INTERVIEW MET BART LOHMEIJER, SENIOR RISK MANAGER RABO VASTGOEDGROEP

Van nullen en enen naar stenen

De gastheer van uw twee reporters, Bart Lohmeijer, had bij wijze van spreken een rol kunnen spelen in de speelfilm 'The Seven Year Itch'. Zijn loopbaan kenmerkt zich vooral door het ongeveer met een dergelijk interval veranderen van werkkring. De laatste 'switch' die Bart heeft gemaakt, is het verlaten van het vakgebied van IT-audit. Dat komt goed uit voor deze rubriek, waarin we regelmatig in gesprek gaan met IT-auditors die van werkkring zijn veranderd.

ACHMED BOUAZZA EN MAARTEN BUIJS

Kun je om te beginnen jouw loopbaan eens schetsen?

'Na mijn diensttijd bleef ik in de tachtiger jaren min of meer in Defensie-sferen werkzaam. Bij het TNO Fysisch en Elektronisch laboratorium (FEL) leerde ik samen met Paul Overbeek hoe je op een veilige manier informatie kunt delen. Ik hield me daar bezig met datacommunicatie en cryptobeheer en beschouw het nog steeds als een goede leerschool. Na een korte zijsprong bij ABB Lummus Crest, een belangrijk ingenieursbureau voor Shell, startte ik als Manager Operations Datacommunicatie bij Ergon installatietechniek, toen nog onderdeel van de Hollandse Beton Groep. Hier was ik medeverantwoordelijk voor het ontwerp en de aanleg van de operationele datacommunicatie infrastructuur van diverse grote bedrijven en overheden.'

'Begin 2000 bleek dat KPMG mij vanwege mijn kennis over datacommunicatie goed kon gebruiken bij de uitvoering van IT-audits. Ik leerde hier onder de vleugels van Edo Roos Lindgreen en Ronald Paans bij de General Practice Amstelveen in de praktijk de mores van de vakken IT-audit en IT-advisory.'

'Ik voerde onder andere KPMG Corporate Information Security (CIS) trajecten, certificeringsopdrachten, Afhankelijkheids- en Kwetsbaarheids-analyses en auditreviews uit. Ook stelde ik met collega's SAS 70-verklaringen en TPM's op. Gedurende langere tijd was ik namens KPMG als auditor meerdere keren per jaar aanwezig bij (middel)grote nationale en internationale ondernemingen evenals bij (semi-)-overheids- en non-profitorganisaties. Vaak leidden deze opdrachten tot adviestrajecten over het verbeteren van de informatiebeveiliging. Bevredigend en uitdagend werk!'

Toch heb je op een bepaald moment een overstap gemaakt en ben je gestopt met IT-audit. Waarom?

'Vanuit KPMG was ik al sinds 2000 betrokken bij het ABN Amro Bouwfonds Nederlandse Gemeenten. Het Bouwfonds was, voordat het werd verkocht aan de Rabobank, een onderdeel van ABN Amro. In eerste instantie kreeg ik hier voor een paar dagen per jaar een certificeringsopdracht rond informatiebeveiliging (conform ISO 27001).'

'ABN Amro, en later de Rabobank, zijn "SOx plichtig". Ik hielp hier mee voor wat betreft de IT-kant, met name met de beoordeling van de general IT-controls templates. Na verloop van tijd kreeg het advieswerk steeds meer nadruk en dat ging op den duur 'knellen' met het eveneens uitvoeren van IT-audits.'

'Uiteindelijk trok de advieskant mij toch meer aan en na acht jaar IT-audit leek het me een natuurlijk moment om te switchen. Er sluimerde een ambitie om intensiever bij één en dezelfde klant betrokken te zijn en hen te helpen succesvol te ondernemen. Nog dichter op de business, een rol die in mijn ogen ook past bij de IT-auditor van de toekomst. Inmiddels werd ik vader en woonde ik in Amersfoort. Nadat de voormalige security officer met pensioen was gegaan, maakte ik de overstap naar het Bouwfonds.'

