Trends in ICT 2003

Kessel, Paul van; Rust, Christa

Published in:
De EDP-auditor

Publication date:
2003

Column
Rekenkoninkjes en drakendoders

Anton Tomas

AUDITORS ZIJN NOG NIET ZO SAAI

Enkele dagen voordat ik dit stukje schreef, bevond ik mij in een eigenaardige situatie: ik was met enkele tientallen auditors canons aan het zingen. Nee, het was niet tijdens de EuroCACS 2003. Dit was een zangmanifestatie met allerlei soorten auditors: financial, operational, IT, internal. En ik moet zeggen: auditors zijn nog niet zo saai.
De liedteksten hadden niet zo veel met ons vak te maken, getuige het volgende bekende kampvuurliedje dat wij vol overgave zongen:

I like the flowers, I like the daffodils,
I like the mountains, I like the green hills,
I like the firestone, I like to walk alone,
Kah do wah Kah do wah Kah do wah Kah do wah dah dah

Als dit al ergens over gaat, dan toch zeker niet over auditing, althans dat vermoed ik. Het bracht me op het idee om eens na te gaan of er eigenlijk ook liederen bestaan die de auditor bezingen en, in verband met de titel van dit tijdschrift, in het bijzonder de IT-auditor. Met het oog op een volgend kampvuur, zal ik maar zeggen. Ik benader het vraagstuk, zoals men van mij gewend is, gestructureerd. Dat wil in dit geval zeggen dat ik eerst nog maar eens naga of IT-auditors zich op enige wijze onderscheiden van anderen. Want als dat niet zo is, dan valt er natuurlijk ook niets onderscheidenlijks te bezingen. Daarna ga ik op zoek naar lyrische teksten over auditors.

Ir. A.J. Tomas RE RI RO is elektrotechnisch ingenieur, informaticus en auditor en 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. Bij de AMBI-opleiding is hij voorzitter van de examencommissie voor het onderdeel *Management van Informatiebeveiliging*. Verder is hij lid van de redactie van het tijdschrift *De EDP-Auditor.*

IT-AUDITORS ZIJN ONZICHTBAAR

Onderscheidt de beroepsgroep van IT-auditors zich, afgezien van het hebben van een eigen vakgebied, in enig opzicht van andere beroepsgroepen? Hebben IT-auditors bijvoorbeeld een eigen cultuur, zoals veel andere beroepsgroepen die kennen?

Neem nu eens de aan IT-auditors verwante beroepsgroep van automatiseerders. Vertegenwoordigers van die groep kenmerken zich vaak door een wat informele kleding en haardracht, tenzij hun carrière ze gebracht heeft in de troebele, doch blijkbaar opwindende wateren van de commercie. In dat geval neigt men meer naar het gelikte-pakken-met-dasspelden uiterlijk van de colporteur en de tweedehands autoverkoper. Enkele jaren geleden tooiden de commercieel ingestelde automatiseerders zich nog wel eens met een paardenstaart boven een strak kostuum. Die trend is geloof ik passé, maar het geeft wel aan dat de beroepsgroep zich wenste te onderscheiden. Overigens was die paardenstaart meer een Amerikaans fenomeen en, neemt u mij niet kwalijk, ik had het eigenlijk over cultuur. Verder heb je onder automatiseerders een meer dan gemiddeld aantal lieden dat neigt naar het mystieke, dat Douglas Hofstadter's 'Gödel, Esscher, Bach' heeft gelezen en tot het diepe inzicht is gekomen van 'er is meer'.

Of neem de groep van accountants, de echte wel te verstaan: die na de middelbare school meteen een volledige baan van ten minste zestig uur per week hebben gezocht en daarna ten minste tien lange jaren hard hebben gestudeerd in de avonduren en de weekeinden; dus niet op de vrije vrijdag bij de huidige vierdaagse werkweek. Dat is ook een aan IT-auditors verwante beroepsgroep en deze groep heeft ook zo zijn eigenaardigheden: veel lederen koffers met de opening van boven, ook wel vliegtuigkoffer genoemd, een hoger dan gemiddeld percentage echtscheidingen, hetgeen men compenseert met het streven toch weer 'partner' te worden maar dan beroepsmatig,

en het zorgvuldig in stand gehouden beeld van de zestigurige werkweek.

En de beroepsgroep van IT-auditors? Nou ja, bij EuroCACS 2003 zag ik misschien een groter dan gemiddeld aantal snorren van het type moustache. Maar voor het overige kwam de EuroCACS-populatie wat uiterlijke kenmerken betreft volledig overeen met de bezetting van een eerteklas treincoupé tijdens de ochtendspits, afgezien van de buitenmodel EuroCACS-ringband in schouderdraagtas met sponsoropdruk, waarin afdrukken van alle tijdens de lezingen vertoonde lichtbeelden waren opgenomen, zoals er bij echte congressen echte teksten zijn opgenomen die de echte inhoud van de lezingen weergeven. Onderscheiden IT-auditors zich, afgezien van het uiterlijk, bijvoorbeeld inhoudelijk, op de een of andere wijze? Volgens mij niet. Grijze muizen! Type ‘opvallen is risicovol’. Auditors mijden nu eenmaal risico’s, getuige de meest gehanteerde zinswending in auditrapporten: ‘ Wij hebben geconstateerd dat er onvoldoende waarborgen aanwezig zijn om…’. Overigens is dat best knap: constateren dat er iets niet is. Na mijn conclusie dat IT-auditors zich niet onderscheiden en dus eigenlijk niet zichtbaar zijn, richt ik mij maar snel op de volgende onderzoeksvraag van mijn betoog.

DE AUDITOR ALS LYRISCH OBJECT

Is de auditor al ontdekt door de kunst? Zijn er al liederen waarin de auditor wordt bezongen? Ik heb wat naspeuringen verricht en ben daarbij zowaar gestuit op het volgende sonnet met de titel ‘Rekenkoninkjes’:

REKENKONINKJES

Jaarlijks heel druk in de weer,
vrijheid van denken wat pover,
hoog in de bol (gaat wel over),
maar wel zeer recht in de leer,

speuren ze door het archief,
slepen met mappen en dozen
die ze vervolgens weer lozen.
Zie hier het vinkcollectief.

Buiten hen mag men niet rekenen.
Niet te vermijden, het moet!
Jaarlijks een stuk ondertekenen

is de essentie van ’t werk.
Wat een bestuurder ook doet,
macht ligt nog steeds bij een klerk.

Als ik mij niet vergis gaat dit sonnet over accountants die belast zijn met de jaarrekeningcontrole. Dat is heel bijzonder! Gelijk allerlei oude eerbiedwaardige ambachten, zoals dat van de boer, de veerman en de metselaar, wordt nu blijkbaar ook het beroep van de accountant bezongen door de dichter. De accountant als object van kunst! Hoewel men bij dit specifieke voorbeeld natuurlijk zo zijn gedachten kan hebben over de kijk van de dichter op het accountantsberoep. Maar daar til ik niet zo zwaar aan, want wat kun je van een dichter wat dat betreft nou verwachten?

Helaas had ik minder succes bij mijn speurtocht naar lyrische teksten over IT-auditors. Die lijken er niet te zijn. Ik hoop nu maar dat dit komt doordat het beroep van IT-auditor daarvoor met een leeftijd van zo’n dertig jaar nog te jong is. Maar ik vrees dat de oorzaak hierin ligt dat de IT-auditor ook voor de dichter onzichtbaar is: de IT-auditor is immers een grijze muis die zich in geen enkel opzicht onderscheidt van anderen, waardoor ook de dichter hem helemaal niet ziet! Het is natuurlijk onmogelijk om daar een lied op te schrijven. Maar misschien, heel misschien, ben ik wat te somber. Tijdens mijn speurtocht naar gezangen op de IT-auditor, die er niet bleken te zijn, kwam ik het gedicht ‘De Drakendoder’ tegen:

DE DRAKENDODER

Zeven koppen telt het monster, en nog
meer dan eens dat aantal vliedt de stroom van
woorden, woorden, meer dan woorden stroomt
het licht door levens vezels, meer dan kennis.

Met zijn pijlen bedwingt hij het beest en zijn
geest temt de stromen van licht en van woord.

Zeven pijlen telt zijn koker, maar geen
mens kan zien hoe zijn magie het beest betovert. Niets is echt en niets is waar.
Niets te weten, immer dolend, drakendoder.

Bij eerste beschouwing dacht ik dat dit gedicht over Sint Joris en de draak gaat of over een ander middeleeuws thema. Maar bij nadere beschouwing verdenk ik de dichter van kennis van IT en zelfs van IT-auditing. Stel dat met het ‘monster’ de automatiseringswereld wordt aangeduid en dat met ‘woorden’ en ‘meer dan woorden’ de dichter doelt op respectievelijk gegevens en informatie; stel dat ‘levens vezels’, de vezels van het leven van het monster waar het ‘licht’ doorheen stroomt, gewoon glasvezels zijn. Dan zou ‘de drakendoder’ de IT-auditor kunnen verbeelden. Dus toch! Een gedicht op de IT-auditor! Alleen de betekenis van de laatste strofe zit me nog een beetje dwars.

Kop xxxxxxxxxxxxxxxxxxx xxxxxxxxxxxx

Xxxxxxxxxxxxxxx Xxxxxxxxxxxxxxx Xxxxxxxxxxxxxxx Xxxxxxxxxxxx
xxx Xxxxxxxxxxxxxxx Xxxxxxxxxx xxxxx Xxxxxxxxx xxxxx Xxx xxx xxxx xxxxx Xx
xxxxxxxxxxxxxxxxxxxxxxx Xxxxxxxxxxxxxxx Xxxxxxxxxxxxxxx
Xxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxx
xxxxx xxx Xxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxxxxxxxx

Auteur xxxxxxx

Auteursnoot xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxx.

Trends in ICT 2003

Onlangs werden de resultaten van het Ernst & Young-onderzoek 'Trends in ICT 2003' bekendgemaakt. In dit artikel wordt met name aandacht besteed aan de uitkomsten met betrekking tot e-business en informatiebeveiliging.

Paul van Kessel en Christa Rust

Medio december 2002 werden de resultaten van het onderzoek Trends in ICT 2003[1] bekendgemaakt. In samenwerking met onderzoeksbureau Blauw Research BV worden per jaar zes on line onderzoeken gehouden, op zoek naar trends in ICT. De vijf ICT-Barometermetingen van 2002 en het uitgebreide onderzoek Trends in ICT geven een interessant beeld van de inzet en het gebruik van ICT in Nederland. De themagebieden beslaan HRM, security, e-business, ICT in de organisatie en de prestaties van ICT-bedrijven. De specifieke onderwerpen waarnaar onderzoek is gedaan, werden bepaald op grond van dilemma's en vraagstukken in de dagelijkse praktijk bij de cliënten van Ernst & Young.

De 650 respondenten zijn afkomstig uit organisaties van verschillende grootte, diverse branches en bekleden deels wel en deels niet een ICT-functie. De respondenten zijn nauw betrokken bij hun organisatie, zijn fulltime werkzaam, hoger opgeleid en bekleden een leidinggevende functie. Aan het onderzoek hebben directeuren, managers en ICT-professionals uit de sectoren productie/industrie, handel/distributie, overheid/not-for-profit en dienstverlening meegewerkt.

GEBREK AAN VERTROUWEN IN SECURITY EN PRIVACY REMT GROEI E-BUSINESS

Ten opzichte van andere westerse landen scoort Nederland goed op het gebied van e-business. Eind 2002 publiceerde de Economist Intelligence Unit (EIU) de nieuwste 'e-readiness ranking', waarin e-readiness wordt gedefinieerd als 'de mate waarin de zakenomgeving van een land op internet gebaseerde commerciële mogelijkheden stimuleert'. Nederland stijgt met stip van de tiende naar de tweede plaats. De redenen hiervoor zijn: een geavanceerde IT-infrastructuur, een hoge penetratiegraad van mobiele telefonie, een laagdrempelige en hoge internetpenetratie, een relatief hoog inkomen per hoofd van de bevolking, een goed overheidsbeleid en een goede algemene zakelijke omgeving.

Eerder publiceerde het Centraal Bureau voor de Statistiek reeds dat het on line landschap (ook wat betreft de consumentenmarkt) volwassen is. 74% van de Nederlandse huishoudens beschikt over een computer, 57% heeft een internetaansluiting en het aantal huishoudens waar wel eens iets via het internet wordt gekocht, is in de periode 1998-2001 gestegen van 2% tot 11%.

Op basis hiervan zou kunnen worden verondersteld dat de hoge verwachtingen, die een paar jaren geleden werden uitgesproken ten aanzien van de e-business-activiteiten in Nederland, zijn uitgekomen. Maar dat is niet het geval. In 2001 gaven de respondenten van Trends in ICT aan te verwachten dat de omzet via het internet (destijds gemiddeld 7%) binnen twee jaar zou groeien naar 15%.
De teller is blijven steken op een gemiddeld percentage van 10%. Het ligt misschien voor de hand om dit grotendeels te wijten aan de economische teruggang van 2002, maar uit het onderzoek blijkt duidelijk dat er meer factoren zijn die hier een rol spelen.

Prof. Drs. P. van Kessel RE RA en C. Rust

Ernst & Young EDP Audit

Als voornaamste oorzaken voor de rem op het succes van e-business worden genoemd: ‘afnemers hebben te weinig vertrouwen in security’ en ‘afnemers hebben te weinig vertrouwen in privacy’. Het gebrek aan vertrouwen in de beveiligingsaspecten wordt al jarenlang genoemd als de voornaamste belemmering voor de ontwikkeling van e-business. Privacy is een nieuw ‘hot issue’ en is dan ook gestegen van een vijfde naar de tweede plaats. Zakendoen via het internet betekent immers veelal dat er privacygevoelige gegevens verstrekt moeten worden. Klanten c.q. consumenten hebben er weinig vertrouwen in dat ondernemingen op de juiste wijze met deze gegevens omgaan.

Opvallend is het dat ‘te weinig vertrouwen in betalen via het internet’ is gezakt van de tweede naar de vierde plaats. Betalingsverkeer via het internet en beveiliging horen weliswaar bij elkaar, maar de afgelopen jaren is men blijkbaar gewend geraakt aan betalen via het internet en zijn de mogelijkheden daartoe ook een stuk veiliger geworden. Het gebrek aan vertrouwen in de beveiliging van websites zelf en de on line uitwisseling van gegevens blijft een belangrijk aandachtspunt.

PRIVACY, EEN NIEUW ‘HOT ISSUE’

Zoals hierboven beschreven bleek uit het onderzoek duidelijk dat privacy een nieuw ‘hot issue’ is. Ondanks de onlangs in werking getreden Wet Bescherming Persoonsgegevens, waarin duidelijke eisen worden gesteld aan de manier waarop persoonsgegevens worden verwerkt, hebben organisaties onderling nog weinig vertrouwen in de manier waarop met deze gegevens wordt omgegaan. Dit geldt in sterke mate ook voor de business-to-consumermarkt, zo blijkt uit het in 2002 door Ernst & Young gepubliceerde onderzoek ‘Privacy On and Off the Internet, What Consumers Want’[2].

Consumenten maken zich ronduit zorgen over de manier waarop organisaties met privacygevoelige gegevens (zoals persoonsgegevens, creditcardnummers en informatie omtrent financiële transacties) omgaan. Het meest wordt ervoor gevreesd dat deze gegevens worden verkocht of zonder toestemming worden gedeeld met andere organisaties. Ook is men er bang voor dat de gegevens worden gestolen of gebruikt door lieden die zich zonder toestemming toegang hebben verschaft tot informatiesystemen van bedrijven. Zaken die aan de ene kant te maken hebben met de integriteit van organisaties en aan de andere kant met de beveiliging en beheersing van de gegevens en de systemen. In dit onderzoek is aan ruim 1.500 consumenten gevraagd welke actie zij zullen ondernemen indien blijkt dat een organisatie niet correct omgaat met persoonsgegevens. Het antwoord liegt er niet om: 99% stelt dat ze de relatie met de betrokken onderneming verbreekt of dat de omvang van de relatie zal worden teruggebracht!

GEBRUIK VAN INTRANET STAAT NOG GROTENDEELS IN DE KINDERSCHOENEN

In hoeverre passen Nederlandse organisaties internettechnologie toe in (de ondersteuning van) de bedrijfsprocessen? Uit het onderzoek blijkt dat zo’n 90% van de ondervraagde organisaties e-mailfaciliteiten heeft, ruim 85% heeft een website en ruim 75% van de medewerkers heeft via de werkplek toegang tot het internet. Veel Nederlandse organisaties zijn met een website vertegenwoordigd op het internet, maar deze sites worden voornamelijk gebruikt voor het verstrekken van informatie en het leggen van contacten met (potentiële) klanten. Van de respondenten geeft 25,6% aan dat via hun website orders geplaatst kunnen worden. Daarbij is het natuurlijk nog maar de vraag of de order dan ook direct in bijvoorbeeld het verkoopsysteem terecht komt of nog handmatig in dit systeem moet worden ingevoerd. Slechts 32% van de organisaties geeft aan orders via de website direct in de interne informatiesystemen verder te verwerken.

Het gebruik van intranet (65% van de ondervraagde organisaties) blijft in vergelijking met het gebruik van het internet wat achter. Intranet wordt toch nog vaak beschouwd als vervanging voor het oude ‘mededelingenbord’. Daarnaast wordt het intranet gebruikt om kennis en informatie (bijvoorbeeld uit databases) beschikbaar te stellen en voor discussiedoeleinden binnen de organisatie. Slechts 34% van de ondervraagde organisaties geeft aan dat het intranet echt een geïntegreerd onderdeel is van de bedrijfsprocessen.

SURFEN OP HET INTERNET: WIE KIJKT ER MEE?

Ruim driekwart van de respondenten geeft aan dat medewerkers in de organisatie vanaf de werkplek toegang hebben tot het internet. Over het algemeen is men van mening dat dit zowel de eigen arbeidsproductiviteit als die van de organisatie als geheel ten goede komt. Toch wordt 32% van de tijd die men onder werkuren op het internet doorbrengt, benut voor privé-doeleinden. Dat is toch nog gemiddeld één uur en drie kwartier per week. Ofwel: één uur en drie kwartier extra pauze. Op jaarbasis is dat ongeveer twee weken extra vakantie…

50% van de organisaties geeft aan dat men toezicht houdt op het surfgedrag van de medewerkers op het internet.

In Trends in ICT 2001 was dit nog 60%. Het monitoren op zich neemt dus af, maar daarentegen wordt nu wel vaker het indivuele surfgedrag van medewerkers in de gaten gehouden. Werden individuele werknemers in 2001 nog slechts in 7% van de organisaties in de gaten gehouden, nu is dit in 18% van de organisaties het geval. Met name in de grotere organisaties is de mate waarin toezicht wordt gehouden toegenomen; dit zal ongetwijfeld gerelateerd zijn aan het feit dat in de grotere organisaties in verhouding ook meer privé gesurft wordt.

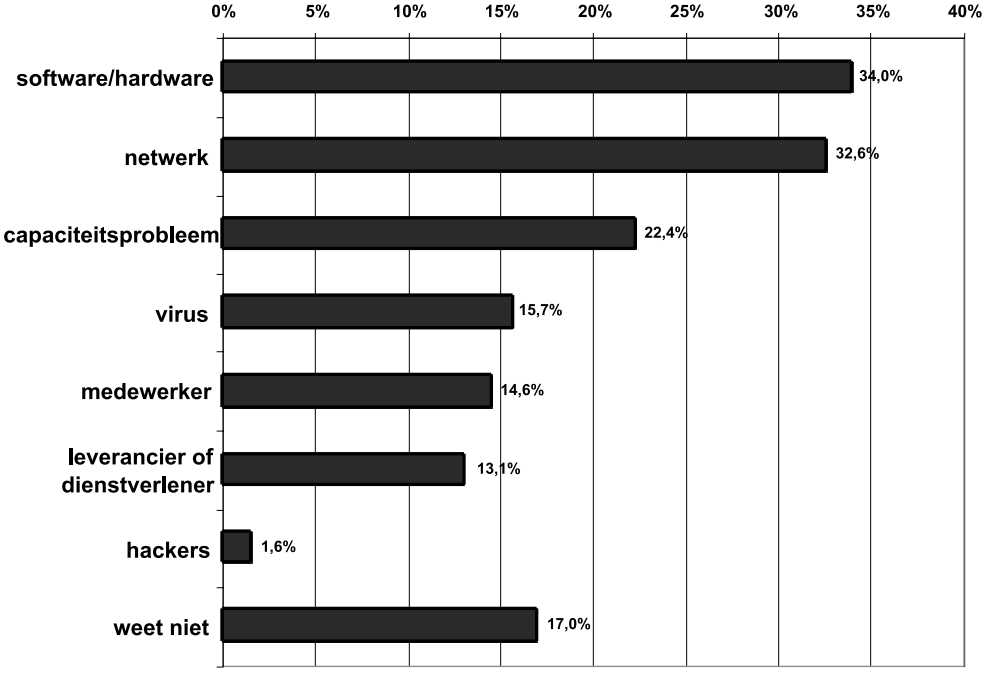
WIE NEEMT DE BESLISSINGEN OP HET GEBIED VAN ICT?

Uit Trends in ICT-onderzoeken van enkele jaren geleden bleek dat in het merendeel van de situaties het financieel management de beslissingen omtrent ICT-vraagstukken nam. Welke functionaris is tegenwoordig eigenlijk verantwoordelijk voor deze beslissingen? Wie bepaalt de toekomst? Uit Trends in ICT 2003 blijkt dat maar liefst 20,6% procent van de directeuren, managers en professionals niet weet wie in hun organisatie de ICT-beslissingen neemt. De beslisprocessen en geformuleerde doelstellingen rond ICT-vraagstukken zijn niet voor iedereen helder.

Naast de 20,6% van de ondervraagden die niet weet wie de beslissingen neemt op ICT-gebied, blijkt uit de antwoorden van de overige respondenten dat de uiteindelijke beslisser over ICT-vraagstukken in 34,2% van de organisaties het algemeen management is. Op de tweede plaats (27,0%) komt het ICT-management als beslisser. Het financieel management lijkt met 7,9% te hebben afgedaan als beslissende partij. Hoewel wij deze ontwikkeling in algemene zin onderschrijven, moet ervoor worden gewaakt dat de verminderde rol van het financieel management niet leidt tot het veronachtzamen van kosten/baten-afwegingen bij ICT-beslissingen.

GROTE AFHANKELIJKHEID VAN ICT, WEINIG CONTINUÏTEITSPLANNEN

De primaire bedrijfsprocessen worden in steeds grotere mate ondersteund door informatiesystemen, waardoor de afhankelijkheid van de systemen enorm is toegenomen. Uit één van de ICT-Barometermetingen is gebleken dat tweederde van de Nederlandse organisaties sterk afhankelijk is van ICT; een kwart van de organisaties is er zelfs volledig van afhankelijk. Met deze cijfers in het achterhoofd zou je verwachten dat de grote meerderheid van de organisaties maatregelen heeft getroffen om de continuïteit te waarborgen. Als de systemen uitvallen, moet de organisatie kunnen terugvallen op formeel vastgelegde protocollen, ofwel plannen waarin procedures zijn vastgelegd voor uitwijk, back-up en recovery.



Figuur 1. Oorzaken voor uitval van computersystemen

Uit het Ernst & Young-onderzoek Global Information Security Survey 2002[3] blijkt dat wereldwijd 53% van de organisaties een continuïteitsplan heeft. In Nederland heeft slechts 32% van de organisaties een formeel continuïteitsplan dat ook goed bekend is in de organisatie. 16% heeft wel een continuïteitsplan, maar daarvan is de inhoud niet goed bekend in de organisatie en 20% weet het niet. De organisaties die een plan hebben, zouden zich ervan moeten verzekeren dat het plan in de praktijk ook werkt, door impact-analyses uit te voeren en de plannen te testen.

