# IT-audit en operational audit: eenmanszaken of maten?

**Peter Hartog en Ron de Korte**

Is het niet verwonderlijk dat IT-audits binnen veel organisaties los staan van de andere audits die worden uitgevoerd? En is het niet vreemd dat veel operational auditors met een boog om de geautomatiseerde systemen heen lopen? In dit artikel wordt ingegaan op de overeenkomsten én verschillen tussen IT- en operational audits. Vanzelf wordt dan ook uitgekomen op de mogelijkheden (soms zelfs noodzaak!) tot samenwerking en de rollen van beiden daarin. We definiëren Management Control auditing en zien dat als een toekomstvaste auditvorm waarin we niet zonder elkaar kunnen.

## Inleiding

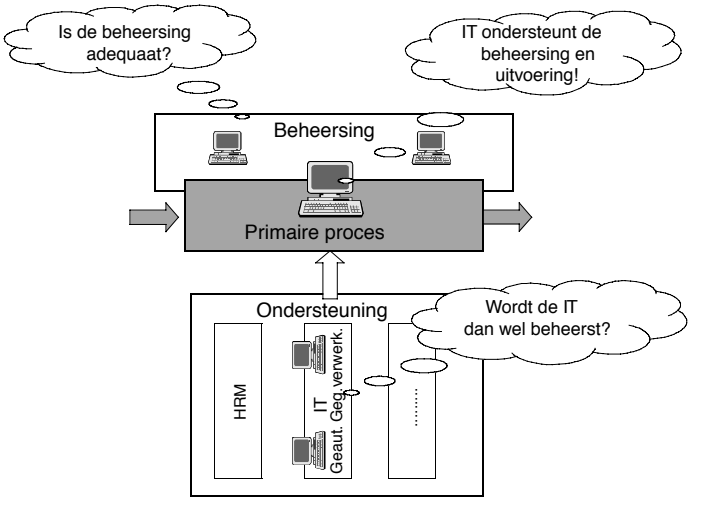
Dit artikel is als volgt opgebouwd. Gestart wordt met een overview van audit en de positie van de operational audit en IT-audit daarbinnen. Daarbij vergelijken we operational audit met IT-audit en stellen we de overeenkomsten en verschillen vast.
Vervolgens wordt ingegaan op de vraag waar deze vakgebieden elkaar kunnen (of moeten) aanvullen en hoe dit kan worden gerealiseerd.

Drs P.A. Hartog CIA is senior auditing consultant bij ACS en docent van de pao Internal/Operational Auditing van de Erasmusuniversiteit Rotterdam.
R.W.A. de Korte RA RE RO is plv. Program Director van de postacademische opleiding Internal/Operational Auditing, docent van de pao EDP-auditing (EUR), associate van ACS en mede-initiatiefnemer van de kennissite www.auditing.nl.
Delen van dit artikel zijn eerder in Informatie, nr. 47/1, verschenen onder de titel 'IT- en operational auditing vloeien in elkaar over'.

## IT- en Operational auditing in verwondering naast elkaar

In dit artikel wordt ingegaan op de relatie en verschillen tussen IT-auditors en operational auditors. Juist met hen vanwege de overlap van hun brede objectgebieden. Operational auditors geven een oordeel over de kwaliteit van de beheersing van de organisatie. Beheersing wordt daarbij veelal ruim geïnterpreteerd als het geheel van maatregelen dat moet waarborgen dat de doelstellingen zullen worden bereikt. Een belangrijk deel van die maatregelen wordt met IT ondersteund. En een deel van die beheersmaatregelen is ook juist weer belangrijk om risico's uit hoofde van de toepassing van IT te beperken. Anders gezegd, de beoogde organisatiedoelen zijn vaak slechts door toepassing van IT realiseerbaar; de realisatie van de doelstellingen kan echter ook staan of vallen met een voldoende beheersing van de toepassing van IT. IT kan tenslotte de 'enabler' vormen voor nieuwe, meer ambitieuze organisatiedoelen. Voldoende reden tot verwondering van het naast elkaar bestaan van IT- en operational auditing.

