AUDIT magazine

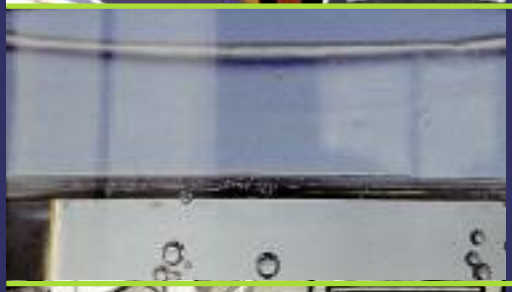
Magazine voor internal en operational auditors

nummer 3 september 2009

thema:

Bijzondere onderzoeken

De *Position Paper Update 2008* en bijzondere onderzoeken



Appreciative auditing: is uw glas halfvol of halfleeg?

Forensic IT-audit: het antwoord op cybercrime

Instituut van Internal Auditors Nederland

SVRO Stichting Verenigde Operational Auditors

CCH® TeamMate
Audit Management System

CCH is helping build intelligent businesses.

With added and more varied responsibilities, the role of the auditor is expanding. Thankfully, so are our world-class product offerings.

Already the industry leader in audit management systems, CCH® TeamMate now offers expanded assets for your business, including AuditNet's global resources.

Access to AuditNet standard and premium content is FREE and simple for TeamMate users, who can supplement their audit planning by searching across thousands of audit steps and programs in TeamMate-compatible format.

What business challenge can we help you address?

Visit **www.CCHTeamMate.com** for more information or contact one of the following regional representatives for the Benelux:

Cuno de Witte +31 20 568 6392 cuno.de.witte@nl.pwc.com

Wim Mandemakers +31 20 568 7374 wim.mandemakers@nl.pwc.com

Carolien Kapel +31 20 568 5124 carolien.kapel@nl.pwc.com

CCH
a Wolters Kluwer business

STRATEGIC BUSINESS PARTNER

AuditNet®
The Global Resource for Auditors


Ronald Jansen voorzitter


Ronald de Ruiter


Laszlo Nagy


Rick Mulders


Reinier Kamstra


Dennis Stabel


Jolanda Breedveld


Nicole Engel


Roy Jansen

Bijzondere onderzoeken

"Het is weer voorbij die mooie zomer" zong Gerard Cox al eens. Het was inderdaad een mooie zomer, mede ingeluid door het IIA Congres 'Auditors on the beach'. Uiteraard vindt u in dit nummer een terugblik op dit inspirerende IIA Jaarcongres.

De meesten van ons hebben de vakantiekiekjes alweer afgedrukt en veilig opgeborgen in de schoenendoos en zijn teruggekeerd naar de dynamiek waarin wij anno 2009 in leven. In dit nummer staan we stil bij de dynamiek en hectiek van de zoekende organisaties waarin wij werken, waarbij de vraag zich opdringt hoe je je auditdienst het best kunt managen in deze dynamische tijden.

Ingegeven door de huidige economische ontwikkelingen komen ook de budgetten van internal auditdiensten onder druk te staan. Binnen diverse organisaties krijgen CAE's te horen dat zij net als andere (staf)diensten moeten inkrimpen. Je zou denken dat dit betekent dat in overleg met de directie en het audit committee wordt bezien in hoeverre een aantal (reeds geplande) activiteiten kunnen worden geschrapt. Echter, met name in deze woelige periode is er vaak behoefte om juist meer audits uit te voeren. In de praktijk zal de auditdienst dan ook meer prestaties moeten kunnen leveren met minder (financiële) middelen. Maar hoe doe je dat dan? Arjan Man gaat in zijn artikel in op deze ontwikkeling en geeft ons aanknopingspunten om hier adequaat mee om te gaan.

Het thema van dit nummer is 'Bijzondere onderzoeken'. Bijzondere onderzoeken zijn onderzoeken met een niet-standaard karakter. Verschillende factoren kunnen een onderzoek een bijzonder karakter geven, zoals het object van onderzoek, de aanleiding voor het onderzoek, het doel van het onderzoek en de te hanteren onderzoeksmethode. De trend dat de dienstverlening van de internal auditfunctie steeds meer verschuift naar bijzondere onderzoeken, zoals gesteld in de *Position Paper Update 2008*, onderschrijft de relevantie van dit onderwerp. Peter Hartog en Elly Stroo Cloeck schenken uitgebreid aandacht aan de kansen en bedreigingen die vanuit de gedachte van de *Update 2008* liggen op het gebied van bijzondere onderzoeken. Ook het aantal reacties en de aard van de reacties op de door *Audit Magazine* op de website geplaatste stellingen geven aan dat het onderwerp leeft onder de lezers.

Verder wordt u meegenomen langs verschillende organisaties waar tal van onderzoeken worden uitgevoerd die voor velen van ons nog onbekend terrein zijn. U kunt onder meer lezen over appreciative auditing, forensic IT-auditing en Proactive Quality Assurance. Daarnaast nemen we een kijkje bij enkele bijzondere onderzoeksvarianten die meer of minder overeenkomsten vertonen met het vakgebied internal auditing. Zo kunt u lezen over de verschillende invalshoeken bij een wetenschappelijk onderzoek, over de onderzoeksmethoden die binnen de mesologie worden gebruikt en over het bijzondere van de onderzoeksaanpak bij de Koninklijke Marechaussee.

Naast de thema-artikelen vindt u in deze editie nog meer bijzondere en lezenswaardige artikelen en columns.

Wij wensen u veel leesplezier!

De redactie van *Audit Magazine*

- ☑ Streamline the audit process
- ☑ Improve audit visibility
- ☑ Increase audit efficiency & productivity
- ☑ Leverage assessments by other GRC groups
- ■ **SAVE TIME, CONDUCT BETTER AUDITS**

INTERNAL AUDIT SOFTWARE • THINK PAISLEY

Internal audit software from Paisley includes features for risk assessment, planning, scheduling, workpapers, reporting, issue tracking, time and expenses, quality assurance and personnel records. It is part of a comprehensive governance, risk and compliance solution that also includes functionality for financial controls management, compliance, risk management and IT governance.

Join over 1,300 leading organizations that utilize software from Paisley to increase efficiencies, reduce costs and improve the overall quality of financial, IT and operational audits.

PAISLEY | *Software for Governance, Risk & Compliance*

PAISLEY *ENTERPRISE GRC* AND **GRC** ON **DEMAND** — Software for integrated audit, operational risk management, financial controls management, IT governance, and compliance.
Call 888-288-0283 or visit www.paisley.com

THOMSON REUTERS™

inhoud

thema Bijzondere onderzoeken

De Position Paper Update 2008 en bijzondere onderzoeken

pag 6 Door ontwikkelingen in governance verandert het speelveld van de internal auditor. En dus verandert ook de dienstverlening van de internal auditfunctie. Peter Hartog (ACS) en Elly Stroo Cloeck (ESCIA) gaan in op de kansen en bedreigingen op het gebied van bijzondere onderzoeken.

De lezer over bijzondere audits

pag 9 In dit themanummer niet alleen de mening van deskundigen maar ook uw mening! De redactie van *Audit Magazine* plaatste drie stellingen op de IIA-website. Daarop ontvingen we maar liefst 94 reacties. De uitslag.

Is uw glas halfvol of halfleeg?

pag 10 Een nieuwe verfrissende kijk op auditing is appreciative auditing, aldus Anthoon Haagsma (UWV). Appreciative auditing kijkt naast de elementen die verbetering behoeven binnen een organisatie ook naar die elementen die al goed gaan en waar men trots op is. Ofwel, is het glas halfvol of half leeg?

Forensic IT-audit: het antwoord op cybercrime

pag 15 Bedrijven en organisaties zijn anno 2009 veel te laconiek als het gaat om het treffen van maatregelen ter voorkoming van cybercrime. Een interview met Matthijs van der Wel (Verizon Business) over gestolen data, beveiliging, hackers en de rol van de auditor.

Verder in dit thema

pag 19 **Proactive Quality Assurance (PQA)**
pag 24 **Van wetenschap via mesologie naar opsporing**
pag 31 **Scheme audit voor de OV-chipkaart**

De lokale overheid in beeld

pag 36 Arie Molenkamp en Ronald Jansen over het toezicht op het gemeentelijk handelen door de raad met in het bijzonder de functie die de lokale rekenkamer in dat toezicht kan vervullen.

Managen van IA in dynamische tijden: meer doen met minder

pag 40 Uit recente studies blijkt dat de budgetten van Internal Audit onder druk staan. De internal auditor moet meer doen met minder. Maar hoe? Arjan Man (PwC) gaat in op de ontwikkelingen en geeft aanknopingspunten.

IIA Congres: Auditors on the beach

pag 44 Een verslag van het inspirerende IIA Jaarcongres 2009 dat werd gehouden in het Circustheater in Scheveningen.

Auditors in het buitenland

pag 52 Johan Hundertmark is een globetrotter. Zijn werkzame leven begon hij in Nederland, maar al snel kwam hij in Saoedi-Arabië terecht om vervolgens neer te strijken in Australië. Hij vertelt over zijn ervaringen.

rubrieken

pag 28 **Personalia**
pag 29 **Column van de sponsor**
pag 35 **Column: een case voor Cees**
pag 47 **De estafettecolumn: Guus van Gameren**
pag 48 **Boekbespreking**
pag 49 **De overstap**
pag 50 **Boekalert**
pag 51 **Column: Hans Nieuwlands**
pag 53 **Verenigingsnieuws**
pag 56 **Nieuws van de universiteiten**
pag 58 **Column Bob van Kuijck**

COLOFON *Audit Magazine* wordt uitgebracht namens Het Instituut van Internal Auditors Nederland (IIA Nederland), tevens eigenaar van het magazine, en de Stichting Verenigde Operational Auditors (SVRO). De redactie nodigt lezers uit een bijdrage te leveren aan Audit Magazine. Bijdragen kunnen worden gemaild aan: Jansen.Ronald2@kpmg.nl **Redactieraad:** F. Steenwinkel (voorzitter), Th. Smit RA CIA, G.M. van Gameren RA RO **Redactie:** drs. R.H.J.W. Jansen RO (voorzitter), drs J.F. Breedveld, drs. N.J. Engel-de Groot, drs. R.J.A.C. Jansen RO, drs. R. Kamstra CIA, drs. H.A. Mulders RA RC, drs. L.Z. Nagy RO EMIA, drs. R. de Ruiter RE RA RO CISA, drs. D.L. Stabel RE CIA **Nieuws van de Opleidingen:** drs J.F. Breedveld en drs. R. Kamstra CIA **Verenigingsnieuws IIA Nederland:** drs. M. Docters van Leeuwen **IIA Nederland:** Postbus 5135, 1410 AC Naarden, tel.: 088-0037100, fax: 088-0037101, e-mail: iia@iia.nl, internet: www.iia.nl **SVRO:** Postbus 5135, 1410 AC Naarden, e-mail: iia@iia.nl, internet: www.iia.nl **Bureauredactie:** R. Harmelink, info@vm-uitgevers.nl **Uitgever:** drs. J.Y. Groenink, jeannette@vm-uitgevers.nl **Vormgeving:** M. Maarleveld **Druk:** Senefelder Misset, Doetinchem **Advertenties:** voor informatie over tarieven kunt u terecht bij Bureau IIA Nederland, tel.: 088-0037100, e-mail: iia@iia.nl. **Abonnementen:** IIA Nederland, Postbus 5135, 1410 AC Naarden, tel.: 088-0037100, fax: 088-0037101, e-mail: iia@iia.nl (zie ook de website: www.iia.nl). Abonnementen kosten € 85 per jaar, losse nummers € 25. Leden van IIA ontvangen Audit Magazine uit hoofde van hun lidmaatschap gratis. Abonnementen hebben telkens een looptijd van een jaar en gelden tot wederopzegging tenzij anders overeengekomen. Partijen kunnen ieder schriftelijk opzeggen tegen het einde van de abonnementsperiode, met inachtneming van een opzegtermijn van twee maanden. Audit Magazine verschijnt vier maal per jaar.

ISSN: 1570-856X
VM UITGEVERS

De *Position Paper Update 2008* en bijzondere onderzoeken

De *Position Paper Update 2008* stelt dat door ontwikkelingen in governance het speelveld van de internal auditor verandert. In samenhang daarmee verandert ook de dienstverlening van de internal auditfunctie (IAF): minder standaardisatie en meer bijzondere onderzoeken. In dit artikel wordt nader ingegaan op de kansen en bedreigingen (of beperkingen) die er, vanuit de gedachte van de *Update 2008*, liggen op het gebied van bijzondere onderzoeken.

Drs. P. Hartog CIA
E. Stroo Cloeck RE RA CIA CISA

In 2005 publiceerden de beroepsgroepen NIVRA, IIA en NOREA de position paper *De Internal Auditor in Nederland*, waarin hun visie op de IAF voor in Nederland gevestigde organisaties uiteengezet werd. In de jaren na publicatie ontstond een toenemende vraag vanuit die organisaties om hulp en assurance op het gebied van governance. Ook de wijze waarop die dienstverlening werd ingevuld veranderde: proactiever, risk based, met meer aandacht voor de strategische en tactische processen. Dus werd het tijd voor een update van de position paper: *De Internal Auditor in Nederland – Position Paper Update 2008* verscheen in juni 2008. In de *Update 2008* wordt een aantal nieuwe werkzaamheden geschetst. Deze omvatten zowel de pure auditrol als consultancy-werkzaamheden. Voor de assurance- of auditrol zijn, zonder dat volledigheid is nagestreefd, de volgende nieuwe werkterreinen benoemd:

- project- en programmamanagement;
- integriteit en compliance;
- het proces van risicomanagement;
- sociaalorganisatorische controls als de cultuur, de stijl van leiding geven en de 'tone at the top';
- duurzaam ondernemen, het beoordelen van de betrouwbaarheid van informatie op het gebied van duurzaam ondernemen.

Welke kansen bieden deze nieuwe (nog) bijzondere onderzoeken de IAF en op welke wijze kunnen deze worden gerealiseerd?

Kansen

De *Update 2008* signaleert niet alleen een verschuiving in werkterrein van de IAF. Het roept ook de meer traditionele IAF's op om, uitgaande van zowel de strategische, tactische als operationele risico's van de organisatie, het werkterrein te verbreden.
Verbreding in de vorm van bijzondere onderzoeken die aansluiten bij de belangrijke zorgen van het (top)management, geeft de IAF de kans haar toegevoegde waarde te vergroten.
Zowel de traditionele onderzoeken als de bijzondere onderzoeken zijn daarbij het best gebaat met een doorontwikkelde houding en aanpak van de IAF. Naast de traditionele focus op de onafhankelijke, objectieve opstelling, zijn van belang:

- het proactief leveren van een bijdrage aan governance;
- risico-georiënteerd, dus met focus op die dingen die er echt toe doen;
- het tijdig onderkennen van risico's en zorgen dat deze een 'eigenaar' krijgen;
- gevraagd en ongevraagd adviseren over normenkaders en beheersmaatregelen.

Overigens biedt dit niet alleen een toegevoegde waarde aan de klanten van de IAF, maar ook aan haar medewerkers. Een gevarieerd werkveld houdt het werk interessant. Interessant werk houdt de auditors vast in hun beroep, algemeen en bij hun organisatie in het bijzonder, maar trekt ook nieuwe auditors met andere achtergronden aan (zoals juristen en organisatiepsychologen of -sociologen en mensen met managementervaring). Daardoor kan er nog meer toegevoegde waarde worden geleverd. En zo is de cirkel weer rond.
Bijzondere onderzoeken hebben nog een indirect voordeel. Zij

geven de internal auditor nog meer inzicht in het opereren van de organisatie, in de cultuur, de mensen en leiderschapsstijlen. Dit heeft vervolgens ook weer een positieve weerslag op de kwaliteit van auditaanpakken (passend bij de cultuur) en op de aanbevelingen (nog beter toegesneden op de stakeholders) van de meer traditionele audits.

Bedreigingen en beperkingen

Er zijn veel kansen en er is veel op te pakken, maar waar liggen de beperkingen, ofwel de grenzen? In de *Update 2008* is aangegeven dat de grondbeginselen niet zijn veranderd. Daarin liggen eigenlijk ook de grenzen besloten.

De kerntaken van de IAF zijn duidelijk. Mogelijke adviestaken liggen al wat moeilijker, men dient niet 'op de stoel van management te gaan zitten'. Bestuurlijke en lijnmanagementtaken overnemen, zoals het nemen van beslissingen over de doelen van de organisatie, de risk appetite en het stellen van prioriteiten, gaat te ver. Juist bij bijzondere onderzoeken kan het vanwege het eenmalige en/of complexe karakter moeilijk zijn de verschillende rollen te onderkennen en de juiste houding aan te nemen en het takenpakket vorm te geven.

Qua reikwijdte bakent de definitie van internal auditing het werkgebied af: 'Internal Auditing is an independent and objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.'

Daarbij gelden de beginselen vanuit de Code of Ethics voor de wijze van uitvoering. Minimale eisen zijn:

- ***Onafhankelijk en objectief; dit blijven de pijlers voor de toegevoegde waarde van de IAF***
  - Als de consequentie van bijzondere onderzoeken is dat de eigen werkzaamheden later beoordeeld moeten worden, kan de onafhankelijkheid voor toekomstige audits in het gedrang komen. De keerzijde is dat het continu erop wijzen dat 'een ander verantwoordelijk is' doorgaans weinig begrip creëert. Het kan dus zijn dat de onderzoeken niet zuiver beperkt blijven tot een auditrol. Als die keuze bewust wordt gemaakt en besproken met het management en de resultaten vervolgens niet binnen een jaar worden beoordeeld door dezelfde auditor, wordt voldaan aan de IIA-standaarden.
  - Objectiviteit vereist 'harde', duidelijk gespecificeerde normen. Dat betekent dat vaker gebruik moet worden gemaakt van kennis van andere vakgebieden om ook de meer 'zachte' aspecten (objectief) meetbaar te maken. Om misverstanden te voorkomen is bespreking van het normenkader met de opdrachtgever van groot belang. Dit vormen uitdagingen bij nieuwe complexe opdrachten, die natuurlijk vaak ook onder hoge tijdsdruk uitgevoerd moeten worden.