TECHNISCHE PROBLEMEN VEROORZAKEN UITVAL KRITISCHE INFORMATIESYSTEMEN

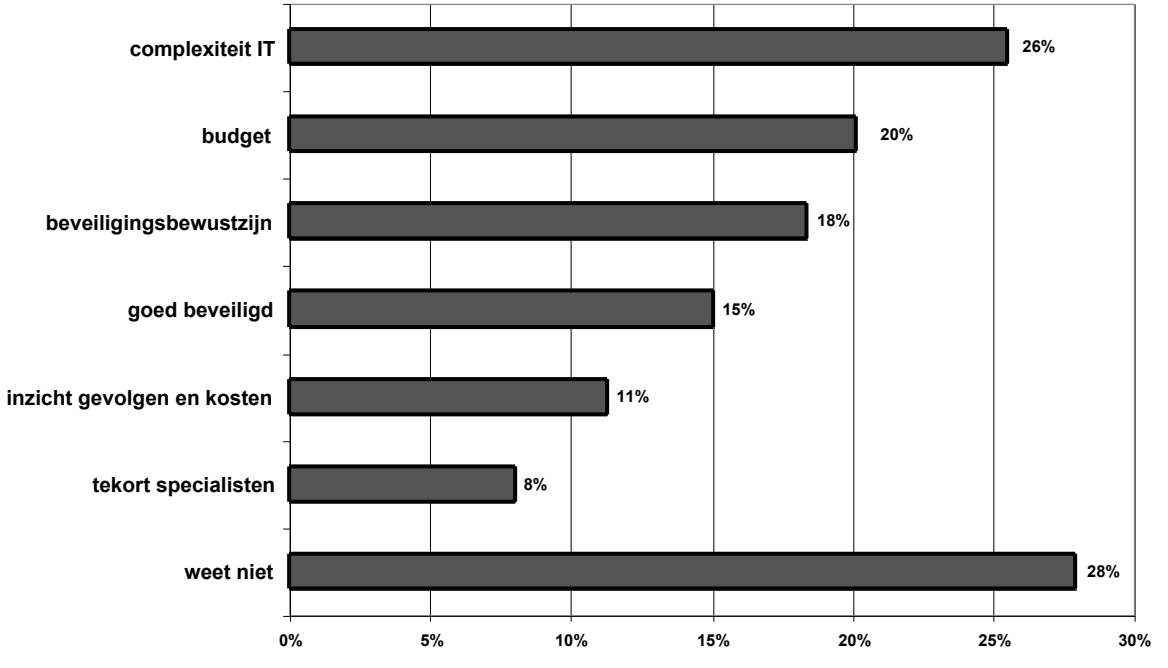
Figuur 1 geeft aan wat volgens de respondenten van het onderzoek de meest voorkomende oorzaken zijn van het uitvallen van computersystemen. Indien deze niet beschikbaar zijn, kan ernstige schade worden gelopen. De eerste drie genoemde oorzaken, te weten hardware/software, netwerk en capaciteitsproblemen staan al jaren bovenaan de lijst en zijn technisch van aard.
Opvallend is het dat virussen toch nog door meer dan 15% van de ondervraagde organisaties worden genoemd, terwijl tegen virussen inmiddels vele eenvoudig te implementeren oplossingen bestaan. Mensen (onder wie medewerkers, leveranciers en dienstverleners) blijven ook nog voor een belangrijk deel van de problemen zorgen.

17% van de ondervraagde organisaties weet niet of de systemen het wel eens laten afweten en/of wat de oorzaak daarvan is. Ongetwijfeld doen zich daar ook problemen voor, maar de oorzaak is onbekend. Zorgwekkend, omdat het kennen van de oorzaak het begin is van het voorkomen.

Hackers staan ergens onderaan in de lijst. Vormen zij dan geen serieuze bedreiging? Schijn bedriegt. Want bedenk wel dat de gevolgen van het uitvallen van de systemen op grond van technische oorzaken weliswaar vervelend zijn, maar vaak met weinig moeite kunnen worden hersteld. De schade van een geslaagde hackpoging is over het algemeen vele malen groter. Volgens de ondervraagden ligt de grootste impact van hackers op het operationele vlak, met overigens alle financiële gevolgen van dien. Maar een geslaagde hackpoging kan ook de reputatie van een organisatie enorm beschadigen.

LOPEN HACKERS IN EN UIT?

Bijna de helft (46%) van de organisaties is er niet zeker van dat een aanval van hackers op tijd wordt gesignaleerd. Dit is zeer zorgwekkend, want dit zou kunnen betekenen dat hackers in en uit lopen zonder dat iemand het in de gaten heeft.
De meest toegepaste technologie op het gebied van infor-



Figuur 2. Belemmeringen voor het bereiken van het gewenste beveiligingsniveau

matiebeveiliging bestaat overigens nog steeds uit standaard beveiligingssoftware. Momenteel wordt nog maar weinig gebruikgemaakt van geavanceerde technologie. De beveiligingsactiviteiten die wel plaatsvinden, zijn vaak de meest elementaire voorzieningen, zoals firewall-beheer en bescherming tegen virussen.
Als er een beveiligingsincident plaatsvindt, stelt 17% van de Nederlandse organisaties geen nader onderzoek in. Dit ondanks herhaalde waarschuwingen dat het doorbreken van de beveiliging vaak leidt tot 'back doors' die later door kwaadwillenden kunnen worden gebruikt.

UITDAGINGEN OP HET GEBIED VAN INFORMATIEBEVEILIGING

Alhoewel de risico's op het gebied van informatiebeveiliging meer en meer door het management worden onderkend, blijkt het in de praktijk moeilijk om de juiste maatregelen te treffen en daarmee de beveiliging op peil te krijgen en te houden. Waar ligt dat aan? Met welke belemmeringen hebben we te maken?

De top drie van grootste belemmeringen voor informatiebeveiliging ziet er volgens het onderzoek als volgt uit:
de snelheid van veranderingen en de toenemende complexiteit van bedreigingen;
beperkte financiële middelen;
het creëren van beveiligingsbewustzijn onder de eigen medewerkers.

Meer dan een kwart van de organisaties geeft aan dat de snelle veranderingen op het gebied van ICT en de toenemende complexiteit daarvan een gevoel geven van 'water naar de zee dragen'. Deze organisaties hebben het gevoel het niet bij te kunnen benen. Zodra beveiligingsmaatregelen zijn getroffen, dienen zich alweer nieuwe risico's aan. Dit wordt uiteraard nog versterkt door het tekort aan beveiligingsspecialisten, het ontbreken van een centraal beveiligingsbeleid in de organisatie en onduidelijke verantwoordelijkheden.

Een andere hoog scorende oorzaak is het gebrek aan financiële middelen. Blijkbaar heeft het erkennen van de risico's nog niet tot gevolg dat er voldoende geld wordt vrijgemaakt om de risico's te bestrijden. Het is echter 'pay now or pay later', waarmee wordt bedoeld: investeer nu in beveiligingsoplossingen of betaal straks de schade.

Het erkennen van de risico's is één, maar het ook bewust zijn van de mogelijke gevolgen en de omvang daarvan is twee! Opvallend is het dat een groot deel van de respondenten aangaf dat gebrek aan betrokkenheid en bewustzijn van de eigen medewerkers als een belangrijke barrière wordt beschouwd voor het realiseren van het vereiste niveau van informatiebeveiliging.

Beveiligingsbewustzijn of 'security awareness' blijkt voor veel organisaties een lastig onderwerp. Het wordt meestal benaderd als technisch probleem, terwijl het eigenlijk een gedrags- en cultuurvraagstuk is. Vaak blijven de activiteiten om de security awareness te verhogen, beperkt tot het uitreiken van een flyer met 'do's en don'ts' aan het personeel. Of en in welke mate resultaten zijn bereikt met deze activiteiten blijft meestal onduidelijk.

Tot slot: het is opvallend dat 28% van de organisaties aangeeft niet te weten waardoor de informatiebeveiliging nog niet op het gewenste niveau is. Ook hebben we gezien dat 17% van de organisaties niet weet door welke oorzaak een kritisch computersysteem is uitgevallen. Dit is een zorgelijke situatie. Immers: zolang de oorzaken van uitval van kritische computersystemen of van onvoldoende informatiebeveiliging nog niet in kaart zijn gebracht, is het begin van een oplossing nog niet in zicht.

Noten

1 Trends in ICT 2003 is de zevende editie van het Ernst & Young-onderzoek Trends in ICT. Het onderzoek werd voorafgegaan door vijf ICT-Barometermetingen (tweemaandelijkse online-onderzoeken). De resultaten van de ICT-Barometermetingen en het uitgebreide onderzoek Trends in ICT zijn gebundeld in het jaarboek 'Trends in ICT 2003', dat verkrijgbaar is via de website www.trends-in-ict.nl.

2 Het onderzoeksrapport, met de verkorte titel 'Privacy, What Concumers Want', is te downloaden via de website www.ey.nl/edp.

3 Global Information Security Survey is een uitgebreid onderzoek naar informatiebeveiliging, dat jaarlijks in internationaal verband door Ernst & Young EDP Audit wordt uitgevoerd. Het rapport van de Global Information Security Survey 2002 kan worden gedownload via www.ey.nl/edp.

VIR-implementaties

Is het VIR wel geschikt voor de overheid?

Sinds 1995 zijn Rijksoverheden en ZBO's bezig met het Voorschrift Informatiebeveiliging Rijksoverheid. Om een antwoord te vinden op de vraag waarom VIR-implementaties zo moeizaam verlopen, is in dit artikel gekeken naar de (impliciete) kenmerken van het VIR. Deze kenmerken zijn beoordeeld op hun bruikbaarheid en afgezet tegen volwassenheidsniveaus van organisaties volgens het INK-model. Het artikel is primair gericht op het verdiepen van het inzicht in de VIR-problematiek. Daarnaast zullen enkele mogelijke oplossingen worden aangedragen.

René Steunebrink

INLEIDING

In 1996 ben ik als medewerker Beveiliging & Controle bij de RDW Dienst Wegverkeer in aanraking gekomen met het Voorschrift Informatiebeveiliging Rijksdienst (VIR). Vanaf het eerste moment sprak het relatief eenvoudige denkmodel achter het VIR mij aan. Het VIR-denkmodel gaat uit van het doel van de organisatie en het belang van een bedrijfsproces daarbinnen. Via afhankelijkheids- en kwetsbaarheidsanalyses wordt voor betrokken informatiesystemen op een navolgbare en beargumenteerde manier gekomen tot betrouwbaarheidseisen en -maatregelen. Dit klonk (en klinkt nog steeds) een stuk beter dan een aanpak waarbij normenstelsels van buiten en/of externe IT-auditors of andere beveiligingsdeskundigen de organisatie voorschrijven (of zelfs verplichten) welke maatregelen ze moeten nemen. Dit vaak zonder (expliciet) verband te leggen met de business van de organisatie. Het VIR gaat uit van de business en legt de verantwoordelijkheid weer terug waar het hoort, namelijk bij het lijnmanagement. Een goed en relatief eenvoudig denkmodel is echter geen garantie voor succes. Ondanks mijn enthousiasme en dat van vele anderen bleek het implementeren van betrouwbaarheidsmanagement volgens het VIR een lange en moeizame weg te zijn…

R. Steunebrink werkt als IT-auditor bij de RDW Dienst Wegverkeer te Groningen. Hij heeft ruime ervaring met het uitvoeren van A&K-analyses bij zowel advies- als audittrajecten. Het artikel is een verkorte weergave van het referaat waarmee hij eind 2002 zijn EDP-audit-opleiding aan de Erasmus Universiteit te Rotterdam heeft afgerond.

Foto binnen nog te scannen

Probleemstelling

In 1994 is voor de overheid het Voorschrift Informatiebeveiliging Rijksdienst (VIR) van kracht geworden. Sindsdien zijn overheidsorganisaties bezig met de implementatie van het VIR. Uit publicaties en uit eigen ervaring is duidelijk geworden dat VIR-implementaties veelal moeizaam verlopen. De ultieme doelstelling, dat het management actief z'n verantwoordelijkheid met betrekking tot de informatiebeveiliging neemt, wordt vaak niet gehaald. De subtitel van dit artikel luid dan ook 'is het VIR wel geschikt voor de overheid?'

Om de problematiek rondom het VIR nader te beschouwen, is onderstaande probleemstelling geformuleerd.

'Beschrijf en analyseer de problemen zoals die zich in de praktijk voordoen bij het implementeren van het Voorschrift Informatiebeveiliging Rijksdienst en draag voor die problemen mogelijke oplossingen aan'.

In dit artikel wordt eerst antwoord gegeven op onderstaande onderzoeksvragen:

1. Wat zijn de belangrijkste kenmerken van het VIR?
2. Wat betekenen deze kenmerken voor de bruikbaarheid van het VIR?
3. Wat is de relatie tussen de kenmerken en bruikbaarheid enerzijds en de volwassenheid van organisaties volgens het INK-model anderzijds?

Op basis van deze antwoorden is vervolgens een groeimodel beschreven, waarin wordt aangegeven hoe VIR-implementaties *kunnen* worden aangepakt, rekening houdend met het volwassenheidsniveau van een organisatie.

DE KENMERKEN VAN HET VIR

Het VIR, maar vooral de uitwerking daarvan in de afhankelijkheids- en kwetsbaarheidsanalysemethode, is een sterk formele, analytische en daarmee rationele topdown-aanpak. Vanuit de bedrijfsdoelstellingen wordt het belang van het betreffende bedrijfsproces vastgesteld. In de afhankelijkheidsanalyse wordt bepaald in welke mate het bedrijfsproces afhankelijk is van informatiesystemen. Die mate van afhankelijkheid bepaalt de betrouwbaarheidseisen waaraan betreffende informatiesystemen moeten voldoen. Vervolgens worden op basis van deze betrouwbaarheidseisen via een dreigingen- en kwetsbaarheidsanalyse de te nemen maatregelen bepaald en vastgelegd in een beveiligingsplan. Bij de afhankelijkheids- en kwetsbaarheidsanalyses wordt benadrukt dat de argumentatie moet worden vastgelegd. Hierdoor ontstaat een beredeneerde, navolgbare en reproduceerbare analyse, met een gelaagde structuur van betrouwbaarheidseisen, maatregeldoelstellingen en concrete maatregelen [VIR94].

Het VIR gaat uit van bedrijfsprocessen, maar beschrijft zelf ook een proces, namelijk het betrouwbaarheidsmanagementproces. Het proceskarakter blijkt uit de artikelen van het VIR die voorzien in een gesloten Demming-cirkel:
- *plan*: plannen en uitvoeren van afhankelijkheids- en kwetsbaarheidsanalyses en opstellen beveiligingsplannen (artikelen 3 en 4);
- *do*: implementatie beveiligingsmaatregelen (artikel 5);
- *check & act*: worden in de artikelen 2, 3, 4 en 5 expliciet genoemd.

Ook dit sluit aan bij het rationele en procesmatige 'control' denken.

Het VIR en de daarin beschreven afhankelijkheids- en kwetsbaarheidsanalyses is – in tegenstelling tot klassieke kwantitatieve risicoanalysemethoden – een kwalitatieve methode voor risicoanalyse [BROU96].
Het VIR richt zich op 'Informatiebeveiliging' en gaat er terecht vanuit dat organisaties steeds afhankelijker worden van informatie. Echter, informatieverzorging – hoe belangrijk ook – is 'slechts' een ondersteunend aspectsysteem naast andere, zoals het feitelijk besturen, beheersen en doen functioneren van een organisatie gericht op het leveren van producten en/of diensten aan klanten [STAR97]. Het informatiebeveiligingsproces – als deelproces van het informatieverzorgingsproces – is nog een verdere inperking. Het VIR beperkt zich dus tot het kwaliteitsaspect betrouwbaarheid (beschikbaarheid, exclusiviteit en integriteit) van de informatieverzorging.

Het VIR stelt in artikel 1 dat een informatiesysteem een geheel is van gegevensverzamelingen, personen, procedures, programmatuur en opslag-, verwerkings- en communicatieapparatuur. In de toelichting wordt gesteld dat het voorschift niet uitsluitend betrekking heeft op geautomatiseerde informatiesystemen [VIR94]. Echter, in de uitwerking van de kwetsbaarheidsanalyse in de door het ACIB uitgegeven handleiding A&K-analyse wordt gesteld dat een informatiesysteem of verantwoordelijkheidsgebied per definitie bestaat uit het samenstel van mensen, apparatuur, programmatuur, gegevensverzamelingen, organisatie, omgeving en diensten [ACIB97]. AO/IC-procedures zijn ondergebracht bij de component organisatie onder gebruikersorganisatie. In de basistabellen maatregelen en voorbeeldmatrices in het handboek wordt verder geen aandacht besteed aan AO/IC-procedures. In de praktijk blijken het VIR en de afhankelijkheids- en kwetsbaarheidsmethode zich te beperken tot het ICT-deel van de betrouwbaarheidsmaatregelen.
Het VIR gaat ervan uit dat de verantwoordelijkheid voor informatiesystemen en verantwoordelijkheidsgebieden eenduidig en duidelijk zijn toegewezen [VIR94].

De vraag 'wat zijn de belangrijkste kenmerken van het VIR' kan als volgt worden samengevat:
- Het VIR is een rationele aanpak.
- Het VIR ziet informatiebeveiliging als een proces.
- De afhankelijkheids- en kwetsbaarheidsanalyse is een kwalitatieve risicoanalysemethode.
- Informatiebeveiliging en daarmee het VIR is een 'beperkt' aspectsysteem.
- Het VIR beperkt zich tot ICT-betrouwbaarheidsmaatregelen.
- Het VIR gaat uit van een eenduidige verantwoordelijkheidsverdeling.

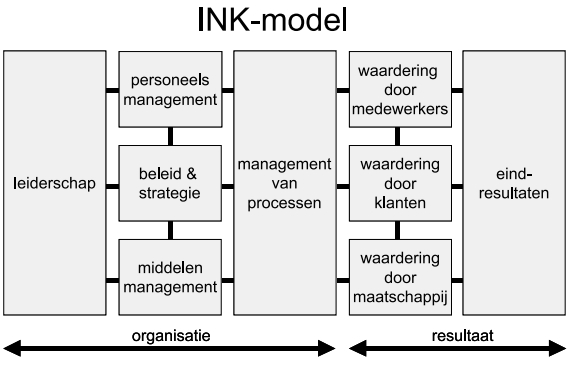
BRUIKBAARHEID VAN HET VIR

Het VIR stelt het lijnmanagment verantwoordelijk voor informatiebeveilging. Dit hoofdstuk geeft antwoord op de vraag of het VIR – gezien de kenmerken ervan – een

bruikbaar hulpmiddel is voor het lijnmanagement.
Het VIR is een rationele aanpak, die sterk is gebaseerd op het 'control' denken. Omtrent het werkelijk gedrag van (succesvolle) managers heeft Mintzberg veel empirisch onderzoek gedaan. Hieruit blijkt dat het planning en control-principe niet expliciet tot uitdrukking komt in de werkwijze. Managers zijn voortdurend bezig met uiteenlopende, veelal niet voorspelbare en formaliseerbare, activiteiten. Zij zien vaak af van delegatie omdat er geen tijd is om zaken goed te delegeren, vertrouwen op hun intuïtie omdat het niet mogelijk is eerst voldoende informatie te vergaren en doen veel om cultureel/politieke redenen (zorgen dat je afdeling in beeld is). Veel managers blijken de voorkeur te geven aan verbale informele communicatie als ondersteuning bij de besluitvorming [KAME95]. Van een zo handelende manager mag niet worden verwacht dat hij/zij goed zal kunnen werken met de 'control'-aanpak van het VIR.

Het VIR ziet informatiebeveiliging als een proces.
Afgezien van hetgeen hiervoor reeds is gesteld over de rationele aanpak van het VIR, is het bij een functioneel ingerichte organisatie buitengewoon lastig informatiebeveiliging procesmatig aan te pakken, omdat men – zelfs met betrekking tot de corebusiness – niet gewend is procesmatig te werken [DEKK00]. In de praktijk wordt informatiebeveiliging daarom veelal organisatorisch in plaats van procesmatig ingevuld [MAAR98].
De afhankelijkheids- en kwetsbaarheidsanalyse is een kwalitatieve risicoanalysemethode. Een kwalitatieve analysemethode sluit beter aan bij de gedachtewereld van het management, omdat een kwantitatieve aanpak nog rationeler is dan de kwalitatieve aanpak. Bovendien worden de A&K-analyses volgens een inzichtelijke redenering tot stand gebracht en vinden er voortdurend iteratieslagen plaats tussen de te nemen stappen. Zo ontstaat voor het management de mogelijkheid om gedurende het analyseproces zo nodig bij te sturen [BROU96].

Informatiebeveiliging is een 'beperkt' aspectsysteem.
Managers halen hun informatie in beperkte mate uit formele informatiesystemen. Naarmate er sprake is van hoger management zal ook meer toekomstgerichte (strategische) informatie nodig zijn, die veelal niet uit formele interne informatiesystemen gehaald kan worden [DAVI87]. Naarmate het management minder belang stelt in stuur- en beheersinformatie zal het ook minder interesse hebben voor de betrouwbaarheid en beveiliging van informatie.
De nadruk bij afhankelijkheids- en kwetsbaarheidsanalyses is sterk gericht op de ICT-deel van de betrouwbaarheidsmaatregelen (general IT-controls) en in mindere mate op de geprogrammeerde 'controls' en nauwelijks op de procesinrichting en -beheersing. Juist die procesinrichting met daarin opgenomen handmatige en geautomatiseerde beheersmaatregelen is de directe verantwoordelijkheid van de manager. Het feitelijk invullen van de IT-controls valt buiten de scope van de manager. Daardoor sluiten het VIR en afhankelijkheids- en kwetsbaarheidsanalyses niet goed aan op de verantwoordelijkheden van de lijnmanager.
In veel grote organisaties, en zeker overheidsorganisaties, is de verantwoordelijkheidsverdeling lang niet zo duidelijk als in het VIR is aangenomen [AALD01], [DEKK00]. Als de verantwoordelijkheid voor bedrijfsprocessen niet eenduidig en duidelijk is belegd, zal dit in versterkte mate ook gelden voor de informatiesystemen die deze processen ondersteunen. Als het dan al mogelijk is de betrouwbaarheidseisen waar informatiesystemen aan moeten voldoen te bepalen, dan is het nauwelijks mogelijk lijnmanagers te vinden die budgetten beschikbaar willen stellen om deze maatregelen te implementeren [DEKK00].
In de praktijk is gebleken dat de complexiteit van een grote hoeveelheid, elkaar beïnvloedende, maatregelen die in een veel-op-veel-relatie staan tot de betrouwbaarheidseisen, maakt dat het uitvoeren van K-analyses niet alleen zeer arbeidsintensief is, maar ook per definitie werk is voor specialisten [CONS98], [DEKK00], [KIEB98], [KOP98], [MAAR98], [WINC01].
Met uitzondering van het kwalitatieve karakter maken de kenmerken het VIR tot een matig bruikbaar instrument voor het lijnmanagement.