Overigens leiden beide auditvormen ook op zichzelf al tot enige verwondering. Operational auditing (OA) blijkt in de praktijk een containerbegrip: de 'leek' denkt aan 'het




*Figuur 1. Samenhang objecten van IT- en operational auditing*

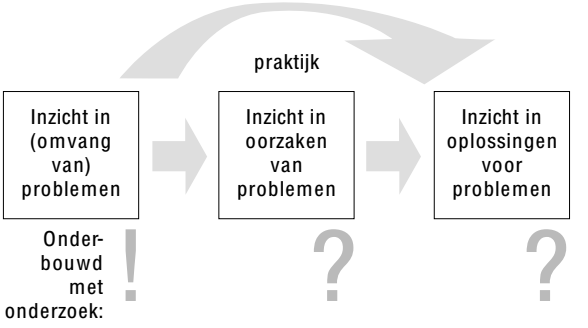
auditen van de operatie' en vertaalt dit naar procesaudits (gericht op de operationele, dagelijkse bedrijfsvoering). De accountant definieert het soms als de interim controlewerkzaamheden gericht op de AO/IC. De (oudere) literatuur benadrukt veelal een top-down benadering gericht op de controle van de naleving en uitwerking van door het topmanagement uitgevaardigde 'tight controls' (centrale beheersmaatregelen). Operational auditing is daarmee een vakgebied dat ook wordt opgeëist door onder meer internal auditors, accountants, controllers, kwaliteitsauditors en consultants.
Ook EDP- of IT-auditing kent een breedte die regelmatig tot discussies leidt. Nadruk ligt dan vaak op de interpretatie van de term 'auditing'. Ben je als IT-auditor als 'koning één-oog' in veel 'blinde' organisaties niet automatisch specialist en 'adviseur'? Zijn IT-auditors vooral 'ICT-techneuten' of redeneren zij vanuit de organisatiedoelstellingen? In die laatste visie is er een grote overlap met de moderne operational auditor. We zien enkele post doctorale opleidingen dan ook naar elkaar toe groeien, leidend tot een eenjarige opleidingsvariant voor IT-auditors tot Internal/operational auditor en vice versa.

## Overeenkomsten en verschillen

### Overeenkomsten

Zowel operational- als IT-auditing zijn vormen van auditing. Dit betekent dat hun primaire product bestaat uit het geven van een oordeel op basis van onderzoek[1].
Echter, vanuit een streven om op voorhand de toegevoegde waarde van die onderzoeken te benadrukken, spreken auditors in de praktijk snel over aanbevelingen en advies.

Een gemeenschappelijk probleem is derhalve dat auditors denken met onderzoeken gericht op het geven van een oordeel een te beperkte toegevoegde waarde te leveren. 'Het management wil niet alleen horen dat het niet goed is, maar wil weten hoe het op te lossen', is dan het argument van de auditor.
In die uitspraak komt het onderzoekstechnische probleem scherp naar voren: om 'het' op te lossen moet niet alleen een onderzoek zijn gedaan naar het verschil in de gewenste en de feitelijke situatie (een zogenaamd probleemsignalerend onderzoek), maar dient tevens bekend te zijn of te zijn onderzocht, wat de oorzaken zijn van dit verschil (een diagnostisch onderzoek).
Pas nadat de oorzaken bekend zijn, kan gericht onderzoek plaatsvinden naar aangedragen mogelijke oplossingen of naar een blauwdruk die de oorzaken van de verschillen tussen gewenste en feitelijk situatie in voldoende mate zal wegnemen (ontwerpgericht onderzoek) [OTTE02], [KORT03].




*Figuur 2. Onderbouwing van 'adviezen' in de praktijk*

Hier gaat het in de praktijk veelvuldig mis.
Probleemsignalerende audits worden vaak beëindigd met een advies[2], zonder dat de oorzaken expliciet zijn bekeken. Hierdoor ontstaat een groot risico dat de voorgestelde oplossing niet de werkelijke oorzaken weg zal nemen. Temeer daar de auditor vaak niet heeft gekeken (en gezien de scope en beperkte middelen ook niet heeft kunnen en hoeven kijken) naar de totale context waarin de problematiek zich afspeelt. De manager zal de geschetste problematiek echter wel plaatsen in de context van zijn totale verantwoordelijkheidsgebied en aldus veel meer factoren betrekken bij de afweging of en hoe het probleem op te lossen. Vaak geeft dat hem andere inzichten en een andere prioriteitstelling, waardoor slechts een deel van de aanbevelingen wordt opgevolgd.
Omgekeerd zien we in veel gevallen dat auditors (standaard) probleemsignalerende audits uitvoeren, terwijl het

management eigenlijk al op de hoogte is van het probleem en daarom meer gebaat is bij een diagnostische audit.

In plaats van aan de achterkant hoort de adviesfunctie aan de 'voorkant' van de audit te liggen. De auditor adviseert de opdrachtgever over het type audit, de doelstelling en scope van het onderzoek, en helpt mogelijk bij het detailleren van de gehanteerde theorieën en frameworks die als basis voor het normenkader worden gebruikt. Zonder uitzondering accordeert de opdrachtgever de te hanteren normering.

