Interview met Paul van Kessel

De noodzakelijke transitie van IT-auditing

3 mei 2017

Paul van Kessel (1958) is sinds 2006 wereldwijd verantwoordelijk voor de (IT-) Risk Assurance en Advisory Services van EY. Zijn rol is momenteel Global Managing Partner Cybersecurity Services. Deze bijzondere positie en zijn ervaring vormen voor ons de aanleiding om hem te interviewen, benieuwd als we zijn naar zijn observaties aangaande de inzet en relevantie van IT-auditprofessionals in Nederland maar ook wereldwijd.

'Wat mij in het bijzonder opvalt is het denken in vastomlijnde hokjes dat in het Nederlandse domein nog steeds rondom de afzonderlijke disciplines en hun beroepsorganisaties heerst. Nergens ter wereld zie je zoveel publicaties of toekomstverkenningen met titels als 'The future of IT-auditing'; 'The future of operational auditing', et cetera. NOREA is 25 jaar geleden opgericht. Vanaf de zijlijn heb ik de totstandkoming van NOREA meegemaakt. De personen die daar destijds het initiatief toe hebben genomen waren voornamelijk accountants en consultants die zich gingen richten op de audit met behulp van IT. Data-analyses werden ondersteund en uitgevoerd met behulp van computers (CAATs, *Computer Assisted Audit Techniques*). We maakten als het ware de data toegankelijk voor accountants die dat zelf niet konden. Die specialisatie voorzag toen in een grote behoefte en het IT-audit vak heeft zich sindsdien als een afzonderlijke discipline doorontwikkeld en verbreed. NOREA en de IT-auditopleidingen van de universiteiten hebben daaraan een belangrijke bijdrage geleverd.'

> *"Er zijn twee soorten bedrijven, bedrijven die al gehackt zijn en bedrijven die dat nog niet weten..."*

'De *core competence* van de IT-auditor heeft te maken met control(s). Als ik naar het beroep kijk, dan is een IT-auditor niet primair een deskundige of consultant op het gebied van IT. Hij is een deskundige op het gebied van IT-controls, dus General IT-controls en application controls. In de opleidingen zit nog steeds een sterke focus op de *solutions* en technologie, zoals database-audit, rekencentrumaudit, systeemaudit, terwijl de vraag en behoefte van de klant en de markt meer leidend zouden moeten zijn. Die behoefte bestaat tegenwoordig vooral uit *assurance, compliance* en *riskmanagement*. We moeten ons daarbij terdege realiseren dat we een onderdeel zijn van een groter geheel.

In dat verband zie ik in toenemende mate een integratie van disciplines gericht op (IT-) audit en riskmanagement, waarbij de IT-auditor bezig is met een succesvolle transitie tot brede riskmanager. Organisaties hebben behoefte aan de competentie van geïntegreerd risicobeheer. Wat zijn daarvoor de relevante *capabilities*? Welke disciplines moeten we bij elkaar brengen en integreren voor de noodzakelijke expertise in dat verband? In Nederland lukt dat met de IT-auditors (RE's), operational auditors en andere professionals van de postacademische opleidingen, maar ook elders in de wereld voorzien we in deze behoefte, zo nodig ondersteund met interne opleidingen of trainingen. In de praktijk zie ik niet veel problemen door het missen van competenties. Het lukt meestal wel om de juiste expertise bij elkaar te brengen.'

'Toen ik tien jaar geleden in een *global managing* rol werd benoemd, had EY twee business units die gericht waren op het helpen van klanten met hun risicomanagement. Eén business unit richtte zich op IT-risico's. In Nederland werden de RE's in deze business unit aangenomen. De andere business unit richtte zich op alle andere risico's.'

