrachtgever van de IT-auditor. Stel dat in dit voorbeeld de accountant een zeer afgebakende opdracht voor de IT-auditor definieert, waarbij de IT-auditor het gevoel krijgt dat hij geen toegevoegde waarde kan leveren naar de organisatie of wellicht nog erger niet op verantwoorde wijze tot de gevraagde beantwoording kan komen. Hoe moet de IT-auditor met dit dilemma omgaan? De gedrags- en beroepsregels van de Nederlandse Orde van EDP-auditors schrijven voor dat een IT-auditor slechts rationele opdrachten mag aanvaarden waarbij hij beschikt over de juiste materiekkennis (NOREA, 2004b). Dit dient in de gegeven situatie de IT-auditor met de

accountant te bespreken als onderdeel van de opdracht-aanvaarding.

4.4 Vragen van het algemeen management

Fijneman (2004) beschrijft hoe de managementvraag zich toespitst op het volgende: 'Hoe kunnen we als management melden dat we de IT in de greep hebben en hoe kunnen we dit ook continu aantonen?' Ook het accountantsberoep spreekt steeds vaker over IT Governance. Zowel de interne als de externe IT-auditor kan een uitstekende rol vervullen zodat een IT Governance-mededeling kan ontstaan. In figuur 1 wordt de opbouw van een dergelijke mededeling schematisch weergegeven.

Figuur 1. Het management van een organisatie kan aan de hand van deze figuur invulling geven aan de vraag of het de IT in zijn greep heeft. Het stelt daartoe een IT Governance-mededeling op, waarbij een IT-auditor de kwaliteit en de inhoud van dit proces toetst.

IT Governance lijkt evenwel enigszins een mode-woord. NOREA (2004a) stelt dat IT Governance een vergaande impact kan hebben op de rol, de werkzaamheden en de opleiding van IT-auditors. IT Governance richt zich daarbij op:

- het zorgdragen voor een heldere visie ten aanzien van IT;
- een goede aansturing en beheersing van IT-inspanningen;
- het afleggen van verantwoording hierover;
- het uitoefenen van toezicht hierop.

De betekenis en inhoud van IT Governance bezien vanuit vraag- en aanbodzijde van IT-auditdiensten zijn naar mijn mening nog niet geheel gelijkwaardig. Het is onmiskenbaar zo dat veel CIO's met IT Governance-projecten bezig zijn, echter niet altijd met inbreng van IT-auditors.

Dilemma 3:

Het management voert een omvangrijk IT-project uit, waarbij alle bestaande (deels eiland-)systemen worden vervangen door een geïntegreerd pakket. Het management wil de interne IT-auditor actief in dit project betrekken. Hierdoor kunnen tijdig alle benodigde interne controles worden gedefinieerd en geïmplementeerd. Tevens wil het management een certificaat van de interne IT-auditor ontvangen over de kwaliteit van de gerealiseerde interne controles. De interne IT-auditor aarzelt of hij deze rollen moet aanvaarden; het lijkt dat hij hiermee in conflict komt met zijn primaire auditfunctie in de organisatie. De IT-auditor aarzelt tussen een proactieve, adviserende rol versus een meer reactieve auditrol.

De vraag is aan de orde waar al deze verwachtingen en ontwikkelingen toe leiden. Roos Lindgreen (2004) stelt dat de IT-ontwikkelingen kunnen leiden tot een krimp- of een groeiscenario voor IT-auditors. In het krimpscenario wordt IT een dagelijks gebruiksmiddel, een wegwerpartikel. De industrie voorziet zelf in haar kwaliteitsstandaarden, IT-auditors worden steeds meer teruggedrongen. In het groeiscenario vergt de toenemende complexiteit van IT steeds diepgaander IT-audits. Roos Lindgreen kiest voor de groei, een optimisme dat de beroepsgroep graag volgt.

5 Toekomstvisie: lange en korte termijn

5.1 Lange termijn

In een seminar, gehouden in november 2004 ter gelegenheid van het afscheidscollege van Van Bienen-Hershey aan de Vrije Universiteit, schetsten Buijs en Harmzen het volgende beeld voor 2015: 'De Informatietechnologie is omgevormd tot Business Technology. De IT-industrie heeft haar standaarden op orde en laat deze ook certificeren. Het management wil vooral weten of de inzet van de businesstechnologie optimaal de bedrijfsdoelstellingen ondersteunt en wil op strategisch niveau geholpen worden door de IT-auditor'. Indien in dit toekomstbeeld wordt nagedacht over de relevante door IT-auditors te beantwoorden vragen, zien we de uitdaging voluit.