Een andere belangrijke overeenkomst is dat beide vormen (voor een belangrijk deel) 'systeem'-audits zijn. In tegenstelling tot 'performance'-audits die zijn gericht op een beoordeling van de uitkomsten zelf, zijn systeemaudits gericht op de waarborgen die er bestaan dat deze uitkomsten naar wens zullen zijn. In de praktijk betekent deze overeenkomst dat we elkaars taal redelijk spreken.
Men zou het doel van de audit kunnen omschrijven als het verminderen van de onzekerheid of het beperken van het risico van de opdrachtgever (of derden) door kennis toe te voegen. Of we de audit dan (meer specifiek) aanduiden als operational of als IT-audit is voor de opdrachtgever niet interessant; de voor de audit benodigde kennis bepaalt de audit-teamsamenstelling. Zodra de beheersmaatregelen worden beïnvloed door informatietechnologie of juist betrekking hebben op een IT-beheer- of IT-ontwikkelorganisatie, is specifieke IT-kennis snel onontbeerlijk. Geconcludeerd kan dan ook worden dat IT-auditors en operational auditors elkaar met regelmaat tegen moeten komen.

Dan is er nog de overeenkomst in de samenwerking met de register accountant. Zowel IT-audit als operational audit heeft een haat-liefde-verhouding met de financial auditdiscipline. Aan de ene kant vinden we dat we niet op onze waarde worden geschat en constateren we dat 'de gemiddelde RA' minimaal uitstraalt 'het wel zelf te kunnen'. Die uitstraling is mogelijkerwijs terug te voeren op onbekendheid met de problematiek.
Aan de andere kant zien we de RA zich op terreinen begeven waar wij vinden dat hij dat niet alleen kan.
Ook bij 'in control'-verklaringen wordt (zowel nationaal als internationaal) als eerste gekeken naar de financial auditor, hetzij als een (meer of minder) onafhankelijk opgehangen interne accountantsdienst, hetzij als de externe accountant met zijn bij wet geregelde certificerende functie. De oplettende RA kent vervolgens de RE en RO een plek toe in zijn multidisciplinair samengestelde auditteam. In de praktijk echter ontstaat er nogal eens een aannemer-onderaannemer-relatie, waarbij de onderaannemer kan worden opgezadeld met een onmogelijke opdracht of vraagstelling, zoals: 'verklaar even dat dit systeem 'in control' is'. Vaak ontbeert de RA als hoofdaannemer de tijd of kennis om de vraagstelling en normstelling duidelijk te omschrijven.

Vanzelfsprekend zijn er ook verschillen. Die bespreken wij door nader in te gaan op het specifieke van beide auditvormen.

## Verschillen

De belangrijkste verschillen zijn (enigszins gestileerd) weergegeven in tabel 1. Deze zullen daarna worden toegelicht in de paragrafen IT-auditing en Operational auditing.

*IT-auditing*
Het specifieke van IT-auditing is vanzelfsprekend in belangrijke mate gelegen in haar objectgebied, de 'IT'. Dit objectgebied is breed. 'De IT' is een ongrijpbaar begrip. IT wordt in een audit pas hanteerbaar zodra het

| | **IT-auditing** | **Operational auditing** |
|---|---|---|
| Reikwijdte rol | Toetsend + (in praktijk veelal ook) inrichtend | Toetsend – verschaffen van additionele zekerheid |
| Object | IT (in al zijn facetten) | Beheersing organisatiedoelen (organisatie-eenheden, processen, thema's) |
| (Kwaliteits)aspecten | Focus op betrouwbaarheid (integriteit) en continuïteit | Alle KSF'en gebaseerd op organisatiedoelstellingen |
| Aard controls | Focus op technisch organisatorische controls | Technisch én sociaal organisatorische controls |

*Tabel 1. De belangrijkste verschillen van IT-auditing en Operational auditing*

wordt benaderd op specifieke onderdelen, zoals het informatiemanagement, de informatiesystemen (applicaties), de gebruikers, de hardware en de IT-organisatie. In de handreiking 'Oordelen van gekwalificeerde IT-auditors' wordt IT-audit als volgt omschreven:
*'IT-audit is de discipline die zich bezighoudt met het beoordelen van en adviseren over de kwaliteit van de informatieverwerking in een omgeving waarin sprake is van informatietechnologie ten behoeve van de beheersing daarvan.'*