Illustratie: Roel Ottow

- ***Voldoende kennis***
  - Zowel per audit als meer in het algemeen, moet expliciet bekeken worden of voldoende kennis aanwezig is binnen de IAF. Zo niet, dan dient deze te worden aangetrokken van elders in de organisatie of extern. Inzet daarvan kan per audit, maar als de bijzondere onderzoeken een meer continu karakter krijgen, kan die kennis ook binnen de IAF worden opgenomen (via training of via het aantrekken van die nieuwe competenties).
  - Een risico is het overschatten van de eigen kennis waardoor, achteraf, schijnzekerheid is ontstaan. De

Peter Hartog werkt als senior auditing consultant bij ACS. Elly Stroo Cloeck is zelfstandig gevestigd onder de naam ESCIA. Beiden waren in 2008 betrokken bij de totstandkoming van *De Internal Auditor in Nederland – Position Paper Update 2008.*

IAF presenteert zich als expert, anderen zijn daardoor wellicht te weinig kritisch.

Overwegingen

Het doen van bijzondere onderzoeken kan invloed hebben op het imago. Dat kan positief maar ook negatief zijn. Sommige bijzondere onderzoeken zijn bijvoorbeeld gericht op het onderzoeken van oorzaken van niet-werkende controles of op fraudes. Bij een te grote focus op dit soort onderzoeken kan de IAF als politieagent te boek komen te staan, wat de 'normale' opdrachten negatief kan beïnvloeden.

Door de focus op governance kan het voorkomen dat de auditor belangrijke projecten vertraagt, of, in de ogen van het direct verantwoordelijke management, onnodig op de rem trapt. Belangrijke adviezen op het gebied van beheersing worden dan niet gezien als toegevoegde waarde. Het vinden van de juiste balans kan een hele uitdaging zijn. Open communicatie met het opdrachtgevend en objectverantwoordelijk management is essentieel.

Het 'bijzondere' van de bijzondere onderzoeken hoeft niet alleen de inhoud of het object van onderzoek te betreffen. Het kan ook zijn dat de audit op een andere wijze wordt geïnitieerd en een andere dan normale opdrachtgever kent. Dat kan bijvoorbeeld het geval zijn als, naast de reguliere auditplanning zoals vastgesteld door raad van bestuur en/of het audit committee (AC), audits op verzoek van het lagere management worden gedaan. Voor die onderzoeken is de vraag of de normale rapportagestructuur richting RvB en/of AC moet worden gehandhaafd. Dat zou immers juist het management ervan kunnen weerhouden de IAF in te schakelen voor een bijzonder onderzoek. Zeker als het het doel van de IAF is om frequent dergelijke onderzoeken uit te voeren, is het belangrijk om zorgvuldig te overwegen of voor die audits vast moet worden gehouden aan de vaste rapportagelijnen richting opdrachtgever van de auditfunctie (RvB en/of AC). Een alternatief is om richting hen te volstaan met een rapportage over wat er is gedaan en de inhoudelijke rapportage (tenzij er overtredingen van wet- en regelgeving worden geconstateerd) wordt overgelaten aan het verantwoordelijke management zelf.

Het doen van bijzondere onderzoeken kan invloed hebben op het imago

Conclusie

Bijzondere onderzoeken passen binnen de gedachte van de *Update 2008*. Toevallig (of juist niet?) kwam dit onderwerp ook ter sprake tijdens het IIA-congres 'Auditors on the beach'. Een van de genomineerden voor de Arie Molenkamp Award had een thesis geschreven over Business – IT alignment, en er ontspon zich een discussie of de IAF wel een onderzoek naar de effectiviteit van de IT-organisatie kon doen. "Trek niet een te grote broek aan", zei de ene CAE. "Het past binnen onze natuurlijke adviesfunctie", zei de andere. De conclusie was: ja doen, maar alleen in een rol die 'goed voelt'.

Door te zorgen dat we als IAF bij strategische en tactische issues betrokken worden, wordt onze toegevoegde waarde vergroot. Geef daarbij vooraf duidelijk de rollen en verantwoordelijkheden weer, steek je nek uit, maar niet te ver. Kortom, houd de IIA-standaarden in de gaten maar ga innovatie niet uit de weg. Pak de uitdaging op!

De lezer over bijzondere audits

In dit themanummer niet alleen de mening van deskundigen, maar ook uw mening! De redactie van *Audit Magazine* plaatste drie stellingen op de website van het IIA waarop we maar liefst 94 reacties ontvingen. Een samenvatting.

Stelling 1
Als internal auditor voer ik ten minste eenmaal per jaar een bijzondere audit uit of ben ik hierbij betrokken

		In %
1.	Helemaal mee eens	45
2.	Mee eens	38
3.	Neutraal	9
4.	Mee oneens	6
5.	Helemaal mee oneens	2

Stelling 2
Bijzondere audits vragen een andere auditattitude dan reguliere of traditionele audits

		In %
1.	Helemaal mee eens	25
2.	Mee eens	37
3.	Neutraal	14
4.	Mee oneens	18
5.	Helemaal mee oneens	6

Stelling 3
In de auditopleidingen en het cursusaanbod die mij ter beschikking staan wordt voldoende aandacht besteed aan bijzondere audits

		In %
1.	Helemaal mee eens	6
2.	Mee eens	34
3.	Neutraal	29
4.	Mee oneens	27
5.	Helemaal mee oneens	4

Verschillende aspecten
Het merendeel van onze lezers (83 procent) is jaarlijks een of meerdere malen betrokken bij de uitvoering van bijzondere audits. Zoals ook uit de reacties is op te maken, bestaat een bijzondere audit uit verschillende aspecten. Belangrijk zijn de bijzonderheid van het te beschouwen onderzoeksobject, het kiezen van een bijzondere onderzoeksaanpak en eventueel bijzondere vaardigheden en kennis die vereist zijn of ingezet kunnen worden om een (bijzondere) audit uit te voeren.

Buiten de gebaande paden
Ten aanzien van de vaardigheden is slechts 24 procent van de respondenten van mening dat een bijzondere audit geen andere auditattitude vereist dan die voor reguliere of traditionele audits. Een enkeling merkt daarbij op dat alle audits een kritische blik en een redelijk vast samenstel van auditmethodieken vereisen. De meerderheid daarentegen meent dat bijzondere audits wel degelijk een andere auditattitude vereisen. Er dient vaker buiten de gebaande paden getreden te worden, waarbij interpersoonlijke kwaliteiten, inlevingsvermogen en creativiteit belangrijke eigenschappen zijn. In de diverse bijdragen in deze uitgave van *Audit Magazine* wordt dit beeld bevestigd.
Een minderheid (40 procent) vindt dat in de aangeboden auditopleidingen en het cursusaanbod voldoende aandacht wordt besteed aan bijzondere audits. Gelet op de vele auditors die jaarlijks betrokken zijn bij bijzondere audits én de veronderstelde wezenlijke verschillen met reguliere audits, roept dit de vraag op in hoeverre de auditor voldoende gekwalificeerd of geschikt is om bijzondere audits uit te voeren. Of ten minste de vraag: op welke wijze wordt de auditor klaargestoomd om bijzondere audits uit te kunnen voeren? Uit de reacties blijkt ook dat vaak samenwerking met experts uit andere disciplines wordt gezocht.

De redactie van *Audit Magazine* heeft een boekenpakket verloot onder de respondenten. De gelukkige winnaar is dit keer Bianca Steentjes, werkzaam bij Ernst & Young. Het volgende nummer staat in het teken van soft contols. Houd de website van het IIA in de gaten en geef uw mening!

Appreciative auditing? A smarter way in auditing

Is uw glas halfvol of halfleeg?

U ziet een half gevuld drinkglas voor u. Iemand vraagt aan u of er nog wat in het glas zit. Wat antwoordt u? Is het glas halfvol of halfleeg? Waar hangt uw antwoord vanaf? Van uw humeur? Van uw persoonlijkheid? Van het feit dat u naar huis wilt? U kunt vanuit verschillende perspectieven naar het glas kijken. Zo kunnen we ook naar organisaties, afdelingen en processen kijken. Zien we alleen de negatieve kant of hebben we ook oog voor de zaken die goed gaan?

A. Haagsma RO EMIA

Binnen de auditfunctie kijken we veelal vanuit een negatieve invalshoek (welke risico's zijn er, wat is het probleem en hoe kunnen we dat oplossen?) naar de te auditen onderwerpen. Auditors worden getraind in het opsporen van de zwakheden en onzekerheden. Met die negatieve benadering moeten organisaties gestimuleerd worden om te gaan verbeteren (verbeteren = veranderen). Dit strookt echter niet met de bestaande theorieën binnen de veranderingsleer. Deze gaan veelal uit van vertrouwen en het benadrukken van de positieve elementen binnen organisaties om een verbetering te initiëren. Willen we als auditors onze toegevoegde waarde kunnen blijven leveren dan vraagt dit om een andere kijk op auditing. Vanuit de theorie en praktijk rondom de internal auditfunctie is duidelijk dat de auditor ook een adviserende rol heeft. Een aanbeveling tot verbeteren kan worden gezien als een advies om te veranderen. De term advies (consultancy) wordt ook expliciet genoemd binnen de definitie van auditing. Wel staat deze rol onder druk in verband met alle ontwikkelingen rondom de kredietcrisis. Er is van alles misgegaan binnen de governance van een aantal financiële instellingen. De neiging is nu om dit 'dicht te timmeren' met meer regelgeving en meer toezicht. Toch is dat de oplossing niet. Er zal meer naar de diepere oorzaken gekeken moeten worden. Dan kom je op begrippen als vertrouwen, integriteit en dus soft controls. Dat heeft op dit moment nog niet die aandacht die het verdient. Een nieuwe verfrissende kijk op organisaties is dus geboden. Kijken vanuit een andere invalshoek. Als auditing die spiegelende, objectiverende, strategiegerichte, proactieve en onafhankelijke rol binnen organisaties wil blijven vervullen, moet deze ook veranderen. Appreciative auditing is die verfrissende verandering binnen de internal auditfunctie. Appreciative auditing combineert de elementen van appreciative inquiry (AI) en operational auditing.

Een nieuwe verfrissende kijk op auditing is appreciative auditing. Appreciative auditing is een combinatie van de effectieve elementen van appreciative inquiry en operational auditing en kijkt naast de elementen die verbetering behoeven binnen een organisatie ook naar die elementen die al goed gaan en waar men trots op is. Dit maakt auditing effectiever en vergroot de toegevoegde waarde voor de internal auditunctie in zijn geheel.

Appreciative Inquiry

In het Nederlands wordt vaak 'waarderend exploreren' of 'onderzoeken' als betekenis aan AI gegeven. AI is een andere manier van denken voor het oplossen van problemen en veranderen van organisaties. Deze 'nieuwe' manier van verandermanagement wint snel terrein binnen het veld van verandermanagement. Op internet zijn vele succesvolle toepassingen te vinden. Wil je verbeteren (verbeteren = veranderen) met meer bezieling en energie dan is het bekrachtigen van het positieve volgens AI een effectieve manier. David Cooperrider (Cooperrider D.L., 2000) geeft de relatie aan tussen positieve beelden en positieve actie en de implicaties daarvan voor het management. In het artikel *A positive revolution in change* (Cooperrider & Whitney, 2003) worden de vijf uitgangs-

punten van AI benoemd. Deze kunnen worden gezien als de basis van de gehele methodiek (zie *kader*).

De basisprincipes van AI

Sociaal constructivisme
Het vermogen van medewerkers en de organisatie om de toekomst vorm te geven. De kracht van sociaal constructivisme en het geloof in de maakbaarheid van de organisatie.

Gelijktijdigheid
Onderzoeken en veranderen zijn geen twee verschillende dingen. Het stellen van vragen en de verandering lopen simultaan. Op het moment dat een vraag gesteld wordt is ook de eerste stap op weg naar de beoogde verandering gezet. Men denkt na en is niet meer dezelfde. Vragen zijn een krachtig middel om mensen te veranderen.

Cocreatie (poëtisch)
Organisaties kunnen gezien worden als een open boek waarvan alle medewerkers coauteur zijn. Het verhaal wordt continu gevormd door zowel de medewerkers als de actoren uit de omgeving die met de organisatie te maken hebben. Dit kan leiden tot een cultuur waarin leren, interpreteren en herinterpreteren belangrijk zijn.

Anticipatie op de toekomst
De belangrijkste hulpmiddelen voor een constructieve organisatieverandering zijn de collectieve verbeeldingskracht en de dialoog over de toekomst.

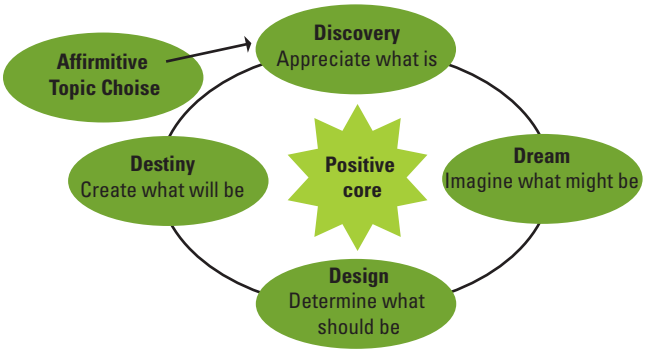
Positivisme
Om een verandering in gang te zetten zijn positieve beïnvloeding en sociale binding nodig. Belangrijk daarbij zijn hoop, inspiratie, plezier en de energie van het met elkaar creëren.

(Bron: Cooperrider & Whitney, 2003)

Sue Annis Hammond beschrijft in haar boek *The thin book of appreciative Inquiry* (Hammond, 1998, pag. 20) de acht aannamen die binnen AI gelden. Deze zijn ook weer afgeleid van de basisprincipes uit het kader.

1. In elke maatschappij, organisatie of groep werkt iets.
2. Waar we ons op focussen wordt realiteit.
3. Realiteit wordt gemaakt op dat moment en er zijn verschillende waarheden.
4. Het stellen van vragen aan een organisatie of groep beïnvloedt de groep.
5. Mensen hebben meer vertrouwen in de reis naar de toekomst (onzekerheid) wanneer men gedeelten uit het verleden mee kan nemen (zekerheid).
6. Als we gedeelten uit het verleden meenemen moet het in ieder geval het mooiste zijn uit het verleden.
7. Het is belangrijk om verschillen te waarderen.
8. De taal die we spreken maakt onze realiteit.

Deze wat filosofische aannamen geven toch goed weer op welke manier AI tegen mensen, organisaties en groepen aankijkt. De acht basisprincipes en de aannamen van Sue Hammond staan weer aan de basis van de praktische uitvoering van AI.
Door middel van het toepassen van de 'Four-D cycle' (ofwel de vijf D's met Definition in plaats van affirmative topic choice als startpunt) geven Whitney en Trosten-Bloom (Whitney & Trosten-Bloom, 2003) een praktische invulling aan AI door stap voor stap op zoek te gaan naar de energie binnen organisaties en deze te vertalen naar de toekomst. Dit is het basismodel dat in alle literatuur genoemd wordt (zie *figuur 1)*.



Figuur 1. De Four-D cycle (Bron: Whitney & Trosten-Bloom, 2003)

AI gaat op een systematische manier (door middel van vijf stappen) op zoek naar het beste in mensen en naar datgene wat mensen 'energie' geeft. Op basis van positieve ervaringen wordt gekeken hoe in de toekomst de organisatie kan verbeteren (zie *kader*).

De praktijkinvulling van de vijf D's

1. Definition (affirmative topic choice) – Bepaal onderwerp
Bepaal gezamenlijk wat het te veranderen onderwerp is. In de praktijk gebeurt dit veelal door een vertegenwoordiging van de organisatie. Het onderwerp moet gedragen worden en positief zijn geformuleerd.

2. Discovery – Waardeer wat er is
Door middel van interviews in tweetallen onderzoeken waar de successen in het verleden zijn ervaren. Dit zet mensen aan tot nadenken. Na het interview in een grotere groep de rode draad uit de interviews halen.

3. Dream – Verbeeld wat het mogelijk kan zijn
De betrokkenen formuleren hun droombeeld, toekomstplaatje, ideaalbeeld. Hiervoor wordt op een constructieve manier gebruikgemaakt van de ervaringenen verworven inzichten uit de discoveryfase. Het resultaat van deze dreamfase is een uitdagende visie waarin de toekomst wordt verwoord.

4. Design – Bepaal wat het zou moeten worden
Werk uit hoe de uitdagende visie vanuit de dreamfase gerealiseerd kan worden. Dit wordt weergegeven in een plan van aanpak.

5. Destiny – Creëer wat het gaat worden
Hier wordt het 'hoe' weergegeven. De kracht van AI is dat door dialoog de visie wordt vertaald naar een aanpak.