'Alweer vijf jaar werk ik nu als Senior Risk Manager samen met twee collega's bij ▶

de afdeling Control & Risk van de Rabo Vastgoedgroep. Risk is verantwoordelijk voor het beleid ten aanzien van en de controle op de risicoposities van Rabo Vastgoedgroep. De risico's van Rabo Vastgoedgroep zijn ingedeeld in zes hoofdcategorieën, te weten: Markt-, Krediet-, Financiering-, IT-, Business Continuity Management (BCM) en informatiebeveiligingsrisico's. Ik ben verantwoordelijk voor de laatste drie. In vergelijking tot een financiële instelling heeft dit bedrijf een relatief kleine IT-organisatie.'

De Rabo Vastgoedgroep heeft vijf divisies. Risk Management is decentraal georganiseerd. De primaire riskmanagementtaken liggen met name in de divisies. Het Risk Managementbestuurscentrum adviseert, consolideert, rapporteert en maakt beleid. Bart is de enige risk manager die opereert vanuit IT, BCM en informatiebeveiligingsperspectief. Hij rapporteert aan de Chief Financial Risk Officer van dit bedrijf. Het beleid dat wordt geïmplementeerd, is gebaseerd op 'sound principles of operational risk', opgesteld naar aanleiding van het Basel III akkoord. In het kader van de beheersing van de operationele risico's moeten alle incidenten (>10K) worden geregistreerd. Bij de CFRO komen alle lijnen van de risico managementfuncties bij elkaar.

Risk Management bedient drie soorten klanten. Op de eerste plaats is daar natuurlijk de Rabobank zelf, de 'moederorganisatie'. Vervolgens definieert Risk Management passend beleid voor de afzonderlijke divisies en draagt zij zorg dat zij hiermee compliant zijn. Ten slotte wil de hoofddirectie dat Risk Management haar ondersteunt met kennis, oordelen en visie.

Je bent nu dus senior risk manager… Wat houdt dit werk in?

'Samengevat: de risk manager helpt de organisatie om de risico's te managen en compliant te zijn met wet- en regelgeving. Voor de risk manager die IT en informatiebeveiliging tot zijn verantwoordelijkheidsgebied heeft, is zowel toereikende kennis van belangrijke onderwerpen die in de financiële sector spelen als van de general IT- controls noodzakelijk.'

'Het primaire proces is gericht op het financieren en realiseren van vastgoed. 'Stenen' zijn belangrijker; de ruimte die het object inneemt kun je zien. IT is ondersteunend aan de bedrijfsvoering, en voor de meeste collega's een stuk virtueler'

'Voor de Rabobank blijft vastgoed een (steen)goede investering. Centrale vraag hierbij is: hoe zorgen we voor een passende governance? De vastgoedsector weet traditioneel niet veel van de hoge kwaliteitsstandaarden voor IT die voor financiële bedrijven al heel gewoon zijn. Voor een risk manager zit er veel vertaalwerk in om dit voor de CFO transparant te maken. Met name omdat deze nogal eens de neiging heeft om te zeggen "kan het allemaal een tandje minder?". Informatiebeveiliging is een onderdeel van Operational Risk Management, evenals BCM. De Nederlandse Bank let sterk op dit laatste, banken moeten een toereikend BCM-beleid hebben.'

Hoe kan risk management bijdragen aan het vergroten van de compliance?

'Ik beschouw risk management als belangrijk instrument in relatie tot het verkrijgen van compliance, want risk management gaat aan de voorkant na welke risico's de businessdoelstellingen in gevaar brengen. ISO27001 wordt gehanteerd als kwaliteitsstandaard voor het inrichten en onderhouden van een stelsel van maatregelen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van gegevens en informatiesystemen waarborgen. Hiermee voldoet de Rabo Vastgoedgroep aan het Rabobank Groepsbeleid. Wij laten de business vanuit de plannen die men wil realiseren IT-risico's definiëren en bijbehorende BIV-waarden bepalen. Hoe wil de business vervolgens deze risico's mitigeren en welke maatregelen wil men daartoe treffen?'