Figuur 1. Het INK model

VIR VERSUS INK-MODEL

Het INK-model (zie figuur 1) is een managementmethode waarbij een organisatie door middel van zelfevaluatie het niveau van volwassenheid kan bepalen. Om tot kwaliteitsverbetering te komen, kan, uitgaande van een vastgesteld volwassenheidsniveau, een verbeterplan worden opgesteld en uitgevoerd. Het INK-model beschrijft de volwassenheidsniveaus als de volgende vijf ontwikkelingsfasen:

INK-fase 2 kenmerken	INK-fase 3 kenmerken	Relatie met c.q. betekenis voor VIR en A&K-analyses
Leiding stimuleert betrokkenheid en verantwoordelijkheid van medewerkers.	Leiding geeft het goede voorbeeld.	Artikel 2 van het VIR stelt dat de leiding het beleid actief moet uitdragen. Lijnmanager is verantwoordelijk voor uitvoeren A&K-analyses en implementatie noodzakelijke maatregelen (trekkende rol). Dit sluit goed aan bij INK-fase 3. Het stimuleren in fase 2 is onvoldoende, omdat dit vooral betrekking heeft op de primaire processen in plaats van op informatiebeveiliging.
Leiding neemt actief deel aan verbeteracties.	Leiding kijkt vooruit.	A&K-analyses kunnen uitstekend worden toegepast bij ontwikkel-/verwervingstrajecten en risico-inschatting bij het (her)inrichten van primaire bedrijfsprocessen (toepassen internet). In fase 2 neemt de leiding wel deel aan verbeteracties, maar deze verbeteringen hebben vooral betrekking op de primaire processen en niet op de informatieverzorgingprocessen.
Werken in verbeterteams wordt bevorderd.	Afdelingen werken samen aan verbetering.	Samenwerken is vooral nodig om generieke maatregelen, zoals fysieke beveiliging en general ICT-controls, te implementeren en te verbeteren. Indien primaire processen door meerdere afdelingen worden ingevuld, bestaat het gevaar van suboptimalisatie door per afdeling aan betrouwbaarheid te werken.
Gebruikte informatie heeft vooral betrekking op beheersing van het primaire proces.	Afwijkingen van normen worden van alle processen gemeten en leiden tot bijstelling.	Het VIR voorziet met betrekking tot informatiebeveiliging in een gesloten pdca-cirkel. Bij fase 2 is onvoldoende aandacht voor informatiebeveiliging. Voorzover er in fase 2 wel aandacht is voor informatiebeveiliging, zal er onvoldoende aandacht zijn voor de controle op de geïmplementeerde maatregelen (check).
Geconstateerde fouten in het proces worden geanalyseerd om herhaling te voorkomen.	Periodieke evaluatie van de gehele organisatie.	Het VIR voorziet in een actieve check op beleid, implementatie en werking van maatregelen. Dat heeft een duidelijk pro-actief karakter en past daarmee goed bij fase 3. Fase 2 is reactief van karakter.
Informatie heeft vooral betrekking op de primaire processen.	Informatiesysteem wordt beoordeeld op toegankelijkheid, betrouwbaarheid en veiligheid.	In fase 3 geeft het VIR geeft hier invulling aan via het betrouwbaarheidsmanagementproces.
Primaire processen en afzonderlijke stappen zijn beschreven.	Alle processen en hun onderlinge relaties zijn systematisch vastgelegd.	Met name de beschrijving van relaties tussen processen is voorwaardelijk voor het efficiënt uitvoeren van afhankelijkheidsanalyses.
	Interne klant-leverancier relaties zijn beschreven.	Dit is voorwaardelijk voor het efficiënt uitvoeren van A&K-analyses om te bepalen waar eigen maatregelen genomen moeten worden en waar afspraken met anderen moet worden gemaakt. Afdelingsleiding heeft beslissende stem.
Proceseigenaar heeft beslissende stem.	VIR neemt bedrijfsprocessen als uitgangspunt, een verantwoordelijke voor complete bedrijfsprocessen maakt de uitvoering van A&K-analyses een-	voudiger, omdat de per afdeling verkregen resultaten niet geconsolideerd hoeven te worden.
INK-fase 2 is procesgericht.	INK-fase 3 is systeemgericht.	VIR en A&K-analyses zijn systeemgericht.

Tabel 1. Analyse van de relatie tussen de INK-fasen 2 en 3 en het VIR.

• fase 1: activiteit georiënteerd;
• fase 2: proces georiënteerd;
• fase 3: systeem georiënteerd;
• fase 4: keten georiënteerd;
• fase 5: totale kwaliteit [INK98].

Alhoewel oorspronkelijk ontwikkeld voor het bedrijfsleven wordt het INK-model veelvuldig toegepast binnen de overheid. Om die reden is er voor dit artikel voor gekozen om de relatie tussen het VIR en de volwassenheidsniveaus van het INK-model te beschrijven. Zie voor de detailanalyse tabel 1.

De VIR-kenmerken die bepalen welk volwassenheidsniveau voorwaardelijk is voor een goede VIR-implementatie, zijn:
• het VIR is een rationele aanpak;
• het VIR ziet informatiebeveiliging als een proces;
• het VIR gaat uit van een eenduidige verantwoordelijkheidsverdeling.

Het VIR gaat uit van het belang van het bedrijfsproces en is in INK-termen minimaal systeemgeoriënteerd (fase 3). Immers, het gehele systeem, bestaande uit het bedrijfsproces en het informatieverzorgingsproces als onderdeel van de procesbesturing, wordt in beschouwing genomen. Indien ook met externe belangen (klanten) en wet- en regelgeving rekening wordt gehouden, kan worden gesteld dat het VIR zelfs ketengeoriënteerd is (fase 4).
Om de betrouwbaarheidseisen helder, beargumenteerd en reproduceerbaar vast te stellen en vervolgens de noodzakelijke maatregelen geïmplementeerd te krijgen, dient de verantwoordelijkheid voor bedrijfsprocessen en bijbehorende informatiesystemen eenduidig te zijn belegd. Volgens het INK-model is hiervan slechts sprake vanaf fase 3, waarbij in plaats van het afdelingsmanagement (fase 2) de proceseigenaar een beslissende stem heeft. Pas bij fase 3 van het INK-model mag gesproken worden van een procesgerichte organisatie. Het is niet aannemelijk dat een organisatie die niet procesgericht functioneert, betrouwbaarheidsmanagement met succes als proces kan implementeren.

Het betrouwbaarheidsmanagementproces volgens het VIR is, mits goed geïmplementeerd, een gesloten regelkring (plan, do, check en act). Volgens het INK-model is pas bij fase 3 sprake van meting en sturing van het proces als geheel inclusief het informatieverzorgingsproces.
De conclusie die hieruit kan worden getrokken is dat het succesvol implementeren van betrouwbaarheidsmanagement volgens het VIR pas redelijk kans van slagen heeft bij organisaties die zich in INK-fase 3 of hoger bevinden. Overigens is het zeer de vraag of hogere volwassenheidsniveaus altijd tot betere resultaten leiden. Aan het bereikte volwassenheidsniveau mag niet zonder meer een waardeoordeel worden gehangen. In hun artikel stellen Nuijten en Van der Pijl dat modellen als CMM, Cobit, ISO-9000 en risicoanalysemodellen veelal geen rekening houden met gedrags- en cultuuraspecten van organisaties en dat het toepassen van dergelijke modellen daardoor soms ongewenste resultaten geven [NUIJ00].

Samenvattend kan worden gesteld dat het VIR een kwalitatieve en arbeidsintensieve aanpak is met een beperkte scope, en die een volwassenheidsniveau INK-fase 3 of hoger veronderstelt. Het kwalitatieve karakter van het VIR blijkt geen problemen te geven. Het arbeidsintensieve karakter geeft in de praktijk wel veel problemen. Doordat het VIR een organisatie veronderstelt die zich bevindt op een volwassenheidsniveau INK-fase 3 of hoger, ontstaan in de praktijk problemen bij VIR-implementaties met betrekking tot:
1. het rationele karakter van het VIR en afhankelijkheids- en kwetsbaarheidsanalyses;
2. het procesmatige karakter van het VIR;
3. de door het VIR veronderstelde eenduidige en duidelijke lijnverantwoordelijkheden met betrekking tot bedrijfsprocessen en bijbehorende informatiesystemen.

Verder blijkt dat het VIR en de A&K-analysemethode niet goed bruikbaar zijn voor het lijnmanagement, omdat de scope van het VIR beperkt is tot:
1. informatiebeveiliging als deelaspect van de informatieverzorging, wat op zich weer een deelaspect van de totale bedrijfsvoering is;
2. de ICT-betrouwbaarheidsmaatregelen (vooral van toepassing op de afhankelijkheids- en kwetsbaarheidsanalysemethode).

EEN GROEIMODEL

Uitgaande van de kenmerken van het VIR in relatie tot de volwassenheidsniveaus van het INK-model, is in dit hoofdstuk een groeimodel beschreven die behulpzaam kan zijn bij VIR-implementaties.

Vaststellen volwassenheidsniveau

Voordat met het implementeren van het VIR en het uitvoeren van afhankelijkheids- en kwetsbaarheidsanalyses wordt begonnen, is het aan te bevelen eerst via een zelfevaluatie of externe audit vast te stellen op welk volwassenheidsniveau een organisatie zich bevindt. Alhoewel er niets tegen zelfevaluatie is, is het aan te raden dit proces

door een onafhankelijke externe deskundige te laten begeleiden en de uitkomsten eventueel door aanvullend (onafhankelijk en objectief) onderzoek te laten staven. Het risico van een te hoog ingeschatte INK-fase kan zijn dat de op grond daarvan gekozen aanpak om het VIR te implementeren zal falen.

Baselines

Onafhankelijk van het volwassenheidsniveau waarin een organisatie zich bevindt, zal een oplossing voor het arbeidsintensieve karakter van de afhankelijkheids- en kwetsbaarheidsanalyses moeten worden gevonden. Het VIR geeft aan dat gebruik kan worden gemaakt van baselines.
Een baseline is een stelsel van eisen en/of maatregelen waarmee een standaard betrouwbaarheidsniveau wordt gerealiseerd. In het kort komt de baselineaanpak erop neer dat A&K-analyses worden uitgevoerd op een beperkt aantal representatieve informatiesystemen. Op basis van de uitkomsten van deze afhankelijkheids- en kwetsbaarheidsanalyses wordt een baseline opgesteld, die vervolgens van toepassing wordt verklaard voor alle overige informatiesystemen [VIR94]. Eventueel kan voor kritische informatiesystemen via afhankelijkheids- en kwetsbaarheidsanalyses worden beoordeeld of de baseline toereikend is en eventueel aanvullende maatregelen noodzakelijk zijn. Deze normcontrole kan ook in het kader van EDP-audits worden uitgevoerd.

Bij de RDW Dienst Wegverkeer is een variant op de baselineaanpak ontwikkeld. In plaats van één baseline zijn drie betrouwbaarheidsniveaus beschreven. Om te bepalen welk betrouwbaarheidsniveau voor een bepaald informatiesysteem van toepassing is, is een typologie van informatiesystemen opgesteld. De typologie kent een hoofdindeling in primaire informatiesystemen en bestuurlijke informatiesystemen. Primaire informatiesystemen zijn systemen die de corebusines van de organisatie uitvoeren en zijn als ‘essentieel’ getypeerd. Bestuurlijke informatiesystemen zijn onderverdeeld op basis van een indeling ontleend aan het boek ‘Management Informatiesystemen’ van Davis en Olsen [DAV87]. Daarin worden vier soorten informatiesystemen benoemd, namelijk systemen ten behoeve van transactieverwerking getypeerd als ‘essentieel’, operationele en managementbeheersing getypeerd als ‘belangrijk’ en strategische planning en persoonlijk computergebruik getypeerd als ‘wenselijk’.
Bij de RDW is deze aanpak redelijk aangeslagen. Bedacht moet worden dat de typologie specifiek is ontwikkeld voor de RDW-situatie en niet zonder meer past bij andere organisaties. Echter, het achterliggende concept van betrouwbaarheidsniveaus gebaseerd op een classificatie van informatiesystemen, bedrijfsprocessen en/of gegevens kan ook z’n nut hebben binnen andere organisaties. Omdat de feitelijke maatregelen in de praktijk maar beperkt schaalbaar zijn, komt het verschil tussen de drie niveaus veelal tot uitdrukking in de mate waarin zekerheid kan worden verkregen of genomen maatregelen effectief zijn. Zekerheid bestaat daarbij uit controleerbaarheid en werkelijk uitgevoerde controles (operationele controles en in- en externe EDP-audits).

Samenvattend blijkt dat baselines bij alle volwassenheidsniveaus zinvol zijn, omdat:
1. baselines het arbeidsintensieve karakter van A&K-analyses helpen op te vangen;
2. baselines het eenvoudiger maken om ICT-maatregelen generiek en architectuurgedreven te ontwerpen, te implementeren en te beheren;
3. baselines een normenkader opleveren voor het ontwerpen, inrichten en beheren van informatiesystemen, die ook kan worden gebruikt bij het uitvoeren van in- en externe EDP-audits;
4. op typologie/classificatie gebaseerde baselines het onderling vergelijken van informatiesystemen faciliteert (interne benchmarking), wat met name de communicatie met lijnmanagers alsmede het afsluiten van SLA’s sterk kan vereenvoudigen.

VIR bij een INK-fase 1

Als het bereiken van hogere volwassenheidsniveaus niet haalbaar of wenselijk is, moet het VIR vooral door organisatorische maatregelen vorm worden gegeven. Dit kan door het aanstellen van security officers of informatiebeveiligingsfunctionarissen. Bij lagere volwassenheidsniveaus zal veel afhangen van deze ‘helden’ of ‘professionele individuen’, zoals het INK-model ze noemt. Zeker in het begin van een VIR-implementatie, zal veel doorzettingsvermogen en tactiek van de interne IBF-ers worden gevraagd. Medewerkers die zo’n rol op zich nemen, dienen voor wat betreft kennis, vaardigheden en ervaring goed voor zo’n taak te zijn toegerust.
Om twee gescheiden trajecten te voorkomen, is het belangrijk dat in- en externe EDP-auditors goed samenwerken met de IBF-ers. Via beveiligingsplannen en/of baselines (plan) en EDP-audits (check) kan druk worden gezet op het management (act) om tot implementatie van de noodzakelijke maatregelen te komen (do). Via EDP-audits kan vervolgens de implementatie worden bewaakt. Hiermee is de pdca-cirkel gesloten en ontstaat een begin van een betrouwbaarheidsmanagementproces. Dat proces zal conform de kenmerken van fase 1 sterk steunen op de inzet van IBF’ers en in- en externe auditors.

Om de koppeling met het VIR te behouden, maar ook om de aansluiting met de organisatie en het management te versterken, is het belangrijk dat de IBF'ers in samenwerking met de in- en externe auditors de EDP-auditnormen opstellen via de A&K-analysemethode. De voordelen hiervan zijn dat de op A&K-analyses gebaseerde normen aansluiten op de bedrijfsprocessen van de organisatie en het management in concrete businesstermen kan worden uitgelegd waarom bepaalde maatregelen moeten worden genomen. Baselines zijn bij lagere INK-fasen goed toe te passen, omdat baselines vrijwel altijd door specialisten (de 'helden') zoals IBF'ers en EDP-auditors worden opgesteld. Het toepassen van op typologie gebaseerde baselines vergroot in deze fase de stuurbaarheid van de informatiebeveiliging voor het lijnmanagement.

VIR bij een INK-fase 2

Bij stijgende volwassenheid van de organisatie zullen de kansen op een succesvolle VIR-implementie gaan toenemen. Om het scopeprobleem van het VIR te ondervangen, kan waar mogelijk worden aangesloten bij andere kwaliteitstrajecten, zoals de invoering van het INK-model. Inpassing van het VIR binnen het INK-model is mogelijk door managementafspraken te maken over het uitvoeren van afhankelijkheids- en kwetsbaarheidsanalyses, het opstellen van baselines, welke systemen/processen via een EDP-audit zullen worden onderzocht en het tijdstip waarop systemen voldoen aan gestelde betrouwbaarheidseisen en noodzakelijke maatregelen daadwerkelijk zijn geïmplementeerd. Hierdoor raakt het management meer betrokken bij informatiebeveiliging.
Naast inpassing in het INK-model kan ook aansluiting worden gezocht bij ITIL-implementaties en andere kwaliteitsmodellen die binnen een organisatie worden toegepast. Hierbij moet rekening worden gehouden met het feit dat tot INK-fase 3 de verantwoordelijkheidsverdeling waarschijnlijk niet goed zal aansluiten op bedrijfsprocessen en informatiesystemen. Het gevaar bestaat dat gehanteerde modellen dezelfde (impliciete) kenmerken hebben als het VIR, waardoor het combineren minder effectief zal zijn dan verwacht. Ook ITIL gaat uit van procesmatig werken. Alhoewel niet onderzocht lijkt het aannemelijk dat ook de invoering van ITIL bij een INK-fase lager dan 3 net als invoering van het VIR nauwelijks uitvoerbaar is. Vrijwel alle modellen als Cobit, KAD-model, VIR, ITIL en andere lijken gericht te zijn op de 'harde' kant van beheersing en er ontbreekt voldoende aandacht voor gedrags-, organisatie- en cultuuraspecten [NUIJ00].

Momenteel wordt binnen de overheid gewerkt aan de operatie 'Van beleidsbegroting tot beleidsverantwoording' (VBTB). Het VBTB is een sterk formeel model en is net als het VIR procesgericht [KORD01], [LUIJ00]. Het is aannemelijk dat ook de invoering van VBTB op de nodige problemen zal stuiten, omdat het erop lijkt dat het VBTB net als het VIR impliciet uitgaat van hogere volwassenheidsniveaus. Echter, de druk vanuit de maatschappij en politiek is zodanig, dat desondanks wel enig succes mag worden verwacht. Er is derhalve voldoende reden om met VIR-implementaties zoveel mogelijk op de ontwikkelingen van het VBTB aan te sluiten.

Samenvattend kan worden gesteld dat integratie van betrouwbaarheidsmanagement met andere ontwikkelingen bij een stijgende volwassenheid meer kans van slagen heeft en de kans op een succesvolle VIR-implementatie doet toenemen. Door het inpassen van het VIR in andere kwaliteitstrajecten kan het scopeprobleem van het VIR worden ondervangen. In zo'n overgangsfase kunnen in- en externe EDP-auditors door hun kennis van processen en modellen als VIR, ITIL, INK en andere een belangrijke rol spelen. Het is belangrijk dat de IBF'ers gedurende deze ontwikkeling hun 'heldenrol' gaandeweg loslaten.

Het VIR bij INK-fase 3 of hoger

Bij een INK-fase 3 of hoger is het aannemelijk dat het rationele en procesmatige karakter van het VIR aanzienlijk minder problemen zal veroorzaken en zullen de verantwoordelijkheden met betrekking tot bedrijfsprocessen en informatiesystemen voldoende duidelijk zijn. Ook hier is het zinvol baselines toe te passen, maar deze zullen sterk door het lijnmanagement worden bepaald, waarbij IBF'ers en EDP-auditors een meer adviserende rol vervullen. Integratie met andere kwaliteitsmodellen zal meer vanzelfsprekend zijn, omdat conform de kenmerken van fase 3 sterker vanuit de organisatiedoelen (klantgerichtheid) wordt geredeneerd.

VIR doel of middel?

Welke aanpak ook wordt gekozen, het gaat uiteindelijk niet om het VIR te implementeren, maar om de risico's die voortvloeien uit de mate waarin de bedrijfsvoering afhankelijk is van informatie(systemen) afdoende te beheersen. Als een (voorgeschreven) aanpak zoals het VIR niet werkt, is het onverstandig met zo'n aanpak door te gaan, maar dient gezocht te worden naar een aanpak die wel effectief is. Dit betekent, dat uitgebreide normenstelsels waar VIR-implementaties aan worden getoetst, feitelijk minder gewenst zijn en dat daarmee geen bijdrage wordt geleverd aan het te bereiken doel.

SAMENVATTING

Is het VIR geschikt voor de overheid? Op grond van de hiervoor beschreven problemen lijkt het voor de hand te liggen de vraag met 'nee' te beantwoorden. Echter, als rekening wordt gehouden met het volwassenheidsniveau van een organisatie kan minimaal naar de geest van het VIR worden gehandeld. Het is derhalve aan te bevelen om voorafgaand aan een VIR-implementatie eerst te onderzoeken op welk volwassenheidsniveau een organisatie zich bevindt.
Baselines kunnen in alle INK-fasen helpen het arbeidsintensieve karakter van de A&K-analyses te ondervangen. Op typologie gebaseerde baselines kunnen de stuurbaarheid voor en communicatie met het lijnmanagement helpen verbeteren.
Bij een INK-fase 1 dient te worden gekozen voor een sterke invulling van de rol van informatiebeveiligingsfunctionarissen (IBF'ers). Zij moeten de rol van 'held' of 'professionele individuen', zoals het INK-model ze noemt, op een goede manier invullen.
Om het scopeprobleem van het VIR te ondervangen, is het bij INK-fasen hoger dan 1 zinvol aansluiting te zoeken bij andere kwaliteitsmodellen die binnen een organisatie worden toegepast, zoals het INK-model, VBTB en/of ITIL. Hierdoor wordt voorkomen dat onevenredig aandacht wordt besteed aan de ICT-beveiligingsmaatregelen en dat de inrichting en beheersing van bedrijfsprocessen worden onderbelicht. Juist door integratie van het VIR in de normale bedrijfsvoering neemt de bruikbaarheid van het VIR voor lijnmanagers sterk toe en zal borging van betrouwbaarheidsmanagement conform het VIR gerealiseerd kunnen worden.

Literatuur

[AALD01] Aalders, R., R. Maalman en T. Rijpers, (2001), Procesbeheersing voorwaarde voor succes e-business, in: Automatiseringsgids, 12 oktober.

[ACIB97] ACIB, (1997), Handleiding A&K-analyse.

[BROU96] Brouwer, A., (1996), De kracht van de kwalitatieve analyse, in: de EDP-Auditor, nr. 2.

[CONS98] Constandse, A.J.C., (1998), Vier jaar VIR, vloek of zegen?, ten Hagen Stam.

[DAVI87] Davis & Olson, (1987), Management Informatiesystemen, Academic Service.

[DEKK00] Dekkers, M., (2000), Implementatie Voorschrift Informatiebeveiliging Rijksdienst. Een praktijkervaring, in: de EDP-Auditor, nr. 3.

[INK98] Instituut Nederlandse Kwaliteit, (1998), Handleiding positiebepaling & verbeteren publieke sector.

[KAME95] Kamermans, M.C., (1995), Administratieve Organisatie, vernieuwing van een vak, Tutein Nolthenius.

[KIEB98] Kieboom, C.W.L.J., (1998), Vier jaar VIR, vloek of zegen?, ten Hagen Stam.

[KOPP98] Koppes, J.N.M., (1998), Vier jaar VIR; vloek of zegen?, t en Hagen Stam.

[KORD01] Kordes, F. en P. Vlasveld, (2001), VBTB maakt audit-functie aantrekkelijker, in: De Accountant, september.

[LUIJ00]] Luijendijk, H. en C. van Schie, (2000), Vitaal besturen, in: De Accountant, februari.

[MAAR98] Maarel, C.J.P. van der, (1998) , Vier jaar VIR, vloek of zegen?, ten Hagen Stam.

[NUIJT00] Nuijten, A.L.P. en G.J. van der Pijl, (2000), Niet altijd volgens het boekje, standaardmodellen schieten soms te kort, in: de EDP-Auditor, nr. 3.

[STAR97] Starreveld, R.W., (1997), Bestuurlijke Informatieverzorging deel 1 Algemene grondslagen, 4e druk, Samson Uitgeverij, Alphen aan den Rijn/Brussel.

[VIR94] Ministerie van Binnenlandse Zaken, (1994), Voorschrift Informatiebeveiliging Rijksdienst.

[WINC01] Winckelmann, S., (2001), Help! De manager verzuipt!, in: Het informatiebeveiliging jaarboek 2001/2002, ten Hagen Stam.

Inrichting en uitvoering van Quality Assurance bij ERP-implementaties

IT-auditor als 'het schaap met vijf poten'

Regelmatig is in de krant te lezen dat weer een miljoenenverslindend IT-project is mislukt. In de praktijk betreft dit veelal implementaties van Enterprise Resource Planning (ERP)-softwarepakketten waarbij getracht wordt om één systeem te implementeren dat de gehele bedrijfsvoering moet ondersteunen en waarbij slechts éénmalige invoer van gegevens hoeft plaats te vinden. IT-auditors zijn vaak van mening dat zij door de inzet van hun kennis en vaardigheden bedrijven kunnen behoeden voor dergelijke mislukkingen, bijvoorbeeld in een rol als Quality Assurance-functionaris (QA) bij de implementatie van een ERP-systeem.

Jan Hoogstra en Richard Vermeulen

INLEIDING

Er zijn zelfs bedrijven, zoals keukenproducent ATAG, die failliet zijn gegaan mede door het mislukken van de implementatie van een ERP-pakket [BEER01].
Dit artikel verschaft IT-auditors meer inzicht in de mogelijkheden van QA bij ERP-implementaties. De auteurs hebben ernaar gestreefd om niet alleen de theorie, maar ook de praktijk te beschrijven.
Het artikel start met een theoretische beschouwing van QA. Hierin komen onder andere de eisen aan bod die aan een IT-auditor in de rol van QA-functionaris kunnen worden gesteld.
In het praktijkgedeelte is de ervaring met QA in implementatieprojecten van ERP van beide auteurs verwerkt aan de hand van een praktijkcase. Ten slotte volgt een conclusie en aanbevelingen voor een IT-auditor die een rol als QA-functionaris bij een ERP-implementatie gaat vervullen.
De bijlage is een introductie tot de implementatiemethodiek Accelerated SAP (ASAP) en is bedoeld om de lezer een voorbeeld te geven van een methodiek die kan worden gebruikt bij het uitvoeren van QA-werkzaamheden.