Volgens professor Kees Ahaus, bijzonder hoogleraar kwaliteitsmanagement aan de faculteit aan de Rijksuniversiteit Groningen (Ahaus, 2006), is er bij AI sprake van een nieuw paradigma. Het nieuwe is dat op een positieve, opbouwende manier wordt gekeken naar mensen, organisaties en situaties. Dat is een duidelijk verschil met het problem solvingparadigma waarin het formuleren van het probleem (verbeterpunt) altijd het vertrekpunt is. Problem solving

is altijd een dominante manier van leren geweest en zal dat ook blijven. Maar volgens Ahaus wordt het nu eens tijd voor een frisse kijk en een verandering van paradigma. Zie het *kader* voor een beschrijving van beide paradigma's.

Problem solving versus Appreciate Inquiry

Problem solving
1. Identificeer het probleem
2. Analyseer de oorzaken
3. Plan acties om het probleem te behandelen

De organisatie is metaforisch een probleem dat moet worden opgelost

Appreciative Inquiry
1. Waardeer het beste van 'wat is' (wat hebben we?)
2. Verbeeld 'wat zou kunnen zijn'
3. Voer een dialoog over 'hoe het eruit zal zien'

De organisatie is metaforisch een mysterie dat moet worden omarmd

(Bron: Whitney, 1999)

In de breedste zin van het woord betreft AI een systematische ontdekking van datgene wat 'energie' geeft om te veranderen en te verbeteren. AI gaat op zoek naar de positieve ervaringen van mensen. Op basis van deze ervaringen wordt gekeken hoe de organisatie in de toekomst kan verbeteren. AI gaat ook op zoek naar de positieve energie binnen de mens en hun organisatie.
De conclusie is dat AI vanuit de vijf basisprincipes een praktische methodiek (Four-D cycle) heeft ontwikkeld waar een aantal aannamen voor gelden. Dit alles geeft vorm aan AI en is gericht op het verbeteren van de organisatie en haar mensen.

Auditing en Appreciative Inquiry
Wil je auditing kunnen beschrijven dan is de definitie van het IIA Inc. de basis. Deze definitie luidt als volgt: 'Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.'

Centraal in deze definitie staan drie woorden: independent, objective assurance en consulting activity. Binnen de huidige IAF kunnen we twee benaderingen herleiden. Namelijk de assurance- (aanvullende zekerheid) en consultingbenadering (advies). Audits kunnen elementen van beide bevatten. Door aanbevelingen te formuleren ter verbetering wordt volgens Sawyer al invulling gegeven aan de adviesrol. Dit is nog een keer herbevestigd in de *Position Paper Update 2008* van IIA Nederland.
Ook speelt The International Professional Practices Framework (IPPF) een belangrijke rol als kader waarbinnen een auditor moet opereren. Deze bevestigt dat assurance en consulting geen strikt gescheiden gebieden zijn: 'Internal audit consulting enriches value-adding internal auditing. While consulting is often the direct result of assurance services, it should also be recognized that assurance could also be generated from consulting engagements.'
Uit deze bronnen is te herleiden dat auditing *onafhankelijk* aanvullende *zekerheid* geeft en *adviseert* over het verbeteren van de bedrijfsvoering. Aangezien de internal auditfunctie en AI beide gericht zijn op het verbeteren van de bedrijfsvoering van organisaties zal een combinatie van deze twee een welkome aanvulling binnen de internal auditfunctie zijn.

Appreciative auditing
De combinatie tussen AI en audit heb ik appreciative auditing genoemd. Dit is een combinatie van de effectieve elementen van appreciative inquiry en het huidige internal auditing.

Appreciative auditing is het uitvoeren van een audit met behulp van de kenmerken van AI. De kenmerken zijn:
- kijken naar de successen;
- kijken naar de kansen;
- interviews, afstemming en overige gesprekken in de vorm van een dialoog;
- het stellen van positief geformuleerde vragen tijdens interviews;
- het creëren van een positieve sfeer tijdens de gehele audit.

Als ik de term appreciative auditing vertaal komt als vertaling 'waarderend auditen' het meest in de buurt. De term appreciative auditing is een nog niet bestaande term en wordt in mijn referaat voor het eerst genoemd. Dit geeft al aan dat we vernieuwend bezig zijn.
Wat duidelijk moet zijn is dat het niet de bedoeling is om alleen de zaken te benoemen die goed gaan en de onderwerpen die verbetering behoeven niet te benoemen. Appreciative auditing zorgt ervoor dat naast de zaken die verbetering behoeven ook de zaken benoemd worden die wel goed gaan en waar men trots op is.
Willen we de term auditing kunnen blijven hanteren dan zullen we onafhankelijk assurance en advies moeten leveren ter verbetering van de bedrijfsvoering.
De essentie is dat appreciative auditing een verdieping van de IAF is. Het komt er niet voor in de plaats maar het is een hulpmiddel om de effectiviteit van de IAF te vergroten. Het is een methodiek waar de effectieve elementen van AI ingebouwd zijn.

Door appreciative auditing toe te passen wordt de effectiviteit van de IAF verhoogd. Elementen van AI worden binnen de diverse fasen van een audit ingebouwd. Over het algemeen kunnen we stellen dat een audit bestaat uit planning, vooronderzoek, veldwerk en een rapportage. Voor elk van deze fasen wordt de effectiviteit verhoogd door de elementen van AI.
In *tabel 1* is weergegeven hoe appreciative auditing is vormgegeven. Binnen alle stappen van het auditproces kunnen elementen van AI ingebouwd worden waardoor de effectiviteit wordt verhoogd. Hierbij wordt de link gelegd tussen de fasen van auditing en de vijf D's van AI. Appreciative auditing is gericht op de positieve elementen binnen de organisatie en hierbij staat de mens meer centraal.

Appreciative auditing kan ook zeer goed toegepast worden door middel van een control risk self assessment (CRSA). Tijdens zo'n

Stap binnen audit	Contactmomenten (beïnvloedingsmomenten)	D-fase van AI	Basisprincipe AI	Appreciative auditing	Effect
Planning	• Afstemmen onderwerpen auditjaarplan • Ondersteunen bij bepalen risico's organisatie (input jaarplan)	• Definition • Discovery	• Sociaal constructivisme • Gelijktijdigheid • Cocreatie	• Dialoog over onderwerpen auditplan • Onderzoeken wat goed gaat • Successen • Zoeken naar kansen i.p.v. risico's	• Meer betrokkenheid om mee te denken • Door successen een positief beeld
Vooronderzoek	• Interviews • Verzoeken om informatie • Referentiemodel afstemmen	• Definition • Discovery • Dream	• Anticipatie op de toekomst • Cocreatie • Positivisme	• Stellen van positieve vragen • Op zoek naar succesmomenten • Dialoog • Meebouwen aan het referentiemodel	• Grotere betrokkenheid • Positief gevoel
Veldwerk	• Interviews • Bespreken en afstemmen bevindingen	• Discovery • Dream • Design	• Gelijktijdigheid • Cocreatie • Positivisme	• Stellen positieve vragen • Dialoog over bevindingen	• Grotere betrokkenheid • Positief gevoel
Rapportage	• Bespreken en afstemmen bevindingen • Rapportage	• Design • Destiny	• Positivisme • Cocreatie	• Communiceren in de vorm van dialoog • meebouwen aan aanbeveling	• Meer betrokkenheid om met de aanbevelingen aan de gang te gaan

Tabel 1. Appreciative auditing

gezamenlijke sessie zijn alle functionaliteiten vertegenwoordigd. Door te vragen naar zaken waar men trots op is en naar waar men hoopt dat de organisatie over een paar jaar staat, ontstaat een positieve dialoog. Dit leidt dan weer tot meer commitment waardoor men meer geneigd is om zaken met elkaar te delen.
Dat de zienswijze 'positieve beelden vertalen zich in positieve actie' ook binnen de internal auditfunctie al gedeeltelijk geland is, blijkt uit het artikel 'A kinder, gentler audit' in *Internal auditor* (Berry, oktober 2007). Het artikel beschrijft het effect van het geven van complimenten in plaats van het uitdelen van klappen. Het succes van een auditrapport is, volgens dit artikel, veelal meer gebaseerd op de houding en specifieke benadering dan op de inhoud. De auteur geeft vijf basisregels om de effectiviteit van een auditrapportage te vergroten:
1. Benader cliënten (opdrachtgevers) met respect.
2. Geef cliënten (opdrachtgevers) het voordeel van de twijfel.
3. Kies je discussiepunten zorgvuldig.
4. Benadruk het positieve.
5. Wees informatief.

Deze vijf punten sluiten aan op de essentie van appreciative auditing. De uitdrukking 'je vangt meer vliegen met stroop dan met azijn' is volgens mij hierop van toepassing. Letterlijk wordt gezegd: 'A positive approach and positive language draw people into dialogue; a negative approach usually results in walls erected to keep auditors and their new ideas at a distance'. Uit de reacties van lezers op het artikel in *Internal Auditor* (december 2007) blijkt dat het artikel erg aanspreekt.

Praktijk

Momenteel pas ik appreciative auditing in de praktijk toe bij mijn huidige werkgever, het UWV. De eerste ervaringen zijn zeer positief. Alleen al door het stellen van positieve vragen is er meer sprake van een dialoog. Tijdens diverse gesprekken werd na het stellen van de positief geformuleerde vragen het gesprek meer open en kwam de auditee spontaan met een aantal verbeterpunten binnen zijn eigen onderdeel. Door ook de positieve elementen te benoemen in de rapportage werd bereikt dat men meer open staat om met de aanbevelingen aan de slag te gaan. Dit komt exact overeen met het gestelde in *tabel 1*.
Het vervolg is om ook de keuze van auditonderwerpen vanuit een waarderende benadering in te steken. Dit betekent dat niet alleen gekeken wordt vanuit de risico's maar ook vanuit hoe men met het pakken van kansen omgaat. Waar een risico is, is ook een kans. De kansen worden vaak niet genoemd en dus niet gepakt.
Door appreciative auditing met gezond 'boerenverstand' in te zetten zal de internal auditfunctie effectiever worden en een positieve bijdrage leveren aan het verbeteren van de bedrijfsvoering binnen veel organisaties.

Anthoon Haagsma is senior auditor bij UWV. Dit artikel is gebaseerd op het referaat *Appreciative Auditing* waarmee hij in 2008 afstudeerde op de EMIA-opleiding aan de UvA. Voor vragen, reacties en discussie kunt u mailen.
✉ anthoon.haagsma@uwv.nl

Independent research firm named BWise a Leader in Enterprise GRC Platforms.*

Let BWise make *you* the GRC frontrunner.

BWise
PROCESS OF SUCCESS

BWise biedt uw organisatie een software oplossing van wereld formaat voor Governance, Risk en Compliance (GRC) uitdagingen. Met GRC uitdagingen bedoelen we ondermeer het voldoen aan externe wet- en regelgeving, zoals Sarbanes-Oxley en Code Tabaksblat. Ook kunt u denken aan onderwerpen zoals het krijgen van grip op Internal Control, Risk management en IT Governance.

Door onze unieke procesgerichte aanpak, bereikt u met BWise niet alleen voordelen op het gebied van procesoptimalisatie, u bespaart ook aanzienlijk op compliancekosten.

Vraag het Forrester rapport gratis aan via **www.grcrace.com**.

FORRESTER®

The Forrester Wave ™: Enterprise Governance, Risk and Compliance Platforms, Q3 2009

Forensic IT-audit: het antwoord op cybercrime

"Cybercrime is voor criminelen veel interessanter dan een bank overvallen." Matthijs van der Wel, managing principle forensics EMEA bij Verizon Business, windt er geen doekjes om: bedrijven en organisaties zijn anno 2009 veel te laconiek als het gaat om het treffen van maatregelen ter voorkoming van cybercrime. Dit terwijl de ergste risico's op vrij eenvoudige wijze kunnen worden ingedamd. Het is mede aan internal auditors om dat nadrukkelijker op de kaart te zetten in hun organisatie.

Interview: drs. L.Z. Nagy RO EMIA
Tekst: B. van Breevoort

Matthijs van der Wel, Verizon Business: "Hackers kunnen dagenlang bezig zijn op een netwerk zonder gezien te worden."

Matthijs van der Wel voert al sinds 2001 forensic IT-audits uit. Eerst vanuit Fox-IT en sinds twee jaar vanuit Verizon Business, waar hij nu verantwoordelijk is voor de 'incident response teams' in de EMEA-regio. Omdat cybercrime zich niet stoort aan landsgrenzen, past hij in de regel een wereldwijde aanpak toe, samen met zijn collega's in de overige werelddelen.

Hoe lang bestaat het vak van forensic IT-auditor en met welke gedrags- en beroepsregels wordt er gewerkt?

"Het is een heel jong vakgebied. Er bestaat een aantal beschermde certificeringen zoals Certified Information System Security Professional, Certified Information System Auditor en Qualified Security Assessor. De titel 'forensic IT-auditor' of 'forensisch IT-onderzoeker' is daarentegen niet beschermd. In dat licht heeft het een parallel met de privédetective van vroeger. In beginsel kan iedereen het vak uitoefenen en kan wildgroei ontstaan. Hierdoor is het moeilijk voor een opdrachtgever om te doorgronden of hij een kwalitatief goede forensic IT-auditor op een onderzoek zet, te meer daar men zelf veelal geen IT-achtergrond heeft. Ik zie dan ook bij de uitvoer van contra-expertises soms rapporten voorbijkomen die ernstig rammelen. In Nederland zijn wel gedrags- en beroepsregels van toepassing. Zo moeten er voor een forensic IT-audit gegronde redenen bestaan binnen het eigen bedrijf, waarbij beginselen als proportionaliteit en subsidiariteit gelden. Bovendien is de privacybescherming onverkort van toepassing. Bij forensic IT-audits in opdracht van derden is de Wet particulier recherchebureaus van toepassing en een bindende gedragscode. Echter, dit soort regelgeving verschilt per land of ontbreekt soms volledig in andere landen."

Illustratie: Roel Ottow

Wat houdt een forensic IT-audit in?

"Forensic IT-audits kunnen enorm verschillen qua budget en complexiteit, waardoor er geen generieke definitie is te geven. Televisieseries als *CSI* dragen wel bij aan de beeldvorming van wat een onderzoeker uitvoert. Uiteraard komen de Hollywoodbeelden niet volledig overeen met de praktijk, maar ze geven wel een idee. Een cybercrimeonderzoek uitvoeren kan veel lastiger zijn dan een moordzaak. Als er een lijk op de grond ligt met een mes in zijn rug snapt iedereen dat je niet aan het mes moet zitten én het is duidelijk dat er daadwerkelijk iets gebeurd is. Het is opvallend: als er iets mis gaat met computers, gaat iedereen er met zijn tengels aan zitten. Systeembeheerders spannen meestal de kroon door bijvoorbeeld tools te installeren om zelf onderzoek te doen. Wat zij zich daarbij niet realiseren is dat ze daarmee 'aan het mes' zitten. Het is dan uiterst moeilijk om sluitend bewijs te leveren voor een security-incident, aangezien de integriteit van het onderzoeksmateriaal in het geding komt en mogelijke sporen wellicht gewist zijn door de acties van de systeembeheerder."

Voor wie werkt een forensic IT-auditor? Bedient hij het publiek domein in het kader van de waarheidsvinding?

"Ja, wij doen aan waarheidsvinding. Niet iedere opdrachtgever is daar blij mee omdat we soms ook ontlastende sporen aantreffen. Security-incidenten kunnen op vele manieren optreden. Iemands account wordt bijvoorbeeld misbruikt doordat collega's een wachtwoord met elkaar delen. Of het ontstaat omdat een pc niet was afgesloten. Of men werkt met computers die besmet zijn met een virus, waardoor hackers via een achterdeur data kunnen laten verdwijnen. De forensic IT-auditor moet uitzoeken waardoor het security-incident is ontstaan. Sturing door de opdrachtgever naar een bepaald resultaat hoor je vanzelfsprekend niet te accepteren."

In hoeverre kunnen bedrijven het justitiële apparaat inschakelen voor forensic IT-audits?

"Bij het vermoeden van strafbare feiten kan een organisatie altijd naar de politie gaan. In de praktijk zien we echter dat bedrijven dat niet altijd meteen doen. In plaats hiervan stappen zij naar een commerciële forensisch IT-onderzoeker. Zij kunnen dan als opdrachtgever onder andere invloed uitoefenen op de schaal en de intensiteit van het onderzoek. Organisaties spreken ook geheimhouding af over gevoelige zaken via een non-disclosure agreement."

En als justitie die gegevens vervolgens opvraagt?

"Dat gebeurt doorgaans via de opdrachtgever en niet via de forensic IT-auditor. Wij hanteren uiteraard dezelfde strikte procedures met betrekking tot de vergaring van mogelijk bewijsmateriaal en kunnen zonder problemen en indien gewenst onze zaken overdragen."

Hoe verloopt een forensic IT-audit doorgaans?

"Het begint meestal met het vermoeden dat systemen zijn gehackt. Via een audit probeert men vast te stellen of er sporen te vinden zijn en of er überhaupt sprake is van een security-incident. Als het beveiligingsrisico eenmaal is gedetecteerd, is het aan de organisatie om de prioriteiten aan te geven. Worden de systemen doorgelicht om de schade vast te stellen of is hier geen tijd voor en is de continuïteit van de bedrijfsvoering belangrijker? Het is tegenwoordig geen reële optie om hele systemen plat te leggen voor nader onderzoek. De vraag is of je dat ook wilt, aangezien er bijvoorbeeld specifieke malware bestaat die niet meer te ontdekken valt als een systeem wordt uitgeschakeld. Daarnaast is het herkennen van een security-incident complex. Een financiële instelling handelt doorgaans volgens het 'four eyes principle': twee mensen moeten kijken voor een betaling wordt goedgekeurd. Het kan echter voorkomen dat een server uit en weer aan wordt gezet, waarbij de server de betalingen die nog in batch staan, uitvoert zonder die controleslag. In dit geval wordt het uit- en aanzetten van de server

naar alle waarschijnlijkheid niet als beveiligingsrisico gezien, terwijl het er wel een is."