Opvallend is dat deze definitie breder is dan de essentie van auditing, zijnde het geven van een oordeel aan de opdrachtgever. In artikel 1 van de Gedrags- en Beroepsregels EDP-auditors (GBRE) staat een definitie van de attestfunctie: *'het geheel van activiteiten dat is gericht op het afgeven van een oordeel'*. In het NOREA-studierapport nummer 2 (kwaliteitsmodel voor Register EDP-auditors[3]) wordt de attestfunctie weliswaar 'de primaire taak van de Register EDP-auditor' genoemd, maar tevens opgemerkt: *'Naast de attestfunctie kan de Register EDP-auditor gevraagd worden om als adviseur op te treden. Ook is het mogelijk dat Register EDP-auditors worden ingeschakeld om het management te ondersteunen of zelfs daadwerkelijk zaken uit te voeren.'* Let daarbij op het woordje 'zelfs'.
In de praktijk zien we IT-auditors met enige regelmaat inderdaad de adviesrol (of zelfs de rol in de lijn) nog wel eens innemen. De IT-auditor is vaak bij uitstek de specialist en wordt daarmee snel adviseur. In plaats van een auditrol vervult de IT-auditor bijvoorbeeld de rol van lid in het project en helpt mee bij het definiëren van de specs. Hij is immers snel de enige die verstand heeft van 'beveiliging' en van het creëren van de 'audit trail'.

De RE treedt, op het moment dat hij instemt met het verzoek bovenstaand genoemde overige werkzaamheden uit te voeren, nadrukkelijk niet op als auditor in de gangbare definitie van dat begrip. Overigens geldt deze rolbeschrijving (rolbeperking) ook voor de operational auditor en is het Instituut of Internal Auditors (IIA) duidelijk wanneer het gaat om implementatiewerkzaamheden: deze zijn voor internal auditors niet toegestaan!

Een belangrijk deel van de IT-audits richt zich op beveiliging en beheersing. Deze begrippen zijn dan veelal teruggebracht tot betrouwbaarheid (van de uitkomsten van het geautomatiseerde proces), integriteit (van de opgeslagen data) en continuïteit (van het geautomatiseerde proces). Mogelijkheden tot verbreding zijn er echter te over. Denk bijvoorbeeld aan de invloed van IT-toepassingen op het gedrag van gebruikers, mogelijkheden tot ondersteuning in het kader van management control of van innovatie en het leervermogen van een organisatie.
Dit zijn interessante gebieden waarin kennis van IT goed van pas kan komen of zelfs essentieel is. Daarmee komen IT-auditor dicht bij hun operational audit-collega's.

*Operational auditing en de ontwikkeling tot Management Control auditing*
Het doel van een operational audit definiëren wij als: *het geven van additionele zekerheid aan de opdrachtgever (of via die opdrachtgever aan derden) over de kwaliteit van de beheersmaatregelen gericht op het realiseren van de organisatiedoelen.*

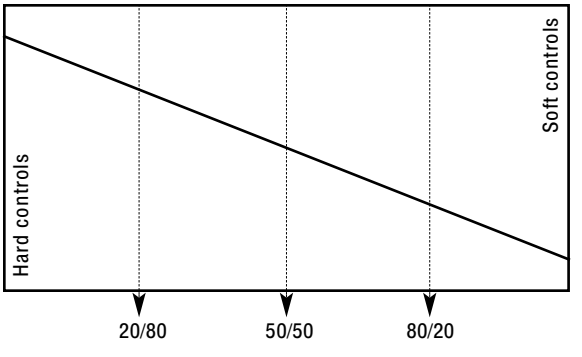
Het geven van *additionele* zekerheid betekent dat de opdrachtgever over het object van onderzoek al over kennis beschikt, maar redenen ziet om aan een auditor een oordeel te vragen dat gebaseerd is op een gedegen onderzoek. Die redenen kunnen voortkomen uit de behoefte aan een onafhankelijk oordeel van een derde (bijvoorbeeld voor een toezichthouder), maar bijvoorbeeld ook uit de wens om informatie die niet wordt geleverd door de reguliere informatiesystemen en overlegvormen. Belangrijk is dat de auditor niet in de plaats treedt van de verantwoordelijk manager en dat de audit geen onderdeel uitmaakt van de reguliere informatieverschaffing die is benodigd voor het beheersen van de organisatie.