'Opmerkelijk was dat de IT-riskpraktijk een enorme groei doormaakte, terwijl de groei van de andere risk-business in vergelijking daarmee achterbleef. Vanuit het business-perspectief was de perceptie dat IT de cruciale factor was en werden de business-risk mensen als niet-relevante gesprekspartners ervaren. Op grond daarvan hebben wij beide risk-praktijken geconsolideerd, waarbij competenties en beroepsprofielen veel scherper geformuleerd zijn. Momenteel maakt de geconsolideerde riskpraktijk de groeidoelstellingen wel waar. De vormgeving van het IT-auditberoep in Nederland is heel succesvol geweest. Niettemin zou je je als beroepsgroep moeten realiseren dat je opereert op een onderdeel van de gehele risk managementmachinerie. Je hebt dan twee mogelijkheden: het IT-auditberoep verder afbakenen en nadrukkelijk samenwerken met andere risicobeheerdisciplines, of komen tot een meer "holistische" definitie van een risk managementberoep.'

'Ook internationaal zie ik die scherpe afbakening wel terug. De Nederlandse IT-auditor is heel deskundig maar praat vaak vanuit een nogal gedetailleerde, gespecialiseerde invalshoek. In de internationale boardrooms bestaat echter behoefte aan een breder risk managementperspectief. We zullen dat spanningsveld tussen een uitgekristalliseerd aanbod van IT-auditdiensten en de ruimere informatievraag van onze klanten moeten bewaken en daarop moeten acteren.'

'De trend richting riskmanagement wordt nog versterkt door de ontwikkeling van cybersecurity. EY heeft een *Threat Intelligence Center* dat wereldwijd de cybersecurityrisico's in kaart brengt. Op grond daarvan kunnen we twee soorten bedrijven onderscheiden: de bedrijven die al gehackt zijn en de bedrijven die dat nog niet weten. Het is immers op dit moment ondenkbaar dat we een systeem zouden kunnen ontwikkelen dat niet gehackt kan worden. In het verleden zijn we sterk gericht geweest op het beschermen van het bedrijf of

het IT-systeem. We investeerden in het bouwen van een *corporate shield* en ontwikkelden en breed scala van controls en security-maatregelen. Het voldoen aan *rules and regulations* was daarvan een onderdeel. Die focus voldoet echter niet meer. We verleggen het accent nu naar een grotere investering in voorbereiding en onderzoek: hoe ziet het speelveld eruit? Wat komt er op ons af? Wie zijn de echte risk-actoren en welke bedreigingen zien we? Vergelijk het maar met de keeper bij het voetbal. Die kan beter met zijn gezicht naar het veld gekeerd staan dan naar de tribune.'

'Een andere *spin-off* is een zekere verandering in het 'corporate DNA'. Er is een veel sterkere focus nodig op *resilience*: hoe ga je om met incidenten en hoe beperk je de impact daarvan op de bedrijfsvoering? We moeten voorbereid zijn op situaties waarin zaken mis gaan. De focus wordt uitgebreid van *threat intelligence naar safe to fail*, waarbij je het als een zekerheid beschouwt dat je geconfronteerd zult worden met incidenten, en je je erop richt een terugkeer naar *business as usual* zo snel mogelijk te bewerkstelligen. Bij die veranderende benadering kan de IT-auditor of riskmanager veel toegevoegde waarde bieden.'

'Bij een jubilerende beroepsorganisatie hoort een terugblik. Je kunt niet anders dan concluderen dat we heel succesvol zijn geweest in het vormgeven en doorontwikkelen van het IT-auditberoep en daar hoort een felicitatie bij. NOREA is in een uitstekende positie om succesvol in te zetten op noodzakelijke ontwikkelingen, zoals het positioneren van het IT-auditberoep in een bredere risk-managementcontext.'

Drs. W. (Wilfried) J.A. Olthof en Ed Ridderbeekx

Wilfried Olthof is directeur van NOREA en heeft daarvoor functies vervuld bij de Perscombinatie, het ministerie van VROM en de Vrije Universiteit Amsterdam. Hij heeft Politicologie en Bestuurswetenschappen gestudeerd. Ed Ridderbeekx is werkzaam als zelfstandig IT-auditor en is lid van de redactie.