Hoe alert zijn bedrijven en organisaties in het signaleren van security-incidenten?

"Eigen onderzoek heeft aangetoond dat hackers dagenlang bezig kunnen zijn op een netwerk zonder gezien te worden en dat het maanden kan duren voor een bedrijf een beveiligingslek dicht. Het blijkt dat men door een goede analyse van logbestanden de incidenten zelf had kunnen signaleren. Het komt zelfs voor dat er een detectiesysteem is dat aangeeft dat er gehackt is en dat data verdwijnen, maar dat men desondanks geen maatregelen neemt. Veel organisaties kopen liever een doos met beveiligingssoftware om van het probleem af te zijn. Echter, zo werkt beveiliging niet. Je moet medewerkers hebben die weten wat er speelt en die ook herkennen wat normaal en abnormaal gedrag op de bedrijfsnetwerken is. De praktijk is dat men beperkte kennis heeft van de applicaties die draaien op een server en dat er zelden een actuele en accurate netwerktekening bestaat. Voorts is dikwijls de verantwoordelijkheid voor het al dan niet uit de lucht halen van bedreigde bedrijfsnetwerken niet geregeld. Dat bemoeilijkt het werk van de forensic IT-auditor."

Kan de IAD daarbij helpen?

"De reactie van IAD's op onze rapporten is steevast dat zij ook al jaren roepen om soortgelijke maatregelen. Ik geef ook altijd aan dat ze ons onderzoek kunnen gebruiken als kruiwagen om het nu eindelijk geregeld te krijgen."

De realiteit is dat cybercrime vrijwel volledig in handen is van de georganiseerde misdaad

Is door de enorme voortschrijdende technologische ontwikkelingen IT niet te complex voor bedrijven?

"In de jaren negentig was het credo om de randen van het netwerk te beveiligen, zodat niemand van buiten naar binnen kon komen. Daarbij vertrouwde men allen die binnen het netwerk actief waren. Deze situatie is nog steeds gemeengoed bij veel bedrijven. Wat men zich niet realiseert is dat één onachtzaamheid binnen dat netwerk andere servers kan infecteren. Bovendien heeft men in de loop der jaren andere partijen of leveranciers toegang gegeven tot bepaalde delen van het netwerk. Je ziet dat een aantal bedrijven zich daardoor gaat richten op het beschermen van de data: data loss protection en data loss prevention. Is IT daarmee te complex geworden? Goede beveiliging draait om risicomanagement en daarin moet men een zekere balans vinden, want het is onwerkbaar om het netwerk hermetisch af te sluiten. Via een doortimmerde risicoanalyse moet het beveiligingsniveau worden bepaald. Stel vast waar de risico's liggen. Bepaal welke risico's verkleind moeten worden en welke aanvaardbaar zijn of afgedekt dienen te worden met een verzekering."

Wat is er nu precies 'forensic' aan deze vorm van IT-auditing als je het vergelijkt met een reguliere IT-audit?

"Forensic houdt in dat onderzoek wordt gedaan na een bepaald security-incident. Hoe heeft het kunnen gebeuren? Welke risico's loopt de organisatie? Wat voor data is er verdwenen en wie is er verantwoordelijk voor? Een andere variant van forensic onderzoek is dat je vooraf alarmbellen gaat installeren, omdat er een vermoeden bestaat dat een security-incident gaat plaatsvinden. 'Forensic' betekent overigens letterlijk 'voor het gerecht'. Forensic IT-audit gaat anders dan bij een reguliere IT-audit meer om een feitenonderzoek met waarheidsvinding als doel."

Hoeveel bedrijven ter wereld zijn slecht toegerust voor een aanval op hun netwerk?

"Zonder te overdrijven durf ik te stellen dat dit geldt voor 99 procent van de bedrijven. In mijn praktijk zie ik allerlei onnodige fouten: geen waterdichte procedure voor het aanmaken van een gebruikersaccount, het IT-incident responseplan is rechtstreeks gedownload van internet en nog nooit goed gelezen. Bij 79 procent van de incidenten is er sprake van een error, ofwel een omissie: men denkt dat er een security control is, maar die functioneert in werkelijkheid niet naar behoren. Het meest voorkomende scenario is dat hackers binnenkomen door middel van SQL-injectie of standaardwachtwoorden als 'admin' en 'welkom1'. Er is dan wel beleid vastgesteld dat wachtwoorden regelmatig gewijzigd moeten worden, maar in de praktijk wordt dit niet nageleefd. Anno 2009 moet men wellicht naar een meer geavanceerde authenticatieprocedure. We spreken in dit verband van 'one, two or three factor identification'. Het getal geeft aan hoeveel elementen er nodig zijn om toegang te krijgen: iets wat je weet, iets wat je hebt of iets wat je bent. De eenvoudigste vorm is toegang verkrijgen met bijvoorbeeld een pasje (iets wat je hebt) of een wachtwoord (iets wat je weet). Bij twee elementen gaat het om een combinatie van bijvoorbeeld een bankpas en een pincode. Ik denk dat organisaties in sommige gevallen wellicht moeten overstappen naar een combinatie van drie elementen."

Wat is de verhouding tussen de benodigde investeringskosten voor afdoende beveiligingsmaatregelen en het schaderisico als men deze maatregelen niet treft?

"Met een geringe investering in betere bescherming kan al heel veel worden bereikt. Uit eigen onderzoek is gebleken dat de helft van de serieuze IT-incidenten voorkomen had kunnen worden met heel eenvoudige aanpassingen in de procedures. Wat bijvoorbeeld vaak vergeten wordt is het belang van een goede beveiliging van de webserver en de applicaties die daar op draaien, ook al staat daar wellicht geen kwetsbare data. Het is echter wel de toegangs-

poort naar de bedrijfsnetwerken daarachter. Uiteraard lopen bepaalde sectoren meer risico. Organisaties moeten zich daarom afvragen of ze een *target of choice* of een *target of opportunity* zijn. Als target of choice loop je een verhoogd risico en dien je zwaardere beschermingsmaatregelen te treffen. Als target of opportunity ben je een van de velen en moet je zorgen dat je niet het eenvoudigste doelwit bent. Vergelijk het met traditionele inbrekers die ook eerst de omgeving verkennen om te bepalen waar het de minste moeite kost om hun slag te slaan. Hackers werken niet anders."

Hoe worden die gestolen data verhandeld?

"Gestolen data worden verhandeld op internet. Momenteel gaat dat via chatboxen, de zogeheten IRC-kanalen. Er is de afgelopen jaren echter veel data verdwenen en als er veel aanbod is, gaat de prijs omlaag. Zo zijn bijvoorbeeld gestolen creditcardgegevens in prijs gedaald van 10 dollar in 2007 naar 50 dollarcent vandaag de dag. Achter 93 procent van de IT-incidenten die wij onder handen hebben gehad in 2008, zit de georganiseerde misdaad. Het is veel lucratiever dan een bank overvallen. Aangezien de prijs van gestolen data is gedaald, richt men zich momenteel onder andere op het verkrijgen van pincode-informatie, waarmee men zich toegang kan verschaffen tot bankrekeningen. Dit vergt een veel langere adem van de hacker, soms wel een jaar. Daarna wordt een aanval uitgevoerd. Hierbij is wel eens sprake van samenwerking tussen externe partijen en een 'infiltrant' binnen de organisatie. Hackers worden maar al te vaak beschouwd als 16-jarigen die op een zolderkamertje hun hobby uitvoeren. De realiteit is dat cybercrime vrijwel volledig in handen is van de georganiseerde misdaad. De winstmarges zijn hoog. De pakkans is zeer klein, want hackers zijn moeilijk te traceren en moeilijk te vervolgen, aangezien ze traditioneel gebruikmaken van veel tussenliggende systemen verspreid over tal van landen die meestal geen wetgeving hebben tegen cybercrime."

Hoe ziet de toekomst eruit? De systemen worden almaar complexer. Werknemers willen steeds meer toepassingen in hun systemen en vanaf meer locaties toegang tot het bedrijfsnetwerk.

"Data breaches zullen blijven toenemen mede als gevolg van de wens om overal toegang te hebben tot het bedrijfsnetwerk en de data. Beveiliging wordt daarbij vaak als hinderlijk ervaren. Voorts wordt het qua procedure en techniek ook moeilijker om onderzoek goed uit te voeren. Er is een enorme toename in data die al dan niet versleuteld is. Een analyse van data en complex dataverkeer is tegenwoordig een gigantische klus. Het vergt gericht onderzoek."

Wie in de organisatie moet de beveiliging van het bedrijfsnetwerk op de kaart zetten?

"Veel organisaties zijn niet optimaal voorbereid op cybercrime of een IT-security-incident. Men heeft daarnaast geen beeld van de vergaande consequenties van een data breach: vermogensschade, juridische claims, toeleveranciers en klanten die zich terugtrekken, et cetera. Risicomanagement hoort ingebakken te zijn in de organisatie. De IAD heeft hier een duidelijke rol. Bij beveiliging tegen cybercrime is echter een check op de 'papieren' procedures niet voldoende. De internal auditor moet de uitvoering van de procedures in de praktijk testen. Ga met een groep medewerkers aanvalsscenario's verzinnen en bepaal hoe die hacks zijn te ontdekken. Controleer het vervolgens door in de eigen systemen te kijken of je deze sporen nu al kunt herkennen. Of analyseer met welke systemen het bedrijf communiceert en controleer of daar ongewone datastromen plaatsvinden. Vertrouw niet blind op beveiligingssoftware maar investeer in personen (intern of extern) die verstand hebben van beveiliging tegen cybercrime." ❑

Laszlo Nagy is associate partner Audit & Risk bij ConQuaestor Consulting en als redacteur verbonden aan *Audit Magazine*.

Proactive Quality Assurance (PQA)

Veel organisaties implementeren brede 'business systems', soms als onderdeel van een veranderingsprogramma. Een dergelijk systeem heeft veelal grote consequenties voor de bedrijfsvoering. De implementatie is ingrijpend en kent vele risico's. Dat geldt zeker voor een wereldwijde roll-out bij een groot aantal vestigingen, maar ook voor een eenmalige implementatie.

Drs. P. Hartog CIA
H. Cleton

Om deze risico's te beheersen, wordt gebruikgemaakt van vaste projectmethoden of 'project roadmaps'. Deze delen de implementatie veelal op in verschillende fasen en stromen en beschrijven de mijlpaalproducten of deliverables die moeten worden opgeleverd. Vaak is daarbij sprake van een quality assurance (QA) die repressief controleert of de gewenste deliverables zijn opgeleverd. Wij pleiten echter voor een meer proactieve QA, die systematisch kijkt naar de risico's en naar de waarborgen dat het project haar resultaten zal behalen, zonder dat dit leidt tot overbelasting van project. Wij spreken daarbij van proactive quality assurance ofwel PQA. PQA kan ook voor de internal auditor een instrument zijn om zijn toegevoegde waarde te vergroten.

In dit artikel wordt ingegaan op:

- de uitgangspunten van PQA als proactief auditframework;
- de werkwijze bij het ontwikkelen daarvan;
- het resultaat.

De uitgangspunten

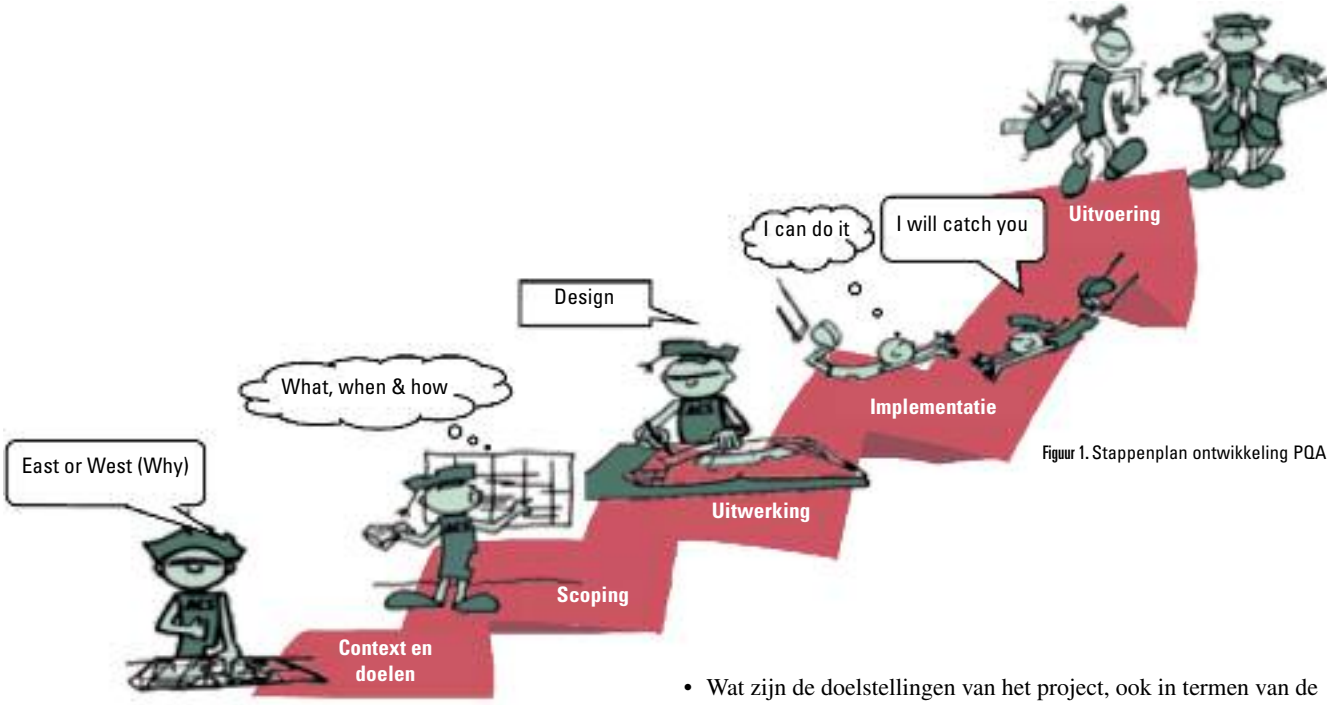
PQA is een auditframework bestaande uit diverse audits die zijn gebaseerd op de gekozen projectmethode of project roadmap, op de doelstellingen van het project[1] en op de risico's die het bereiken van die doelen (kunnen) bedreigen. In de meeste project roadmaps is de Quality Assurance-stroom onvoldoende ingericht om alle risico's van een implementatie tijdig te kunnen beheersen.

Belangrijke kenmerken van PQA zijn:

- *Proactief*: proactief betekent dat niet wordt gewacht tot deliverables worden opgeleverd, maar dat vroegtijdig wordt gekeken naar de waarborgen die er bestaan dat de deliverables conform de gestelde kwaliteitseisen (kwaliteit, tijd en kosten) zullen worden opgeleverd. Dat komt tot uiting door een zwaar accent op de kwaliteit van het projectmanagement alsmede door een zodanige timing van audits op deliverables zodat tijdig correcties kunnen plaatsvinden.
- *Minimale belasting van de organisatie*: om de gewenste extra zekerheid te verkrijgen dienen aanvullende werkzaamheden in de vorm van audits te worden uitgevoerd. De belasting hiervan, zowel in termen van de hoeveelheid werk als de planning, wordt echter zo klein mogelijk gehouden.

De audits worden in beginsel zo opgezet dat zij niet op het kritieke pad liggen en de voortgang van het project dus niet hinderen

- *Risicogeoriënteerd*. Zeker niet alles hoeft te worden geaudit. De keuze van de uit te voeren audits wordt gebaseerd op een risicoanalyse, waarbij wordt vastgesteld op welke punten de grootste risico's worden gelopen en waar dus extra zekerheid is gewenst.
- *Niet op het kritieke pad*. De audits worden in beginsel zo opgezet dat zij niet op het kritieke pad liggen en de voortgang van het project dus niet hinderen. Dat betekent dat bij audits op deliverables die op het kritieke pad liggen, niet wordt gewacht op de oplevering daarvan, maar dat wordt gekozen voor een systeemgerichte benadering waarbij kort voor de oplevering wordt gekeken of aan alle voorwaarden is voldaan om een adequaat product op te leveren.



Figuur 1. Stappenplan ontwikkeling PQA

- *Afstemming met andere audits*. De invulling van PQA wordt afgestemd met andere audits binnen en buiten de organisatie om overlap te minimaliseren en zoveel als mogelijk gebruik te maken van elkaars resultaten.

- *Afgestemd op de gebruikte projectmethode*: PQA dient te worden afgestemd op de door de organisatie gekozen projectmethode (bijvoorbeeld Prince II of ASAP[2]) en de daarin benoemde fasen, producten en standaarden.

PQA is in de eerste plaats een instrument voor de QA-functie in het project. Het kan echter ook worden gehanteerd door een meer onafhankelijke auditdienst.

De werkwijze

De ontwikkeling van PQA binnen een project verloopt als volgt (zie *figuur 1*):

1. vaststellen van de context en uitgangspunten;
2. benoemen van de gewenste audits (scoping);
3. uitwerken van de werkprogramma's voor de onderscheiden audits;
4. implementeren van het framework, zodanig dat de diverse audits adequaat kunnen worden uitgevoerd.