Het objectgebied van de operational auditor is de beheersing ofwel 'management control'. De beheersing kan processen en organisaties betreffen, maar ook thema's zoals integriteit, klantgerichtheid of verandervermogen. Operational auditors investeren daartoe in kennis van verschillende control frameworks.
Accountants daarentegen redeneren van oudsher voornamelijk vanuit het gedachtegoed van Starreveld et al. Vanuit hun controleopdracht formuleren zij de betrouwbaarheid van de informatie vaak als belangrijkste doelstelling en toetsen de inrichting vanuit het mensbeeld dat medewerkers vooral de persoonlijke doelen (kunnen) nastreven.
Het denken over 'control' van IT-auditors (RE) is veelal in lijn met dat van de RA, van oorsprong de grootste opdrachtgever van veel IT-auditors. Deze zoeken naar mogelijkheden tot het automatiseren van beheersmogelijkheden. Wanneer het systeem de Starreveld-functiescheidingen en -controles afdwingt, heeft het management een zorg minder. Kijkend naar de beheersing van de IT-organisatie hanteert de RE overigens veelal een aanmerkelijk bredere focus. Dan wordt onderkend dat de wijze van samenwerken, stijl van leidinggeven, cultuuraspecten, verandervermogen et cetera een belangrijke

invloed hebben op de mate waarin de beschreven procedures worden nageleefd. Noem het een verschil tussen opzet en werking.

De operational auditor moet eerst nagaan hoe het (top)management denkt over de beheersing van het object. De inrichtingseisen vloeien daar logischerwijs uit voort. De informatie en betrouwbaarheid daarvan is dan slechts één van de onderzoeksobjecten. Natuurlijk met de (betrouwbaarheids)eisen vanuit wet- en regelgeving als minimumnorm.
Daarbij is het belangrijk te benadrukken dat het voor de manager (en dus voor de auditor) niet alleen gaat om de betrouwbaarheid, maar om alle van toepassing zijnde doelen en kritieke succesfactoren van het object dat de operational auditor in beschouwing neemt. Juist de beheersing van mogelijk tegenstrijdige doelen en hoe met die tegenstrijdigheid om te gaan, is een belangrijk aandachtspunt van de operational auditor.

De verschillende control frameworks hanteren vaak een andere definitie en invulling van beheersing. Zo bestaan er belangrijke verschillen in de mate waarin aandacht wordt besteed aan de 'soft' controls ofwel de sociaal-organisatorische maatregelen, zoals de motivatie, cultuur en managementstijl. Hoewel deze aspecten vaak worden bestempeld als moeilijk meetbaar en daardoor leidend tot subjectieve oordelen, weet iedereen hoe sterk deze 'zachte' aspecten bepalend zijn voor het goed functioneren van de organisatie. We zien dan ook een toenemende belangstelling en integratie van deze aspecten in operational audits.
Vaak wordt door auditors gebruikgemaakt van het COSO-model en het daarin opgenomen 'Control Environment'. Wij merken op dat deze criteria zich kenmerken door een sterk instrumentele benadering van 'soft' controls en vooral procedureel van aard zijn. Dit maakt het relatief makkelijk te auditen, maar doet concessies aan 'de werkelijkheid'. Een alternatief is meer inhoudelijk (en daarmee meer diepgaand) te kijken naar de sociaal organisatorische controls. Een onderzoeksvraag kan dan bijvoorbeeld zijn: 'Is de stijl van leiding geven passend bij de aard van de taken?' of 'Is de managementstijl consistent met de beoogde cultuur?' In dat geval is het nodig om gebruik te maken van theorieën uit andere vakgebieden, zoals uit de sociale wetenschappen.

