# Enige capita selecta

*Ir. drs. J. van der Vlugt RE*

De wordingsgeschiedenis van het vakgebied brengt met zich mee dat sommige onderwerpen inherent 'multidisciplinair' zijn. Een prima zaak, dat toont immers aan dat de veranderingen en de toenemende breedte en complexiteit van de IT-wereld kunnen worden geabsorbeerd.

Een voorbeeld van zo'n ontwikkeling is het groeiende gebruik van digitale handtekeningen, certificaten en dergelijke, waarmee een basis van vertrouwen wordt gegeven in het elektronische berichtenverkeer. Enigszins vreemd dat zoiets nodig is, we vertrouwen tenslotte normaliter zeer veel van de traditionele post die we ontvangen – en die is niet zo veel moeilijker te vervalsen dan elektronische post. Maar het is niet zo vreemd als de explosie aan potentiële daders in ogenschouw wordt genomen. Plotseling staan we immers in het wereldwijde adresboek. Bovendien zijn de berichten moeilijker op authenticiteit te controleren. Een gevolg is dus dat er behoefte is aan eenvoudige controlemogelijkheden. Met de komst van SET worden die gerealiseerd.

Een ander voorbeeld van zo'n ontwikkeling is de introductie van de euro. Al eerder in dit boek werd er aandacht aan gegeven, maar dan vanuit het traditionele IT-auditorperspectief. Dit artikel houdt de IT-auditor een spiegel voor door aan te geven dat voor veel organisaties een andere (primaire) invalshoek toch betere resultaten kan opleveren. Door de euro vanuit strategisch perspectief te benaderen, blijkt de introductie beter te kunnen worden beheerst, en de voordelen van de euro te kunnen worden uitgebuit.

Ook voor het wat meer traditionele werkterrein van informatiebeveiliging kan een top-downbenadering verfrissend werken. De klassieke insteek om alle kwaliteitsaspecten zomaar bij alle objecten tot in detail uit te spellen en te implementeren, draagt op z'n zachtst gezegd het risico wat minder efficiënt te zijn dan nodig is. Vandaar dus dat er moet worden onderhandeld; over de risico's en maatregelen, hetgeen uiteindelijk uitdraait op de kosten en baten van informatiebeveiliging. Uiteindelijk, dat wel, want een te oppervlakkige benadering is natuurlijk vlees noch vis terwijl juist de zo dadelijk geschetste systematische benadering resultaat levert.

Als dan de analyses vooraf zijn gedaan, is het zaak ook te zorgen dat de continuïteit wordt gewaarborgd of beter, wordt gemanaged. Want continuïteit is niet zomaar synoniem met een noodplannetje, maar wordt pas werkelijk goed beheerst als deze vanuit een risicoanalytische benadering stapsgewijs is verfijnd, en de juiste selectie van aanvaardbare en niet-aanvaardbare risico's is gemaakt. Pas als dan een juiste selectie van maatregelen tegen de niet-aanvaardbare risico's is gemaakt, kan aan de feitelijke implementatie van continuïteitsborgende maatregelen worden begonnen, en kan de controle op handhaving ervan worden uitgestippeld.

Bij het onderwerp maatregelen komt nogal eens, en terecht, de term ITIL naar voren. Tot nu toe ontbrak daarin het stuk Security Management. Maar de komende vijfentwintig jaar van ons vakgebied kan worden ingegaan met een raamwerk dat er wezen mag. ITIL Security Management is niet blijven steken in een dun boekje over *do's* en *don'ts*, maar is juist een uitgebreid handvat voor eenieder die de beveiliging van de informatievoorziening in een organisatie op een gestructureerde wijze wil vormgeven en die dan ook stapsgewijs uitwerken.

Een stapsgewijze verfijning ligt in wezen ook besloten in de benadering van informatiebeveiliging als geheel door eerst het Voorschrift Informatiebeveiliging Rijksdienst te analyseren, en door direct te vervolgen met een implementatie van de Code voor Informatiebeveiliging. Met een implementatie van de Code die op zichzelf ook een stramien volgt van voorzorg: algemene kaders, richtlijnen en randvoorwaarden tot zorg: feitelijke implementatie, en nazorg in de vorm van evaluaties.

De zorgsector op zich heeft een aanzienlijke ontwikkeling achter de rug. Pas de laatste jaren beginnen de contouren van een heldere structuur opnieuw duidelijk te worden. Ook begint de toepassing van IT in de gezondheidszorg volwassen te worden. Deze twee bewegingen brengen met zich mee dat de IT-auditor volgens een meer heldere structuur zijn methodologie kan inrichten, maar ook dat het belang van informatieverwerking en dus de rol van de IT-auditor als helper bij de beveiliging ervan, sterk toenemen.

Het boek sluit met het begin, van het IT-auditvakgebied. Immers, doordat IT-auditors zich in de loop der jaren steeds explicieter onderscheiden van de 'traditionele' accountants, zijn de accountants nog niet gevrijwaard van invloed van automatisering op hun vakgebied. Integendeel welhaast. Vandaar dat een overzicht van IT-auditland van oude stamlanden tot en met de nieuwe buitengebieden, niet compleet is zonder het grensgebied met het belangrijke buurland te verkennen.