Bij de ontwikkeling van PQA is zowel kennis van het project en de projectmethode vereist, als kennis van auditing. Daarmee kunnen de risico's en auditobjecten enerzijds gericht worden bepaald en anderzijds deugdelijk én doelmatig worden geaudit.

1. Context, doelen en uitgangspunten

De eerste stap betreft het vaststellen van de uitgangspunten inzake de doelen, de inhoud en de wijze van uitvoering van de audits. Dit gebeurt op basis van een contextanalyse en een bespreking met het verantwoordelijke management. Vragen die in de contextanalyse aan de orde komen zijn:

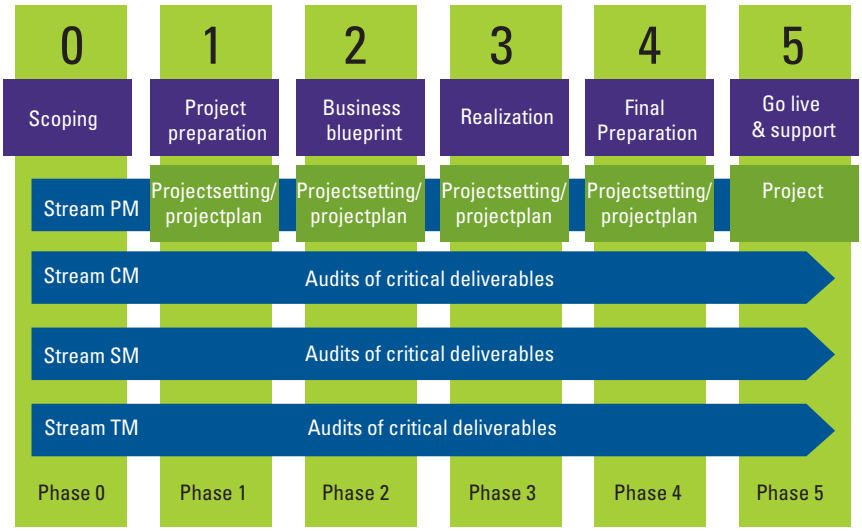
- Wat zijn de doelstellingen van het project, ook in termen van de (achterliggende) doelen van de business?
- Welke projectmethode wordt gebruikt en in hoeverre wordt daarbij gebruikgemaakt van de in de methode beschikbare standards en templates (ook wel quality control (QC) genoemd)?
- Waar liggen de grootste risico's van het project?
- Wat is het doel van de PQA in de beheersing van het project en wie is de (primaire) opdrachtgever van de audits?
- Welke andere assurance is in en rond het project aanwezig?
- Wie gaat de audits uitvoeren? Welke deskundigheden zijn vereist?

2. Scoping

Nadat de doelstellingen en de aard van PQA zijn vastgesteld, dienen de uit te voeren audits te worden benoemd. Zoals genoemd is de door de organisatie gekozen projectmethode het uitgangspunt. Bij het benoemen van de audits wordt een onderscheid gemaakt tussen:

- audits van de door het project op te leveren mijlpaalproducten of deliverables;
- de projectmanagement (PM)-audit.

De PM-audit is een vast onderdeel van elk auditframework. In de beheersing van het project ligt immers de basis voor het succes van het project en voor het adequaat opleveren van de gewenste deliverables. Met de PM-audit kan worden gekeken of een fase inderdaad kan worden afgesloten, maar zal tevens worden onderzocht of er voldoende zekerheid bestaat dat in de volgende fase de doelstellingen zullen worden behaald. Afhankelijk van de gekozen projectmethode en de planning zal de PM-audit bij elke faseovergang of periodiek worden uitgevoerd (zie *figuur 2*).
In aanvulling op de PM-audits wordt nog additionele zekerheid verkregen door de audits op de deliverables. Vanzelfsprekend hoeven niet alle deliverables te worden geaudit. Met behulp van een risicoanalyse worden de meest kritieke mijlpaalproducten geselecteerd. Projectmethoden voor de implementatie van business systems bestaan veelal uit een aantal stromen en fasen. Per stroom en fase



Figuur 2. De PM-audit per fase

is een aantal deliverables (processen of producten) gedefinieerd. Voor elk van die deliverables wordt – bijvoorbeeld in een workshop met het projectmanagement, consultants met kennis van de PM-methode en materiedeskundigen – geëvalueerd hoe belangrijk en hoe complex de betreffende deliverables zijn. Dit resulteert in een overzicht van de meest kritieke deliverables die zullen worden geaudit.
In aanvulling op de benoeming van de auditobjecten wordt tevens het type audit en de globale planning bepaald. Bij het type of de aard van de audit kan een onderscheid worden gemaakt naar:

- systeemaudits waarbij (prospectief) wordt gekeken of er voldoende waarborgen bestaan dat het goed zal gaan;
- performance of product audits, waarbij het doel is om (retrospectief) een oordeel te geven of de betreffende deliverable voldoet aan de eisen.

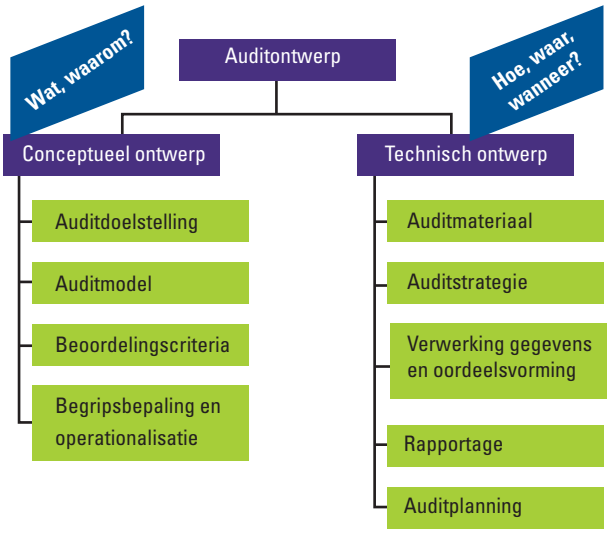
Bij de performance audit kan er vervolgens voor worden gekozen om het product zelf te beoordelen dan wel het proces dat tot het product heeft geleid. Beoordeling van het product zelf geeft meer zekerheid, maar kost over het algemeen meer. Daarbij kan de productbeoordeling pas in een later stadium (na de afronding van het product) worden uitgevoerd. Als de oplevering van het product op het kritieke pad van het project ligt, kan dat betekenen dat de audit het project vertraagt. De vraag is dan of, alle risico's afwegend, niet voldoende zekerheid kan worden verkregen door middel van een beoordeling van het proces. Dat zou zelfs op een zodanig moment kunnen plaatsvinden dat nog tijdig kan worden gecorrigeerd als blijkt dat niet alles naar wens verloopt.
De resultaten van de voorgaande activiteiten worden verwerkt in het scopingdocument ofwel de 'audit roadmap'. In dit document wordt het auditframework beschreven in de vorm van een overzicht van de uit te voeren audits. Daarnaast worden de uitgangspunten, de te hanteren normenkaders en de doelstellingen van PQA voor de organisatie vastgelegd. Aanvullend wordt tevens een aantal mogelijke randvoorwaarden voor de ontwikkeling en uitvoering van PQA beschreven waaraan voldaan moet worden om PQA succesvol te laten zijn.

3. Auditontwerpen

Als duidelijk is welke audits zullen worden uitgevoerd, dient de inhoud en de wijze van uitvoering nader te worden uitgewerkt. Hierbij wordt gebruikgemaakt van de auditmethodologie[3] (zie *figuur 3*).
In de voorgaande stappen zijn de context en de doelstellingen van de audits reeds vastgesteld. De belangrijkste aspecten nu zijn de uitwerking van het normenkader en het bepalen van de bronnen en wijze waarop die te benaderen. Zeker in geval van projecten met vele deskundigen en aanpakken is het belangrijk dat de auditor een concreet normenkader opstelt dat aangeeft naar welke aspecten wordt gekeken én wanneer die aspecten adequaat zijn ingevuld.
Dat normenkader hoeft niet van scratch af aan ontwikkeld te worden, maar dient wel op maat voor het betreffende project te worden gemaakt. De basis is gelegen in:

- de projectmethode, waarin de op te leveren deliverables zijn gedefinieerd en veelal zijn uitgewerkt in templates. Dit zijn vooral de 'procedurele' eisen (vormvoorschriften);
- eerder opgeleverde deliverables, die meer de inhoudelijke criteria aangeven. Zo dient de inhoud van de business blueprint aan te sluiten bij de business case;
- de in de projectmethode aanwezige wijze van projectmanagement;
- andere veelgebruikte beheers- en veranderkundige modellen, zoals COSO en de Balanced Change Card (Koster e.a.).

Ten aanzien van de PM-audit is het belangrijk dat niet alleen naar de 'harde' aspecten van projectmanagement wordt gekeken. Juist



Figuur 3. Auditmethodologie als hulpmiddel voor het ontwerpen van de audits

Een betere aanpak van uw interne beheersing en toch kosten besparen?

Hoe gaat u slagen?

Interne beheersing en Cost of Control vragen volop aandacht in deze tijd. Hoe combineert u deze schijnbare tegenstelling?
KPMG Internal Audit, Risk & Compliance Services adviseert en ondersteunt bij het versterken van de interne beheersing en governance binnen uw organisatie. Verrassende en slimme oplossingen die èn de beheersing verstevigen en kostenreducties realiseren. Voor nu en in de toekomst.

Meer weten? Bel: (020) 6568160

KPMG

AUDIT ▪ TAX ▪ ADVISORY

Figuur 4. Balanced Change Card

in de afstemming met de organisatie (draagvlak en verandervermogen) en in de samenwerking binnen het project liggen vaak risico's voor het project. Een model dat evenwichtig aandacht besteedt aan die diversiteit aan aspecten is de Balanced Change Card[4] (zie *figuur 4*).

4. Implementatie

Afhankelijk van de omvang en frequentie van de project- en PQA-activiteiten, kunnen de volgende activiteiten in dit kader worden uitgevoerd:

- verdere uitwerking van de auditontwerpen in praktische tools, zoals interviewvragenlijsten en formats voor de verslaglegging;
- opleiding en training van de auditors;
- communicatie met de betrokkenen om duidelijkheid te creëren over de toegevoegde waarde van PQA en de diverse audits;
- afstemming met andere auditors en toezichthouders om afspraken te maken over de rol- en taakverdeling en over de waarborgen voor het kunnen steunen op elkaars resultaten.

Voor projecten waarbij sprake is van meerdere implementaties of roll-outs speelt daarbij nog het volgende: veelal zal gekozen worden voor een generiek auditframework waarbij de concrete samenstelling van het framework per roll-out, op basis van een risicoanalyse, specifiek wordt gemaakt. Bepalende factoren daarbij zijn:

- Greenfield, of is er al ervaring met een business systeemimplementatie;
- de mate van afwijking van de standaard werkprocessen;
- de mate van ondersteuning door consultants.

Eigenlijk is hierbij sprake van een soort nadere scoping aan het begin van een nieuwe roll-out.

Het resultaat

Het resultaat van voorgaande stappen is een auditframework bestaande uit een overall plan (de audit roadmap), auditontwerpen en tools voor de uitvoering. Dat framework is bruikbaar voor het betreffende project, maar vaak ook voor andere projecten nadien.

Met behulp van PQA wordt de projectbeheersing versterkt. Er worden extra waarborgen in het project ingebouwd.
PQA is geen panacee dat de bekende projectproblemen geheel kan en zal voorkomen. Wel zien we in de praktijk dat PQA helpt om deze problemen in een vroegtijdig stadium inzichtelijk en daarmee bespreekbaar en oplosbaar te maken. Juist dat proactieve geeft het gevoel van echte waarde bij de stuurgroep en projectmanager waar wij PQA hebben toegepast, omdat bijsturing mogelijk is voordat een fase echt is afgerond.
Door de audits van PQA komen risico's en probleempunten objectief op tafel en ontstaat een extra communicatiekanaal. Juist doordat vooraf afspraken zijn gemaakt over de PQA-activiteiten komen deze niet bedreigend over, wat nog wel eens het geval kan zijn als gedurende het project alsnog besloten wordt om audits uit te voeren. In aanvulling op de veelal operationele besprekingen wordt systematisch de wijze en kwaliteit van samenwerken, communiceren en besluitvorming besproken.

Noten

1. In dit artikel worden de termen project en programma door elkaar gebruikt.
2. Prince II staat voor Projects IN Controlled Environments, MSP staat voor Managing Succesful Programmes, ASAP staat voor Accelerated SAP, de implementatiemethode van SAP.
3. Otten, J.H.M., Hartog, P.A. en A. Babeliowsky, 'Auditmethodologie, metatool voor klantgericht auditen', *Audit Magazine*, nummer 4, 2002.
4. Koster, E. en W. Bouman, 'Een raamwerk voor het vormgeven en evalueren van veranderorganisaties', *Management & Organisatie*, nr. 5, 1997.

Peter Hartog (l) is senior auditing consultant bij ACS. Hans Cleton is managing partner bij ACS.

Bijzondere onderzoeken:

van wetenschap via mesologie naar opsporing

Tijdens de brainstormsessies over het thema 'Bijzonder onderzoek' had de redactie al snel een lijstje met onderwerpen die binnen ons vakgebied tot een bijzonder onderzoek gerekend kunnen worden. Zoals het een goede brainstorm betaamt, dachten wij ook 'out of the box' en zo kwamen we op een aantal andere onderzoeksvarianten, die niet per se overeenkomsten vertonen met ons eigen vakgebied. *Audit Magazine* sprak met Frits Schipper (VU Amsterdam) over de criteria voor wetenschappelijk onderzoek, met Rob Muts (Academie voor Mesologie) over de onderzoeksmethodologie van de mesoloog en met Bart Hulsbosch (Brigade Zuid-Holland) over de onderzoeksaanpak in het vakgebied van de Koninklijke Marechaussee.

Drs. R.H.J.W. Jansen RO
Drs. N. J. Engel-de Groot
Drs. R.J.A.C. Jansen RO

Oog hebben voor beperkingen!

Wat zijn de criteria voor goed wetenschappelijk onderzoek? Welke gelijkenissen zijn er tussen de onderzoeksaanpak door een wetenschapper en de auditor? Een gesprek met Frits Schipper (VU Amsterdam) over wetenschappelijk onderzoek.

Dr. Frits Schipper studeerde natuurkunde en filosofie. Hij is coördinator van de MA-opleiding Filosofie in Bedrijf aan de Vrije Universiteit Amsterdam en was eind jaren negentig tijdelijk gedetacheerd bij Paardekooper & Hoffman, het huidige Mazars, waar hij adviseerde over filosofische vraagstukken. Schipper: "Alle wetenschap is op zoek naar een gedeeld begrip: hoe is iets en waarom is het zoals het is? Een andere overeenkomst met wetenschappelijke onderzoeken is de methodische aanpak als zodanig. Echter, in de wetenschap is er ook verscheidenheid, namelijk in de verschillende methoden en verklaringsstrategieën. De natuurwetenschap zal vooral zoeken naar verklaringen met behulp van algemene (causale) wetten. In de psychologie bijvoorbeeld is dat niet afwezig, maar daar wordt ook verklaard door een beroep te doen op de bewuste intenties van mensen. Met andere woorden, de invulling van de methode en strategie van verklaring verschilt."

Goed onderzoek is methodisch verantwoord

Onafhankelijk van de invulling en strategie van verklaring zal

goed onderzoek altijd verbonden moeten kunnen worden met een methode. Schipper: “Dat is nodig omdat daarmee een inhoudelijke kritiek op aanspraken op kennis mogelijk wordt. Maar dat is nog niet voldoende. Wordt er bijvoorbeeld gemeten, dan is een (heldere) methode cruciaal. De ermee verbonden operationalisering van de begrippen moeten echter ook betrouwbaar en valide (geldig) zijn. Bij betrouwbaarheid gaat het erom dat onderzoekers in vergelijkbare omstandigheden tot dezelfde resultaten komen. Bij validiteit gaat het om de vraag: doe je recht aan het object van onderzoek? Met andere woorden, meet je wat je denkt te meten? Een voorbeeld van dit laatste is dat een intelligentietest aangepast dient te zijn aan de culturele achtergrond van de persoon die wordt onderzocht.”
Ook auditing heeft met betrouwbaarheid en validiteit te maken. Ben je als auditor tevreden als er is vastgesteld dat voldaan wordt aan normen en procedures (ook een methode)? Meet je dan wat je denkt te meten, met uitzicht op een adequate beheersing van risico’s? Dergelijke vragen kunnen niet omzeild worden.

Beter zicht op de werkelijkheid?
Een kritische houding impliceert dat je vanuit een professionele zorgvuldigheid als wetenschapper, maar ook als auditor, dus oog zal moeten hebben voor de beperkingen van de methode, bijvoorbeeld om begrippen te operationaliseren. Schipper: “Een oplossing is dan al snel transparantie: maak zichtbaar welke methode gehanteerd wordt. Dit is helaas ook niet voldoende. Een transparante methode is niet per definitie een goede. Ook de gedachte dat met het volgen van een methode de werkelijkheid zelf transparant wordt is te simpel. Er is altijd het risico van pseudotransparantie. Immers, welke methode je ook kiest (gestructureerd interview, kwantitatief onderzoek, statistische bewerkingen, et cetera), ook deze keuze blijft een oordeel. Hierdoor is het niet uitgesloten dat we te maken hebben met een schijnwerkelijkheid. De financiële crisis heeft dat extra duidelijk gemaakt. Methoden zijn nodig, maar dat geldt ook ten aanzien van een gezond wantrouwen met betrekking tot elke gehanteerde methode. Het volgen van methoden, procedures, et cetera, is uiteindelijk een kwestie van een keuze. Wetenschappers en auditors moeten daarom bereid zijn wat ze doen steeds kritisch te bezien en te verantwoorden in het licht van de concrete situaties waarin zij werken.”