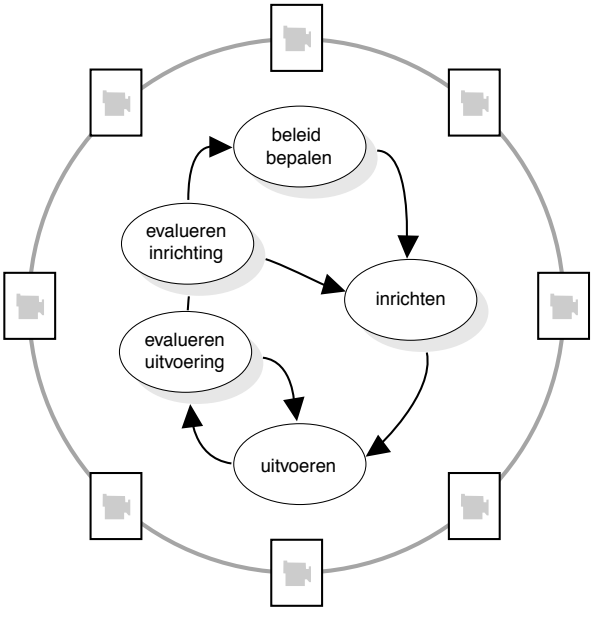



*Figuur 3. Relatieve belang van 'hard' en 'soft' controls*

Het (relatieve) belang van de diverse (technisch én sociaalorganisatorische) controls is overigens afhankelijk van het type organisatie, haar kritieke succesfactoren en de dynamiek waarin deze zich bevindt. In een stabiele situatie zou de beheersing zich kunnen richten op het afdekken van bekende risico's door het met gedetailleerde procedures en richtlijnen 'dichttimmeren' van de organisatie. In een onvoorspelbare, dynamische omgeving wordt echter meer flexibiliteit en verandervermogen vereist.
In de eerste situatie kan de nadruk meer liggen op technisch organisatorische controls, terwijl in de tweede situatie aandacht voor de sociaal organisatorische controls extra belangrijk zijn. Taakgerichte, gedetailleerde regelgeving is dan immers minder zinvol. Er moet voor de aansturing van medewerkers meer worden gesteund op meer abstracte, doelgerichte uitgangspunten, waarbinnen de medewerkers zelf beslissingen nemen [HART03].
In het algemeen kan worden gesteld dat het relatieve belang van sociaal organisatorische controls in de beheersing van de organisatie toeneemt. Dit komt door sociale ontwikkelingen zoals het opleidingsniveau en de mate van 'empowerment' van medewerkers en de (hiervoor beschreven) toenemende complexiteit en dynamiek van de omgeving waarin organisaties opereren.

De enorme breedte van het (in de praktijk gehanteerde) begrip operational auditing is aanleiding tot het gebruik van een nieuwe term voor audits die zich richten op de gehele management control cyclus (zie figuur 4): Management Control Auditing (MCA) [PAAP99].

Door audit expliciet te positioneren buiten die management controlcyclus, wordt het managementproces als geheel object van onderzoek. Zo kan de auditor ook worden gevraagd te beoordelen of de organisatiedoelen hebben geleid tot adequate aanpassingen in de organisatie-inrichting, of signalen uit de evaluaties hebben geleid tot voldoende aanpassingen van de inrichting of de doelen. Het onderzoeken van de management controlcyclus betekent kijken naar het leer- en verandervermogen van de organisatie, rekening houdend met de dynamiek van de omgeving. Zaken waar veel operational auditors mogelijk nog niet volledig voor zijn geëquipeerd of door




*Figuur 4. De management control cyclus en audit*

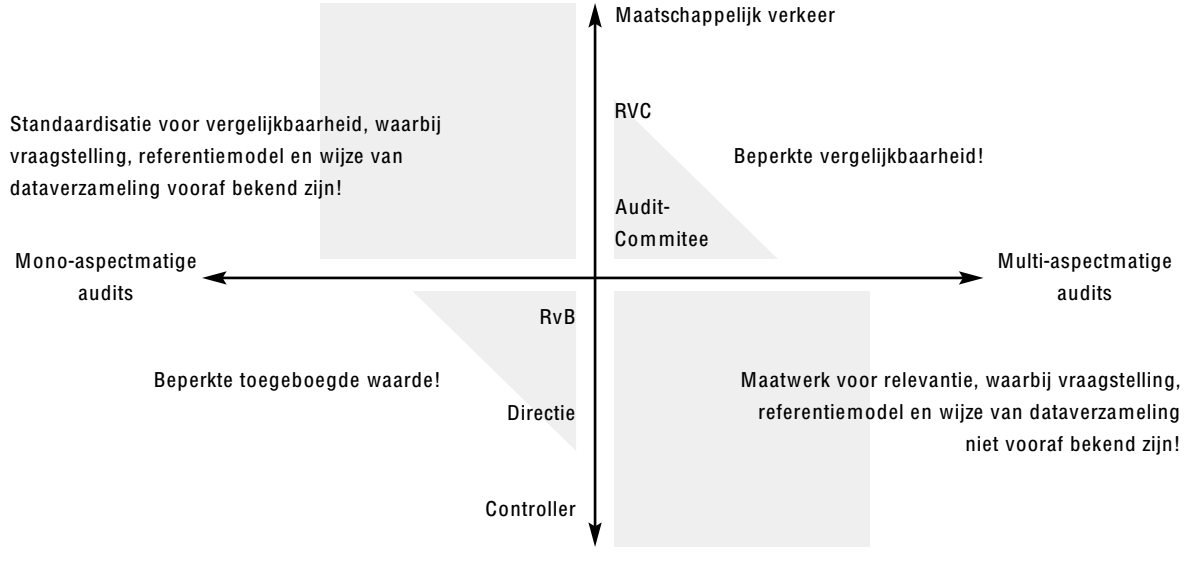
het management nog niet voor worden gevraagd. Wij zien het echter als dé insteek om te komen tot een waardevolle 'in control'-verklaring. Het is bovendien dé manier om audit op executive-niveau aan tafel te krijgen, in lijn met het auditberoep eigene, en zonder je zorgen te hoeven maken over de toegevoegde waarde van je acteren als auditor.