Drs. Jan Hoogstra en Ir. Richard Vermeulen
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

QUALITY ASSURANCE IN THEORIE

Wat is ERP en Quality Assurance bij ERP?

ERP is ontstaan vanuit de goederenstroombesturing. Voorheen was het zo dat bedrijven voor de ondersteuning van elk deel van de productieketen, zoals inkoop, opslag, productie en verkoop, een apart geautomatiseerd systeem hadden.
Dit had inconsistenties en inefficiënties (zoals het meerdere malen moeten invoeren van gegevens) tot gevolg. Vervolgens ontstonden zogenaamde Manufacturing Resource Planning (MRP)-softwarepakketten, waarbij rekentechnieken werden gebruikt waarmee de goederenstroom integraal kon worden aangestuurd en informatie beschikbaar werd gesteld voor productiecapaciteitplanning. De behoefte aan het éénmalig invoeren van gegevens en de integratie van systemen leidde ten slotte tot het ontstaan van ERP-softwarepakketten, waarbij de administratieve ondersteuning werd gecombineerd met de aansturing van de goederenstroom.
De implementatie van een ERP-systeem raakt in de praktijk vaak vrijwel alle processen en heeft daarmee een grote impact op de organisatie. Meestal blijkt dat ook de organisatie moet worden aangepast, waardoor de implementatie niet alleen een technisch, maar ook een organisa-

tieveranderkundig karakter heeft. In de praktijk blijkt dat veel ERP-implementaties niet het gewenste resultaat opleveren dan wel vroegtijdig worden afgebroken. Bekende voorbeelden zijn de ERP-implementatie bij keukenproducent ATAG en bij containeroverslagbedrijf Vopak [BEER01].
Uit onderzoek blijkt dat ERP-implementaties veelal door min of meer dezelfde factoren mislukken, de zogenaamde faalfactoren [HOOG02].

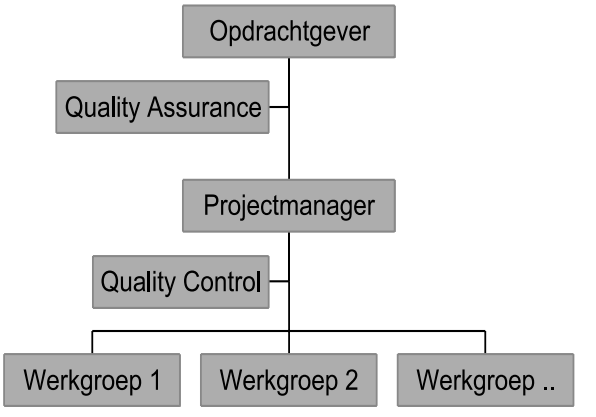
Faalfactoren ERP-implementaties
Uit de vergelijking van een tweetal onderzoeken naar faalfactoren bij ERP [KPMG99 en MORE97] kan worden geconcludeerd dat de belangrijkste faalfactoren zijn:
- Geen of onvoldoende managementcommitment en -betrokkenheid bij de ERP-implementatie.
- Te brede, onduidelijke of wijzigende scope van het project. Het gevolg hiervan kan zijn dat mijlpalen niet worden gehaald, waardoor continu achter de feiten wordt aangelopen. Bij een onduidelijke scope kan niet worden vastgesteld of aan de eisen is voldaan.
- Onvoldoende aandacht voor de menselijke factoren (bijvoorbeeld communicatie naar medewerkers, vroegtijdige betrokkenheid van de medewerkers en acceptatie van veranderingen).
- Complexiteit van het pakket. Doordat de verschillende ERP-systemen zo flexibel mogelijk willen zijn om zo goed mogelijk aan te sluiten bij de processen van de klant, zijn er duizenden tabellen en parameters in het pakket aanwezig die ingesteld/ingericht moeten worden.
- Onvoldoende inzicht in de bedrijfsprocessen en het (toekomstige) besturingsmodel van de organisatie. Organisaties hebben vaak wel inzicht in de huidige bedrijfsprocessen (‘as-is’), maar onvoldoende inzicht in de toekomstige processen (‘to-be’).

Opvallend is dat in beide onderzoeken het aspect kosten niet voorkomt. Zoals vaak met IT-projecten het geval is, kost een ERP-implementatie over het algemeen meer dan begroot. Een voorbeeld daarvan is het containeroverslagbedrijf Vopak [BEER01].
Geconcludeerd kan worden dat deze redelijk algemeen zijn en niet bijzonder verschillen van reguliere IT-projecten. Dit wordt bevestigd door Kluyskens [KLUY01].
Hij heeft onderzoek uitgevoerd naar de faalfactoren bij IT-projecten, waarbij door middel van systeemontwikkeling een applicatie wordt opgeleverd die een bedrijfsproces ondersteunt. Uit zijn onderzoek blijkt dat de faalfactoren bij ERP-implementaties niet veel verschillen van de faalfactoren van reguliere IT-projecten.
Een methode voor het bewaken en monitoren van de kwaliteit van ERP-implementaties is QA.

Quality Assurance bij ERP
QA wordt vaak gelijkgesteld aan kwaliteitsmanagement: het beheersen van de kwaliteit van het product. Kwaliteit wordt [HELD00] gedefinieerd als de mate waarin aan klantbehoeften en -verwachtingen tegemoet wordt gekomen of de mate waarin deze worden overtroffen. Hierdoor komen de auteurs van dit artikel tot de volgende definitie van QA:

Quality Assurance is gericht op het signaleren van risico’s en het adviseren over beheersing van deze risico’s door (een) onafhankelijke en onpartijdige deskundige(n). Dit betekent dat door de geboden inzichtelijkheid vroegtijdig het optreden van een ongewenste situatie als gevolg van het zich manifesteren van een bedreiging wordt gesignaleerd. Daarmee wordt aan de verantwoordelijken mogelijkheden geboden om het implementatieproces te kunnen laten voldoen aan de klantbehoeften en -verwachtingen.

QA wordt soms verward met Quality Control. Het wezenlijke verschil tussen beide begrippen is de organisatorische ophanging ten opzichte van de projectgroep. Quality Control maakt onderdeel uit van de projectgroep zelf, terwijl QA onafhankelijk van de projectgroep ingevuld wordt. Dit betekent dat de QA-functionaris in de praktijk geen verantwoording af zal leggen aan de projectmanager, maar aan de opdrachtgever (vaak een stuurgroep). Van belang is dat deze opdrachtgever niet direct bij de operationele uitvoering van de opdracht betrokken is, immers een IT-auditor in de rol van de QA-functionaris zou daarmee een oordeel moeten geven over het functioneren van de opdrachtgever, hetgeen de onafhankelijkheid en onpartijdigheid in gevaar kan brengen. Schematisch is het verschil tussen QA en Quality Control in figuur 1 weergegeven.



Figuur 1

Soorten Quality Assurance bij ERP-implementaties
De QA-functie kan bij ERP-implementaties op diverse wijzen worden ingevuld:
- door de leverancier van de software (bijvoorbeeld SAP en Oracle);
- door de implementatiepartner (bijvoorbeeld LogicaCMG en Atos Origin);
- door een onafhankelijke derde.

In alle gevallen is de overeenkomst dat de QA-functie gericht is op de kwaliteitsbewaking. De eerste twee vormen voldoen feitelijk niet aan de definitie van QA, omdat de uitvoering niet bij een onafhankelijke partij ligt. De derde vorm is daarentegen een echte QA-functie.
In de praktijk worden al deze vormen toegepast onder de noemer van QA.

Quality Assurance door de leverancier
Verschillende leveranciers van ERP-systemen hebben een implementatiemethodiek ontwikkeld die erop gericht is om een effectieve en efficiënte implementatie te verrichten waarbij de kwaliteit voldoet aan de vooraf gedefinieerde eisen. Deze methodieken zijn daarmee gericht op het leveren van QA in het project. Een voorbeeld van zo'n methodiek is ASAP van de firma SAP. Een korte beschrijving hiervan is opgenomen in het kader.

Bij een implementatieproces van softwarepakketten is het belangrijk om de implementatie-inspanning (evenwichtig) te verdelen over de volgende drie aandachtsgebieden en om deze aandachtsgebieden integraal te benaderen:
1. Technologie: inrichten van het ERP-softwarepakket en de technische infrastructuur.

De implementatiemethodiek ASAP biedt organisaties die ERP-software van SAP willen implementeren een standaard-aanpak om de implementatie stapsgewijs en daardoor beheersbaar te laten verlopen. Binnen ASAP worden de volgende vijf fasen onderscheiden die een organisatie opeenvolgend dient uit te voeren tijdens het implementatieproces:
1. Projectvoorbereidingsfase (Project Preparation).
2. Concept- of bedrijfsblauwdrukfase (Business Blueprint).
3. Realisatiefase (Realization).
4. Voorbereiding voor productieve ingebruikname (Final Preparation).
5. Go-Live en ondersteuning (Go Live & Support).

Deze vijf fasen zijn logisch met elkaar verbonden via een resultaatpad dat ook wel de ASAP Roadmap wordt genoemd (figuur 2). Elke fase dient eerst volledig te zijn afgerond alvorens te starten met de volgende fase. Om vast te kunnen stellen of een fase is afgerond, wordt binnen ASAP iedere fase afgesloten met een quality check. In een quality check wordt onder verantwoordelijkheid van de projectmanager (en is daarmee Quality Control en geen Quality Assurance) vastgesteld of alle activiteiten behorende tot de fase zijn voltooid en de resultaten (deliverables) voldoen aan de vooraf opgestelde kwaliteitscriteria.

Figuur 2

Bij een ASAP-implementatie is snelheid de belangrijkste factor. ASAP is opgezet om binnen een relatief korte periode (zes tot negen maanden) de door de organisatie gewenste modules van SAP te implementeren vanuit de optiek van een zogenaamde 1:1-implementatie. Dat houdt in dat de huidige bedrijfsprocessen als uitgangspunt worden genomen en dat slechts aanpassingen worden gepleegd waar het pakket dit afdwingt. De praktijk leert echter dat ondanks deze doelstelling een dergelijke implementatie vaak veel veranderingen met zich meebrengt [ROOS99]. In de bijlage van dit artikel wordt nader ingegaan op de structuur en de inhoud van de implementatiemethodiek ASAP.

2. Proces: (her)inrichten van bedrijfsprocessen en (her)ontwerpen en implementeren van AO/IC.
3. Mens: (organisatorische) veranderingsmanagement.

Hoewel de implementatiemethodiek ASAP[1] rekening houdt met deze drie aandachtsgebieden, wordt de nadruk gelegd op het aandachtsgebied technologie en wordt (aanzienlijk) minder rekening gehouden met de overige twee aandachtsgebieden. Hierbij moet worden opgemerkt dat ASAP met name het aandachtsgebied mens binnen de staande organisatie te sterk onderbelicht [VERM01].
Binnen het aandachtsgebied proces wordt binnen ASAP geen expliciete aandacht besteed aan het beoordelen, (her)ontwerpen en implementeren van de AO/IC.
Binnen het aandachtsgebied mens wordt weinig aandacht besteed aan organisatorisch veranderingsmanagement.
De door een leverancier uitgevoerd onderzoek naar de kwaliteit van (implementatie)projecten voldoet niet aan de in dit artikel gegeven definitie van QA, omdat er geen onafhankelijke en onpartijdige deskundige bij betrokken is. De opdrachtgever krijgt op deze manier geen echte 'assurance', omdat er geen sprake is van een onafhankelijk en (mogelijk) onpartijdig oordeel.

Quality Assurance door de implementatiepartner
Indien de ERP-implementatie niet wordt uitgevoerd door de leverancier maar door een implementatiepartner van de leverancier, dan kan deze implementatiepartner de QA zelf invullen door het hanteren van een methodiek voor de implementatie.
Om dezelfde reden als bij QA door de leverancier is hier geen echte sprake van QA.

Quality Assurance door onafhankelijke derde
Conform de definitie in dit artikel wordt QA door een onafhankelijke en onpartijdige derde uitgevoerd.
Een IT-auditor kan deze rol vervullen.
De toegevoegde waarde van een IT-auditor als QA-functionaris wordt zowel in de praktijk als in de theorie gevonden in de onafhankelijkheid en de onpartijdigheid alsmede in de deskundigheid en de vaardigheden die een IT-auditor bezit. Deze onafhankelijkheid en onpartijdigheid zijn vastgelegd in de beroepsregels van de NOREA, waardoor de betrokkenen erop kunnen vertrouwen dat deze worden nageleefd door een IT-auditor [HOOG02].
Bij de uitvoering van QA kan een IT-auditor mede gebruikmaken van methodieken die worden gehanteerd door de leverancier of de implementatiepartner. In dat geval dient een IT-auditor zich bewust te zijn van de tekortkomingen van die methodieken. Zo is eerder reeds gesteld dat ASAP geen expliciete aandacht besteedt aan het beoordelen, (her)ontwerpen en implementeren van de AO/IC en is het organisatorische verandermanagement onderbelicht. Tevens kan een IT-auditor gebruikmaken van algemeen geaccepteerde normenkaders zoals Cobit en Prince2. In de praktijk zal een IT-auditor een mix van de diverse normenkaders gebruiken voor de uitvoering van zijn werkzaamheden.

Eisen aan een IT-auditor als QA-functionaris

In de literatuur wordt summier ingegaan op de eisen die worden gesteld aan een IT-auditor die een QA-functie bij een ERP-implementatie vervult. Van Lierop [SLIE00] schrijft dat het vereist is dat een IT-auditor bekend moet zijn met de architectuur van ERP-systemen en de geboden functionaliteiten. Een IT-auditor dient volgens hem inzicht te hebben in de impact die het gebruik van ERP-systemen kan hebben op de organisatie. Daarnaast is het volgens hem wenselijk dat een auditor systeemspecifieke kennis heeft; dit kan de efficiency van de opdrachtuitvoering vergroten.
Naast theoretische kennis is volgens hem ook ervaring van groot belang. Het deelnemen in ERP-implementaties, waarbij een inhoudelijke rol wordt vervuld, is volgens hem uitermate geschikt om deze ervaring op te doen.
Ook volgens Brouwers [SLIE00] is ervaring met veranderingstrajecten door middel van ERP-systemen van wezenlijk belang voor het nut van een QA-functie. Dit betreft ook het hebben van pakketinhoudelijke ervaring en kennis van de implementatiemethoden van een specifiek pakket. Brouwers geeft aan dat voor het opdoen van ervaring het vervullen van een projectleidersrol en het ondersteunen bij projecten de voorkeur verdient.
Het uitvoeren van audits vereist een kritische houding, waarbij een IT-auditor continu denkt in termen van risico's en beheersing van deze risico's.
Sloesen [SLOE91] heeft aangegeven aan welke generieke eisen van deskundigheid een IT-auditor dient te voldoen. Deze eisen zijn in tabel 1 vergeleken met de specifieke eisen die aan een IT-auditor in de rol van QA-functionaris kunnen worden gesteld [HOOG02]. Hierbij is geredeneerd vanuit de specifieke eisen. Bij de specifieke eisen zijn de overeenkomstige generieke eisen gezocht.

Uit de vergelijking in tabel 1 blijkt dat vrijwel alle specifieke eisen die kunnen worden gesteld aan een QA-functionaris onderdeel uitmaken van het functieprofiel van een IT-auditor, met uitzondering van onder andere verandermanagementvaardigheden. Het blijkt dat aan een IT-auditor enkele additionele eisen worden gesteld die, in eerste instantie, niet relevant zijn voor het vervullen van een QA-functie, zoals geheimhouding. Echter vanuit de gedrags- en beroepsregels Register EDP-auditors (GBRE)

Specifieke eisen aan een IT-auditor in de rol van Quality Assurance-functionaris	**Generieke eisen aan een IT-auditor**
Onpartijdigheid	Onpartijdigheid
Onafhankelijkheid	Onafhankelijkheid
Kennis van de organisatie	Inzicht in de verschillende typologieën van huishoudingen
Kennis van het te implementeren ERP-pakket en van de te hanteren methode voor projectmanagement	Materiekennis van het object van onderzoek
Vaardigheden om risico's te signaleren	Controlekennis
Vaardigheden om risico's te vertalen in beheermaatregelen	Adviesvaardigheid
Communicatieve vaardigheden om onder andere: • De mogelijk optredende risico's duidelijk te maken aan de opdrachtgever; • De adviezen om deze risico's te minimaliseren helder over te brengen	Communicatieve vaardigheid Duidelijkheid Onbevooroordeeldheid
Verandermanagementvaardigheden	-
Persoonskenmerken, zoals vasthoudendheid en eigen meningsvorming	Onbevooroordeeldheid Controlekennis
-	Geheimhouding
-	Kwaliteit
Organisatiesensitiviteit	-
Inschattingsvermogen organisatie en project	Materiedeskundigheid
Kennis van de 'soft controls'	Controlekennis
Vaardigheden om de aanwezige pakketkennis te relateren aan de kennis van de organisatie in al haar facetten	-

Tabel 1. Vergelijking functieprofiel Quality Assurance-functionaris met functieprofiel IT-auditor

dient een IT-auditor altijd aan de geheimhoudingsplicht te voldoen en dus ook in de rol van QA-functionaris.
Opvallend is dat een aantal specifieke eisen die aan een IT-auditor in de rol van QA-functionaris bij een ERP-implementatie kunnen worden gesteld niet voorkomen in het functieprofiel van een IT-auditor. Dit betreft met name de 'softere' eisen, zoals verandermanagementvaardigheden, organisatiesensitiviteit en vaardigheden om pakketkennis te kunnen relateren aan de inrichting en cultuur van een organisatie. Deze vaardigheden zijn met name nodig ter bevordering van de acceptatiegraad van de aanbevelingen.
Gezien het aantal eisen dat wordt gesteld aan een IT-auditor in de rol van QA-functionaris bij een ERP-implementatie, lijkt het zeer onwaarschijnlijk dat alle kennis en vaardigheden in één persoon vertegenwoordigd zijn.

QUALITY ASSURANCE IN PRAKTIJK

Implementatie SAP-Payroll

Deze paragraaf beschrijft ervaringen met de inrichting en de uitvoering van de QA-functie bij een implementatie van SAP-Payroll. SAP-Payroll maakt onderdeel uit van de module Human Resources (HR) van het ERP-softwarepakket SAP en omvat functionaliteiten voor de totale salarisverwerking (van de registratie van salarisgegevens tot de uitbetaling van salaris). Op het moment van schrijven van dit artikel bevindt het implementatieproces zich in de realisatiefase. Voor de implementatie van SAP-Payroll is in totaal twee jaar uitgetrokken. Het op te leveren systeem dient maandelijks aan circa 45.000 personeelsleden het salaris uit te betalen. Omdat de salarisverwerking nu nog uitbesteed is aan een derde partij, dient naast de implementatie van SAP-Payroll binnen de gestelde termijn van twee jaar ook een nieuwe organisatie te worden ingericht voor het toekomstige beheer en de exploitatie van het systeem. Bij de implementatie van SAP-Payroll wordt zowel Quality Control als QA toegepast. Quality Control wordt in opdracht van de projectmanager uitgevoerd door de leverancier (firma SAP) van het ERP-softwarepakket, terwijl QA in opdracht van de voorzitter van de stuurgroep wordt uitgevoerd. De QA-functie wordt vervuld door een samengesteld team auditors van de eigen organisatie. Binnen de eigen organisatie is voldoende kennis en ervaring aanwezig om aan het functieprofiel voor een QA-functionaris, zoals beschreven in de vorige paragraaf, te kunnen voldoen. In het vervolg wordt ingegaan op de inrichting en de uitvoering van QA bij de implementatie van SAP-Payroll.

Inrichting van de QA-functie

Bij de inrichting van QA bij de implementatie van SAP-Payroll is gekozen om gedurende de looptijd van het project periodiek proces- en productaudits uit te voeren. Zowel de proces- als productaudits staan onder regie van een projectleider (eindverantwoordelijke auditor) binnen het auditteam. Voor beide soorten audits is een multidisciplinair team van auditors samengesteld. Voor een multidisciplinair team is gekozen om te waarborgen dat de QA met de vereiste kennis en ervaring kan worden uitgevoerd. Beide teams variëren in omvang van drie tot zes personen en bestaan uit één of meer IT-auditors, financial auditors en operational auditors. Binnen de teams is gezorgd voor materiedeskundigheid en ervaring met het auditen van:

- salaris(verwerking)processen;
- de module SAP-Human Resources (in het bijzonder SAP-Payroll);
- de module SAP-Financials (voor doorboeking van salarisgegevens);
- projectmanagementvaardigheden;
- implementatie van SAP.

Naast het uitvoeren van de proces- en productaudits vervult het team van auditors een ondersteunende rol bij het implementatieproject door te adviseren bij het opstellen van kwaliteitseisen en de bijbehorende maatregelen, te adviseren over de aanpak voor het opstellen van procesbeschrijvingen en op te treden als procesbegeleider bij de uitvoering van risicoanalyses door de werkgroepen binnen het implementatieproject op de processen van de salarisverwerking (bijvoorbeeld de invoerprocessen bij de personeelsadministratie en de verwerkings- en uitvoerprocessen bij de salarisadministratie). Om de onafhankelijkheid te kunnen waarborgen, geeft een IT-auditor tijdens zijn ondersteunende rol uitsluitend adviezen met betrekking tot de aanpak voor het opstellen van de procesbeschrijvingen en het uitvoeren van risicoanalyses door mogelijk te hanteren methodieken aan te reiken zonder daarbij in te gaan op inhoudelijke aspecten van de procesbeschrijvingen en de risicoanalyses. De definitieve kwaliteitseisen en bijbehorende maatregelen worden vastgesteld door de opdrachtgever. De inhoudelijke beoordeling van de procesbeschrijvingen en de risicoanalyses kan een IT-auditor dan in een later stadium uitvoeren.

Uitvoering van de QA-functie

Bij de uitvoering van QA wordt naast de bewaking van de kwaliteit van het proces ook aandacht besteed aan de bewaking van de kwaliteit van het product. De wijze waarop de kwaliteitsbeheersing voor het proces en het product is vormgegeven, staat beschreven in deze subparagraaf.

Bewaking van proceskwaliteit
Vanuit de bestaande literatuur over implementaties van ERP-softwarepakketten is getracht om inzicht te krijgen in de meest voorkomende faalfactoren. Bij het uitvoeren van de audit wordt hierbij rekening gehouden. Faalfactoren die mogelijk van toepassing zijn op het project worden gerapporteerd aan de voorzitter van de stuurgroep. Op deze wijze wordt getracht om mogelijke faalfactoren expliciet onder de aandacht te brengen, zodat het project hierop kan participeren door vroegtijdig adequate maatregelen te treffen. Onvoldoende aandacht voor organisatorisch verandermanagement en onvoldoende inzicht in de toekomstige processen en het toekomstige besturingsmodel van de organisatie waren de belangrijkste onderkende faalfactoren. Opvallend is dat deze factoren ook worden genoemd

bij de vijf belangrijkste faalfactoren bij de theoretische beschouwing van QA.
Bij de bewaking van de kwaliteit van het proces is met name beoordeeld op welke wijze het project wordt beheerst. Aspecten die daarbij een rol spelen, zijn:
- organisatie van het project;
- personeel (onder andere deskundigheid en gebruikersinbreng);
- middelen en faciliteiten;
- communicatie;
- planning;
- documentatie;
- procedures en processen (bijvoorbeeld kwaliteitsbewaking binnen het project).

Bij het uitvoeren van de kwaliteitstoets maken de auditors gebruik van een binnen de eigen organisatie samengestelde vragenlijst en de aanwezige kennis van en ervaring met projectmanagement binnen het auditteam. De vragenlijst besteedt aandacht aan alle hiervoor vermelde aspecten. Voor het kunnen beoordelen van de proceskwaliteit worden periodiek interviews gehouden met de projectleiding, projectadviseurs, de voorzitters en enkele medewerkers van diverse werkgroepen (werkgroep Proces, werkgroep Systeem & Beheer en werkgroep Verandermanagement). Een specifiek punt van aandacht voor het auditteam vormt de afstemming van de werkzaamheden van de verschillende werkgroepen binnen het project.