Wetenschap en auditing is een kunst
Onderzoek blijft daarmee een kunst, gebaseerd op een oordeel, welke methode je ook kiest. Deze uitdaging geldt wellicht nog meer voor auditors dan voor wetenschappers. Schipper wijst hierbij op het boek *The Philosophy of Auditing*[1]: ‘…the auditor must frequently be content with something less than the best possible evidence pertinent to a given problem, whereas the scientist can be satisfied only if he is confident that he has conclusive evidence…’ (pag. 30).

Noot
1. Mautz, R.K. en H.A. Sharaf, *The Philosophy of Auditing*, American Accounting association, 1981.

Wat kunnen we leren van de mesologie?

Zijn er raakvlakken tussen de onderzoeksaanpak van een mesoloog en die van een internal auditor? De redactie ging op onderzoek uit en sprak met Rob Muts van de Academie voor Mesologie.

Een interview in het populaire lifestyle magazine *Happinez* met Rob Muts, grondlegger en boegbeeld van de mesologie, en het feit dat deze beroepsorganisatie van mesologen door de Consumentenbond is beoordeeld op kwaliteit en daarbij de hoogste score heeft behaald, triggerde ons om te kijken of er raakvlakken zijn tussen de onderzoeksaanpak van een mesoloog en van een internal auditor.

Mesologie in een notedop
Mesologie is een vorm van geneeswijze die reguliere kennis combineert met alternatieve geneeswijzen. De mesologie is gebaseerd op de westerse geneeskunde, maar ook op de traditionele Chinese geneeskunde en Ayurveda (India), homeopathie, kruidenleer en orthomoleculaire geneeskunde, electrofysiologische diagnostiek, de filosofie en psychologie. Meso is Grieks voor ‘midden’, mesologie positioneert zich dan ook tussen de reguliere en alternatieve geneeswijzen.

Generalisten versus specialisten
“De reguliere westerse geneeskunde kent een lange traditie. In die traditie zijn veel protocollen ontwikkeld om acute problemen (ongeveer 30 procent van de klachten), bijvoorbeeld bij een hartinfarct of een ontsteking, het hoofd te kunnen bieden. En die protocollen hebben hun nut door de jaren heen ruimschoots bewezen”, zo begint Muts. “Maar soms blijken de testen in de protocollen niet altijd toereikend of past een patiënt met zijn klachten simpelweg niet goed in de protocollen. Bij meer chronische klachten blijken die checklisten bijvoorbeeld veel minder bruikbaar en wordt vaak geen echte oorzaak gevonden. Klachten worden soms als

psychosomatisch afgedaan. Maar met een andere bril op je neus zie je ook andere dingen…”

De mesoloog is volgens Muts een generalist daar waar de reguliere geneeskunde zich heeft doorontwikkeld tot een vakgebied van specialisten. Daarbij steunt de specialist in zijn analyse zwaar op het gebruik van apparatuur. En als de specialist met zijn beschikbare apparatuur geen problemen kan vaststellen, dan is het dus geen probleem. Daarbij komt dat ook de alternatieve geneeskunde zich meer is gaan specialiseren, daar waar ze eigenlijk de rol van generalist vertegenwoordigt. Een manueel therapeut bijvoorbeeld kijkt met zijn bril niet veel verder dan de wervelkolom. In de westerse acupunctuur worden ook veel protocollen gebruikt, in tegenstelling tot de traditionele acupuncturist op het platteland in China. Ook in de grote steden van China is hun traditionele geneeskunde ‘verwesterd’.

Preventief werken!

“In de Chinese en Indiase traditie werd primair ingestoken op preventie. De geneesheer werkte in dienst van de landheer van de commune. De landheer wilde de arts alleen betalen als alle bewoners gezond waren en arbeid konden leveren. De arts werkte dus vooral preventief om in zijn eigen levensonderhoud te kunnen voorzien. Bij kleine klachten of symptomen werd de arts al ingeschakeld. Om preventief te kunnen werken had hij een generalistische aanpak nodig. Heel anders dan in onze huidige westerse cultuur. Wij wachten zolang mogelijk voordat wij naar een (huis)arts of therapeut gaan.”

Alle lichaamsfuncties onder de loep

In de eerste fase van het onderzoek kijkt de mesoloog naar het geheel en maakt hij een analyse van de diverse lichaamsfuncties. Hoe gezond voel jij je, hoe gedraag jij je of hoe is je spijsvertering op een schaal van 1 tot 10? De reguliere arts kijkt daarentegen meer naar absolute getallen (cholesterolgehalte, bloeddruk, ijzer in bloed). De mesoloog stelt aan de hand van vele metingen vast welke functies afwijkingen vertonen. Naast pols- en tongdiagnostiek en lichamelijk onderzoek, meet de mesoloog een groot aantal acupunctuurpunten op het lichaam. Pas daarna vraagt de mesoloog naar de klachten van de patiënt en probeert hij een verband te vinden tussen de klachten en de afwijkende functies. Muts: “Eigenlijk hebben de afwijkende functies altijd met elkaar te maken. Dat kan ook niet anders want het betreft functies binnen een en hetzelfde lichaam. Het is één systeem waarbij de functies onderling met elkaar in verband staan.”

Disfuncties om te overleven

Dan komt de volgende fase. “In deze fase richt de mesoloog zich op het waarom van de disfuncties. Elk organisme heeft namelijk een zelfregulerend vermogen. Dat gaat soms heel ver. Sommige aanpassingen noemen wij overigens een ziekte. Maar waarom zijn deze disfuncties ontstaan? Wat is het doel ervan? Waarom is dit gebeurd? Welke aanpassing heeft het lichaam nodig? Ofwel, wat is de functie van de disfunctie? Want alleen het organisme dat zich weet aan te passen zal overleven. Volgens Darwin gaat de ‘survival of the fittest’ niet over de sterkste maar over degene die zich het best weet aan te passen”, aldus Muts (zie *kader*).

Voorbeeld: de disfunctie

Iemand komt bij de mesoloog met klachten over zijn heup. Dit gewricht doet zeurderig pijn bij het lopen, hij kan er moeilijk op staan. De pijn zit niet op de lijn waar zenuwen lopen. Lokaal onderzoek van de heup wijst eigenlijk niets uit, afgezien van het feit dat het gewricht als geheel wat stijf is.
Nader onderzoek laat zien dat een stuk darm opgezet is, met gassen erin. Metingen in de darm tonen aan dat er een andere darmcultuur actief is. De mesoloog meet een disfunctie in de darm en de klacht is een pijnlijke heup.

Eigenlijk is dit een eenvoudig voorbeeld want de darm en de heup zitten heel dicht tegen elkaar aan en daartussen lopen heel veel bloedvaten. Door een verminderde doorbloeding van de heup krijgt de darm onvoldoende voeding en kan deze bovendien de afvalstoffen niet goed kwijt. De heup raakt hierdoor ‘vergiftigd’ en kan daardoor sneller slijten.
De oplossing richt zich dus ook niet op de heup zelf maar op de bacteriecultuur in de darm. Het voedingspatroon van deze persoon moet (waarschijnlijk) worden aangepast om het probleem in zijn heup op te heffen. Dit is geen normaal logische gedachte in onze westerse maatschappij.

Bewustwording versus het kopen van een aflaat

De derde stap richt zich op de therapie. Daar heeft mesoloog Muts ook een duidelijke mening over. “Boeddhistisch gesteld heeft elk mens een ziel die in een enorme bak met cellen is neergedaald, om het zo maar voor te stellen. Vervolgens heb je de verantwoordelijkheid om als chauffeur met je voertuig van de wieg naar het graf te rijden. En als er iets aan mankeert moet je dus ook met je eigen disfunctie(s) (zelf)bewust omgaan. Of dit nu een psychologisch of een lichamelijk probleem is. Het gaat, zoals eerder gezegd, om de survival of the fittest: met een aanpassing moet je proberen verder te komen in je leven. Dat geldt voor iemand die een hartaanval heeft gehad maar ook voor iemand met een disfunctie in zijn darmcultuur die zijn eetpatronen moet aanpassen.
Preventie is dus jezelf aanpassen aan de omstandigheden. Dat is je eigen verantwoordelijkheid! En dat strookt niet altijd met de opvattingen in onze huidige maatschappij. Mensen willen alles kunnen doen zonder ziek te worden of daar een beperking aan over te houden. En ze zijn bereid om daar fors voor te betalen. In Duitsland worden voor veel geld integrale scans aangeboden om maar vast te stellen dat een persoon niets mankeert. Ik noem dat een moderne aflaat: ‘als er een probleem is in een van mijn lichaamsfuncties moet de geneeskunde het maar voor mij oplossen want ik wil mijn levensritme niet aanpassen’. Echter, juist in die aanpassing zit de preventie. Dat vraagt dus om bewustwording.”

Zelfdiagnose werkt niet!
"In de geneeskunde heb je altijd een externe nodig om een diagnose vast te stellen. Een zelfanalyse werkt simpelweg niet. Er zijn zolang we kunnen opmaken uit de overleveringen altijd medicijnmannen geweest. Niemand is blijkbaar in staat om zelf vast te stellen wat de problemen zijn en wat daaraan gedaan zou moeten worden. Je kunt het simpelweg niet zelf vaststellen. Dat is blijkbaar de prijs van de hersenen. Ons instinct is te zeer ingekapseld door een dikke deken met hersenen. Dieren luisteren daarentegen wel primair naar hun instinct. Dat maakt een groot verschil."

Mesologie versus Internal Audit
Geconcludeerd kan worden dat er best wat raakvlakken zijn tussen de onderzoeksaanpak van de mesoloog en die van de internal auditor.

- Internal auditors investeren net als de mesoloog tijd in het 'leren kennen' van hun object van onderzoek zodat waarnemingen in de goede context kunnen worden geplaatst. Dit is essentieel bij het onderzoeken van de oorzaken en het formuleren van realistische aanbevelingen.
- Veel van het internal auditonderzoek is vastgelegd in dikke protocollen en checklisten. Maar het meest boeiende deel van ons vakgebied, waarmee wij ook de hoogste toegevoegde waarde kunnen leveren aan onze opdrachtgevers, zit in het onderzoek naar de kwaliteit van beheersing in de organisatie – wat nog niet eerder is gedaan en nog niet is uitgekauwd. Standaardprotocollen en checklisten blijven daarbij achterwege en een maatwerkoplossing moet worden gezocht en gevonden. Een meer generalistische aanpak is daarbij een voorwaarde.
- Binnen ons vakgebied kennen wij naast generalisten ook specialisten die bijvoorbeeld alles afweten van specifieke regelgeving (compliance) binnen een bepaalde branche. De generalist en specialist zijn net als in de geneeskunde complementair aan elkaar!

Mesologen hebben zich verenigd in de Nederlandse Vereniging voor Mesologie (NVVM). Gediplomeerde mesologen staan geregistreerd bij het Nederlands Register voor Mesologen (NRM). Voor meer informatie over de behandeling en therapeuten kunt u terecht op www.mesologen.nl. Voor de opleiding gaat u naar www.mesologie.nl.

Tegenspraak bij de Koninklijke Marechaussee

Wat is tegenspraak? Wanneer gaat een onderzoeksteam 'tunnelen'? Wat zijn maatregelen om objectiviteit van opsporingsonderzoeken te waarborgen? Een gesprek met majoor Bart Hulsbosch over onderzoekmethoden bij de Koninklijke Marechaussee en de ontwikkelingen op dit gebied.

Sinds de Schiedammer Parkmoord hebben de onderzoekmethoden een grote ontwikkeling doorgemaakt, aldus Bart Hulsbosch, voorheen commandant van een brigade Recherche en Informatie in het district West van de Koninklijke Marechaussee en tegenwoordig commandant van de brigade Zuid-Holland in hetzelfde district. Het openbaar ministerie, de politie en het Nederlands Forensisch Instituut (NFI) hebben een verbeterprogramma opgesteld naar aanleiding van het evaluatierapport van de Schiedammer Parkmoord.
"In het programma 'Versterking van opsporing en vervolging' staat de doorlopende bevordering van de professionaliteit van het optreden van politie en OM in strafzaken centraal. Het programma heeft zich primair gericht primair op de kwaliteit van de waarheidsvinding in het proces van opsporing en vervolging." Vanuit de taakstelling van de Koninklijke Marechaussee hebben Hulsbosch en zijn mensen dagelijks met de maatregelen uit dit verbeterprogramma te maken.

Tegenspraak
Tegenspraak is een van de methoden om het risico van tunnelvisie en groepsdenken in een onderzoeksteam te beperken. Tegenspraak is het intern georganiseerd, doorlopend toetsen van beslissingen

Reflectie – tegenspraak – review

Reflectie is het dagelijks ter discussie stellen van oordelen die ten grondslag liggen aan belangrijke beslissingen in de opsporing en vervolging. Reflectie behoort dan ook onderdeel uit te maken van de reguliere werkprocessen binnen opsporing en vervolging. Zolang dit nog niet tot in de diepste krochten van de rechercheculture is ingedaald, blijft de noodzaak van de georganiseerde vormen *tegenspraak* en *review* bestaan. In de gevallen dat een rechercheonderzoek vastloopt of dreigt vast te lopen, moet het onderzoek aan een review worden onderworpen. Een review is een diepgaande herbeoordeling van alle onderzoeksinformatie en de daarop genomen beslissingen in zowel de opsporings- als de vervolgingsfase.

door niet bij het onderzoek betrokken medewerkers. De organisatie van tegenspraak is in het verbeterprogramma 'Versterking opsporing en vervolging' beschreven in de vorm van de driedeling reflectie – tegenspraak – review (zie *kader*).
Hulsbosch: "Reflectie en tegenspraak vragen om een enorme cultuurverandering. Feedback geven en ontvangen dient hiervoor in de haarvaten van de organisatie en haar mensen te zitten. In een hiërarchisch opgebouwde organisatie als de KMar dient hier aandacht aan besteed te worden."

De 'gouden W-vragen'
Een opsporingsonderzoek krijgt inhoudelijk vorm aan de hand van de 'gouden W-vragen':
1. Wie kan in verband worden gebracht met het misdrijf?
2. Wat is er precies gebeurd?
3. Waar heeft het misdrijf plaatsgevonden en waar zijn de sporen achtergebleven?
4. Waarmee is het misdrijf gepleegd?
5. Op welke wijze heeft het misdrijf plaatsgevonden?
6. Wanneer heeft het misdrijf plaatsgevonden?
7. Waarom heeft het misdrijf plaatsgevonden?

Risicomanagement
Risicomanagement wordt nadrukkelijk toegepast in het opsporingsmodel. Hulsbosch: "Daarnaast dient consequent in hypothesen en scenario's te worden gedacht. Zo lang nog geen bewijsmateriaal voorhanden is, blijven alle scenario's opportuun. Vrijkomende informatie wordt in de verschillende scenario's geplaatst, waardoor sommige meer voor de hand liggen dan andere. De uiteindelijke keuzen dienen expliciet te worden genomen, zodat een audittrail beschikbaar is."

Overeenkomsten met audit
Hulsbosch ziet in zijn werk meer overeenkomsten dan verschillen met audit. "Waar het recherchewerk toch vooral repressief van aard is kan audit meer preventief werk verrichten. Beide vakgebieden hanteren een risicogebaseerde aanpak. Auditors en opsporingsambtenaren kunnen voor betrokkenen aan de andere kant van de tafel bedreigend overkomen. De 'standaard' houding van een opsporingsambtenaar is vaak de oorzaak van deze reactie." Hulsbosch benadrukt dat auditors en opsporingsambtenaren met de juiste houding en gedrag hun inhoudelijke werk effectiever vorm kunnen geven.

De politieacademie leidt medewerkers zelfs op om de rol van tegenspreker bij onderzoeken te vervullen

Concluderend: de overeenkomst tussen onderzoekmethoden bij de Koninklijke Marechaussee en Internal Audit is vooral te vinden in de constante zoektocht naar objectiviteit. Hoewel auditors bij een 'verkeerd' oordeel niemand onterecht een gevangenisstraf bezorgen, zouden de principes van reflectie en tegenspraak wellicht een aanwinst zijn voor het auditproces. De politieacademie leidt medewerkers zelfs op om de rol van tegenspreker bij onderzoeken te vervullen.

Personalia

Berichten kunt u mailen naar iia@iia.nl

Edward Roozenburg is per 1 april 2009 werkzaam als adviseur concerncontrol en organisatieontwikkeling bij de Sociale Verzekeringsbank (SVB). Daarvoor werkte hij bij de Algemene Rekenkamer.

Johan Veldhuis werkt sinds 1 mei 2009 als internal auditor bij Aegon Nederland. Hij was daarvoor werkzaam als internal control auditor bij Cordares.

Per 1 mei 2009 is **Ron Beumers** werkzaam bij ICTU. Voorheen werkte hij bij de Raad voor de rechtspraak.

Bent u een internal (fr)auditor?

Drs. J.H.A. van Vliet RA CFE*

Ligt u ook wel eens wakker van al die berichten in de media over fraudes bij bedrijven en publiekrechtelijke lichamen? Nee? Gelukkig maar, dat zou immers toch niet helpen. U kunt er beter voor zorgen dat u 's morgens vol energie en met een scherpe blik uit bed stapt om fraudeurs te stoppen.