## Soorten audits en de basis voor samenwerking

De verschillende soorten auditopdrachten: globaal bezien is het voor de auditor zeer bepalend wie we als gebruiker van de audituitkomsten voor ogen hebben (zie figuur 5).

Audits ten behoeve van het maatschappelijk verkeer, of het topmanagement die de uitkomsten gebruikt voor zijn stakeholders, kenmerken zich door algemene toepasbaarheid; standaardisering. Voorbeelden zijn de jaarrekeningcontrole en audits naar de compliance met relevante regelgeving. Ook de op COSO-gebaseerde Sarbanes Oxley-normering (voorzover uitgewerkt) valt hieronder. Voor IT-audits kan worden gedacht aan een algemeen statement over de kwaliteit van de informatiebeveiliging gebaseerd op de Code van Informatiebeveiliging of een audit op basis van SAS70. Een voorbeeld van een operational audit is ook de beoordeling van 'in control statements' van de diverse business units binnen een holding. Het is voor elk van deze audits belangrijk dat aan de uitkomsten van elke audit die volgens die normering is uitgevoerd dezelfde betekenis mag worden toegekend. Wetgeving zoals Sarbanes Oxley en Tabaksblat doen dit type audits in belang toenemen.

Aan de andere kant van het continuüm staan de specifieke, meer maatwerkgerichte audits: de opdrachtgever heeft een concrete auditvraag geformuleerd, die op dat moment specifiek voor hem relevant is. Daarbij is de algemene




*Figuur 5. Diverse soorten audits*

normering (indien relevant) hoogstens te zien als minimumnormering, die moet zijn geïncorporeerd in de normering die voor die specifieke audit geldt. Juist hier ervaart het (lagere) management de toegevoegde waarde van de auditors, door het toegesneden zijn van de audit op de eigen specifieke kennisbehoefte.

Natuurlijk zijn in dit continuüm vele voorbeelden te bedenken die in de ruimte tussen deze uitersten te plaatsen zijn. De beoordeling van de mate waarin decentrale organisaties zich, onder toepassing van integraal management, houden aan de 'tight controls' vanuit het hoofdkantoor, is een vorm van audit die dicht tegen de standaard audits aan ligt en een belangrijk onderdeel uitmaakt van het auditjaarplan van onder meer de grote financiële instellingen.

Bovengenoemd onderscheid tussen standaard en maatwerk heeft belangrijke implicaties voor de samenwerking tussen de IT- en operational auditor. Daarbij kan het uitvoeren van beide soorten audits de auditafdeling in een spagaat brengen. Beide stellen verschillende eisen aan de bemensing van de auditafdeling. Slechts een multidisciplinair bemenste auditgroep kan goed met deze spagaat omgaan. Wij zullen dat nader toelichten.

Audits in de hoek van 'standaardvragen ten behoeve van de vergelijkbaarheid' kenmerken zich door een opgelegde algemene, relatief globale normering en een voorgeschreven onderzoeksaanpak. Deze onderzoeksaanpak laat weinig ruimte voor onderscheid naar situationele uitwerkingen gericht op specifieke organisatiebehoeften. Het 'oppervlakkige' in deze onderzoeken maakt dat relatief beperkt opgeleide auditors het veldwerk kunnen doen en er vaak geen noodzaak zal zijn voor een auditteam dat meerdere specialismen herbergt.
Voor de relatie en samenwerking tussen de operational auditor en de IT-auditor betekent dit het volgende.
Beiden doen het werk dat ze zelfstandig prima kunnen of laten zich als onderaannemer inschakelen daar waar de hoofdaannemer een specifieke opdracht moet uitbesteden. In lijn met de genoemde ontwikkelingen zal de hoofdaannemer in veel gevallen de accountant zijn. Kortom, de IT-auditor en operational auditor kunnen op deze wijze, zonder verwondering, naast elkaar bestaan. Beiden hebben hun eigen, separate toegevoegde waarde.

De maatwerkonderzoeken kenmerken zich echter door de noodzaak dat de auditor zich diep inleeft in de situatie en specifieke problematiek van de opdrachtgever en auditee. Alleen dan kunnen de auditor en de opdrachtgever komen tot de meest passende onderzoeksvraag en -aanpak.