'Een van de zaken om dit traject te verbeteren, is het opstellen en bottom-up hanteren van een IT-controlframework. Op basis van COBIT is er binnen de Vastgoedgroep een IT-controlframework opgesteld om de compliancy beter in de grip te houden. Aan externe toezichthouders wordt gevraagd om hun controlframework aan COBIT te relateren. Zo kan een koppeling worden gemaakt met de interne AO/IC en kan de IT-organisatie eenvoudig het benodigde bewijs opleveren. Bovendien weet men daar dan ook: als wij deze COBIT-controls naleven, zitten wij in de goede richting voor wat betreft het compliant zijn.'

'Risk management is belangrijk om vanuit het framework de juiste elementen te gebruiken om een *best fit* te realiseren. Uitgangspunt hierbij is dat de IT-organisatie zelf verantwoordelijk is voor het nemen van de maatregelen. In het algemeen bestaat bij mij het gevoel dat de stand van zaken rond de general IT-controls in brede zin een redelijk betrouwbaar beeld geeft over de kwaliteit van de informatiebeveiliging.'

Risk Management zit samen met interne IT-auditors rond de tafel om hun visie op de business en risico's te geven zodat het controleprogramma scherper wordt gesteld. Internal Audit bestaat naast het hoofd Internal Audit uit drie auditmanagers en drie auditors. Er is een directe samenwerking met ARG (Audit Rabobank Groep). Door het feit dat de wet- en regelgeving alleen maar toeneemt, groeit ook de behoefte aan een geïntegreerde auditbenadering.

Als vrucht van alle inspanningen wordt de Rabo Vastgoedgroep jaarlijks gecertificeerd tegen ISO 27001. Het certificaat wordt afgegeven door de certificerende instantie BSI.

Wat ervaar je als de belangrijkste verschillen tussen IT-audit en risk management?

'Ik heb acht jaar ervaring als IT-auditor bij een groot kantoor. Hier is vaak sprake van kortdurende relaties, je voert een audit uit en je bent klaar. Door het vele reizen, de diversiteit qua niveau van onderwerpen en diepgang van de audits ervaar ik het ook wel als topsport. Je bent bovendien omringd door jonge ambitieuze collega's die alles even interessant vinden!

Als risk manager bij de Vastgoedgroep werk je in veel kleinere teams. Je hebt meer tijd om je in de materie te verdiepen en het onderzoek rustig af te ronden. Interessant is ook de politieke dimensie die zeker van zich doet spreken. De risk manager wordt meer onderdeel van de bedrijfscultuur en als zodanig meer aangesproken op zijn kennis.

Bestuurders vinden het ook niet makkelijk om risico's te duiden, en vragen daarom advies. Het is leuk om ze daarbij te helpen.

Ik zie overeenkomst met de mogelijke gevolgen van een zogeheten qualified audit rapport met betrekkelijk veel tekortkomingen. Dit kan binnen de organisatie tot de nodige spanningen leiden. Net als een (IT-)auditor moet je als risk manager ▶

hier je rug recht houden en tevens de onafhankelijkheid bewaren.'

Hoe zijn jouw huidige ervaringen met IT-auditors, je vroegere beroepsgenoten? Ervaar je toegevoegde waarde van IT-auditors?
'De afgelopen jaren heb ik met externe IT-auditors in het algemeen positieve ervaringen opgedaan. Ik zie dat de interne IT-auditors enorm in kennis investeren. Soms weet de IT-auditor het niet helemaal goed als het gaat om Cloud, Big Data, Mobile, Outscouring, Cyber Crime, Security maar dat is een mooie uitdaging om samen op te trekken. Daarnaast levert een rapport wel eens spanningen op als er risico's worden beschreven die reeds bekend zijn of al voldoende worden beheerst. Het lijkt er dan op alsof de auditors met hun bevindingen hun toekomstige werkgelegenheid creëren.'

'De risk manager helpt de organisatie om de risico's te managen en compliant te zijn met wet- en regelgeving'

'Van IT-auditors verwacht ik een goede voorbereiding, een op feiten gebaseerd verhaal en een gedegen *professional judgement*. Als hier sprake van is, merk ik zeker de toegevoegde waarde van IT-auditors. Wel ben ik van mening dat IT-auditors het best eens mogen opschrijven als beheer en inrichting van de IT goed zijn geregeld. Vaak lijkt het in de rapportages of er alleen aandacht is voor negatieve aspecten. Interne auditors willen trouwens nog wel eens wat vaker positievere aspecten opnemen in hun rapport.'