Er bestaan grofweg twee soorten fraudeurs. Het eerste type fraudeur profiteert van een toevallige omissie in de administratieve organisatie en interne beheersing (AO/IB). Om daadwerkelijk tot fraude over te gaan is naast de gelegenheid om te frauderen veelal ook sprake van druk en rationalisatie (zie bijvoorbeeld ook NV COS240). Druk kan ontstaan door geldproblemen of een te hoge levensstandaard. Rationalisatie is als het ware het excuus voor de fraude en kan ontstaan uit onvrede over het salaris of verkeerd voorbeeldgedrag van bijvoorbeeld de directie.
Bij het andere type fraudeur is de druk en rationalisatie veelal al aanwezig en gaat hij of zij actief op zoek naar de gelegenheid om te frauderen. Fraude veroorzaakt door het tweede type fraudeur is veelal veel moeilijker te ontdekken. De fraudes zijn meestal complexer van aard en beter verborgen in (de administratie van) de organisatie. Deze fraudeurs bedenken creatieve oplossingen om bestaande AO/IB-maatregelen te omzeilen of ervoor te zorgen dat deze niet effectief zijn.

Maar hoe komt u nu een mogelijke fraudeur op het spoor? Voor het ontdekken van beide type fraudeurs is het belangrijk dat u als internal auditor een kritische houding (professional scepticism) heeft. Wat houdt deze kritische houding in? U dient te onderkennen dat ook binnen uw organisatie mogelijk sprake is van fraude. Bij uw dagelijkse werkzaamheden dient u een vragende houding aan te nemen. U moet zich continu afvragen of hetgeen u aantreft wel past binnen uw organisatie. De verkregen antwoorden op gestelde vragen dient u nauwgezet op hun merites te beoordelen. Neem hierbij geen genoegen met een half antwoord, een ontwijkend antwoord of zelfs helemaal geen antwoord. Ditzelfde geldt natuurlijk ook voor verkregen controle-informatie. Het is van belang dat u steeds het geheel van feiten en omstandigheden beoordeelt en u zich hierbij de vraag stelt of verschillen, onduidelijkheden of andere gebeurtenissen het gevolg kunnen zijn van fraude. Houd hierbij in gedachten dat de fraudeur altijd zal proberen de fraude te verhullen. Hij of zij zal immers niet ontdekt willen worden.

Een ander belangrijk punt om fraude te voorkomen of te ontdekken is het hebben van een goede frauderisicoanalyse. In een frauderisicoanalyse onderzoekt u waar uw organisatie kwetsbaar is voor fraude. Deze kwetsbaarheid kan ontstaan door de gevoeligheid van processen.
Bijvoorbeeld: het opslagproces van dure elektronica-artikelen is kwetsbaarder dan het archiveringsproces. De kwetsbaarheid kan ook ontstaan door een gebrekkige AO/IB.
Om de kwetsbaarheid van uw organisatie inzichtelijk te maken, zou u zich in de fraudeur moeten verplaatsen. Kruip in zijn of haar huid en verzin zoveel mogelijk manieren waarop u zelf binnen uw eigen organisatie zou kunnen frauderen. Geef uw creatieve geest de ruimte. Schuif potentiële mogelijkheden niet opzij omdat u denkt dat deze mogelijkheid door interne controle wordt afgedekt. Een fraudeur zal dat ook niet doen! Hij of zij zal juist proberen deze controle te ontwijken of ervoor zorgen dat deze niet effectief is.
Vraag vervolgens uw collega's ook op deze wijze een lijst samen te stellen. Daarna kunt u de mogelijkheden gezamenlijk bespreken. Waarschijnlijk zult u verbaasd zijn over het aantal mogelijkheden voor fraude. Mogelijk bent u nog verbaasder over uw eigen creativiteit of die van uw collega's. Als u de gezamenlijke lijst heeft samengesteld, is dat niet het punt om alsnog wakker te gaan liggen. Zoals gezegd, dat helpt toch niet. Het is juist tijd om tot actie over te gaan. Niet om de mogelijkheden van fraude in daden om te zetten, maar om de fraude op te sporen of te voorkomen.
Door periodiek in de huid van een fraudeur te kruipen krijgt de functie van internal auditor een nieuwe dimensie, namelijk die van internal frauditor. Uw organisatie zal er sterker door worden en beter bestand zijn tegen potentiële fraudeurs.

* Jurgen van Vliet is manager bij Deloitte Forensic & Dispute Services

Deloitte.

Inspired & Insightful

It's a promise.

Risk Advisory. Finance Management. As the business challenges facing our clients continue to grow, so do our service offerings and areas of expertise. Inspired by their needs, we design our insightful solutions to provide the right people and processes to resolve even the most complex issues. That's our promise to our clients - and to you.

We are Jefferson Wells

To learn more about the Jefferson Wells difference visit www.JeffersonWells.com

JEFFERSON WELLS™
A Manpower Company

Plaza Arena, gebouw Apollo
Herikerbergweg 9
1101 CN Amsterdam Z.O.
Tel. 020-3468900

RISK ADVISORY | TAX | FINANCE MANAGEMENT

Scheme audit voor de OV-chipkaart

Trans Link Systems (TLS) is in 2001 opgericht om het OV-chipkaartsysteem te realiseren. Een bedrijfsmodel, het 'scheme', dient om de realisatie bij alle deelnemers te faciliteren en is tevens het normenkader voor de scheme audit. Hoe worden met behulp van audit aspirant-deelnemers beoordeeld voor toelating en is toezicht mogelijk over de keten voor het elektronisch betalen in het OV?

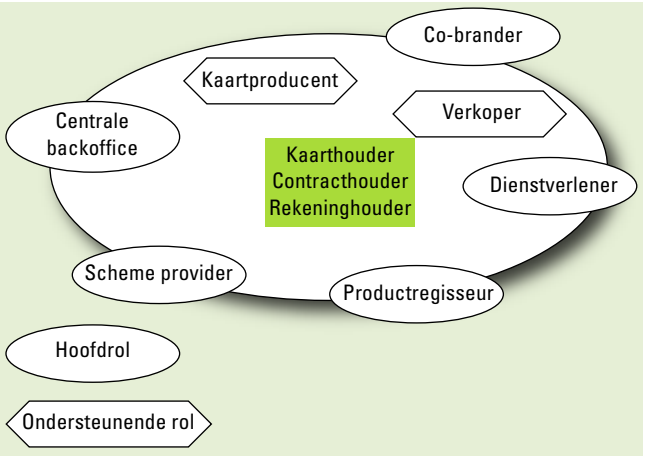
Drs. A.C. Ruoff EMIA RO CIA

Trans Link Systems (TLS) is een joint venture, opgericht door openbaar vervoer (OV-)bedrijven voor het realiseren van een elektronisch betaalsysteem in het Nederlandse openbaar vervoer met behulp van de OV-chipkaart. Primair bevat de OV-chipkaart het elektronisch saldo waarmee kaarthouders hun OV-reis kunnen betalen. Secundair kunnen reisrechten (proposities) zoals korting, vooraf gespecificeerde reizen en abonnementen worden gedefinieerd en op de kaart worden geladen.

Scheme

De aangesloten en aan te sluiten OV-bedrijven en TLS zijn deelnemers van de OV-chipkaart. Voor de samenwerking tussen de deelnemers is in samenhang met de bestaande contracten een bedrijfsmodel gebouwd dat de naam 'OV-chipkaart Scheme' (verder: het scheme) draagt. Het scheme kent rollen, regels per rol, regels voor algemene beheersprocessen, voor informatiebeveiliging en voor bescherming van persoonsgegevens. Een van de hoofdrollen van TLS, de rol van scheme provider, is verantwoordelijk voor het onderhouden van het scheme en het toezien op de naleving van het scheme. Deze rol ondersteunt de realisatie van een gelijkwaardige en objectief toetsbare samenwerking en het beheersen van mogelijke afbreukrisico's. De voorwaarden hiervoor zijn in het normenkader verder uitgewerkt.

Naast de rol van scheme provider zijn in het scheme andere rollen vastgelegd die overeenkomen met bedrijfsfuncties die nodig zijn voor het realiseren van de OV-chipkaart en het betaalsysteem. Zo vervullen de OV-bedrijven onder andere de rollen van 'dienstverlener' (of vervoerder) en 'verkoper'. TLS vervult naast de rol van scheme provider de hoofdrollen van 'kaartuitgever' en 'clearing operator', die onderdeel zijn van de centrale backoffice (zie *figuur 1*).



Figuur 1. De rollen in het scheme

Normenkader

Het scheme is vastgelegd in a) het *Handboek Regels en Procedures* (HRP), in b) de specificatie van de open architectuur (SDOA) en in c) een set van voorgeschreven parameterinstellingen van de apparatuur (registrar document). Met name de organisatorische afspraken die zijn vastgelegd in het HRP zijn een weerslag van contractueel overeengekomen, voor alle partijen gelijkluidende, regelingen. Deze zijn deels verder uitgewerkt in regels c.q. normen, die in gezamenlijk overleg zijn goedgekeurd. Deze zijn op alle deelnemers van toepassing, hoewel afhankelijk van de gekozen rollen. Bepaalde hoofdstukken gelden voor elke deelnemer, zoals informatiebeveiliging. Andere zijn rolafhankelijk, zoals die voor de 'verkoper' en 'kaartproducent' – en dus alleen van toepassing als een partij de betreffende rol voor de OV-chipkaart

invult. Sommige hoofdstukken zijn afhankelijk van het hebben van apparatuur, zoals configuratiebeheer.
De realisatie van de samenwerking en de beheersing van afbreukrisico's worden in het scheme ondersteund door drie kernwaarden, te weten:

- *Interoperabiliteit*: dit aspect geeft aan in welke mate de OV-chipkaart bij alle apparatuur van de deelnemers gebruikt kan worden (kaartinteroperabiliteit), in welke mate interoperabele producten (reisrechten) tegen gelijke voorwaarden gebruikt kunnen worden (productinteroperabiliteit) en in welke mate systeemcomponenten gekoppeld kunnen worden aan die van andere leveranciers (systeemcompatibiliteit).
- *Integriteit*: dit aspect geeft aan in welke mate de gegevens in het OV-chipkaartsysteem in overeenstemming zijn met de werkelijkheid (data-integriteit) en in welke mate vergelijkbare functies beheersbaar en vergelijkbaar werken, ongeacht tijd, plaats of deelnemer (procesintegriteit).
- *Vertrouwelijkheid*: dit aspect geeft aan in welke mate het gebruik van gegevens (persoonsgegevens en bedrijfsgegevens) behoorlijk en zorgvuldig is en beschermd is tegen onrechtmatig gebruik.

Op deze kernwaarden is het normenkader gebouwd. Het subsidiariteitsbeginsel is gehanteerd om te bepalen welke eisen vanuit de rol van de scheme provider worden voorgeschreven en welke vanuit de organisatiedoelstelling van de deelnemer zelf. Dat leidt ertoe dat de schemeregels vooral op effectiviteit zijn gericht en niet of in mindere mate op efficiëntie: de aspecten beschikbaarheid, tijdigheid en volledigheid zijn belangrijker voor iedere deelnemer zelf dan voor andere deelnemers. Daarom ligt de verantwoordelijkheid voor de bewaking van deze aspecten primair bij iedere deelnemer zelf.

Governance

Besturing en toezicht zijn georganiseerd in het directeurenoverleg OV-chipkaart (DOC) en in de raad van commissarissen (RvC). Het directeurenoverleg stuurt het gezamenlijk programma voor de nationale invoering van de OV-chipkaart aan. Via de RvC wordt naar de aandeelhouders verantwoording afgelegd.
Wijzigingen die gevolgen hebben voor het scheme worden in een aantal gremia besproken, afhankelijk van hun impact. Zo is er een klantenraad van advies (KRvA) die, zoals de naam aangeeft, alleen adviesrecht heeft. Het directeurenoverleg neemt besluiten of bekrachtigt besluiten die in een andere gremia, zoals in het business architecture council (BAC) binnen TLS en de Nationale Release Board (NRB) zijn genomen. De BAC beoordeelt wijzigingsaanvragen op hun impact. De NRB zorgt voor de afstemming en coördinatie tussen de betrokken partijen bij de realisatie en invoering. Binnen de RvC is het audit committee belast met het onafhankelijk toezicht op de activiteiten van TLS.
Nieuwe bedrijfsmodellen zijn mogelijk. Bij de opzet van de OV-chipkaart is niet uitgesloten dat de kaart en het erop geladen elektronisch geld voor andere toepassingen bruikbaar worden. In het normenkader zijn daar momenteel beperkte mogelijkheden voor die naar aanleiding van gewenste ontwikkelingen kunnen worden uitgebreid. Het governancemodel zorgt voor beoordeling en goedkeuring van nieuwe afspraken waarvan de behandeling is geregeld en vastgelegd in het wijzigingsproces. Het wijzigingsproces staat er garant voor dat wijzigingen in samenhang worden voorbereid, gecoördineerd en doorgevoerd. Daarnaast geeft het model de mogelijkheid om bij calamiteiten snel actie te kunnen nemen.

Aansluitingstoets en jaarplan

Partijen kunnen aansluiten nadat zij hebben aangetoond dat hun organisatie, processen en systemen in opzet en bestaan voldoen aan de in het scheme vastgelegde afspraken. De scheme auditor van TLS doet bij elke partij scheme audits, voorafgaand aan de introductie van de OV-chipkaart. Deze audits worden aangeduid als aansluitingstoetsen. Partijen komen in aanmerking voor toet-

Scheme audit ontleent elementen aan andere auditvormen

Operational audit	• Procesgericht onderzoek
IT-audit	• Informatiebeveiliging • Configuratiebeheer • Wijzigingenbeheer • Testmanagement
Financiële audit	• Volledigheid van opbrengsten, van transactieverwerking • Werkingstoets geeft zekerheid over een van tevoren bepaalde periode
SAS 70-audit	• Opzet/bestaan (type I) is vertaald in A-, B- en C-toets • Werking inclusief opzet en bestaan (type II) is vertaald in D-toets
Compliance-onderzoek	• Normen uit (onder andere) Wft, Wbp

Tabel 1. Vergelijking met andere auditvormen

sing indien zij het contract voor deelname hebben getekend en zij over gecertificeerde apparaten beschikken. Na aansluiting worden werkingstoetsen afgenomen. Onder andere op basis van de resultaten van de toets besluit de scheme provider, of en zo ja, op welk moment en onder welke voorwaarden een partij haar OV-chipkaartsystemen en -organisatie op het landelijke systeem en ondersteuning mag aansluiten.
Het jaarplan scheme audit is de afgelopen jaren primair afhankelijk gesteld van de aansluiting van nieuwe deelnemers. Na de eerste introducties in 2005 vormen zij immers het belangrijkste risico a) voor de bestaande deelnemers, b) voor de reizigers en c) voor de betrouwbare werking van de OV-chipkaart. Daarnaast wordt, waar de planning dat mogelijk maakt, toetsing uitgevoerd van de rollen van TLS zelf en van eerder aangesloten deelnemers. De aanleiding daarvoor is eveneens op risico's gebaseerd, bijvoorbeeld bij de introductie van nieuwe modaliteiten (trein naast bus, en dergelijke), nieuwe apparaattypen en samenwerkingsvormen. In de toekomst zal de toetsing verschuiven naar periodieke werkingstoetsen voor alle aangesloten partijen.

Auditobject

In afwijking van een reguliere (interne) audit voeren de scheme auditors de scheme audit uit bij alle partijen die willen deelnemen aan de OV-chipkaart en met gebruikmaking van hetzelfde normenkader. Dit zijn in aanvang de oprichters van de OV-chipkaart. Inmiddels zijn bijna alle OV-bedrijven in Nederland deelnemer of aspirant-deelnemer. OV-bedrijven kunnen de OV-chipkaart invoeren als 'dienstverlener'. Daarbij hoort de zorg voor gebruiksapparatuur, zoals poorten (metro, trein) en kaartlezers (bus, tram) voor het vastleggen van de in- en uitstapregistratie. Aan de hand hiervan vinden de prijsberekening en de betaling vanaf de kaart plaats.

Bij gebleken succes kunnen bepaalde functies ook door andere partijen worden uitgevoerd, zoals de verkoopfunctie die ook bij de traditionele strippenkaartverkoop door andere partijen is ingevuld. Ook zij zullen een overeenkomst voor deelname tekenen en vervolgens zijn zij in hun gekozen rol object van de scheme audit. Binnen de organisatie van de deelnemer zijn alle processen, organisatieonderdelen en systemen die door de invoering van de OV-chipkaart worden geraakt, onderdeel van het auditobject.

Audittechniek

Bij de keuze van auditmethoden en -technieken is gebruik gemaakt van diverse auditvormen en normenkaders (zie *tabel 1*).

Auditaspect

Bij het opzetten van het normenkader en de methodieken is gebruikgemaakt van de kenmerken van projectfasering. Het doel daarvan is om de aspirant-deelnemer al in een vroeg stadium additionele zekerheid te kunnen geven over de mate waarin hij voldoet aan de eisen die de samenwerking stelt. Gebleken is dat dit de doelgerichtheid van zijn projectaanpak, werkwijze en besluitvorming verbetert. De auditaspecten opzet, bestaan en werking zijn hiertoe expliciet gemaakt in de methodiek.