Bewaking van productkwaliteit
Bij de implementatie van SAP-Payroll werd tijdens de ontwerpfase gebruikgemaakt van een kwaliteitseisenmodel gebaseerd op extended ISO (ISO/IEC 9126-model). Dit model onderscheidt 32 verschillende kwaliteitscriteria, variërend van beveiligbaarheid tot gebruikersvriendelijkheid, die de kwaliteit van het softwareproduct dienen te waarborgen [FLOR01]. Verschillende participanten die betrokken zullen zijn bij het toekomstig gebruik van het systeem, hebben in verschillende workshops hun kwaliteitseisen en de daarvoor te treffen maatregelen kenbaar gemaakt. Dit is ook het moment voor een IT-auditor om zijn eisen en de daarbij te treffen maatregelen kenbaar te maken. Een IT-auditor zal vanuit zijn deskundigheid met name hoge prioriteit geven aan de kwaliteitscriteria beveiligbaarheid, juistheid, compliance (naleving van wet- en regelgeving), traceerbaarheid en herstelbaarheid van het systeem. Voor deze kwaliteitscriteria heeft het auditteam op basis van een risicoanalyse eisen en maatregelen ingebracht. Het definitieve kwaliteitseisenmodel is, zoals eerder aangegeven, vastgesteld door de opdrachtgever. Een van de maatregelen voor het kwaliteitscriterium beveiligbaarheid is dat autorisaties in het SAP-systeem conform een door de organisatie goedgekeurde functie-autorisatiematrix moet worden ingericht en dat deze autorisaties moeten voldoen aan het 'need-to-know'-principe. Gedurende het vervolgtraject toetst het auditteam de kwaliteit van het product aan de hand van het ingevulde kwaliteitseisenmodel. Op deze wijze is bijvoorbeeld de ontwerpdocumentatie (onder andere de business blueprint) beoordeeld.

Een uitdaging voor een IT-auditor bij het inbrengen van zijn eisen en maatregelen voor een kwaliteitseisenmodel is het in voor de projectgroep begrijpelijke bewoordingen duidelijk stellen en meetbaar (SMART) maken van de eisen en de te treffen maatregelen. In de praktijk is gebleken dat hiervoor veel inspanning nodig is. Een voorwaarde voor het toepassen van een kwaliteitseisenmodel is om éénduidige definities te gebruiken voor de verschillende kwaliteitscriteria en om ervoor te zorgen dat alle betrokken participanten daadwerkelijk dezelfde betekenis geven aan deze definities. Dit voorkomt onnodige discussie over het belang van de verschillende kwaliteitscriteria. Daarnaast is gebleken dat het belangrijk is om de afhankelijkheden tussen de verschillende kwaliteitscriteria in kaart te brengen. Zo geldt bij het gebruik van het extended ISO kwaliteitseisenmodel dat een blijvende juistheid van gegevens (bijvoorbeeld salaris- en personeelsgegevens) mede gewaarborgd kan worden door voldoende aandacht te besteden aan de beveiligbaarheid (bijvoorbeeld door de inrichting van autorisaties in het salarissysteem) van het softwareproduct. In het kwaliteitseisenmodel extended ISO zijn juistheid en beveiligbaarheid gedefinieerd als twee verschillende kwaliteitscriteria. Het kwaliteitscriterium juistheid is binnen het extended ISO kwaliteitseisenmodel gedefinieerd als de kwaliteitseigenschap die betrekking heeft op de voorziening van goede of overeengekomen resultaten of effecten (bijvoorbeeld uitbetaling van het juiste nettosalaris). Het kwaliteitscriterium beveiligbaarheid is binnen het extended ISO kwaliteitseisenmodel gedefinieerd als de kwaliteitseigenschap die betrekking heeft op het belemmeren van oneigenlijke toegang (al dan niet opzettelijk) tot het product of proces.

Er is naar gestreefd om de proces- en productaudits zoveel mogelijk gelijktijdig en gezamenlijk uit te voeren om zodoende maximale synergievoordelen te behalen. Immers, het project brengt de producten voort. Indien de processen binnen het project niet adequaat worden beheerst, vormt dit een extra signaal van waakzaamheid voor een auditor ten aanzien van de kwaliteit van de producten. Naast de eerder genoemde vragenlijst en het kwaliteitseisenmodel wordt bij het uitvoeren van QA de implementatiemethodiek ASAP gebruikt. Hierbij wordt

met de tekortkomingen van ASAP (zoals beschreven in de paragraaf Quality Assurance door de leverancier) rekening gehouden door naast ASAP ook andere normenkaders te betrekken, waaronder binnen de eigen organisatie opgestelde normenkaders en voorschriften.

Het vroegtijdig inbrengen van verbeterpunten door het auditteam wordt door het project gewaardeerd. Dit blijkt onder andere uit de snelle opvolging van de adviezen van het auditteam door de projectgroep tijdens de eerste projectfasen. Naarmate het project vordert, neemt de tijdsdruk sterk toe. Alhoewel de inbreng van het auditteam door de projectgroep nog steeds gewaardeerd wordt, ondervindt het auditteam als gevolg van de toenemende tijdsdruk binnen de projectgroep weerstand ten aanzien van de opvolging van de adviezen. Door middel van communicatie wordt getracht om de projectgroep te overtuigen van het belang van de adviezen. Daarnaast worden de belangrijkste adviezen aan de voorzitter van de stuurgroep gerapporteerd.

Conclusies en aanbevelingen

Implementatie van ERP-softwarepakketten is complex, veelomvattend en kent veel afhankelijkheden. Uit de praktijk blijkt dat ERP-implementaties niet in alle gevallen het gewenste resultaat opleveren. Een middel om de kwaliteit en voortgang van ERP-implementaties te bewaken is QA. QA bij ERP-implementaties dient onafhankelijk van de projectmanager te worden uitgevoerd. Vanwege zijn onafhankelijkheid, onpartijdigheid en deskundigheid op het gebied van automatisering binnen organisaties kan een IT-auditor hierbij uitermate geschikt zijn voor het uitvoeren van een dergelijke QA-functie. Om een werkelijk toegevoegde waarde te hebben bij het uitvoeren van de QA-functie bij ERP-implementaties dient een IT-auditor ook voldoende ervaring met en deskundigheid te hebben van:

- de specifiek te implementeren modules van het ERP-softwarepakket;
- projectmanagementvaardigheden;
- implementatieprocessen (inclusief verandermanagement-vaardigheden);
- processen binnen de organisatie;
- risicomanagement.

Het is zeer wenselijk om bij het uitvoeren van de QA-functie naast de bewaking van proceskwaliteit ook te investeren in de bewaking van de productkwaliteit. Hierdoor kan QA de grootste toegevoegde waarde bieden aan het project. Een IT-auditor kan bij de uitvoering van de QA-functie zijn toetsingsnormen afleiden uit algemeen aanvaarde normenkaders (bijvoorbeeld Code voor Informatiebeveiliging, CobiT en Prince2) en gebruik maken van door een leverancier geleverd standaard implementatiemethodiek (bijvoorbeeld ASAP), mits deze zich bewust is van de tekortkomingen van deze implementatiemethodiek en hiervoor bij de uitvoering van de QA-functie voldoende maatregelen treft.
Uit de opsomming van gewenste deskundigheden en vaardigheden moge duidelijk zijn dat er nogal wat eisen aan een IT-auditor worden gesteld voor het goed kunnen uitvoeren van de QA-functie. Vanuit praktisch oogpunt is het zeer onwaarschijnlijk dat al deze eisen binnen één persoon vertegenwoordigd zijn. Eén persoon heeft hooguit voldoende kennis van één of enkele modules van een specifiek ERP-softwarepakket. Daarnaast zijn de relaties tussen de verschillende modules complex te noemen. Alleen kennis van het ERP-softwarepakket is voor het uitvoeren van de QA-functie niet voldoende. Ook kennis van de organisatie, haar processen, de inrichting van de interne controle en van veranderingsprocessen is een vereiste. We kunnen dan ook gerust stellen dat zo'n schaap met vijf poten niet bestaat.

De praktijk leert dan ook dat voor het goed uitvoeren van de QA-functie een (multidisciplinair) team moet worden ingezet, waarbij aan alle noodzakelijke eisen tegemoet wordt gekomen. Wenselijk is het om dat team zodanig samen te stellen dat voorzien wordt in voldoende kennis van de specifieke modules van het te implementeren ERP-softwarepakket en materiedeskundigen op het gebied van de processen, de interne controle, de organisatie en veranderingsprocessen. Daarnaast biedt een deskundige met voldoende ervaring met het implementeren van betreffende modules een toegevoegde waarde bij de uitvoering van QA. Het vroegtijdig inbrengen van verbeterpunten wordt gewaardeerd door de projectgroep. Dit betekent dat een auditor pro-actief moet zijn en gedurende het project reeds audits uit moet voeren om de projectorganisatie vroegtijdig te attenderen op aanwezige risico's en bedreigingen om zodoende de projectmanager de mogelijkheid te bieden om het project bij te sturen.

Literatuur

[BEER01] Beerens, H., (2001), De kille jaren voorbij, keukendivisie ATAG grijpt na faillissement terug naar 'oud' maatwerk, in: *IT Logistiek*, december.

[FLOR01] Florijn, G. en D. Greefhorst, (2001), Softwareproductkwaliteit – ervaringen en ontwikkelingen, in: *Informatie*, januari/februari.

[HELD99] Helden, P. van en K. Jansen, (1999), Enterprise Resource Planning implementatie: het wordt tijd voor kwaliteit, in: *Management & Informatie*, nr. 5.

[HELD00] Helden, P. van en K. Jansen, (2000), Enterprise Resource Planning, de rol van de EDP-auditor, in: *de EDP-auditor*, nr. 2.

[HELD01] Helden, P. van, (2001), Kwaliteitsborging van ERP-implementaties, in: *De Accountant*, nr. 8.

[HOOG02] Hoogstra, J.P., (2002), *ERP-implementaties: IT-auditor en Quality Assurance, zo'n schaap met 5 poten bestaat niet?!*, Erasmus Universiteit Rotterdam.

[KLUY01] Kluyskens, M., (2001), *Project Risk Management, de toegevoegde waarde van een onafhankelijke partij bij de beheersing van IT-projecten*, Universiteit Twente.

[KPMG99] KPMG EDP Auditors, (1999), *Enterprise Resource Planning*, deel 2 uit de reeks rapporten van EDP naar ICT: op de grens van een millennium.

[MEUL01] Meuldijk, A.M. en M.A.P. op het Veld, (2001), Betere beheersing van ERP-projecten door Quality Assurance, in: *Compact*, nr. 6.

[MORE97] Moret Ernst & Young Management Consultants, (1997), *ERP-implementaties, praktijkervaringen inclusief resultaten Benchmark-onderzoek ERP-implementaties*, Ten Hagen & Stam, Den Haag.

[ROOS99] Roos, P., (1999), Change management en ERP-implementaties; De zachte factoren als aandachtsgebied voor de IT-auditor, in: *de EDP-Auditor*, nr. 3.

[SLIE00] Slieker, L.J.G. e.a., (2000), De rol van de EDP-auditor in relatie tot ERP-ontwikkelingen, in: *Compact*, jubileumuitgave.

[SLOE91] Sloesen, L.J.H.M., (1991), Deskundigheid van de EDP-auditor, in: *Handboek EDP-auditing* C.3.2.4.

[VECH99] Vechgel, M. van en J. Truijens, (1999), Kardinale kwesties bij ERP-pakket-implementaties, in: *Management & Informatie*, nr. 3.

[VERM01] Vermeulen, R.J.J., (2001), *ASAP – aanknopingspunten voor een IT-auditor*, Erasmus Universiteit Rotterdam.

[WEST97] Westerveld, W., (1997), ERP-implementatie, onderschatting is een struikelblok, in: *De Automatiseringsgids*, week 24.

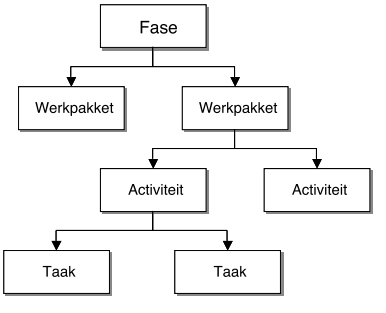
Noot

1 Beoordeeld is AcceleratedSAP For 4.0.

BIJLAGE: EEN INTRODUCTIE TOT DE IMPLEMENTATIEMETHODIEK ASAP

ASAP: een overzicht

Zoals in het artikel vermeld, worden er in ASAP vijf verschillende fasen onderscheiden. Binnen iedere afzonderlijke fase is een aantal werkpakketten gedefinieerd. Ieder afzonderlijk werkpakket bestaat uit een aantal samenhangende activiteiten die op hun beurt weer bestaan uit een aantal taken. De relatie tussen een fase en de hierbinnen gedefinieerde werkpakketten, activiteiten en taken vertoont een hiërarchische structuur zoals in figuur B.1 is weergegeven.



Figuur B1. Hiërarchie van componenten binnen ASAP

Voor ieder afzonderlijk component (fase, werkpakket, activiteit en taak) is een doelstelling gedefinieerd. Als gevolg van de bestaande hiërarchische relatie tussen de componenten binnen ASAP is de doelstelling van een activiteit te realiseren door alle binnen die activiteit gedefinieerde taken te voltooien. De informatie binnen een component wordt steeds gedetailleerder naarmate men lager komt in de hiërarchische structuur. Binnen een fase wordt alleen beschreven wat de doelstelling van die fase is en uit welke werkpakketten die fase bestaat. Binnen een taak wordt naast de doelstelling beschreven welke stappen uitgevoerd moeten worden om aan deze doelstelling te kunnen voldoen, wie deze stappen binnen het project dient uit te voeren en wordt verwezen naar implementatieversnellers (accelerators). Voorbeelden van implementatieversnellers zijn templates voor projectdocumentatie, procedurebeschrijvingen van standaard in SAP gedefinieerde bedrijfsprocessen, standaard procedurebeschrijvingen voor diverse projectactiviteiten, opleidingsmateriaal voor eindgebruikers, white papers, checklists en diverse handleidingen en questionnaires om snel het systeem te kunnen inrichten.

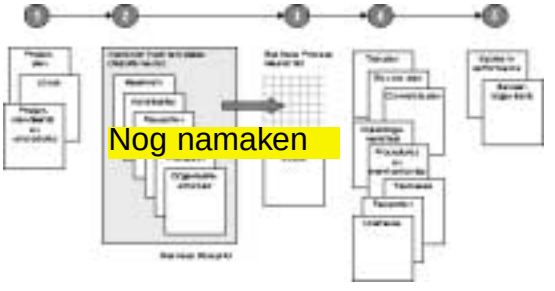
Binnen de implementatiemethodiek ASAP (die op CD wordt geleverd) is een 'Implementation Assistant' beschikbaar. Dit is een tool bestaande uit een question & answer database, de ASAP roadmap, een knowledge corner en een business process masterlist. De 'Implementation Assistant' kan worden geïnstalleerd op zowel een stand-alone PC als een PC die via een netwerk is verbonden. Door deze tool via het netwerk beschikbaar te stellen, kunnen meerdere projectmedewerkers er gebruik van maken, hetgeen de samenwerking tussen de projectmedewerkers kan bevorderen. Binnen de 'Implementation Assistant' is het mogelijk om verschillende autorisaties aan de projectmedewerkers toe te kennen. Vanuit de 'Implementation Assistant' kunnen de parameters en tabellen rechtstreeks binnen SAP worden ingericht.

Voor het per fase te besteden percentage van de totale implementatietijd, kan de volgende vuistregel worden gehanteerd:

- Fase 1: 'Project Preparation' 10%
- Fase 2: 'Business Blueprint' 15%

- Fase 3: 'Realization' 45%
- Fase 4: 'Final Preparation' 20%
- Fase 5: 'Go Live & Support' 10%

In iedere fase wordt een aantal producten (deliverables) opgeleverd. In figuur B.2 zijn de belangrijkste deliverables per fase vermeld.



Figuur B2. ASAP project deliverables

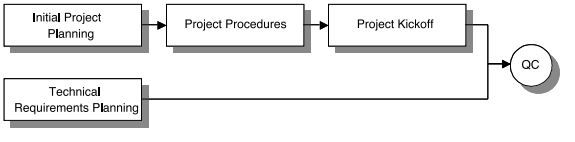
ASAP: de vijf fasen

Hieronder worden de vijf fasen, die de implementatiemethodiek ASAP binnen een implementatieproces voor ERP-software van SAP definieert, uitvoerig besproken. De beschrijving van de verschillende fasen zijn bedoeld om de lezer van dit artikel inhoudelijk nader kennis te laten maken met de implementatiemethodiek ASAP.

Fase 1: Projectvoorbereiding

In deze fase wordt de projectomgeving in kaart gebracht en wordt het project voorbereid. De volgende aspecten komen daarbij uitvoerig aan de orde:
- inrichting van de projectorganisatie (stuurgroep, projectmanagement en werkgroepen);
- opleiding en training van projectmedewerkers in de implementatiemethodiek ASAP;
- opstellen van een globaal projectplan;
- in kaart brengen van de vereiste hardware.

De werkpakketten die in fase 1 volgens de implementatiemethodiek ASAP moeten worden uitgevoerd, zijn weergegeven in figuur B.3. In deze figuur is tevens aangegeven of de afzonderlijke werkpakketten opeenvolgend of simultaan moeten worden uitgevoerd. De lengte van een werkpakket is een maat voor de relatieve tijdsbesteding aan het werkpakket gedurende de betreffende fase.



Figuur B3. wewrkpaketten in fase 1

Initial Project Planning
In dit werkpakket worden mission statements (visie op SAP R/3), business drivers (doelstellingen voor implementatie van SAP R/3) en business measurements (meeteenheden voor doelstellingen) geformuleerd. Daarnaast wordt de initiële implementatiestrategie vastgesteld, waarin een implementatievoorstel (wat), methode (hoe) en roll out-strategie (wanneer) is vastgelegd en worden projectmijlpalen bepaald. De uitkomst van deze fase is een geaccordeerde implementatiestrategie. Tot slot wordt de projectorganisatie opgezet, worden taken en verantwoordelijkheden vastgelegd, wordt een opleidingsplan voor projectmedewerkers en een initieel projectplan opgesteld.

Project Procedures
In dit werkpakket worden afspraken en procedures vastgelegd ten aanzien van de werkwijzen binnen het project. Het doel hiervan is om dubbel of overbodig werk te voorkomen, consistentie van de werkzaamheden te bewaken en de communicatie binnen het project te stroomlijnen. Voorbeelden van activiteiten zijn:
- vaststellen van projectstandaards en -procedures (vergaderschema, inrichting change management, wijze van projectaansturing, et cetera);
- opstellen van een Issue Management plan, waarmee de 'issues' (openstaande punten) die zich gedurende het project voordoen efficiënt en effectief worden afgehandeld;
- opstellen van een Scope Management plan (zoals procedures voor het wijzigen van de projectscope);
- opstellen van een Quality Assurance plan;
- opstellen van implementatiestandaards en -procedures (configuratie, training, documentatie, testen, postimplementatie beheer, afspraken met betrekking tot transporteren van ontwikkelingen naar verschillende systeemomgevingen, et cetera).

Project Kickoff
Aan het eind van de projectvoorbereidingsfase wordt het project officieel gestart met een 'kickoff meeting' voor de medewerkers van het projectteam, de consultants en de belangrijkste lijnmanagers. Het doel van deze 'kickoff meeting' is het onderstrepen van het belang van het project voor het realiseren van de doelstellingen van de onderneming. Een doelstelling kan bijvoorbeeld zijn om efficiënter te werken door de bedrijfsprocessen te standaardiseren en te integreren om daarmee kostenbesparing en dus concurrentievoordelen te behalen. Het is in deze fase essentieel om commitment te behalen bij het (top)management, project- en organisatieleden bij het project te betrekken en om ervoor te zorgen dat alle neuzen dezelfde kant op wijzen. Indien in deze fase onvoldoende commitment van het management wordt behaald, dan is het implementatieproces gedoemd te mislukken.

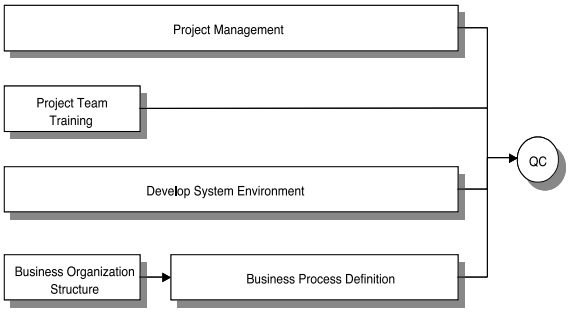
Technical Requirements Planning
In dit werkpakket worden de technische eisen gedefi-

nieerd die nodig zijn om het SAP R/3-systeem te implementeren. De verwachtingen van de organisatie ten aanzien van de technische eisen worden vastgesteld en hardwarecapaciteit wordt beoordeeld. Om mogelijke vertragingen tijdens het implementatieproces te voorkomen, wordt na het in kaart brengen van de benodigde hardware spoedig overgegaan tot het aankopen daarvan.

Quality Check
Alvorens over te gaan naar een volgende implementatiefase, wordt aan het eind van iedere fase een quality check uitgevoerd. Tijdens een quality check wordt gecontroleerd of alle binnen de betreffende fase op te leveren producten (deliverables) daadwerkelijk zijn opgeleverd en voldoen aan de binnen het project overeengekomen kwaliteitscriteria. De quality check wordt onder verantwoordelijkheid van de projectmanager uitgevoerd.
De projectmager beslist uiteindelijk of het resultaat van de quality check voldoende is om aan te vangen met de volgende fase.

Fase 2: Concept- of bedrijfsblauwdruk

Het doel van de conceptfase is om inzicht te krijgen in de doelstellingen van de organisatie, te bepalen welke bedrijfsprocessen hiervoor nodig zijn en vast te stellen welke modules nodig zijn ter ondersteuning van die bedrijfsprocessen. Om te controleren of de wensen en eisen van de organisatie goed zijn begrepen, wordt er een zogenaamde ‘business blueprint’ van de gewenste situatie opgesteld en ter goedkeuring overlegd.
De werkpakketten die in fase 2 volgens de implementatiemethodiek ASAP moeten worden uitgevoerd, zijn weergegeven in figuur B.4.



Figuur B4. Werkpaketten in fase 2

Project Management
In dit werkpakket worden maatregelen getroffen die de voortgang van het project dienen te waarborgen (projectplanning, beheersing, en update-activiteiten). Tevens wordt nagegaan wat de risico’s zijn van het implementatieproject ten aanzien van de wijzigingen in de organisatie.

Project Team Training
In dit werkpakket ondergaan projectmedewerkers indien nodig trainingen om de Business Blueprint-fase kwalitatief goed uit te voeren. De focus binnen dit werkpakket is erop gericht dat projectmedewerkers een gedegen kennis van de functionele en technische aspecten van de ERP-software van SAP verkrijgen.

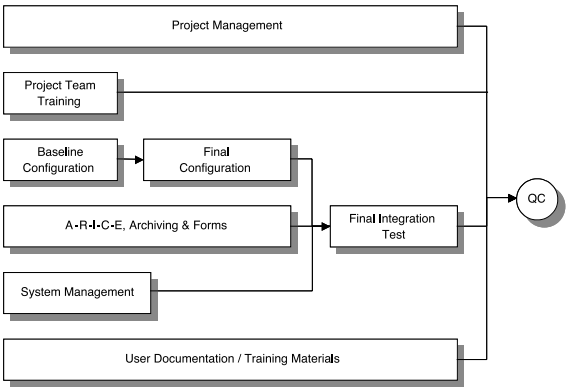
Develop System Environment
In dit werkpakket wordt de technische configuratie van het SAP R/3-ontwikkelsysteem opgezet. De activiteiten die binnen dit werkpakket worden uitgevoerd zijn:
- ontwikkelen van het technisch ontwerp voor de technische infrastructuur. Dit houdt in het inventariseren van de huidige IT-infrastructuur en het ontwerpen van de toekomstige IT-infrastructuur;
- inrichten van de ontwikkelomgeving. Dit houdt onder andere in het installeren van de hardware, het installeren en inrichten van de ontwikkelmandant (ontwikkelclient), en het inrichten van bevoegdheden voor het projectteam;
- inrichten van het SAP R/3-systeemlandschap. Dit houdt in het inrichten van het SAP R/3-transportsysteem, het vaststellen van de verschillende mandanten (waarvoor worden de mandanten gebruikt), en het inrichten van het beheer/onderhoud van mandant-overkoepelende SAP R/3-objecten;
- opstellen en testen van procedures voor het systeembeheer van het ontwikkelsysteem;
- initiëren en inrichten van de Enterprise en Project Implementation Guide (IMG). De IMG is de SAP R/3-functionaliteit waarmee SAP R/3 kan worden ingericht.

