IT-auditor, wordt wakker?!

FRANS KERSTEN

Tijdens de IT-auditdag 2008, op 4 juni 2008, heeft onze voorzitter, Hans Donkers, in zijn inleiding benadrukt blij te zijn met het lidmaatschap van de NOREA aan de IFAC, de International Federation of Accountants. Dit lidmaatschap is te zien als een erkenning van het hoge niveau van beroepsuitoefening. Aan dit lidmaatschap is echter de eis verbonden van het implementeren van de door de IFAC uitgegeven standaarden. Om meerdere redenen is het echter de vraag of wij als IT-auditors hier zo blij mee moeten zijn. Wij staan immers niet voor niets apart van de RA's en de AA's. Is de IT-auditor niet immers veel meer adviseur dan controleur?

De aanleiding voor deze bijdrage is het uitkomen van het Raamwerk [NORE07-1] en de Richtlijn [NORE07-2] voor de uitvoering van *assurance*opdrachten. Later bleken er ook opeens – of had ik iets gemist? – nieuwe voorbeeldteksten voor 'Oordelen' op grond van deze richtlijn op de website van de NOREA te staan. In de eerste plaats was ik al niet gelukkig met bepaalde terminologie uit het raamwerk en de richtlijn. Waren we opgegroeid met de termen als 'bewijsmateriaal' of zo u wilt *evidence*, nu zijn we kennelijk bezig met het verzamelen van assurance-informatie. Ik dacht eerst dat dit stond voor de mededeling die wij afgeven aan onze opdrachtgever: informatie waarmee wij zekerheid – assurance – bieden. Dat was dus niet het geval. Ik blijf het hier moeilijk mee hebben. Ik ben dan ook opgegroeid met de opvatting dat gegevens pas informatie worden op het moment dat ze iets betekenen en waarde hebben voor de ontvanger van die gegevens.[1] Het bewijsmateriaal bestaat in de eerste plaats uit gegevens, bij voorkeur feiten, en deze moeten waarde krijgen door het werk van de IT-auditor: er wordt wel of niet voldaan aan de norm. Dit is waar onze opdrachtgever op zit te wachten. Mijn verbazing was daarom groot toen in het origineel, de IFAC's 'International Framework for Assurance Engagements' [IFAC05], de term 'evidence', ofwel bewijsmateriaal, gebruikt bleek te worden… Was hier gekopieerd uit het 'Stramien voor assurance-opdrachten' van het Koninklijk NIVRA [NIVRA07]?

Onduidelijkheid

Waar onze opdrachtgevers kennelijk ook niet op zitten te wachten, is terminologie dat 'de interne beheersingsmaatregelen *in alle van materieel belang zijnde opzichten effectief* zijn'. De eerste 'verantwoordelijke partij' die deze woorden in mijn auditrapportage las, vroeg direct om een toelichting. Hij meldde dat de term 'materieel belang' hem niets zei. Nu was dit begrijpelijk: het ging hier om een opdracht op het gebied van de beheersing van (grote) IT-projecten en niet om een opdracht met een directe link naar de jaarrekeningcontrole. Hij legde vervolgens de nadruk op 'alle opzichten' en vond dat dit zo breed kon gaan dat hij daar onmogelijk aan kon voldoen. Een reactie die ik gedurende vijftien jaar optreden als IT-auditor – ik heb tussendoor ook nog wat andere dingen gedaan – op eerdere mededelingen in de lijn van de NIVRA-geschriften 26 [NIVRA82] en 53 [NIVRA89] nooit heb gekregen.
Inmiddels zijn genoemde voorbeeldteksten gepubliceerd. Daarin blijkt de tekst te zijn aangepast in 'de maatregelen in alle van materieel belang zijnde opzichten

'Hij meldde dat de term "materieel belang" hem niets zei'

hebben voldaan aan de normen'. (Op zich is het al vreemd dat deze teksten vanuit de beroepsorganisatie afwijken van de eigen richtlijn!) 'Voldoen aan normen' is in mijn optiek duidelijker dan 'effectief zijn'. Dit laatste roept immers direct de in deze tijd zeer actuele vraag op 'was het ook efficiënt?'. Een vraag die zo mogelijk nog moeilijker te beantwoorden is.

Materialiteit

Blijft nog over de problematiek van 'materieel belang'. Duidelijk is dat deze gerelateerd is aan de controle van de jaarrekening en daar kwantitatief benaderd kan worden. (Dat dit dan ook weer ruimte voor interpretatie biedt, blijkt dan weer uit de noodzaak om hiervoor grenswaarden op te nemen in de richtlijnen voor de jaarrekening.) Onze collega's van ISACA melden hierover in IS Auditing Guideline G6 Materiality [ISACA08]: 'Unlike financial auditors, IS auditors require a different yardstick to measure materiality. Financial auditors ordinarily measure materiality in monetary terms, since what they audit is also measured and reported in monetary terms. IS auditors ordinarily perform audits of non-financial items, e.g. physical access controls, logical access controls, program change controls, and systems for personnel management, manufacturing control, design, quality control, password generation, credit card production and patient care. Therefore, IS auditors may need guidance on how materiality should be assessed to plan their audits effectively, how to focus their effort on high-risk areas and how to assess the severity of any errors or weaknesses found.'