5.2 Korte termijn

Laten we echter eerst maar eens, in de tijd gezien dichter bij huis, de IT-audituitdagingen oplossen. In het jaarboek 2004/2005 van NOREA (2004b) bespreken enkele IT-auditors ontwikkelingen in het werkkterrein. Het valt op dat vooral het begrip control en de monitoring daarvan een expliciete IT-component

blijkt te bevatten. Brouwers (2004) beschrijft in zijn bijdrage de ontwikkelingen omtrent Sarbanes-Oxley. Deze wetgeving verplicht de accountant bij de aan de Amerikaanse beurs (Security and Exchange Committee) geregistreerde instellingen tot een toetsing van en mededeling over de kwaliteit van de beheersingsmaatregelen voorzover gericht op de kwaliteit van de financiële verslaglegging. Zowel het management van deze ondernemingen als de accountant onderkent dat er een serieuze IT-component te beoordelen is. Startpunt vormt echter het inrichten van de juiste IT controls. De IT-auditor wordt zichtbaar zowel in adviesrollen als in auditrollen. Het lijkt – zoals eerder is gesteld – materie te zijn die de IT-auditor terugbrengt bij de roots van zijn vakgebied. Of dit te beschouwen is als een limitering is wellicht een kwestie van smaak.

Ten Have (2004) schetst een soortgelijke ontwikkeling voor de publieke sector. Onder invloed van de regeringsnota 'Van Beleidsbegroting tot Beleidsverantwoording' is het management op zoek naar een verantwoording van zijn taken en vraagt auditors om deze verantwoordingen te toetsen. Ten Have stelt dat de IT-auditor om in te kunnen spelen op de managementvragen voor een grote uitdaging staat; hij heeft andere competenties, normen, instrumenten en aanpakken nodig. 'Van Beleidsbegroting tot Beleidsverantwoording' betekent niet alleen investeren in nieuwe IT-systemen, maar beslaat de gehele organisatie. De IT-auditor moet bij de departementen beoordelen of de informatiekundige gevolgen voldoende aan de orde zijn geweest.

Koning (2004) schetst vanuit zijn functie als toezichthouder bij De Nederlandsche Bank een soortgelijk beeld. In de bancaire sector moeten instellingen voldoen aan specifieke regelingen zoals de Regeling Organisatie Beheersing en Basel II. De IT-auditor kan zijn bijdrage leveren als hij het beoordelen van c.q. het adviseren over IT-risico's weet in te passen in het denken omtrent operationele risico's.

Kortom, er dienen zich nieuwe toepassingsgebieden aan voor de IT-auditor. Dit zijn niet per se verbredingen van het werkkterrein, maar veeleer verdiepingen op zeer specifieke terreinen. NOREA spreekt in dit verband over een 'rekenschapsauditor' die kritisch meekijkt, denkt en participeert in het proces van verantwoording afleggen in plaats van een 'afrekenauditor' die achteraf komt.

6 Samenvatting en conclusies

De vraag dringt zich op hoe alle tot nu toe geschetste problemen kunnen worden opgelost. Het onderscheid

tussen adviseur en controleur is soms, met een kwinkslag, academisch van aard te noemen, echter in de praktijk zien we wel dat helderheid van belang is. Voor het verkrijgen van deze helderheid wordt hierna een aantal belangrijke initiatieven genoemd.

6.1 Assurancemodel

Als eerste is te wijzen op het verder uitwerken van het Assurancemodel (International Federation of Accountants, 2004). De soorten IT-audits dienen nader te worden gedefinieerd en te worden voorzien van vaktechnische voorschriften. Standaardisering van oordelen kan daarbij een hulpmiddel zijn. De huidige nuancerings naar verschillende niveaus van zekerheid blijken in de praktijk overigens ook problemen te veroorzaken. Een formulering als 'met een beperkte mate van zekerheid concluderen wij dat het IT-systeem betrouwbaar is' geeft de opdrachtgever niet het antwoord op de door hem gestelde vraag.