Om op voorhand niet de fout te maken dat de kennis van de auditor bepaalt welk probleem hij onderkent, zal bij voorkeur reeds bij de opdrachtverkenning sprake moeten zijn van een multidisciplinair samengesteld auditteam. Afhankelijk van de onderzoeksvraag is vervolgens meer of minder specialisme noodzakelijk. De IT-auditor en operational auditor moeten dus samen optrekken. Zij dienen aan deze zijde van het continuüm een grote bereidheid tot samenwerking én kennis van elkaars vakgebied te hebben om aan het verzoek van de opdrachtgever te kunnen voldoen.

Anders gezegd, het gaat bij de audit om het verminderen van onzekerheid bij de opdrachtgever. Of we de audit dan (meer specifiek) aanduiden als operational of als IT-audit is voor de opdrachtgever niet interessant; de voor de audit benodigde kennis bepaalt de auditteamsamenstelling. Mogelijk moet er kennis worden georganiseerd die noch de IT- noch de Operational auditor bezit. Zodra de beheersmaatregelen worden beïnvloed door informatietechnologie of ook betrekking hebben op de IT-beheer- of IT-ontwikkelorganisatie, is specifieke IT-kennis echter snel onontbeerlijk.
De IT-auditor kan hier dan ook niet volstaan met standaard IT-audit aanpakken en -normering. De normering dient te worden afgeleid van de ondernemingsdoelstellingen. Dat was reeds de insteek van de operational auditor, waardoor deze mogelijk de 'lead' dacht te nemen [HART99]. Noodzakelijk is dat echter allerminst; ook IT-auditors zien we steeds meer vanuit deze insteek redeneren.
Daarbij speelt de vraag of de sociaalorganisatorische controls wel ruimte bieden voor de vaak 'op Starreveld c.s. gebaseerde' IT-controls. Positief geformuleerd: of de werking van deze 'soft' controls, zoals medewerkermotivatie of teamworking, enkele 'harde' IT-controls niet onnodig maken, ten gunste van flexibiliteit, leer- en verandervermogen.

Verder concluderen wij dat met name in deze maatwerkhoek zeer goede beheersing van auditmethodologie (als hulpmiddel voor het ontwerpen van audits) vereist is.
Er kan immers niet worden gesteund op reeds eerder zorgvuldig ontworpen onderzoeksaanpakken om de relevantie, deugdelijkheid en de doelmatigheid van de audit te waarborgen. Het is een geruststelling te constateren dat auditmethodologie aan opleidingen van zowel de IT- als de operational audit-beroepsgroepen in toenemende mate wordt gedoceerd.

U heeft nog het antwoord op de vraag in de titel van deze bijdrage te goed.

**IT-audit en operational audit: MATEN, met nadrukkelijk enkele eigen verantwoordelijkheidsgebieden.**

### *Literatuur*

[HART99] Hartog, P.A. en M. Nieuwendijk (1999), Operational Auditing en IT-Auditing, toch minimaal een LAT-relatie..., in: *De Accountant*, december.

[HART03] Hartog, P.A. en R.W.A. de Korte (2003), Soft controls, object van de auditor, in: Twintig over Internal/Operational Auditing, VERA/EURAC.

[KOCK03] Kocks, C. (2003), Auditing, audit, auditor, wat moeten we ermee?, in: Twintig over Internal/Operational Auditing, VERA/EURAC.

[KORT03] Korte, R.W.A. de (2003), Audit en/of advies; kunnen we die discussie beëindigen?, in: *Audit Magazine*, maart.

[OTTE03] Otten, J.H.M., P.A. Hartog en A. Babeliowsky (2002), Auditmethodologie, metatool voor klantgericht auditen, in: *Audit Magazine*, 1 december.

[PAAP99] Paape, L. en R.W.A. de Korte (1999), Van Operational naar Management Control Auditing?, in: *De Accountant*, oktober.

### *Noten*

1 Een in beide beroepsgroepen gangbare definitie van auditing is van Prof. Kocks: *Auditing is het vakgebied dat zich bezighoudt met het, op grond van onderzoek (audit) door een deskundige (auditor), beoordelen van één of meerdere (audit)objecten in relatie tot (toetsings)normen en het weergeven van de uitkomsten van het onderzoek in de vorm van een oordeel aan de opdrachtgever en/of (via de opdrachtgever) aan derden.* Zie [KOCK03].

2 Met advies bedoelen we hier niet het weinig relevante maar onschuldige 'herhalen van de norm'. Bedoeld wordt een advies over HOE de situatie te verbeteren en aan de norm te voldoen.

3 In lijn met het besluit van NOREA spreken wij van IT-auditing, tenzij in de letterlijke tekst waarnaar wij verwijzen de term EDP-auditing wordt gehanteerd.