Vervolgens is dan nog ongeveer één A4-tje nodig om uit te leggen hoe de IT-auditor met het begrip materialiteit moet omgaan. Feitelijk is sprake van het uitvoeren van een risicoanalyse. Meetpunten zijn dan gebruikelijke gevolgen, zoals financiele schade en imagoschade (in paragraaf 3.1.11) of het niet halen van de bedrijfsdoelstellingen (*objectives*), onregelmatigheden en de overtreding van wet- en regelgeving. Deze laatsten laten zich vertalen met 'niet *in control* zijn'. Hierbij dient de auditor rekening te houden met onder meer het risicogedrag van de organisatie: 'aggregate level of error acceptable to management'.

Wakker?

Nu passen de meeste organisaties tegenwoordig risicoanalyse toe en streven zij ernaar om 'in control' te zijn. Zij hanteren hiervoor duidelijke interne doelstellingen, de objectives, of normen. Zij hanteren daarbij ook criteria zoals beschikbaarheid, integriteit en vertrouwelijkheid. Als de IT-auditor heeft vastgesteld dat de organisatie dit op de juiste manier doet, dan hoeft hij de term 'materieel belang' ook niet meer te gebruiken. Dan kan hij eenvoudig verklaren dat de interne beheersingsmaatregelen wel of niet voldoen aan de normen. Is dit niet de zekerheid die wij onze opdrachtgevers moeten bieden? (De interne auditafdeling die mij thans heeft ingehuurd, heeft bewust voor deze duidelijkheid gekozen.)

Hiermee kom ik terug op de titel van deze bijdrage. De accountancy is de afgelopen jaren even opgeschud geweest door de opkomst van wakkere accountants. Inmiddels is deze storm gaan liggen en hebben we te maken met de orkaan van de huidige financiële en economische crisis. Het is de vraag of de *financial* auditors deze ook zo gemakkelijk zullen doorstaan. In ieder geval staan hun toegevoegde waarde én de tekst van hun accountantsverklaring weer volop in de belangstelling. Voorts zijn er weer volop discussies over of de financial auditor niet te weinig kennis heeft van IT, de reden waarom IT-auditors zijn ontstaan.

Ondertussen constateer ik dat ik, en kennelijk anderen met mij, onvoldoende wakker zijn geweest toen we juist de kant van de financial auditors opgingen door ons aan te sluiten bij de IFAC. De nadruk ligt in de standaarden van de IFAC nog steeds primair op financial audit. Daarentegen constateer ik bij onze zusterorganisatie ISACA aandacht voor de eigen positionering van de IT-auditor. De CISA-kwalificatie heeft met zijn ANSI-status ook duidelijk erkenning gekregen. Voorts merk ik dat ik voor mijn relatief beperkte contributie van ISACA een schat aan praktische, wel op de IT-auditor gerichte documentatie krijg, ofwel *value for money.*

Als lid van de uitstervende[2] groep van RE RA's, met wellicht dus wat meer binding met financial auditors dan de gemiddelde RE, doe ik dan ook de oproep: IT-auditor, wordt wakker: *time for a change?* ■

Noten

1 Onder anderen prof. dr. ir. G.C. Nielen (Gegevensleer) en prof. R.W. Starreveld en anderen (Bestuurlijke informatieverzorging, deel 1).

2 Woorden van dr. J.P.J. Verkruijsse RE RA in de inleiding op zijn presentatie tijdens het Alumnicongres van VUrORE en NOREA, woensdag 12 november 2008, aangekondigd als 'Nieuwe IFAC-regels verminderen de schijnzekerheid'.

Literatuur

[IFAC05] IFAC, *International framework for audit engagements,* 2005.

[ISACA08] ISACA, *IS Auditing Guideline G6 'Materiality',* 2008.

[NIVRA82] NIVRA, NIVRA-geschrift 26, *Automatisering en control deel IV, Mededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking,* 1982.

[NIVRA89] NIVRA, NIVRA-geschrift 53, *Automatisering en control deel VII, Kwaliteitsoordelen over informatievoorziening,* 1989.

[NIVRA07] NIVRA, *Stramien voor assurance-opdrachten,* 2007.

[NORE07-1] NOREA, *Raamwerk voor assurance-opdrachten door IT-auditors,* 2007.

[NORE07-2] NOREA, *Richtlijn 3000 – assurance-opdrachten door IT-auditors,* 2007.

F.H.B. (Frans) Kersten RE RA is werkzaam als Principal Consultant IRM voor Logica Nederland B.V.. Voor zijn indiensttreding bij Logica is hij van 1987 tot 1997 werkzaam geweest als IT-auditor RA en later lid van het managementteam van de departementale accountantsdienst van het ministerie van Landbouw, Natuur en Visserij. Van 1 januari 2006 tot 1 maart 2009 werkte hij als ingehuurd IT-auditor voor een interne IT-auditafdeling. Dit artikel is geschreven op basis van ervaringen in deze functie.