Business Organization Structure
Het doel van dit werkpakket is het definiëren van een bedrijfsbrede organisatiestructuur binnen SAP R/3, waarbij gebruik wordt gemaakt van organisatorische eenheden die SAP R/3 biedt (zoals Inkooporganisatie en Verkooporganisatie). Dit onderdeel van ASAP wordt ondersteund door de Question & Answer Database (Q&A).

Business Process Definition
In de Business Process Definition worden eisen en wensen gedefinieerd aan de hand van de binnen SAP R/3 gedefinieerde bedrijfsprocessen. Zodoende wordt de vereiste functionaliteit en daarmee de Business Blueprint vastgesteld.
De Q&A database wordt gehanteerd om het vaststellen van de bedrijfsprocessen te bewerkstelligen. ASAP voorziet in een template om de Business Blueprint op te stellen. In Business Process Workshops worden door implementatieconsultants in samenwerking met gebruikers alle functionele eisen vastgesteld, waaronder de bedrijfsprocessen, rapportages, interfaces, conversie, maatwerk en autorisaties.

Fase 3: Realisatie

Tijdens deze fase wordt het systeem ingericht conform de geaccordeerde bedrijfsblauwdruk. Het geconfigureerde systeem weerspiegelt de organisatie van de klant, bevat stamgegevens en ondersteunt een volledig geïntegreerde proces-flow door het systeem. Tijdens dit proces vindt maximale kennisoverdracht plaats van (externe) implementatieconsultants aan de sleutelgebruikers in de organisatie. Deze sleutelgebruikers worden ingezet bij de opleiding van overige gebruikers.
De werkpakketten die in fase 3 volgens de implementatiemethodiek ASAP moeten worden uitgevoerd, zijn weergegeven in figuur B.5.



Figuur B5. Werkpaketten in fase 3

Baseline en Final Configuration
Het SAP R/3-systeem wordt in twee werkpakketten ingericht: de Baseline Configuration (grootste deel) en de Final Configuration. De Business Process Master List (BPML) wordt gebruikt om de Activiteiten te plannen en te documenteren. In de BPML wordt de volgorde van realisatie, het testen en het accorderen van de SAP R/3-onderdelen aangegeven. De BPML consolideert alle relevante informatie voor de realisatie, zoals verantwoordelijkheden, Business Blueprint en gebruikersdocumentatie. In de BPML wordt de relatie gelegd tussen SAP R/3 transacties (transactiecodes) en de te implementeren bedrijfsprocessen.

Het inrichten van het SAP R/3-systeem gebeurt met behulp van de R/3 Business Engineer. De Business Engineer is een geïntegreerd hulpmiddel binnen SAP R/3 en bestaat uit de Implementation Guide (inrichten van parameters en tabellen), het Reference Model (standaard in SAP R/3 gedefinieerde processen), de Profile Generator (inrichten van autorisatieprofielen) en het Change Request Management (managen van transporten naar verschillende systeemomgevingen). Het inrichten is een iteratief proces van implementeren en testen (Cycles genoemd). Een Cycle is een logische set van bedrijfsprocessen die, na inrichting, een mijlpaal vormt.

Develop Conversion Programs, Applications Interface Programs, Enhancements, Create Reports, Forms, Establish Authorisation Concept en Archiving Management
Het doel van dit werkpakket is het realiseren van conversieprogramma's, interfaces, maatwerkprogramma's, rapporten, formulieren, het autorisatieconcept en archiveringsmogelijkheden. ASAP biedt een aantal hulpmiddelen ten behoeve van deze activiteiten. Een voorbeeld is de Interface Adviser die informatie biedt ten behoeve van het technisch ontwerp en realisatie van interfaces tussen SAP R/3 en niet-SAP R/3-systemen.

Final Integration Test
Het doel van dit werkpakket is het voorbereiden en uitvoeren van de Final Integration Test. Deze integratietest houdt een volledige simulatie in van het toekomstige systeem en werkwijze. De integratietest is noodzakelijk om na te gaan of het systeem is ingericht volgens de verwachtingen en eisen van de gebruikersorganisatie.
In de integratietest worden eveneens het testen van interfaces, uitvoer (printen) en maatwerk uitgevoerd.

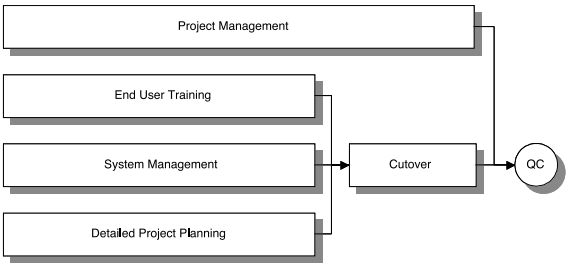
System Management
Het doel van System Management is het voorbereiden van de IT-infrastructuur en automatiseringsorganisatie op de komst van het SAP R/3-systeem. System Management houdt in:
- het definiëren van het niveau van dienstverlening (Service Level);
- het opzetten van een SAP R/3 Quality Assurance-omgeving (ten behoeve van de integratietest);
- het inrichten van de SAP R/3-productieomgeving;
- het implementeren van (systeem)beheerfuncties en -procedures (onder andere back-up & recovery);
- het ontwikkelen van testplannen.

User Documentation/Training Materials
Het doel van dit werkpakket is het ontwikkelen van de gebruikersdocumentatie en het trainingsmateriaal.
De volgende activiteiten worden uitgevoerd:
- het opstellen van een plan van aanpak voor het ontwikkelen van gebruikersdocumentatie;
- het ontwikkelen van de gebruikersdocumentatie;
- het ontwikkelen van het trainingsmateriaal;
- het voorbereiden van de trainingen.

Fase 4: Voorbereiding voor productieve ingebruikname

De belangrijkste mijlpalen van deze fase zijn opleiding van eindgebruikers en het overbrengen van gegevens en systeem naar een productieomgeving. De laatste systeemtests bestaan uit het testen van conversieprocedures en -programmatuur, de interfaceprocedures en -programmatuur, volume- en stresstests en een afsluitende gebruikersacceptatietest.

De werkpakketten die in fase 4 volgens de implementatiemethodiek ASAP moeten worden uitgevoerd, zijn weergegeven in figuur B.6.



Figuur B6. Werkpaketten in fase 4

End User Training
In dit werkpakket worden de gebruikers opgeleid in het gebruik van het SAP R/3-systeem en het werken volgens de vernieuwde processen.

System Management
In dit werkpakket wordt het productiesysteem ingericht en getest (onder andere performance) en worden de toekomstige beheerders opgeleid.

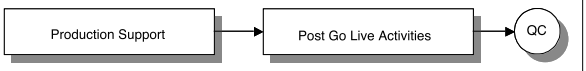
Detailed Project Planning
Ten behoeve van de overgang naar productie wordt de projectplanning in meer detail uitgewerkt (onder andere inrichten helpdesk).

Cutover
Het doel van het dit werkpakket is het voorbereiden en uitvoeren van de activiteiten die noodzakelijk zijn voor het in productie nemen van het SAP R/3-systeem. Activiteiten die worden uitgevoerd zijn onder andere het transporteren van de configuraties en maatwerk naar de productieomgeving en het converteren van vaste gegevens en transactiegegevens van de oude systemen naar het nieuwe SAP R/3-systeem. Dit werkpakket moet worden afgesloten met een formeel akkoord van de stuurgroep.

Fase 5: Go-Live en ondersteuning

Direct nadat het systeem in productie is genomen, moet het nog eens worden nagelopen en waar nodig bijgesteld om te garanderen dat alle facetten van de bedrijfsomgeving in het systeem worden gerepresenteerd. Hiertoe moet niet alleen de nauwkeurigheid van de bedrijfstransacties worden gecontroleerd, maar moet ook onder de eindgebruikers worden geïnventariseerd of aan al hun (informatie)behoeften wordt voldaan.

De werkpakketten die in fase 5 volgens de implementatiemethodiek ASAP moeten worden uitgevoerd, zijn weergegeven in figuur B.7.



Figuur B7. Werkpaketten in fase 5

Production Support
In het werkpakket Production Support wordt een ‘Go Live’ review uitgevoerd om de belangrijkste risico’s te identificeren ten aanzien van het in productie nemen van het systeem. Daarnaast worden nazorgactiviteiten, waaronder het inrichten van een helpdesk, voor gebruikers binnen de staande organisatie opgezet. Een adequate beheerorganisatie wordt opgezet om toekomstige problemen snel te kunnen verhelpen. De firma SAP biedt organisaties hiervoor ook de mogelijkheid om gebruik te maken van het R/3 Online Service System (OSS). Via OSS kan de organisatie problemen melden bij SAP, de status van het probleem volgen en naar oplossingen zoeken. OSS is te beschouwen als een centrale elektronische helpdesk waar alle organisaties gebruik van kunnen maken.

Post Go Live Activities
Dit werkpakket besteedt aandacht aan de activiteiten die moeten worden uitgevoerd nadat het R/3-systeem in productie is genomen. Hierbij valt te denken aan het opleiden van nieuwe medewerkers en medewerkers die van functie wijzigen, hoe om te gaan met het upgraden van hard- en software en het uitbreiden en optimaliseren van functionaliteiten. Daarnaast worden de laatste openstaande ‘issues’ opgelost en wordt het project formeel afgerond.

Een Nobelprijswinnaar over risicomanagement

Op zaterdag 1 februari 2003 verongelukte het ruimteveer Columbia. Dat ruimtevaart niet zonder risico's is, bleek opnieuw. Ruimtevaart eist dus een adequaat risicomanagement. Methodieken voor risicomanagement zijn er voor het oprapen. Alle methodieken beloven dat het management daarmee alle risico's kan beheersen. Toch blijft het de grote kunst om niet alle risico's op te sommen, maar vooral om de belangrijkste te onderkennen, de kritische succes- of faalfactoren. Soms schuilt het gevaar in de kleinste details of in uitzonderlijke situaties. Adequaat risicomanagement houdt in dat de risico's in kaart zijn gebracht, dat maatregelen zijn genomen om die te beperken, maar vooral dat de besluitvorming goed is georganiseerd. Anders gaat het ondanks alle moeite toch nog mis. EDP-auditors kunnen lering trekken uit de eerdere ramp met het ruimteveer Challenger; het voorbeeld van falend risicomanagement in de jaren tachtig van de vorige eeuw.

Sjaak Boone

Op 28 januari 1986 explodeerde de Challenger met de bemanning voor de ogen van een groot publiek, onder wie de Amerikaanse president. De vlucht had maar 72 seconden geduurd. Voorafgaand aan de start van de spaceshuttle was er veel publiciteit geweest. Aan boord was een Amerikaanse onderwijzeres Christa McAuliffe. Het plan was dat zij na de start een gesprek zou hebben met president Reagan. De vlucht was maar liefst vijf keer eerder uitgesteld, waarvan drie keer wegens slecht weer. De NASA, de organisatie die vooral betrokken was bij het ruimtevaartprogramma, kon de vele publiciteit goed gebruiken. De begroting van nieuwe programma's stond onder druk. De gevolgen van de ramp, die zich afspeelde voor de ogen van vele televisiekijkers, waren echter enorm. Het publiciteitsoffensief van de NASA keerde zich tegen de organisatie. Miljarden televisiekijkers over de gehele wereld waren ooggetuige van de ramp. De NASA moest wel een grondig onderzoek beloven om het geschonden imago te herstellen.

I. Boone was van 1991 tot eind 2002 security officer bij de nv Bank Nederlandse Gemeenten. In die periode heeft hij regelmatig als (co-)auteur gepubliceerd op het gebied van informatiebeveiliging en risicomanagement. Hij is nu werkzaam bij BNG Management Services, een dochteronderneming van de nv Bank Nederlandse Gemeenten.

EEN COMMISSIE VAN ONDERZOEK

De NASA vroeg de Nobelprijswinnaar en natuurkundige Richard Feynman om deel te nemen aan een Presidentiële commissie die de oorzaak van de ramp moest onderzoeken. Die was aanvankelijk niet enthousiast, maar nam de uitdaging toch aan. In de commissie zaten vooral veel personen, die hun sporen in de ruimtevaart hadden verdiend. De eerste vrouw in de ruimte, de eerste man op de maan en de eerste piloot die de geluidsbarrière doorbrak. Het was eigenlijk niet de bedoeling dat de commissie iets anders zou rapporteren dan dat zij door de NASA werd voorgeschoteld. Door de deelname van Feynman aan de commissie leek die opzet niet te lukken. De natuurkundige Feynman was een interessante figuur. Hij had in zijn jeugd meegeholpen met de ontwikkeling van de atoombom en had baanbrekend natuurkundig onderzoek verricht. Voor een professor hield hij er vreemde hobby's op na. Zo trok hij zich soms terug in het bos om te gaan trommelen en was hij een herhaald bezoeker van het carnaval in Zuid-Amerika. Hij was een begenadigd docent, zijn 'Feynman lectures on physics' worden vrijwel overal ter wereld gebruikt door studenten Natuurkunde. Aan het einde van zijn leven publiceerde hij

zijn memoires met een groot aantal komische anekdotes. Feynman was op het moment van de uitnodiging ernstig ziek en wist dat hij nog maar enkele maanden had te leven. Hij hield ervan om te worden uitgedaagd en was een echte onderzoeker, fanatiek op zoek naar feiten. Door zijn eigen gang te gaan kwam hij achter de oorzaak van de ramp. De rubberpakkingen om de verschillende delen van de raket aan elkaar te bevestigen, de O-ringen, konden bij temperaturen van rond het vriespunt niet snel genoeg uitzetten. Hij gaf voor de televisiecamera een demonstratie met een model van de rubber ringen in een glas ijswater. Zijn verklaring werd bevestigd door televisiebeelden die tijdens de lancering waren gemaakt. Bij de start van de spaceshuttle waren die lage temperaturen gemeten, maar men besloot de start toch door te zetten. Omdat de ring niet snel genoeg kon uitzetten, lekte er brandstof langs de zijkant van de raket. Dat lek was uiteindelijk de oorzaak van de explosie van de raket met de spaceshuttle. Feynman beschreef zijn belevenissen in de commissie in zijn boek 'What Do You Care What Other People Think?', (Nederlandse titel: 'Laat ze maar praten'). Zowel het verhaal van Feynman als het rapport van de commissie meldden niet, dat uit milieuoverwegingen bij de Challenger in de ringen voor het eerst geen asbest was verwerkt.

OPZET VAN RISICOMANAGEMENT BIJ NASA

Risicomanagement stond in 1986 bij de NASA hoog in het vaandel. Hoge functionarissen bij de NASA hadden Feynman verteld dat de kans op een ramp met de spaceshuttle 1 op 100.000 was. Zij legden hem hun methodieken uit op basis waarvan zij tot hun schatting kwamen.
In allerlei handboeken was gedetailleerd vastgelegd wat gedaan moest worden om zoveel mogelijk risico's uit te sluiten. Daarbij ging het niet alleen om handboeken van de NASA, maar ook om die van toeleveranciers of dienstverleners. Tot in de kleinste details waren de werkinstructies vastgelegd. Technisch onderhoudspersoneel moest zich houden aan die werkinstructies en was verplicht om bijzonderheden te rapporteren.
Het stelsel van handboeken met gedetailleerde instructies was bedoeld om risico's zoveel mogelijk te voorkomen. Bijzonder veel aandacht was besteed aan de beveiliging van de informatietechnologie. De ruimtevaart was daarvan steeds afhankelijker geworden. Men had programmatuur geschreven voor de besturing van het ruimteveer. Voor de lancering, de vlucht en de landing moesten aparte cassettes worden geladen met programmatuur, want de apparatuur bezat maar een beperkt intern geheugen. In 1986 waren de eerste computers nog niet erg bedrijfszeker.
In ieder geval had men er weinig ervaring mee. Vanzelfsprekend waren er reservekopieën van de cassettes met programmatuur aanwezig in het ruimteveer. Omdat de computer wel eens defect kon zijn, waren zelfs vier systemen geïnstalleerd. Met de opzet van het risicomanagement leek het dus dik in orde te zijn.

BESTAAN VAN RISICOMANAGEMENT BIJ NASA

Al bij de eerste gesprekken werd het Feynman duidelijk, dat er iets schortte aan het risicomanagement bij NASA. Dat was ook niet zo verwonderlijk, want Feynman had ervaring met onderzoek naar rampen in de ruimtevaart.
In de jaren vijftig was hij betrokken geweest bij een mislukte lancering van een communicatiesatelliet. Men begreep niet dat men geen verbinding kon krijgen met de satelliet na de lancering en men vroeg zich af wat daarvan de oorzaak was. Het hoofd van de computerafdeling herinnerde zich zijn vroegere hoogleraar en nodigde hem uit om mee te doen in het onderzoek. Feynman wedde dat hij het wel zonder computer kon uitrekenen en begon aan het werk.
De computer die men voor de berekeningen gebruikte, was een mainframe van IBM, dat toen nog een kamer vulde. Inderdaad wist Feynman binnen een dag te melden, dat de satelliet in de Atlantische Oceaan was geplonsd. Dat werd een paar uur later bevestigd door de computerberekeningen.
'Vraag het de specialist', was het motto van Feynman. Hij voerde een groot aantal gesprekken met technici.
Al snel viel hem op, dat die de risico's heel anders ingeschat hadden, dan de marges waarop het management van NASA zich stelde te baseren. Feynman legde meteen de vinger op de zere plek door aan te tonen dat sommige berekeningen onjuist waren. Feynman berekende een kans van 1 op 100, de kans die ook door de technici bij benadering was opgegeven. Het oordeel van Feynman was duidelijk: de methode van de NASA voor de schatting van de risico's was 'een hoop rotzooi' (' a bunch of crap'). Feynman stelde dat de uitkomsten van de berekeningen waren aangepast om toch vooral maar binnen de vooraf gestelde marges te blijven. Door de complexiteit van de berekeningen konden de fouten onontdekt blijven.
Ondanks dat de perceptie over de foutenmarges van het management verschilde van de technici, deed men er binnen de NASA alles aan om risico's zoveel mogelijk te verlagen. Er werd voortdurend onderzoek gedaan naar alle mogelijke kleine fouten, die zich bij eerdere vluchten hadden voorgedaan. Op basis van die ervaringen nam men ook extra beveiligingsmaatregelen. Het was iedereen duidelijk dat een ongeluk geen goed zou doen aan de reputatie van de NASA. Die opstelling gold niet alleen voor de NASA, maar ook voor de toeleveranciers en de dienstverleners.
Het Amerikaanse congres had ook een onderzoekscommissie ingesteld. Deze commissie was overigens in haar eindrapport opmerkelijk minder mild dan Feynman of de

commissie van de NASA. In het eindrapport werden kritische noten gekraakt over de procedure waarmee incidentmeldingen werden afgehandeld. Ook de wijze waarop de rapportage was ingericht kreeg er van langs. Zo werd gerapporteerd aan personen die ook verantwoordelijk waren voor de dagelijkse gang van zaken. Het gevolg laat zich raden: feiten die niet in het beeld pasten, leidden tot aanpassingen in de rapportage.

WERKING VAN HET RISICOMANAGEMENT BIJ DE NASA

Al in de eerste fase van zijn onderzoek kreeg Feynman in de gaten, dat de oorzaak van de ramp moest worden gezocht in een lek in de afdichtingsringen van de brandstoftanks van de hulpraketten. De brandstoftanks werden steeds hergebruikt. De tanks bestonden uit verschillende componenten, die aan elkaar waren gekoppeld. Tussen de componenten was een sluitende rubberring aangebracht. Voor het geval dat die ring het geheel niet goed afsloot, was nog eens een tweede ring aangebracht. Feynman concludeerde uit de briefwisseling tussen technici van de NASA en de toeleverancier Morton-Thiokol, dat de afdichtingsringen steeds een probleem hadden gevormd. Bij eerdere lanceringen had men wel eens kleinere lekkages opgemerkt. Bij de ramp met de Challenger was er een lek ontstaan. De vrijkomende gassen werkten als een snijbrander. Doordat de hulpraketten als gevolg van het lek elk een andere kant op stuurden, werd de hoofdtank uit elkaar gerukt en explodeerde de vrijkomende brandstof. Een ander lid van de commissie was generaal majoor Kutyna van de US Air Force. De luchtmachtgeneraal kende veel technici en astronauten. Hij had uit die hoek wat opmerkingen gehoord over de mogelijke oorzaak van de ramp, maar kon onmogelijk zijn bron prijs geven. Hij raakte bevriend met Feynman en vroeg hem om zijn verzameling oldtimers te zien. Op een werkbank in zijn garage lag een carburateur. Kutyna vroeg aan Feynman hoe het mogelijk was dat een carburateur in een koude omgeving lekte. Feynman had onmiddellijk door dat de lage temperatuur tijdens de start de oorzaak zou moeten zijn van de ramp.
Toch was de ramp geen gevolg van slechte onderlinge samenwerking of communicatie. De ingenieurs van de raketfabriek hadden het probleem onderkend en de top van de NASA ervan op de hoogte gebracht. Men had zelfs de maatregel genomen dat voorafgaand aan de lancering een medewerker van de NASA de temperatuur controleerde. Zijn bevindingen moest hij rapporteren, dat had hij ook gedaan op de dag van de ramp. Tijdens het onderzoek concludeerde Feynman van de hand van de reeks waarnemingen, dat de medewerker zijn apparatuur niet conform de instructies had gebruikt. Maar ondanks die verkeerde methodiek wees de rapportage van de medewerker uit, dat de temperaturen te laag waren geweest. Ondanks de negatieve signalen werd door het management van de NASA toch besloten om de lancering door te laten gaan. Het gevolg was rampzalig.

BESLUITVORMING EN RISICOMANAGEMENT

De druk op de raketfabriek en de NASA was groot om de start na vijf keer afstel toch door te laten gaan. Er stonden grote belangen op het spel: een nieuw contract of een nieuwe subsidie.
Ondanks negatieve adviezen besloot het management van de NASA toch om het ruimteveer te lanceren. Men negeerde de negatieve signalen en zette feitelijk een streep door de uitkomst van het stelsel van risicomanagement. Eerdere gelukte lanceringen hadden tot onderschatting van de gevaren geleid. De managers geloofden niet dat de eerder waargenomen effecten van het te laat uitzetten van de O-ringen tot een grote ramp konden leiden. Het was eerder steeds goed gegaan. De managers zagen de ingenieurs als perfectionisten, die altijd maar op zeker wilden gaan. Ingenieurs willen altijd nog wat meer gegevens hebben en kunnen niet het grote geheel overzien. Als je teveel naar ze zou luisteren, gebeurde er nooit wat, was de visie van het management van de NASA. Feynman merkte over de opvatting dat het met eerdere lanceringen ook goed was gegaan met zijn gebruikelijke gebrek aan tact op, dat het steunen op ervaringscijfers bij een onderkend risico veel weg heeft van Russische roulette. Hij constateerde verder dat de astronauten niet in de besluitvorming waren betrokken. Daardoor speelde het verlies van mensenlevens nauwelijks een rol in het besluitvormingsproces. De astronauten, voor wie de tocht met de Challenger letterlijk een zaak van eigen leven of dood was, kenden de risico's niet van een start bij een te lage temperatuur.
Hoe kan een besluitvormingsproces rond risicomanagement beter worden ingericht in een uiterst complexe omgeving, was de vraag na de ramp. Een manager is ook maar een mens, en het menselijk brein heeft zo zijn beperkingen. In een optimaal besluitvormingsproces moet men alle mogelijkheden en wegingsfactoren gecoördineerd aan elkaar afwegen. Maar dat kunnen mensen niet. Het menselijk brein werkt vaak op basis van simpele rekenmethoden met verkeerde aannames. Mensen houden ervan om naar de gewenste uitkomst toe te redeneren. Dus is er een methodiek of een systeem nodig, dat zulke valkuilen vermijdt. Naast de beperking van het menselijk brein is er ook een psychologische factor: groepsgedrag van managers. Kleine groepjes van blanke mannen, die al jaren met elkaar hebben samengewerkt kunnen een groepsvisie ontwikkelen. Die groepsvisie bepaalt hun kijk op de wereld, waarbij

zij nieuwe maatschappelijke ontwikkelingen of feiten die er niet mee in overeenstemming zijn niet toelaten. Vanuit die visie wordt de mening van niet-managers, zoals ingenieurs, niet op de juiste waarde geschat. Men heeft alleen nog maar waardering voor het oordeel van andere leden uit de groep. In een nieuwe opzet van het besluitvormingsproces verzamelt de NASA gegevens uit verschillende groepen. Een van de technische consultants daarover: 'Er blijft altijd een bepaalde mate van onzekerheid bestaan bij risicoanalyse, die wordt verpakt in termen van mogelijkheden en gemiddelden. Maar de analyse kan trends aan het licht brengen en helpt managers om te bepalen waaraan zij meer aandacht moeten schenken'. Na de ramp met de Challenger werd het besluitvormingsproces bij de NASA zo ingericht dat een enkele astronaut de uiteindelijke beslissing neemt voor de lancering.
Feynman heeft met zijn aanbeveling voor de besluitvorming feitelijk het principe geïntroduceerd dat degene die het meeste last heeft van de gevolgen, de zwaarste stem heeft bij het nemen van maatregelen van risicomanagement. Zelfs dus tot aan het afblazen van de vlucht. De ramp met de Challenger brengt aan het licht dat zelfs bij een goed ingericht stelstel van risicomanagement er toch nog door de top foute beslissingen kunnen worden genomen.