6.2 Ethische standaarden

Het uitwerken van ethische standaarden, waarbij de nadruk wordt gelegd op de 'principle based'-benadering. NOREA spreekt in een aantal publicaties al over een 'principle based'- in plaats van een 'rule based'-auditbenadering. NOREA zoekt aansluiting bij de Code of Ethics van de International Federation of Accountants. De Code of Ethics gaat uit van principes, in tegenstelling tot de huidige Gedrags- en Beroepsregels voor Register EDP-auditors die veel meer geboden en verboden bevatten (NOREA, 2004b).

De vijf beginselen uit de Code of Ethics zijn (Nederlands Instituut voor Register Accountants, 2004):

- 1 integriteit: duidelijk en eerlijk zijn in alle beroepsmatige en zakelijke relaties;
- 2 objectiviteit: geen beïnvloeding door vooroordelen, belangenverstrengeling of bovenmatige invloed van anderen bij de professionele en zakelijke oordeelsvorming, ofwel onafhankelijkheid;
- 3 deskundigheid en zorgvuldigheid: het op peil houden van vak kennis door middel van actuele ontwikkelingen in de praktijk, de wetgeving en de vaktechniek;
- 4 geheimhouding: het betrachten van geheimhouding ten aanzien van informatie die voortvloeit uit beroepsmatige en zakelijke relaties;
- 5 professioneel gedrag: het naleven van relevante wet- en regelgeving en zich onthouden van handelingen die het beroep in diskrediet brengen.

Normen moeten niet verworden tot standaardvragenlijsten die iedereen kan invullen. Het spreken over

een rekenschapsauditor die kritisch meekijkt, denkt en participeert in het proces van verantwoording afleggen in plaats van een afrekenauditor die achteraf komt, is een sterke uiting hiervan.

6.3 Kerncompetenties

Het verhelderen van de kerncompetenties van de IT-auditor en daarmee het benoemen van de identiteit van het vakgebied is zeer cruciaal.

Redenerend vanuit de primaire taak van de IT-auditor staat de attestfunctie centraal. Dit betekent niet per se een stap terug in de tijd, echter een logische stap in de evolutie van de IT-auditor. De auditingprincipes en -vaardigheden dienen op orde te zijn, ook als de IT-auditor als adviseur actief is. In de praktijk blijkt dat een IT-auditor in bepaalde opdrachten als controleur optreedt en daarnaast in andere opdrachten als adviseur. Juist deze kruisbestuiving maakt dat de IT-auditor in beide rollen groeit en maakt het vakgebied interessant voor studenten en toetreders, maar ook voor opdrachtgevers. De opdrachtgever weet dat hij een materiedeskundige binnenhaalt op het terrein van IT, die in staat is volgens verantwoorde werkmethodes zijn audit of advies uit te voeren.

Onafhankelijkheid en onpartijdigheid zijn voor de IT-auditor, in welke rol hij ook actief is, belangrijke voorwaarden. Zoals eerder vermeld zal het advieswerk van de IT-auditor zich vooral richten op IT-risico's en IT-beheersingsvraagstukken. Daarbij zal een IT-auditor bijvoorbeeld samenwerkingsverbanden met IT-leveranciers altijd vermijden. Dergelijke samenwerkingsverbanden worden juist wel vaker aangegaan door IT-consultants, hetgeen invloed heeft op de positie waarmee de opdrachtgever wordt benaderd. Bij de jaarrekeningcontroleklanten geldt per definitie dat elk 'advies' voort moet komen uit een primair beoordelende functie van de IT-auditor. De ruimte die er nog ligt bij auditklanten wordt mede bepaald of ze wel of niet beursgenoteerd zijn en op welke IT-object (wel of niet financieel gerelateerd) het advies betrekking heeft.

Van belang is verder dat de kerncompetenties worden vertaald in kennis- en opleidingstermen. Het begrip 'common body of knowledge' wordt hierbij geïntroduceerd. Dit begrip beschrijft een basisniveau aan kennis, kunde en vaardigheden die van een IT-audit-professional mogen worden verwacht. Hiermee wordt niet alleen binnen de beroepsgroep helderheid gegeven, maar juist ook aan de opdrachtgevers. Een

'common body of knowledge' kan de eindtermen van de IT-auditopleidingen aanscherpen en voor NOREA een toetsingsinstrument bieden. Figuur 2 geeft in het kort een eerste indeling naar onderwerpen.

Figuur 2. Een 'common body of knowledge' beschrijft de kennisgebieden die iedere IT-auditor paraat moet hebben. Daarbovenop ontstaan specialisaties naar IT-objecten of markten.

