Column **Over de auditorsfuik en het nut van auditopleidingen**

Anton Tomas

Is het eigenlijk niet vreemd dat we speciaal opgeleide auditors nodig hebben om de kwaliteit van een object te beoordelen? Een timmerman die zijn vak verstaat kan heel goed het werk van een collega beoordelen.Voor andere vaklieden zoals metselaars geldt hetzelfde. Maar om het werk van IT-deskundigen te beoordelen zouden we speciaal opgeleide IT-auditors nodig hebben? Kom nou toch. Dat werk kan toch ook wel gedaan worden door goede IT-deskundigen zonder postdoctorale auditopleiding? Maar, zult u misschien vragen, is voor het uitvoeren van een audit dan niet een heel andere expertise nodig? Volgens mij is dat niet zo. Nou ja, ze moeten meestal nog even leren het allemaal goed op te schrijven. Wel worden volgens mij steeds meer zaken ontworpen en gebouwd door ondeskundigen of door mensen die weliswaar theoretische kennis bezitten maar nog zeer onervaren zijn. Die lieden beschikken natuurlijk niet over de expertise om een audit uit te kunnen voeren. Voor een audit heb je gewoon mensen nodig die hun vak verstaan; en dan bedoel ik niet het auditvak, maar het vak dat nodig is om het auditobject te ontwerpen en te bouwen. Bij IT-objecten gaat het trouwens meestal niet alleen om IT-deskundigheid, maar bijvoorbeeld ook om organisatiedeskundigheid en expertise op het terrein van de desbetreffende business. Mijn mening wordt bevestigd door de praktijk. Want in de praktijk zie je inderdaad dat audits steeds vaker worden uitgevoerd door personen die niet zijn opgeleid tot auditor. Dat gaat prima en misschien zelfs wel beter. Neem als voorbeeld het onderwerp informatiebeveiliging (toegegeven, het wordt een heel eenvoudig voorbeeld). Ik ken een organisatie waar personen die niet tot auditor zijn opgeleid regelmatig een audit uitvoeren op het gebied van informatiebeveiliging. Ze hebben weliswaar geen verstand van auditing maar wel van informatiebeveiliging. Zo gingen deze auditors bijvoorbeeld een keer gewapend met een videocamera het gebouw door om allerlei situaties vast te leggen waarin vertrouwelijke informatie voor het grijpen lag. Deuren en kasten stonden onbeheerd open, de ingangscontrole van het gebouw liet te wensen over, et cetera. Over de bevindingen werd een rapportje geschreven en een week later werden de meest sprekende videofragmenten aan de directie getoond. En reken maar dat dit resulteerde in een snelle verbetering. Een ‘officiële’ auditor zou in dezelfde tijdsspanne waarschijnlijk nog bezig zijn met het afstemmen van de normen met de opdrachtgever (als hij al niet was blijven steken in de fase ‘knowing the business’). Want volgens de regels van het auditvak zoals dat gedoceerd wordt aan onze universiteiten, dient men eerst met de opdrachtgever overeenstemming te verkrijgen over de normen alvorens men bevindingen gaat verzamelen.

Onze postdoctorale auditopleidingen worden bevolkt door mensen met relatief weinig werkervaring en dan soms ook nog met een vooropleiding in het verkeerde vakgebied. Dat gaat ze opbreken. Je zult maar opgeleid zijn tot informaticus of tot (al of niet bestuurlijk) informatiekundige, nooit in dat vak gewerkt hebben en, omdat je je eerste baan nu eenmaal bij een auditafdeling hebt gevonden, een postdoctorale opleiding IT-auditing volgen. Boekenkennis gestapeld op boekenkennis! En dan heb ik het nog niet

Ir. A.J. Tomas RE RI RO is elektrotechnisch ingenieur, informaticus en auditor. Hij werkt als account manager bij de Internal Audit Department van de Nederlandse Spoorwegen. Hij is betrokken bij de postdoctorale opleiding EDP-Auditing van de Erasmus Universiteit als extern lid van de examencommissie voor het afsluitende examen. Verder is hij lid van de redactie van de EDP-Auditor.

eens over nog maar net afgestudeerde accountants die een opleiding IT-auditing volgen. Een bijspijkercursus IT op een paar vrijdagen waarin het IT-fundament gelegd zou moeten worden voor een gedegen IT-auditopleiding? Zo'n (postdoctorale!) opleiding kan natuurlijk nooit boven het propedeuseniveau van een IT-opleiding uitkomen. Cursisten zonder gedegen IT-vooropleiding en zonder ruime werkervaring in IT kunnen natuurlijk nooit uitgroeien tot de all-round IT-vakman of -vrouw die het werk van een collega IT-deskundige kan beoordelen; ook niet via een postdoctorale IT-auditopleiding. Overigens kan ik soortgelijke woorden schrijven over de postdoctorale opleidingen operational auditing, maar dan erger. Want wat is in vredesnaam het onderliggende vakgebied? Een operational auditor zou in staat zijn procesbeheersing te beoordelen ongeacht wat er in het proces omgaat. Een operational auditor is dus net zoiets als een manager die wel verstand heeft van managen maar niet van zijn business. Zulke managers bestaan. Een paar jaar geleden was dit zelfs mode, maar die tijd is inmiddels passé.