FEYNMAN PLEEGT ONDERZOEK

Anders dan de andere leden van de commissie hanteerde Feynman een onorthodoxe aanpak: hij ging meteen naar de mensen die de raket in elkaar hadden gezet. 'Vraag het aan de echte specialist', was zijn motto. Hoewel de NASA er alles aan had gedaan om de commissieleden te voorzien van informatie, ging Feynman zijn eigen gang. Hij wilde niet vermoeid worden met feiten, die hij niet relevant vond. Ook gedurende de weekeindes werkte hij door. Zo beoordeelde hij 250.000 regels programmatuur en las hij in detail de handboeken en inspectieverslagen. Zo leerde hij dat het niet alleen de afdichting in de brandstoftanks waren, die problemen veroorzaakten. Hij constateerde dat er ook problemen waren geweest met de motoren. De extreme omstandigheden in de ruimtevaart veroorzaakten scheuren in de brandstofturbines. Bij de test of de motor nog wel naar behoren functioneerde, werden de testcriteria steeds bijgesteld.
Door zijn harde werken en de kennis van de details, dwong Feynman respect af van de technisch specialisten. Feynman realiseerde zich, dat zijn rapportage ernstige gevolgen zou kunnen hebben voor een of meer toeleveranciers in de ruimtevaartindustrie. Ook zou zijn rapportage de carrières kunnen breken van managers bij de NASA. Het was de kracht van Feynmans persoonlijkheid, waarmee hij het vertrouwen won van de technisch specialisten. Een van die specialisten was Roger M. Boisjoly, de belangrijkste ontwerper van de hulpraketten, die werden geproduceerd door Morton Thiokol (MTI). Boisjoly hoorde bij de groep specialisten, die nutteloos hadden geprobeerd om de lancering te stoppen. Eigenlijk werd Feynman niet geacht om zelf met ingenieurs te gaan praten, maar hij deed het toch. Ondanks de risico's voor zijn carrière en het voortbestaan van zijn werkgever, besloot Boisjoly de waarheid te vertellen aan de onderzoekscommissie. Hij vond dat Feynman het enige lid was van de commissie die echt probeerde om de waarheid boven tafel te krijgen. Na zijn optreden achter gesloten deuren en zijn latere publieke optreden, werd Boisjoly steeds gebeld door Feynman. Het viel hem op, dat Feynman hem steeds aansprak met Dr. Boisjoly. Hij probeerde nog een paar keer uit te leggen, dat hij nooit was gepromoveerd, maar Feynman bleef dezelfde fout maken. Boisjoly voerde vele telefoongesprekken met Feynman, waarbij deze steeds opnieuw details wilde weten. Boisjoly werd uitgenodigd om commentaar te leveren op het officiële eindrapport van de NASA, maar had daarvoor maar een enkele dag de tijd gekregen. Toen hij die dag in Washington in de rij stond voor een kopje soep en een broodje, hoorde hij opeens roepen: 'Hé, jongens, kan ik bij jullie komen zitten?' Het was Feynman die toch nog iets wilde weten en de lunch liep uit tot een uur. Feyman vertelde steeds grappige anekdotes. Later vertelde Boisjoly het verhaal van het gebruik van de titel door Feynman aan een van diens collega's. De professor vertelde Boisjoly, dat hij een persoonlijke eretitel van Feynman had gekregen omdat hij de waarheid over de oorzaak van de ramp met de Challenger had onthuld. In de rapportage wilde de commissie aanvankelijk niets van de bevindingen van Feynman opnemen. Het eindrapport zou vooral moeten aangeven, dat ruimtevaart ondanks de risico's toch vooral zou moeten worden voortgezet. Ook zou er meer geld naar het onderzoeksprogramma moeten gaan. Feynman was het daar niet mee eens en dreigde met opstappen of met het publiceren van zijn eigen rapport. De andere leden van de commissie waren het optreden van Feynman beu. Een journalist hoorde in het toilet een van hen zeggen dat Feynman 'nu echt een doorn in het vlees was geworden'. Uiteindelijk werd een compromis bereikt, waarbij het verslag van Feynman als bijlage bij het rapport was opgenomen. Die bijlage was aanmerkelijk kritischer over de NASA dan het officiële rapport. Feynman besluit die bijlage met: 'De NASA is verplicht open, eerlijk en informatief te zijn tegenover de burgers van wie zij steun vragen, zodat deze burgers de verstandigste beslissingen kunnen nemen bij gebruik van hun beperkte middelen. Voor een succesrijke technologie moet realiteit voorrang krijgen boven een goede presentatie aan het publiek, want de natuur laat zich niet voor de gek houden.'

HERSTELD VERTROUWEN

Critici van Feynman verwijten hem dat zijn onderzoek alleen maar is verwoord in een aparte bijlage. Toch heeft de opstelling van Feynman belangrijke gevolgen gehad voor de Amerikaanse samenleving. Feynman was een schoolvoorbeeld van iemand die gebruik kon maken van de omstandigheden in de Verenigde Staten, het land van de onbegrensde mogelijkheden. Hij was zich ervan bewust, dat hij met zijn opstelling zijn land diende.
Na de ramp met de Challenger leek opeens alle technologie verdacht. Kon de gemiddelde Amerikaan nog wel vertrouwen op zijn auto? De gevolgen van de ramp waren dus veel groter dan alleen maar een ruimtevaartprogramma.
Het besluitvormingsproces bij de NASA is als gevolg van de aanbevelingen veranderd, waarbij de astronauten de belangrijkste stem kregen om de vlucht al dan niet door te zetten. De opstelling van 'dr' Roger Boisjoly heeft ook geleid tot veranderingen binnen het Amerikaanse Instituut voor Ingenieurs. In de beroepscode voor Amerikaanse ingenieurs is expliciet verwoord, dat deze zich dienen te houden aan ethische principes. Die hebben voorrang boven de mogelijke schade aan eigen carrière of aan de organisatie waar men werkzaam is.
Het rapport van Feynman was het grootste monument ter nagedachtenis aan de bemanning van de Challenger. Omdat geleerd is van het ramp waarbij zij waren betrokken, is hun offer niet tevergeefs geweest.

WAT KUNNEN EDP-AUDITORS VAN FEYNMAN LEREN?

Samenwerking met andere disciplines

Feitelijk is het plegen van ruimtevaart een vrij simpel bedrijfsproces, hoe groot de technische uitdagingen ook zijn. Men wil een shuttle lanceren en na een verblijf van een bepaalde tijdsduur in de ruimte weer veilig laten landen op aarde. Ruimtevaart is voor een belangrijk deel afhankelijk van een goede en ongestoorde informatievoorziening, een vakgebied waarop EDP-auditors zich bewegen.
Voor risicomanagement van de informatievoorziening zijn inmiddels verschillende methodieken ontwikkeld. Uit het voorbeeld van de Challenger blijkt duidelijk dat het niet alleen gaat om de risico's van de informatievoorziening, maar ook om de technische risico's.
Bij het vormen van een oordeel over het door een bedrijf gevoerde risicomanagement zullen EDP-auditors in toenemende mate moeten samenwerken met andere specialisten.

Keuzecriteria voor methodiek van risicomanagement

Bij de keuze voor een methodiek van risicomanagement zal men niet alleen moeten letten op de criteria voor de IT-risico's. Afhankelijk van het type bedrijfsproces zal de methodiek ook rekening moeten houden met andere bedrijfsrisico's.

Inrichting van de besluitvorming

De NASA had er alles aan gedaan om een sluitend stelsel van risicomanagement te ontwerpen. Ondanks die inspanningen kon het toch nog mis gaan omdat het besluitvormingsproces niet goed was ingericht. Ondanks de negatieve adviezen van technisch specialisten besloot het management toch om de vlucht te laten doorgaan. De argumenten voor die beslissing waren niet sterk en kunnen hoogstens worden verklaard uit groepsgedrag van managers. In dit geval bleek het management de grootste risicofactor.

Onafhankelijk onderzoek en rapportage

Ook een EDP-auditor zal zich een onafhankelijk oordeel moeten vormen over een aangetroffen situatie. Hij zal de grenzen van zijn onderzoek moeten aangeven. Voor de EDP-auditor is de onderzoeksopdracht van wezenlijk belang. Hij zal ook afspraken moeten maken over de opzet van zijn onderzoek, waarbij hij ook gesprekken zal voeren met de belangrijkste technische specialisten. Daarnaast is van belang dat de EDP-auditor rapporteert aan het juiste niveau. Dat zal dus niet dezelfde moeten zijn als de functionaris die verantwoordelijk is voor de IT-sector in een organisatie.

Literatuur:

Boone, I., (1998), Informatiebeveiliging in metaforen, Den Haag.
Bautz, J., I. Boone en J. Dudok van Heel, (2001), Risicomanagement voor de informatievoorziening, Den Haag.
Bautz, J., I. Boone e.a., (2000), Checklist Informatiebeveiliging, Den Haag.
Feynman, R.P., (1990), Laat ze maar praten, Bloemendaal.
Nederlands Normalisatie Instituut, Code voor Informatiebeveiliging, Delft.
Gleick, J., (1992), Genius, The life and science of Richard Feynman, New York.
ISO TR 13335, Guidelines for the Management of IT Security.
www.riskinfo.com.

Feynmans bijlage:
www.virtualschool.edu/mon/SocialConstruction/FeynmanChallangerRpt.html.
Rapport van de NASA:
http://spacelink.nasa.gov/NASA.Projects/Human.Exploration.and.Development.of.Space/Human.Space.Fligt/Shuttle/Shuttle.Missions/Flight.025.STS-51.L/.index.html.
Een beschrijving van de ramp en het onderzoek:
www.scienceandsociety.ucsd.edu/soc130/dossiers/challanger/challanger.htm.

Symposium Audit Effectiviteit

Op vrijdag 24 januari 2003 werd op de Erasmus Universiteit Rotterdam het Symposium Audit Effectiviteit georganiseerd door de postdoctorale opleidingen EDP Auditing, en Internal Operational Auditing van EURAC.

Roeland Aernoudts

De redenen om dit symposium te organiseren, zijn de vele recente veranderingen die op het terrein van audit zijn opgetreden. De verschillende financiële schandalen waarmee het audit beroep worden geconfronteerd, noodzaken tot een maatschappelijke discussie. Het symposium vervulde in die zin dus een maatschappelijke rol. Mede om de maatschappelijke rol te benadrukken, zijn coryfeeën uit diverse geledingen van het bedrijfsleven uitgenodigd. Het symposium werd voorgezeten door Prof. Dr. K. Mollema RE RA, hoogleraar EDP-auditing te Rotterdam. De forumleden waren J.P. Bostoen (General Auditor van Fortis), Mr. P. van Dijken (adviseur en plaatsvervangend rechter), Prof. J.C.A. Gortemaker RA (hoogleraar Accountancy te Rotterdam), P. Koster RA (bestuurslid Autoriteit Financiële Markten), Prof. Dr. G.J. van der Pijl RE (hoogleraar EDP-auditing te Rotterdam) en Prof. Drs. K. Wezeman RA (emeritus hoogleraar AO en voormalig partner E&Y).

De voorzitter poneerde verschillende stellingen. Vervolgens werd door steeds twee verschillende forumleden een standpunt voor, dan wel tegen ingenomen, wat leidde tot interessante, en soms verhitte discussies. Hoewel de stellingname soms inhoudelijk niet volledig aansloot bij de mening van de sprekers, kweten zij zich met verve van hun taak.
De eerste stelling geponeerd luidde als volgt:

Is audit effectief als opspoorder van mismanagement en/of corruptie in het bedrijfsleven?

Drs. R.H.R.M. Aernoudts, Erasmus Universiteit Rotterdam, Accounting & Finance/EURAC

De heer Bostoen verdedigde deze stelling, de heer Van Dijken fungeerde als zijn opponent. De heer Bostoen stelde dat het management verantwoordelijk is voor de control environment, voor ethiek en toonzetting aan de top van een organisatie. Kortom, het management draagt verantwoordelijkheid voor de organisatiecultuur welke van belang is voor de interne beheersing. De auditor is vanuit zijn functie aanwezig in alle geledingen van de organisatie. De auditor kan in die hoedanigheid de zwakke plekken in de interne beheersing opmerken. Dit vergroot de kans op detectie van fraude en mismanagement. Volgens de heer Van Dijken beschikt de accountant niet over de juiste kennis om fraude op te sporen. De waarheidsvinding nam bij zijn betoog een centrale rol in. De functie van de rechercheur en de accountant verschillen teveel van elkaar. De rechercheur is belast met waarheidsvinding en is vanuit zijn functie dus bekend met forensische technieken. Een accountant beschikt niet over deze kennis. Er is sprake van een confrontatie van disciplines, waarbij een duidelijke taakverdeling wenselijk is. Alleen wanneer men onderkent dat er verschillen zijn, kan er sprake zijn van een goede waarheidsvinding. De accountant en de rechercheur kunnen elkaar in dat opzicht in theorie en praktijk aanvullen. Ergo, de accountant vervult wel een aanvullende rol, maar kan niet fungeren als opspoorder. De auditor maakt wel deel uit van het proces. De heer Bostoen bevestigde de heer van Dijken in zijn stellingname, ook hij is van mening dat beide specialismen elkaar aanvullen. De externe accountant kan bij forensisch onderzoek een rol spelen, maar kan ‘het varkentje niet alleen wassen’. Een goed voorbeeld hiervoor vindt men wanneer men de zaak betreffende burgemeester Peper van Rotterdam onder de loep neemt. ‘Hier ging de

Wel of geen foto?

externe accountant de mist in, omdat deze de zaak alleen wenste aan te pakken'. Concluderend kan men stellen dat de disciplines elkaar aan moeten vullen.

De tweede stelling geponeerd luidde als volgt:

Is financial audit een beproefd en bewezen effectief control-instrument voor (beurs)toezichthouders?

De heer Koster beaamde deze stelling. Echter, als extern toezichthouder eist hij ook internal control en eist hij self-assesment; de internal operational auditor speelt hierbij een belangrijke rol. De AFM wil weten hoe men opereert conform de wet. De Raad van Commissarissen van een organisatie moet veel meer gebruikmaken van de interne accountantsdiensten. Zij moet deze vragen om meer specifieke onderzoeken en meer gebruikmaken van interne controls. Concluderend stelde hij dat de jaarrekening een beproefd controlmiddel is voor extern toezicht, ook voor het management. De heer Wezeman bracht ten aanzien van deze stelling een aantal bezwaren naar voren. De financial audit is teveel gericht op financiële verantwoording. Gelet moet worden op scope, kwaliteit en tijdigheid. De scope is te beperkt, en de audits zijn niet tijdig genoeg en daarbij te geaggregeerd. Wil men weten wat er effectief gebeurt in de organisatie, dan is de financial audit hiervoor te beperkt. De financial audit is te zeer gebonden aan voorschriften. Dit leidt tot anticiperend gedrag, waardoor fraude mogelijk wordt. Regels leiden tot anticipatie, gericht op compliance, wat vervolgens leidt tot valse gerustheid. De heer Koster voegde hieraan toe dat de AFM in feite toe wil naar een prospectief oordeel over betrouwbaarheid. Een risicobenadering dient daarvoor zowel financieel als niet-financieel gericht te zijn. Risico's kunnen worden ingekaderd, maar kunnen nooit worden weggenomen. Cultuur is, evenals de anderen stellen, van essentieel belang. Een principle-based audit, in plaats van een rule-based audit zou in dit kader beter passen.
De heer Wezeman reageerde hierop door te stellen dat de toezichthouder in feite machteloos is. De macht van de externe toezichthouder wordt overdreven, kijk maar eens naar de Amerikaanse SEC. De focus van de audits is niet juist.
De heer Mollema vroeg vervolgens of men niet de effectiviteit van de jaarrekeningcontrole dient te onderzoeken vooraleer daarop te steunen: 'Heeft de SEC misschien boter op het hoofd? Is de accountant wellicht overbodig?'
De heer Koster reageerde: 'De accountant is niet overbodig'. Met de komst van het Blue Ribbon rapport, en de Sarbanes-Oxley-wet omtrent het ondertekenen van de jaarrekening door de executive president, is de waarde van de accountantsverklaring verminderd.
De heer Wezeman vermeldde dat hij zeer gelukkig is met de Sarbanes-Oxley act. Echter, de SEC wekt de indruk dat binnen zes weken een hele organisatie kan zijn omgetoverd, wat zeker discutabel is! De SEC lijkt een schijnoplossing te hebben geleverd. Het wordt ook duidelijk dat het accountantsberoep in paniek is. De Europese executive kan ook onder Sarbanes-Oxley worden gepakt, wanneer zijn onderneming in New York een beursnotering heeft.
De heer Wezeman toonde zich positief over de Audit Committees, echter, men moet erop bedacht zijn dat deze geen staat in een staat (mogen) vormen. De Raad van Commissarissen heeft de rechten En mandateert als het ware de audit committee.

De derde stelling luidde als volgt:

Is het zo sterk benadrukken van de onafhankelijkheid van de auditor misschien een afleidingsmanoeuvre, terwijl het werkelijke probleem mogelijk zit in de kwaliteit waarmee audits worden gedaan?

De heer Koster was zeer stellig met zijn reactie op deze stelling. Het benadrukken van de onafhankelijkheid draagt kenmerken van een afleidingsmanoeuvre, de kwaliteit van audits is sterk afgenomen. De accountants hebben zich een oor aan laten zetten met audit fees. Dit heeft geleid tot een uitholling vanwege de mogelijkheden tot het uitvoeren van extra werkzaamheden. Goede voorbeelden vindt men bij Arthur Andersen en Coopers & Lybrand.
De sterren uit de audit-praktijk worden weggelokt naar andere beroepen: 'Als men na vijf jaar nog in audit zit, dan doet men toch iets verkeerd'. De heer Mollema vulde aan, dat in plaats van de audit fees te verhogen, als alternatief ook de partner fees omlaag kunnen.
De heer Koster benadrukte het belang van onafhankelijkheid. De organisatie, welke gebruikmaakt van accountantsdiensten bij haar ontstaan en opbloei, raakt teveel verweven met de accountant. Na beursnotering verandert de taak van de accountant en het management sterk.
Er is veel meer exposure. De accountant moet dan worden gewisseld, om de verwevenheid teniet te doen.
De heer Gortemaker repliceerde: de financial audit heeft volgens hem zeker waarde. Immers, kijk naar de feiten en kijk naar de beurs. Hier wordt volgens hem nog een beeld geschapen van de traditionele financial audit. We moeten zien, dat er werkelijk iets veranderd is. Het toezicht en de accountant moeten elkaars rol versterken. 'Financial Audit, hij staat!'.
De kern van de audit is vertrouwen, gebaseerd op objectiviteit, integriteit en reputatie, en de perceptie rondom onafhankelijkheid en natuurlijk de onafhankelijkheid zelf. De onafhankelijkheid is van groot belang, maar er zijn

wel veel gouden koorden in de winkel van Sinkel! Er is synergie tussen advies en controle, maar de accountant moet hierbij wel een rechte rug tonen. De accountant moet gebruikmaken van het professionele scepticisme. Niet te dicht bij de klant staan, af en toe partnerruil, en een frisse blik. 'Kortom, onafhankelijkheid is de essentie, daarzonder geen vertrouwen! Het vertrouwen heeft wel een deuk opgelopen, maar hier moeten we aan werken.'
De reactie uit de zaal was licht ironisch: er zijn fees, dus er is een relatie, dus geen onafhankelijkheid. De heer Gortemaker stelde dat de onafhankelijkheid geoptimaliseerd dient te worden. De corporate governance-structuur is hierbij essentieel. Voor de accountant moet de rechte rug het vertrekpunt zijn. Van de accountant een overheidsdienst maken is dan ook onzin, safeguards kunnen leiden tot de juiste balans.
Uit de zaal kwam de vraag of de Raad van Commissarissen wel weet wat ze moeten doen. De heer Koster van de AFM antwoordde ontkennend: 'Dat weten ze niet'. De wet toezicht accountants moet fungeren als een steun in de rug van de accountant. De accountant bevindt zich altijd in een defensieve positie. Er is altijd een verwachtingskloof tussen de accountant en het publiek. De accountant wordt altijd in de hoek gezet. We moeten daarom accountants opleiden met een rechte rug.
Uit de zaal werd gesteld dat de concurrentie tussen kantoren dit ondergraaft. De heer Gortemaker reageerde door te stellen dat ook de grote kantoren leren, er is immers een tendens ingezet naar hogere fees en het inbouwen van meer safeguards. Er komt extra toezicht op het beroep, de AFM komt in de keuken kijken. De beloning wordt nu een trigger voor het toezicht. Concurrentie houdt mensen bovendien scherp. De AFM ondersteunt echter geen kartelvorming, immers de NMA ligt op de loer.

De vierde stelling die werd behandeld, luidde als volgt:

Is het onderscheid tussen operational, ICT en financial audit rationeel vanuit een management perspectief gezien?

De heer Gortemaker gaf direct aan dat het onderscheid zeker rationeel is. De doelen van deze audits zijn immers verschillend. De stakeholders zijn verschillend, het primaat voor de audit ligt bij de klant. De deskundigheden zijn anders en specialisatie is dus een vereiste. Er is wel convergentie en synergie, de geïntegreerde audit is natuurlijk wel nuttig en misschien ook mogelijk, maar er zijn duidelijk verschillen.
Een heldere reactie gaf de heer Bostoen: 'Het onderscheid is bullshit', althans vanuit het perspectief van het management. Een organisatie is natuurlijk een geheel van processen, en deze kunstmatig opsplitsen is niet wat het management wil. Het management wil uitspraken over het geheel van interne beheersing, c.q. interne control. De klant heeft liever one-stop-shopping. Men moet dus integreren, teams vormen. ICT, Business en Financial Audit maken een gemeenschappelijke planning en doen een gemeenschappelijke inspanning. De auditors moeten, zowel intern als extern, goed kunnen ageren tegen het management.
De financial auditor doet uiteindelijk toch wel 'zijn eigen ding'. Er moet een evolutie zijn naar overleg. Efficiëntie wordt vanuit het management geëist, dus 'one-face'. Vanuit de zaal de opmerking: 'Dus een RERARO-opleiding?'
De heer Gortemaker reageerde: 'Er is een common body of knowledge, laten we zeggen, 'rondom AO'.' Volgens de heer Bostoen is het echter lastig om mensen te laten samenwerken. We moeten toewerken naar een gemeenschappelijk platform.

Kunnen risk management en risk en control self assessment audit in belangrijke mate vervangen?