In hoeverre heeft jouw ervaring als IT-auditor je geholpen in je huidige functie?
'Van een aantal aspecten die ik als belangrijk heb ervaren in de IT-auditpraktijk maak ik vandaag de dag nog gebruik. Een voorbeeld hiervan is het besef dat je een goed product moet leveren en geen half werk. Ook het nastreven van *operational excellence* valt in deze categorie. In de Norea-richtlijnen zitten hiervoor goede aanknopingpunten. Een goede communicatie en afstemming zijn volgens mij essentieel voor een effectieve audit. Dat zijn zaken die ik heb meegenomen en enorm goed helpen in de praktijk. En wat voor alle huidige IT-auditors ook geldt: realiseer je wat jouw advies of aanbeveling teweeg kan brengen. Wees je heel bewust van jouw rol. Luister ook goed naar de boodschap van de ander, soms is het goed om hier iets van mee te nemen in de rapportage.'

Welk advies zou je IT-auditors willen meegeven?
'Met name interne auditors zouden beter en in een vroeger stadium van de audit moeten communiceren. Ik heb ervaren dat externe audits eerder worden aangekondigd dan interne audits. Er gaat een zorgvuldig proces vooraf aan de totstandkoming van een auditprogramma. De opgestelde auditprogramma's worden echter nogal eens slecht gecommuniceerd binnen organisaties. Maak bijtijds duidelijk wat je gaat doen en geef bijvoorbeeld aan wat je verplicht bent te doen. Dit geldt ook tijdens de uitvoering. Je kunt niet drie maanden niets van je laten horen en dan opeens een rapport op de bus doen. Een auditor moet ook tussentijds communiceren. Voor een auditee voelt een audit toch vaak aan als een tentamen. Iets anders: de auditor wil het management doorgaans wijzen op verbeterpunten, maar gaat daar soms te ver in door en moet afgeremd worden. Je kunt op meerdere manieren naar de wereld kijken!'

Is er ooit een comeback mogelijk naar de IT-audit?
'Ik sluit niets uit, maar het is niet het eerste waar ik naar kijk. Het vak risk management biedt mij nog veel mogelijkheden om verder te groeien.'

Tot slot: hoe kijk jij als CISA aan tegen de fusie tussen NOREA en ISACA?
'Zoals ik al aan het begin zei, heb ik het auditvak geleerd in mijn periode bij KPMG. Ik heb geen RE-auditopleiding gedaan, omdat ik eigenlijk gelijk ging samenwerken met zeer ervaren hoogleraren en docenten van deze opleidingsinstituten. Met mijn IT-ervaring kon ik direct aan de slag en wat is mooier dan het IT-auditvak gelijk in de praktijk toe te passen? Ik moest echter wel het CISA-examen doen om op z'n minst zelfstandig als auditor te kunnen werken, zeker bij opdrachten in het buitenland. Daar hoef je bij het begrip "CISA" verder niets meer uit te leggen, in tegenstelling tot "RE". Ik ben van mening dat de RE-opleiding een grotere diepgang heeft dan het CISA-traject. Een RE heeft er ook meer voor moeten doen. Maar, hoewel NOREA en ISACA beide hun eigen historie hebben, kunnen ze elkaar wel degelijk aanvullen en dat is goed voor het vakgebied.'

Bart werpt naar aanleiding van de recente incidenten rond het afgeven van assurance-verklaringen nog een interessante vraag op: 'Moeten RE's zich niet bezinnen op de vraag wat het leveren van 'assurance' feitelijk betekent?'
'Ik denk dat dit voor de kantoren mede naar aanleiding van elk recent incident steeds vaker een riskante opgave wordt. Naar mijn mening zouden RE's en CISA's wel eens meer "gewoon" hun bevindingen moeten rapporteren in plaats van assuranceverklaringen af te geven. Mede op basis van deze vraagstelling verwacht ik nog wel grote veranderingen in het auditvak.' ■