Tot slot het volgende. Voor de opdrachtgevers geldt dat voor kwaliteitsvragen over IT-risico's en IT-beheersing de IT-auditor bij uitstek een geschikte gesprekspartner is. Of een opdrachtgever een controleur zoekt of een adviseur doet daarbij niet zoveel ter zake, als het probleem van het management maar wordt opgelost. ■

Literatuur

- American Institute of Certified Public Accountants, (2005), *2005 Top Technology Survey*.
- Biene-Hershey, M.E. van, (2004), *Audit van IT en het IT-auditberoep*, afscheidsrede Vrije Universiteit, Amsterdam.
- Brouwers, P.P.M.G.G., (2004), *Papieren tijgers moeten tot leven komen*, in: *Jaarboek 2004/2005 Nederlandse Orde voor Register EDP-auditors*, Amsterdam, pp. 15-16.
- Fijneman, R.G.A., (2004), *Beat IT or Control IT*, in: *Kracht van de vernieuwing, Visies op ICT*, Amsterdam.
- Fijneman, R.G.A., (2005a), *IT auditing: grenzeloos of gelimiteerd?*, inaugurele rede, Tilburg.
- Fijneman, R.G.A., (2005b), *IT auditor: adviseur of controleur*, in: *Automatiseringsgids*.
- Fijneman, R.G.A., (1999), *De betekenis van 'jaarrekening ICT-auditing' als onderdeel van de jaarrekeningcontrole, 'Common body of knowledge'. Consequenties voor de accountantsopleiding*, Tilburg.
- Gartner Group, (2004), *Preparing for the Upswing: The 2004 CIO Agenda*.
- Gartner Group, (2005), *10 CIO resolutions for 2005: Re-asses your role, embrace change and have a backup plan*.
- Have, M. ten, (2004), *IT-auditor beoordeelt waarborgen voor de publieke sector*, in: *Jaarboek 2004/2005 Nederlandse Orde van Register EDP-auditors*, Amsterdam, pp. 16-17.
- International Federation of Accountants, (2004), *International framework for Assurance engagements*.
- Kessel, P. van, (2005), *Interview IT-auditor: adviseur of controleur?*, in: *de EDP-auditor* 2005-3, pp. 44-47.
- Kocks, H.C., (1991), *EDP-auditing teneinde ... of zwart schaap met vijf poten*, inaugurele rede, Rotterdam.
- KPMG (2004), *Factsheet KPMG Information Risk Management*, Amstelveen.
- Koning, E. (2004), *Toezicht: in principe onder vier ogen*, in *Jaarboek 2004/2005 Nederlandse Orde van Register EDP-auditors*, Amsterdam, p. 17, 19.
- Mollema, K.I.J. (1999), *IT-auditing in an integrated audit concept*, inaugurele rede, Rotterdam.
- Moonen, H.B., (1991), *Kwaliteitsnormen bij EDP-auditing: een kritische beschouwing*, inaugurele rede, Tilburg.
- Nederlands Instituut voor Register Accountants, (2004), *Trends in Accountancy, brancheverkenning, 2004-2005*, Amsterdam.
- Nederlandse Orde voor Register EDP-auditors, (1997), *Studierapport 2, Een kwaliteitsmodel voor Register EDP-auditors*, Amsterdam.
- Nederlandse Orde voor Register EDP-auditors, (1998) *Geschrift no. 1, IT-auditing aangeduid*, Amsterdam.
- Nederlandse Orde voor Register EDP-auditors, (2004a), *IT Governance, een verkenning*, Amsterdam.
- Nederlandse Orde voor Register EDP-auditors, (2004b), *Jaarboek 2004/2005*, Amsterdam.
- Pijl, G.J. van der, (2000), *IT auditing in a changing world*, inaugurele rede, Rotterdam.
- Roos Lindgreen, E., (2002), *Over informatietechnologie, accountancy en informatiebeveiliging*, Amsterdam.
- Roos Lindgreen, E., (2004), *IT-auditing: krimp of groei?*, in: *Kracht van de vernieuwing, Visies op ICT*, Amsterdam.
- Zee, H. van der, (2002), *Measuring the value of Information Technology*, Tilburg.

www.deloitte.com
www.ey.nl
www.isaca.org
www.kpmg.com
www.pwc.com