De heer Van Dijken en de heer Gortemaker hadden een gelijkende mening: beide zijn noodzakelijk. Wanneer er geen audit is, is er geen toets, en valt men in slaap. Beide pijlers moeten op de juiste wijze worden ingevuld, maar een kritische toets blijft noodzakelijk.
De heer Gortemaker vulde aan: 'Het moet helder zijn: De huishouding heeft natuurlijk meer kennis over de eigen business, maar audit blijft een noodzaak'. De heer Bostoen stelde, dat naarmate de kwaliteit van de AO/IC toeneemt de kwantiteit van de interne accountantsdienst kan afnemen. Ook de heer Gortemaker gaf aan, er is een verschuiving waar te nemen, de kwaliteit van audits neemt toe, de kwantiteit neemt af. De scope van de audits wordt verbreed. De heer Van Dijken merkte op: Bij Shell is niet alleen de auditor verantwoordelijk voor de audit, maar ook de business leaders, de IAD kan niet fungeren als rookgordijn.

Is de belangstelling van de accountant voor management control en ICT niet ver onder de maat?

De heer Van der Pijl stelde dat audit meer is dan financial audit, en dat er te weinig aandacht is voor de ICT-component. De heer Mollema vulde aan: 'We zijn inderdaad op een keerpunt, ICT verdient meer aandacht. Ook bij het NIVRA zien we dat er meer aandacht is voor de component ICT in de opleiding.' De heer Koster was het hier erg mee oneens, ICT krijgt genoeg aandacht. 'En daarmee is de kous af!'.
Krijgt management control niet te weinig aandacht?

De heer Bostoen merkt op: ‘MD&A (Management Discussions & Answers) is geen deel van de jaarrekening, het is mooi gepraat, externe auditors kunnen geen uitspraken doen over de kwaliteit van de business, van in mijn geval bijvoorbeeld, de banken’. Er zijn immers te veel risico’s, de MD&A is lastig controleerbaar.
Het management van een organisatie is primair verantwoordelijk, openheid van zaken geven is een natuurlijke taak. Transparantie staat centraal. De markt is in feite effectief toezichthouder, de rol van de accountant wordt kleiner. We zien nu dat kredietbeoordelaars vele malen machtiger worden. Kijk bijvoorbeeld naar ABB, de creditratings werden negatief, en het is verworden tot een klein zielig hoopje. De heer Mollema vulde aan: ‘Enige bescheidenheid past echter ook de kredietbeoordelaars.’

Heeft financial audit nog een toekomst (gezien de vele missers) en hoe zou die eruit moeten zien?

De heer Wezeman vindt van wel, mede daar de scope van de audits is verbreed. Er is echter nog steeds sprake van een verwachtingskloof, waarbij wel een onderscheid moet worden gemaakt naar beursgenoteerde en niet-beursgenoteerde ondernemingen. Het probleem is verder dat er legio exoneraties zijn. Wat is de financial audit wel, daar moeten we de nadruk op leggen. Men moet zich verzetten tegen exoneraties, een duidelijke scope hanteren, meer prospectief rapporteren, dieper graven en betere risicoanalyses plegen. De financial auditor moet echter wel uit zijn ivoren toren klauteren, alleen dan is er echt toekomst.
De heer Bostoen had een hele andere mening: ‘Weg met de Financial Audit’. Er zijn voldoende voorbeelden van blunders. Klanten kopen verklaringen en handtekeningen.
De heer Wezeman gaf aan dat prospectief rapporteren niet kan leiden tot het verkleinen van de verwachtingskloof, het kan echter wel zaken inzichtelijker maken. Dit dwingt mede tot perfectie, vanwege afstraffing door de markt.
De financial audit moet niet langer vraaggestuurd zijn, maar aanbodgestuurd.

Moet, gezien de bedrijfscomplexiteit, minstens de helft van het auditvak niet worden uitgevoerd door vakspecialisten met een randje auditopleiding?

De heer Wezeman gaf aan dat specialisatie altijd doorgaat.
De heer van der Pijl voegde toe dat de audit ‘sec’ wel moet overleven. Audit is het specialisme dat het auditingproces moet aansturen en beheersen. Men moet zich bewust zijn van de complexiteit, en daarom smart sourcing toepassen. Specialisatie heeft als positief effect, onderlinge kennisoverdracht en natuurlijk waardering.
Dit schept ook een maatschappelijk draagvlak.

IT-Toezicht Conferentie 2002

Evert Koning

Medio november 2002 heeft de IT-Toezicht sectie (T-Bit) van De Nederlandsche Bank NV (DNB) voor het eerst een internationale IT-Toezicht Conferentie voor bancaire toezichthouders georganiseerd. In Amsterdam waren aanwezig de IT-toezichthouders van e;f Bazelse toezichtorganisaties uit acht verschillende landen. Het betrof de Verenigde Staten (zowel de FED als de FDIC), Canada (OSFI), Engeland (FSA), Zweden (FI), Duitsland (zowel Bafin als Bundesbank), België (CBF), Italië (Banca d'Italia) en uiteraard Nederland. Helaas waren Frankrijk (Commission Bancaire) en Zwitserland (EBK) verhinderd.

Gedurende drie dagen zijn de deelnemers bijeen geweest om te discussiëren over de strategie, de organisatie en de aanpak van het IT-toezicht van elke organisatie. Zowel de overeenkomsten als de verschillen zijn nadrukkelijk aan bod geweest.
Enkele overeenkomsten zijn:

- toezichtwet met aanvullende verdere regelgeving, die op website beschikbaar is, vormt de basis van de werkzaamheden;
- adagium dat management van een bank primair verantwoordelijk is voor goed IT-risicobeheer;
- toepassing van een risicoanalysemodel met specifieke aandacht voor IT, soms als onderdeel van operationeel risico;
- een verbijzonderde afdeling of sectie die uitvoerend IT-toezicht verricht;
- werkzaamheden worden deels uitgevoerd op locatie in de vorm van het voeren van gesprekken en verrichten van onderzoeken;
- gebruik wordt gemaakt van werkzaamheden van de externe accountant.

De verschillen betreffen met name de mate waarin gebruik wordt gemaakt van de werkzaamheden van de externe accountant en de mate van detaillering van de verdere regelgeving. Ook zijn sommige organisaties al ver gevorderd met benchmarking, terwijl andere organisaties hierover nog nadenken.

Tevens is gesproken over het gehanteerde toezichtinstrumentarium en de samenwerking met lokale toezichthouders, zoals in Nederland bijvoorbeeld de AFM en de PVK. Nadrukkelijk is ook gesproken over de verbetering van de internationale samenwerking en het in het kader van de efficiency optimaal gebruikmaken van elkaars werkzaamheden. Doublures dienen zoveel mogelijk beperkt te worden, zonder dat er leemtes ontstaan. Hetzelfde geldt uiteraard ook op nationaal niveau.

Eén dag van het programma stond geheel in het teken van outsourcing. Aan bod is geweest een aantal richtlijnen zoals die zijn ontwikkeld in de VS en in Nederland (ROB hoofdstuk 2.6). Vervolgens is gesproken over de marktontwikkelingen, die erop duiden dat met name de uitbesteding van IT een toenemende tendens lijkt te vertonen. Voor toezichthouders is dan van belang dat de betreffende bank de verantwoordelijkheid blijft houden voor de uitbestede activiteiten, maar ook dat de toezichthouders in staat moeten zijn om te kunnen beoordelen of de IT-risico's nog in voldoende mate beheerst worden. SLA's dienen hierbij volop aandacht te krijgen. Indien de tendens zich voortzet bestaat een kans dat er Service Providers (SP's) ontstaan die voor meerdere grote banken belangrijke IT-activiteiten verrichten, waardoor die banken een bepaalde afhankelijkheid hebben van de SP's. Een mogelijk systeemrisico is een mogelijk gevolg van die ontwikkeling. De toezichthouders in de VS zijn reeds met deze problematiek geconfronteerd en oefenen een bepaalde vorm van (afgeleid) toezicht uit op enkele grote SP's.

De aanwezigen waren allen zeer tevreden over deze unieke conferentie en hebben zich voorgenomen om in 2003 een vervolg te geven in de vorm van een tweede conferentie, waarbij met name verder zal worden ingegaan op outsourcing, maar waar ook zal worden gesproken over de implicaties van Bazel-II, IT Governance, benchmarking, mobile banking, et cetera.

BOEKBESPREKING

Een goede technische boekhandel heeft altijd boeken over *technische informatiebeveiliging.* Bij Donner in Rotterdam zijn over dit onderwerp enkele meters boeken aanwezig. In deze recensie bespreek ik vier boeken die mijn blik hebben verbreed en die ik zelf bij mijn onderzoeken kon gebruiken. Op het moment dat ik dit artikel schrijf, zijn ze nog steeds te koop en ik kan iedereen aanbevelen om ze te lezen.

De risico's van 'social engineering'

Titel: The art of deception
Auteurs: Kevin D. Mitnick & William L. Simon
Uitgever: Wiley Publishing, Inc., Indianapolis, Indiana, 2002,
ISBN: 0-471-23712-4

Als je de keurige consultant op de achterkant van het boek ziet, zou je niet denken dat hij vijf jaar gevangen heeft gezeten voor het plegen van computerinbraken. Maar in hoofdstuk 1 geeft Kevin Mitnick zelf toe dat hij niet altijd braaf is geweest. Hij maakt nu echter een nieuwe start en wil bedrijven beschermen tegen mensen als hijzelf.

Zijn boek gaat over *social engineering*, waar Mitnick zelf een meester in was. De definitie die hij geeft is nogal moeilijk, maar in essentie betekent het: *mensen dingen laten doen die ze niet zouden moeten doen – door te liegen, te bedriegen en te manipuleren*. Het boek betoogt dat de menselijke factor de zwakste schakel in de informatiebeveiliging is, omdat mensen goedgelovig, ongeïnformeerd, goed van vertrouwen en behulpzaam zijn.

De eerste twaalf hoofdstukken laten zien hoe een fraudeur het vertrouwen van medewerkers kan winnen en vervolgens kan misbruiken. Het eerste en eenvoudigste voorbeeld – het opvragen van andermans kredietregistratie – werkt als volgt. Het is een Amerikaans voorbeeld en niet direct bruikbaar in Nederland:

De fraudeur belt een filiaal van de National Bank met de vraag: 'Ik maak een werkstuk en wil graag controleren of ik het jargon goed begrijp. Hoe noemen jullie de code die gebruikt wordt als jullie iemands kredietgegevens opvragen bij CreditCheck?'
Vervolgens belt de fraudeur een ander filiaal op en vraagt: 'Ik ben bezig met een klanttevredenheidsenquête voor CreditCheck. Hebt u een paar minuten voor mij?'
En een van de vragen op zijn lijst is: 'Welke klantcode gebruiken jullie als jullie gegevens bij ons aanvragen?'
Ten slotte belt de fraudeur CreditCheck met de vraag: 'Ik werk voor de National Bank en wil graag de kredietgegevens van een van onze klanten controleren. Onze klantcode is …'

Dit voorbeeld is te eenvoudig om direct te overtuigen. Maar in de rest van het boek worden de voorbeelden subtieler, gewaagder en gevaarlijker. Zo worden aanvallen met *social engineering* gecombineerd met elementair computermisbruik. Ook worden wachtwoorden gekraakt, toetsaanslagen van werkstations gekopieerd, netwerkgegevens afgeluisterd en telefoongesprekken omgeleid. In een praktijkvoorbeeld worden zelfs eenvoudige hangsloten geopend. Maar de methoden zijn nooit technisch hoogstaand, de kern van de aanval ligt altijd op de zwakke menselijke plekken. Mitnick beweert dat alle voorbeelden zijn verzonnen. Maar ze worden wel met veel plezier verteld en elk voorbeeld leest makkelijk weg, als een kort detectiveverhaal. Ik vermoed dat Mitnick vaak uit eigen ervaring schrijft.

Elk voorbeeld wordt afgesloten met een analyse waarin wordt aangegeven waar de zwakke plekken in het menselijk gedrag, de procedures of de systemen zitten. Vervolgens worden mogelijke tegenmaatregelen genoemd.

Deze analyses en tegenmaatregelen worden in hoofdstuk 15 *Awareness & training* en hoofdstuk 16 *Policies*

samengevat. Mitnick verwijst naar onderzoek waaruit blijkt dat mensen manipuleerbaar worden omdat ze:

- gehoorzamen aan verzoeken die hoger uit de hiërarchie komen;
- niet graag afwijken van het gedrag van hun omgeving;
- graag een dienst verlenen als ze een dienst terugverwachten;
- aardig doen tegen mensen die aardig lijken;
- zich graag houden aan eenmaal gegeven beloftes;
- graag profiteren van iets dat als een 'buitenkans' wordt gepresenteerd.

Als belangrijkste tegenmaatregel wordt *beveiligingbewustzijn* genoemd. Als medewerkers bewust zijn van het risico van manipulatie zijn ze minder eenvoudig om de tuin te leiden. Daarom wordt veel nadruk gelegd op opleiding. Vervolgens wordt een uitgewerkt beveiligingsbeleid gepresenteerd. De kern hiervan wordt gevormd door de classificatie van bedrijfsgegevens en door procedures voor identificatie en autorisatie van personen voor toegang tot deze gegevens. Dit wordt verder uitgewerkt in een gedetailleerd stelsel van maatregelen.

Het boek is inspirerend en geeft veel stof tot nadenken. Het leest makkelijk en is daarom ook geschikt voor in de trein of op het nachtkastje. Vele aandachtspunten en vragen kunnen makkelijk in een controleprogramma worden verwerkt. Maar er zijn ook enkele zwakke plekken. De voorbeelden zijn elk op zich goed bedacht en uitgewerkt, maar door de hoofdstukken heen wordt geen duidelijke lijn of structuur opgebouwd. De theoretische onderbouwing van het boek is dun: er wordt volstaan met de verwijzing naar één boek over de psychologie van manipulatie. Er wordt niet voortgebouwd op de uitgebreide literatuur over informatiebeveiliging, privacy en IT-auditing. Ten slotte ontbreekt elke vorm van statistiek, dus is het niet mogelijk om een idee te vormen van de ernst en omvang van de geschetste risico's. Desondanks een boek dat ik kan aanbevelen.

De hacker in zijn natuurlijke omgeving

Titel: Dagboek van een hacker, Bekentenissen van tienerhackers
Auteur: Dan Verton
Uitgever: E-Com Publishing, Haarlem, 2002
ISBN: 90-7690-326-3

Achter de banale titel gaat een heel aardig boekje schuil. In acht hoofdstukken geeft Dan Verton, een onderzoeksjournalist uit Washington, inzage in de werkwijze en motivatie van jonge hackers. Hij gebruikt informatie die de hackers hem zelf hebben gegeven, maar heeft ook gesproken met opsporingsfunctionarissen, psychologen en beveiligingsspecialisten.

In de acht hoofdstukken worden vele hackercarrières beschreven, waarvan de overeenkomst is dat ze allemaal zijn begonnen met een fascinatie voor techniek. Maar terwijl sommige carrières eindigen bij gerenommeerde beveiligingsbedrijven, eindigen andere in de gevangenis.

Hoofdstuk 3 beschrijft bijvoorbeeld de speurtocht naar Mafiaboy, de hacker die op zijn 15de Yahoo, Amazon en CNN van het internet blies. Op zijn 16de werd hij getraceerd en in 2001 tot acht maanden cel veroordeeld. Als contrast gaat hoofdstuk 8 over H.D. Moore, die op zijn 17de een presentatie mocht geven op een congres van SANS, op zijn 18de onderzoek deed voor de Amerikaanse marine en kort daarna beveiligingsonderzoeken bij banken mocht uitvoeren.

Het boek maakt duidelijk dat deze gewone jongens (en één meisje) toch respectabele tegenstanders kunnen zijn. Zij bezitten jeugdig enthousiasme en nieuwsgierigheid naar de technische details van systemen en infrastructuren. Zij kunnen alle benodigde informatie vinden op internet. Zij vormen groepen, clubs en bendes (soms fysiek, soms alleen via internet), waarin ze informatie uitwisselen en van elkaar leren. En – misschien wel het meest belangrijk – zij hebben nog geen verplichtingen en hebben alle tijd van de wereld om met de techniek te experimenteren.

De nadruk ligt op de belevingswereld van de jeugdige hacker, zijn persoonlijkheid en zijn levensstijl. De techniek van het hacken wordt alleen op hoofdlijnen beschreven en technische details worden niet behandeld. De beschreven hacks zijn vrij eenvoudig en overstij-

gen nauwelijks het elementaire script-kiddie niveau. Het gaat voornamelijk over ‘denial of service aanvallen’ (platgooien van systemen) en ‘web defacements’ (veranderen van andermans websites). Hierbij worden kant-en-klare scanners, password crackers, hack-tools en scripts gebruikt.

Er komen echter ook verschillende leuke voorbeelden van ‘social engineering’ in het boek voor. De leukste vindt plaats in een klaslokaal. Leerling A leidt de lerares af terwijl leerling B krijtsof uit een bordenwisser op haar toetsenbord strooit. Nadat zij haar wachtwoord heeft ingetoetst leidt leerling A haar opnieuw af, zodat leerling B kan zien welke toetsen zij heeft aangeslagen. Vervolgens kunnen zij allebei hun cijfers aanpassen.

Het boek bevat twee bijlagen. De eerste bijlage is een samenvatting van de hackgeschiedenis van 1981 (Kevin Mitnick) tot 2001 (Mafiaboy).
De andere bijlage bevat een lijst van interessante websites waarvan de meeste links het nog doen. Het boek leest makkelijk. De paar technische onnauwkeurigheden en enkele vertaalfouten storen mij niet. Het boek geeft een zeldzaam objectief en genuanceerd beeld van de hackercultuur en is daarom alleen al een aanrader.

Hoe doen ze het toch …

Titel: Web Hacking
Auteurs: Stuart McClure, Saumil Shah en Shreeraj Shah,
Uitgever: Addison-Wesley, 2003
ISBN: 0-201-76176-9

Als je niet dagelijks websites bouwt, dan is dit geen boek voor op het nachtkastje. Het is technisch en gedetailleerd. Maar het geeft zoveel nieuwe inzichten dat het loont om hier even voor te gaan zitten.

Het uitgangspunt is simpel: firewalls zijn tegenwoordig erg goed. Een systeem dat achter een firewall staat, is bijna onzichtbaar en onkwetsbaar. Waar kan een hacker dan wel mee aan de gang? Met die systemen die vanaf het internet bereikbaar móeten zijn: websites, e-commerce systemen en de bijbehorende databases.
Voor deze systemen móet namelijk een opening in de firewall worden gemaakt. Dit boek beschrijft wat allemaal via deze opening mogelijk is.

Een kort voorbeeld om dit te verduidelijken. In het begin van het internet waren websites ‘statisch’. In de browser (bijvoorbeeld Netscape) werd de vaste pagina opgevraagd via de URL – de regel die je boven in de browser intikt. Een karakteristieke statische URL ziet er als volgt uit:

http://www.website.nl/pagina.html

Jouw browser vraagt deze pagina bij de webserver op en de webserver stuurt hem naar je toe. Dit is simpel en risicoloos. Moderne websites zijn echter niet meer zo simpel. Het zijn complete bedrijfsapplicaties. Ze zijn actief. Tegenwoordig zien de meeste URL’s er als volgt uit:

http://www.website.nl/webapplicatie.cfm?invoer1=parameter1&invoer2=parameter2

Jouw browser stuurt dit verzoek naar de webserver en de webserver roept de ‘webapplicatie’ aan en geeft daarbij ‘parameter1’ en ‘parameter2’ mee. Hier gaat een hele wereld van potentieel misbruik open. Wat gebeurt er als de webapplicatie voor parameter1 een cijfer verwacht, maar ik geef 1000 cijfers mee? Wat gebeurt er als de webapplicatie letters verwacht, maar ik geef een rij van leestekens mee? Als de webapplicatie de input niet strikt controleert, kan een hacker hele onverwachte effecten veroorzaken. Meestal krijgt hij foutmeldingen te zien die niet voor zijn ogen bedoeld zijn. Soms kan hij via deze weg zelfs inbreken.

In zeventien hoofdstukken worden alle gangbare risico’s, aanvallen en verdedigingsmaatregelen van moderne websites beschreven. De nadruk ligt met name op e-commerce-toepassingen. Elk hoofdstuk beschrijft een bepaalde klasse van aanvallen, zoals:
- misbruik van Unicode om gevaarlijke programma’s op de webserver aan te roepen;
- misbruik van invoervelden om prijzen van artikelen te veranderen;
- misbruik van URL’s om SQL-com-

mando's op de achterliggende databases aan te roepen;
- kraken van wachtwoorden van de beveiligde gebieden van websites;
- stelen van iemand anders zijn authenticatiegegevens uit een cookie;
- gebruik van 'buffer overflows' om willekeurige programma's op de website te starten;
- misleiding van detectieapparatuur zodat aanvallen ongemerkt blijven.

Elke aanval wordt uitgebreid geanalyseerd en de bijbehorende beveiligingsmaatregelen worden besproken. Het zou (met enige moeite) mogelijk zijn om een normenkader op basis van het boek op te stellen.

Het boek legt een (enigszins fragmentarisch) theoretisch fundament door de architecturen van websites te bespreken en in te gaan op de eigenschappen van programmeertalen voor websites. Hoofdstuk 15 is heel praktisch en beschrijft de hulpmiddelen die een hacker van het internet kan downloaden en voor zijn aanvallen kan gebruiken. Maar de auditor kan dezelfde hulpmiddelen gebruiken voor zijn beveiligingsonderzoek.

Het boek is niet zomaar een leesboek, maar meer een doe-boek. Het grootste leereffect wordt bereikt door op het internet te gaan kijken hoe websites in elkaar zitten, door de hulpmiddelen te downloaden en door er – binnen legale kaders – mee te experimenteren. Dan krijgt de lezer inzicht in risico's die het IT-management soms nog onderschat.

Zelf voor detective spelen

Titel: Hacker's Challenge 2, Test your Network Security & Forensic Skills
Auteur: Mike Schiffman, Bill Pennington, Adam J.O'Donnel en David Pollino
Uitgever: Mc Graw Hill, Osborne, Berkeley, 2003
ISBN: 0-07-222630-7

In bijna alle organisaties worden audit logs bijgehouden. Hierin worden relevante gebeurtenissen op systemen en applicaties vastgelegd. Meestal wordt er nauwelijks naar omgekeken. Tot op het moment dat een incident plaatsvindt, want dan zijn goede logbestanden goud waard.

Het boek Hacker's Challenge 2 daagt de lezer uit om een duik te nemen in deze brij van loggegevens. In deel 1 van het boek (19 hoofdstukken en 200 pagina's) worden aanvallen op applicaties, systemen en infrastructuren beschreven. Bij elke aanval wordt een uitgebreide beschrijving van de infrastructuur gegeven. Vervolgens worden de symptomen van de aanval beschreven en ten slotte worden de relevante registraties in de logfiles gepresenteerd. Dan dagen de schrijvers de lezer uit om de pet van Sherlock Holmes op te zetten, uit te zoeken wat er is gebeurd en de slachtoffers te adviseren over corrigerende maatregelen.

In deel 2 staan de oplossingen opgesomd. Elke aanval wordt duidelijk geanalyseerd en er wordt aangegeven waar de eerste sporen van de aanvaller terug te vinden zijn. Vervolgens wordt aangegeven welke tegenmaatregelen mogelijk zijn – en tot mijn verbazing worden ook aanvallen beschreven waar (nog) geen kruid tegen gewassen is!

De hoofdstukken in deel 1 zijn vlot en met gevoel voor humor geschreven. Bij sommige hoofdstukken is direct duidelijk welk soort aanval gebruikt is. Er wordt aandacht gegeven aan aanvallen van buitenaf, maar ook aan aanvallen door interne medewerkers. Buffer-overflows, denial-of-service aanvallen, social engineering en zwakke wachtwoorden komen allemaal langs. Om de details uit te zoeken en tegenmaatregelen te verzinnen is echter een redelijke inspanning vereist. Verschillende voorbeelden gaan over draadloze netwerken en daar weet ik nog niet genoeg vanaf. Daar word je dan meteen met de neus op gedrukt.

De oplossingen in deel 2 zijn kort, zakelijk en duidelijk. Waar nodig wordt verwezen naar meer uitgebreide documentatie op het internet. De schrijvers presenteren de materie goed en op een originele manier. Zij hebben in het verleden meegewerkt aan bestsellers als Hacking Exposed en Hack Proofing your Network. Zij werken bij gerenommeerde organisaties als Foundstone en @stake. Een leuk boek, waar ik nog niet alle puzzels uit heb opgelost.