Des te verbazingwekkender is het dat er toch af en toe heel goede IT-auditors van de opleiding komen met als enige IT-werkervaring die welke is opgebouwd tijdens de twee jaar waarin ze tevens de deeltijd-opleiding IT-auditing volgden. Ik denk dat dit iets zegt over deze mensen en niet over de auditopleiding. Toch blijft het jammer. Want hoeveel meer profijt zouden zij van hun vakopleiding gehad kunnen hebben als ze eerst een jaar of tien als IT-deskundige waren gaan werken. En na tien jaar werkzaam geweest te zijn als IT-deskundige zouden ze een auditopleiding nauwelijks nog nodig hebben om goede IT-audits te kunnen uitvoeren. Een vakman die zijn vak verstaat kan immers heel goed het werk van collega's beoordelen. Maar nu ze rechtstreeks na hun vakopleiding full-time aan het auditen zijn geslagen, zal het moeilijk worden de theoretische kennis uit de vakopleiding te verrijken met de ervaring die nodig is om uit te groeien tot de all-round IT-vakman of -vrouw die diepgaande IT-audits kan uitvoeren. Erger nog, zonder dagelijkse IT-werkervaring zal het ze moeilijk vallen hun IT-vakkennis op peil te houden waardoor het ze onmogelijk wordt na enige tijd alsnog naar een IT-functie te kunnen ontsnappen, terwijl ze als auditor niet kunnen doorgroeien: de auditorsfuik.

Laten we eens bezien welk soort IT-audits er grofweg bestaan en wat dat ons zegt over de auditopleidingen. In de eerste plaats zijn er audits die ten doel hebben na te gaan of men zich aan voorschriften houdt. Dit zijn audits op velerlei terreinen, maar omdat het auditobject zich soms afspeelt in een geautomatiseerde omgeving zijn er ook IT-auditors die dit soort audits uitvoeren. De voorschriften kunnen wettelijke voorschriften zijn maar ook zelfopgelegde standaarden en normen zoals de Code voor informatiebeveiliging. Deze audits gaan niet diep. In de kern gaat het om het afvinken van een rijtje regels waaraan moet zijn voldaan. Veelal worden dit soort audits periodiek herhaald. In de tweede plaats zijn er IT-audits die bedoeld zijn om vast te stellen of bepaalde doelstellingen van het management worden gehaald. Bijvoorbeeld bij de bouw van een informatiesysteem met een beschreven functionaliteit binnen een bepaalde tijdsduur en tegen overeengekomen kosten kan de IT-auditor zowel voor, tijdens als na de bouw worden gevraagd te onderzoeken hoe het zit met de haalbaarheid of de realisatie van een of meer van de doelstellingen van het management. Ook deze audits gaan niet zo diep. Het gaat hier in feite om het afvinken van een rijtje doelstellingen. Tenslotte zijn er de diepgaande IT-audits. Soms puur technisch diepgaand, soms organisatorisch diepgaand en meestal een combinatie van beide. Deze audits hebben als kenmerk dat de auditor diepgaand de werking van een bepaald technisch of organisatorisch systeem doorgrondt en analyseert en zich een mening vormt over de betrouwbaarheid van de functionaliteit ervan. Deze audits worden niet vaak en zeker niet periodiek uitgevoerd. De resultaten leiden tot afzonderlijke verbetertrajecten en staan soms ook ten dienste van de eerder beschreven twee categorieën afvink-audits.

De twee eerstgenoemde categorieën audits rechtvaardigen geen universitaire auditopleiding. Het is zelfs heel goed denkbaar dat een groot deel van dit soort audits in de toekomst verregaand geautomatiseerd zal plaatsvinden.
De meer diepgaande IT-audits zullen in de toekomst steeds meer worden uitgevoerd door IT-deskundigen die een gedegen IT-opleiding hebben genoten en die een ruime ervaring hebben in hun eigen vakgebied. Deze mensen zijn goed in staat het werk van vakgenoten te beoordelen. Wel is het zo dat de praktijk heeft aangetoond dat zij nog moeten leren het resultaat van hun audit op te schrijven. En als men het gaat opschrijven, zo weten wij ervaren auditors al lang, lijkt de audit pas echt goed te beginnen! Alleen mensen met een gedegen IT-opleiding en ten minste 10 jaar IT-werkervaring zouden moeten worden toegelaten tot de IT-auditopleidingen. Deze opleidingen hoeven niet meer te pretenderen dat ze IT-leken snel op een geschikt niveau van IT-kennis kunnen brengen. De opleidingen kunnen zich helemaal richten op vakken als auditmethodologie en de diverse wijzen van rapportage en overige managementondersteuning. De tijd die vrijkomt door het wegvallen van de IT-vakken kan worden gebruikt voor een cursus schrijfvaardigheid. Voor alle zekerheid moet het RE-register natuurlijk worden gesloten voor mensen jonger dan 35 jaar.