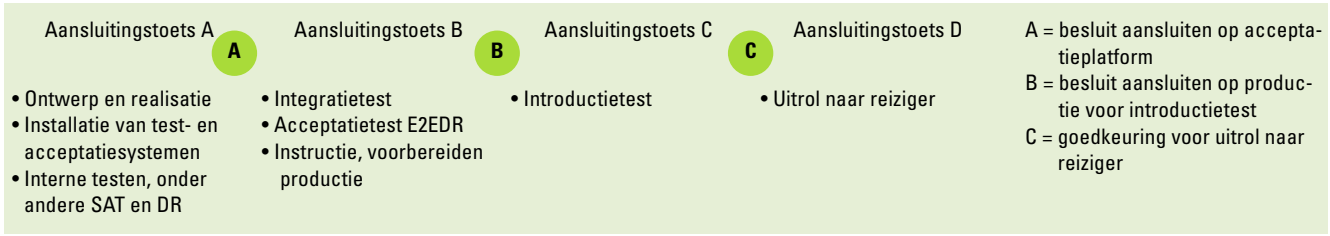
Operationalisering

De auditors hebben methodieken ontwikkeld op basis van het *HRP*, dat onderdeel is van het scheme. Bij de ontwikkeling van het handboek is de scheme provider de verantwoordelijke partij. De scheme auditor is behulpzaam door aan te geven waar gebruik kan worden gemaakt van (formuleringen uit) standaard normenkaders (Cobit, ITIL, COSO, ISO) of waar gebruikte formuleringen onvoldoende effectief, specifiek of meetbaar zijn.

De aansluitingstoets is een voorwaarde voor elke aspirant-deelnemer. De scheme provider besluit tot aansluiting op basis van het resultaat

Aansluitfase

In een projectmatige aanpak van de ontwikkeling van organisatie, processen en systemen voor de OV-chipkaart hanteren de deelnemers in het algemeen hun eigen projectaanpak die veelal is gebaseerd op een standaard, zoals Prince II. In zo'n aanpak worden onder andere de fasen van ontwerp, realisatie, test en invoering onderscheiden. Om op deze fasen te kunnen inspelen wordt in de eerste toetsing vrijwel uitsluitend onderzoek gedaan naar het ontwerpaspect (A-toets). In een volgende toetsing ligt de nadruk op het aspect 'bestaan'. In deze toets wordt bijvoorbeeld met behulp van testresultaten de verwachte werking van organisatorische en systeemtechnische maatregelen getoetst. De testfasen die de deel-



Figuur 2. De aansluitingstoetsen

nemer doorloopt zijn onderscheiden naar de reikwijdte en diepgang en zijn hierna vereenvoudigd aangegeven:

- een afnametest en een interne integratietest worden binnen de eigen organisatie uitgevoerd;
- een gezamenlijke testfase wordt in samenwerking met TLS uitgevoerd. Deze bestaat uit een technische integratietest en een procesgerichte acceptatietest;
- ten slotte volgt een introductietest waarbij de organisatie in productie gedurende een beperkte periode met gebruik van beperkende systeeminstellingen dient aan te tonen dat organisatie en systemen zich in productie gedragen volgens de gestelde verwachting.

De aansluitingstoets is gefaseerd, waarbij de keuze van het auditaspect in lijn is gebracht met de ontwikkelingsfase van de OV-chipkaartinvoering

Het onderzoek naar opzet en bestaan is verdeeld in twee stappen. In de B-toets, de eerste stap na de A-toets, worden de maatregelen beoordeeld zoals die binnen de eigen organisatie aantoonbaar zijn. Bijvoorbeeld of de betrokken medewerkers zijn getraind. In de tweede stap (C-toets) gaat het erom vast te stellen dat de maatregelen in samenhang met de organisatie van de centrale backoffice werken zoals verwacht werd op basis van de eerdere fasen. De toetsing van de werking (D-toets) vindt, analoog aan de aanpak bij SAS 70-onderzoeken, plaats over een van tevoren bepaalde periode, na de aansluiting van een partij. Daarbij wordt bijvoorbeeld gebruikgemaakt van operationele rapportages en van logs van het systeemgebruik en wijzigingen (zie *figuur 2*).

Auditrapport en -uitkomst

De rapportage is enerzijds bedoeld voor de scheme provider als ondersteuning bij de besluitvorming over de aansluiting van een (nieuwe) partij. De resultaten van werkingstoetsen dienen voor de scheme provider ter evaluatie van de naleving van het scheme door bestaande deelnemers.[1] Anderzijds is de rapportage bedoeld voor de (aspirant-)deelnemer om duidelijk te maken op welke punten verbeteringen zijn vereist om te voldoen aan het scheme. De bevindingen worden na het veldonderzoek aangeboden aan en afgestemd met de geauditeerde.

Van de deelnemer wordt verwacht dat hij een reactie formuleert op de in het onderzoek gedane en met de geauditeerde afgestemde bevindingen. Daarin geeft hij aan welke (additionele) maatregelen hij binnen een afgesproken termijn zal nemen ter oplossing van de gerapporteerde bevindingen. Deze reactie wordt opgenomen als een apart hoofdstuk in de definitieve versie van het rapport voordat het wordt verspreid onder de directies van de scheme provider en de 'deelnemer'.

Noot

1. Bevindingen over tekortkomingen in het scheme zelf, zoals ontwerpfouten, worden separaat gerapporteerd aan de scheme provider.

Fred Ruoff is scheme auditor bij TLS.
✉ fred.ruoff@translink.nl

C. Klumper RA MBA CIA

Buitenkansjes

Bijzondere onderzoeken zijn doorgaans buitenkansjes. Vaak ontstaan ze doordat de organisatie een acuut probleem dan wel een belangrijke zorg heeft waarvoor de expertise en (onafhankelijke) capaciteit van de internal auditafdeling dankbaar ingezet wordt. Een extra kans dus voor Internal Audit om te laten zien wat ze waard is.
Voorbeelden van situaties waarin een bijzonder onderzoek door Internal Audit gewenst kan zijn:

- geconstateerde of vermoede fraude;
- materiële fouten in (interne of externe) rapportages;
- opmerkingen vanuit een externe toezichthouder;
- vragen vanuit de raad van commissarissen;
- behoefte vanuit het management aan toetsing van de voortgang van een omvangrijk project.

Internal Audit is in dit soort situaties doorgaans zeer goed in staat om een deskundig en onafhankelijk onderzoek te doen en op basis daarvan adviezen te geven waarmee de organisatie haar voordeel kan doen. Immers, Internal Audit beschikt vaak over bedrijfsbrede en diepgaande kennis van de relevante processen, is getraind in het analyseren van problemen en het formuleren van mogelijke oplossingen en, misschien nog wel het belangrijkste, heeft geen direct belang bij de uitkomsten.
Tevens is Internal Audit relatief flexibel waar het gaat om de inzet van de medewerkers, zodat vaak op korte termijn capaciteit vrij te maken is.
Ook voor de medewerkers van de afdeling zijn bijzondere onderzoeken vaak een mooie gelegenheid om waardevolle additionele ervaringen op te doen.

Vaak is er sprake van hoge tijdsdruk en is het tegelijkertijd van groot belang dat het onderzoek grondig wordt uitgevoerd omdat van de uitkomsten veel kan afhangen. Niet zelden moeten alle zeilen worden bijgezet in termen van aanpak, projectplanning en creativiteit. Ten slotte is het goed mogelijk dat de uitvoering van het onderzoek bemoeilijkt kan worden, bijvoorbeeld wanneer er sprake is van tegengestelde belangen.

Als ik me de vele bijzondere onderzoeken voor de geest haal die ik zelf in de loop der jaren heb mogen doen, dan kan ik daar de volgende aanbevelingen uit distilleren:

- denk heel goed na over wat er precies bereikt moet worden;
- besteed nog meer aandacht aan de te volgen aanpak en de daarvoor in te zetten mensen en middelen;
- blijf flexibel, vraag je steeds af of de gevolgde aanpak wel de beste is; pas desnoods meerdere tactieken toe om er achter te komen wat het meeste resultaat oplevert;
- schakel bij al dit denkwerk liever te veel dan te weinig teamleden in;
- zorg voor voldoende ‘buffers’ in de planning;
- begin al in een relatief vroeg stadium met het formuleren van mogelijke hypothesen/conclusies waaraan de gevonden informatie getoetst kan worden;
- rapporteer kernachtig.

Aanbevelingen die in feite altijd relevant zijn...

De lokale overheid in beeld

In dit artikel over de lokale overheid beperken we ons tot de gemeenten. Deze bestuurslaag staat het dichtst bij de burger. Burgers merken het meest van veranderingen die binnen het gemeentelijke domein plaatsvinden. Zelden zullen ontwikkelingen bij provincies (Ceteco, Icesave) het 'gewone publiek' bereiken, laat staan in vervoering brengen. Het aantal ambtenaren dat bij gemeenten werkt is ook vele malen groter dan bij provincies of waterschappen. De gemeente is de meest transparante vorm van lokale overheid.

Drs. R.H.J.W. Jansen RO
A. Molenkamp RO

Ontwikkelingen op het vlak van governance en bedrijfsvoering lijken zich in gemeenteland eerder te manifesteren dan bij provincies. Bij gemeenten is verhoudingsgewijs veel meer gevolg gegeven aan de op artikel 213a GW gestoelde doelmatigheid- en doeltreffendheidonderzoeken (zie *kader*). In dit artikel besteden we aandacht aan het toezicht op het gemeentelijk handelen door de raad, in het bijzonder op de functie die de lokale rekenkamer in dat toezicht kan vervullen.

Professionaliteit taakvervulling door raad en college

De vraag die we in dit artikel willen beantwoorden is: hoe het staat met het 'horizontaal toezicht' binnen gemeenten, in het bijzonder waar het gaat om de controle op het handelen van de gemeenteraad en de gemeentelijke organisatie? Met andere woorden, welke maatregelen zijn er getroffen om objectief en onafhankelijk onderzoek te doen naar de wijze waarop de raad en het college van burgemeester en wethouders haar taken vervuld?

Artikelen in de gemeentewet

Artikelen in de gemeentewet die ingaan op de onderzoeksvormen die voor verschillende doeleinden in deze wet worden onderscheiden.

- Artikel 213a stelt dat het college van bestuur van de gemeente onderzoek uitvoert naar de doeltreffendheid en de doelmatigheid van het door hen gevoerde bestuur.
- Daarnaast kan ook de gemeenteraad volgens artikel 155 onderzoek uitvoeren naar het door het college gevoerde bestuur.
- Verder bestaat er een rekenkamer of rekenkamercommissie die volgens artikel 182 de rechtmatigheid, doeltreffendheid en doelmatigheid van het door het gemeentebestuur gevoerde beleid kan onderzoeken. De rekenkamer stelt zelf haar onderzoeksprogramma op. Ditzelfde artikel geeft aan dat de raad de rekenkamer(commissie) om een onderzoek kan verzoeken.

NB: Voor provincies geldt een soortgelijke opbouw in de Provinciewet.

Nederland kent verschillende vormen van lokale overheid. De belangrijkste van deze 'lagere' overheden zijn de provincies, de waterschappen en de gemeenten. Deze eenheden van bestuur zijn gelaagd opgebouwd. Onder het ministerie van Binnenlandse Zaken figureert de provinciale overheid; vervolgens zijn daaronder de gemeenten gepositioneerd. Een nieuwe bestuurslaag tekent zich af in de vorm van de zogenaamde Stadsregio's. Deze regionale overheden lijken zich, in weerwil van het ontbreken van adequaat beleid op dit punt, voorspoedig te ontwikkelen. Dat laatste is vooral aan de orde waar infrastructurele vraagstukken om een oplossing vragen, zoals in Haaglanden en binnen de regio Utrecht. Ook kunnen gemeenten ertoe overgaan om (bijvoorbeeld onder het construct van de 'gemeenschappelijke regeling' of anderszins) een bovengemeentelijke samenwerking aan te gaan.
Lokale overheden zijn in hoge mate autonoom. Veelal laten gemeenten niet na daarop te wijzen en gedragen zij zich dienovereenkomstig. Zowel Franssen (commissaris der Koningin in Zuid-Holland) als Jorritsma (burgemeester van Almere) benadrukken met enige regelmaat dat het Rijk een beperkte invloed heeft op de lokale overheden en zich dient te houden aan de gemaakte afspraken.

Een dergelijke reflectie is juist nu aan de orde omdat de invoering van het duaal systeem de raad en het college zou moeten nopen tot ander gedrag. De raad heeft in het duale stelsel nadrukkelijk de taak het gemeentelijke apparaat op doorvoering van het overeengekomen beleid te controleren. In de praktijk blijkt dat niet in alle gevallen de raad haar nieuwe taakinvulling voldoende inhoud geeft. Datzelfde geldt voor het functioneren van het college: er wordt aan getwijfeld of het college wel voldoende verantwoording aflegt aan de raad over de mate waarin het beleid is gerealiseerd en het gemeentelijke apparaat in control is qua rechtmatigheid, doeltreffendheid en doelmatigheid.

Incidenten kunnen leiden tot imagoschade

Een twijfelachtige verantwoording van het college aan de raad en een beperkte invulling van controle door de raad kan leiden tot incidenten die de landelijke pers halen. Het zijn vooral deze incidenten die bij het 'grote publiek' tot de verbeelding spreken. Voorbeelden daarvan zijn de Haagse Tramtunnel, de gemeente Amsterdam met de aanleg van de Noord-Zuidlijn, de gemeente Arnhem met het Stationsgebied, de gemeente Deventer met haar Fietstunnel en de gemeente Almelo met de verlening van vergunningen en de daarop gerichte handhaving.

De operationele bedrijfsvoering

De vraag dient zich aan hoe het proces verloopt om na de besluitvorming in de raad tot een realisatie van het geformuleerde beleid te komen, inclusief de verantwoording die daarover aan de raad moet worden afgelegd. Het heeft er alle schijn van dat de gemeentelijke overheid moeite heeft met de professionele invulling van de bedrijfsvoering; de door de raad genomen besluiten lijken in de uitvoering door het gemeentelijke apparaat te stranden op kwesties die mogelijk onvoldoende in de raadsbesluiten waren afgedekt. Ook is het mogelijk dat de eenmaal in gang gezette uitvoering van een project de politieke gemoederen blijft bezighouden.

Kennelijk wordt er, mede door de hiervoor genoemde oorzaken, onvoldoende onderscheid gemaakt tussen het (politieke) proces dat leidt tot een bepaald besluit en de operationele bedrijfsvoering voor de realisering van een op het beleid gestoeld project. Het college maakt daarbij schaars gebruik van de mogelijkheid onderzoek uit te (laten) voeren (volgens artikel 213a) om dit soort risico's beter te kunnen managen.

Toezicht op gemeentelijk handelen

In de praktijk blijkt de invoering van het dualisme slechts beperkt te hebben geleid tot een adequate controle van de raad op het handelen van het college. De afstemming tussen de gemeenteraad en het college blijkt, zoals aangegeven, niet altijd vlekkeloos te verlopen. Daarnaast hebben de uitvoerende diensten problemen om het benodigde kwaliteitsniveau te realiseren, een omstandigheid die nauwelijks lijkt door te dringen tot de raad want de informatievoorziening aan de raad is zeer beperkt. In ieder geval leiden vraagstukken op het gebied van kwaliteit, effectiviteit en efficiëntie niet tot de discussies in de raad die soms wel gevoerd zouden moeten worden. De raad kan vervolgens de wethouder en/of de betreffende afdelingshoofden vanuit haar controlerende rol verzoeken een nadere toelichting te geven in de raadsvergadering en de raadsleden in de gelegenheid te stellen hun vragen te adresseren. Het duale stelsel blijkt in de praktijk van alledag weerbarstig.

Middelen voor toezicht

De vraag dient zich aan over welke middelen de gemeenteraad kan beschikken om de taak – die haar via het dualisme is toebedacht – uit te oefenen.

Vanouds kent men de commissie voor de rekening, een orgaan dat het financiële reilen en zeilen van de gemeente, op basis van rapportages van de extern accountant, tegen het licht houdt. Andere, minder toegepaste middelen zijn het vragenuurtje in de wekelijkse raadsvergadering, het enquêterecht en het onderzoeksrecht van de raad. Zo initieerde de gemeenteraad van de gemeente Almelo begin 2009 een onderzoek naar de vergunningverlening en handhaving binnen de gemeente (zie www.almelo.nl).

Heeft de lokale rekenkamer toegevoegde waarde?

Tot nu toe is de beheersomgeving van de gemeente besproken. Hierna wordt verder ingezoomd op het toezicht dat op de besturing en beheersing van het gemeentelijk handelen kan worden uitgeoefend. We mengen ons daarmee in de lopende discussie over een instrument dat sinds januari 2006 behoort tot het wettelijk kader (gemeentewet) waarover de raad beschikt om zich in haar toezichthoudende taak te laten bijstaan. Het gaat om de lokale rekenkamerfunctie, en wel om kwaliteit van het functioneren daarvan. Een kwestie die de gemoederen in gemeenteland bezighoudt.

Het dualisme heeft slechts beperkt geleid tot een adequate controle door de raad

De vraag is wat in de praktijk als toegevoegde waarde van de lokale rekenkamer wordt ervaren. De belangrijkste partijen die daarop invloed hebben zijn de gemeenteraad, het college van B&W en de rekenkamer zelf.

De gemeenteraad

Voor de raad heeft de lokale rekenkamer de functie van een extra instrument in haar controlerende rol naar het college en het ambtelijk apparaat. Anders dan bij de overige instrumenten werkt de rekenkamer onafhankelijk en bepaalt deze, zo mogelijk na raadpleging van de raad, haar eigen onderzoeksagenda. Verzoeken van de raad tot het uitvoeren van een bepaald onderzoek hoeven dus niet te leiden tot daadwerkelijke uitvoering onder auspiciën van de lokale rekenkamer.

Klaar voor veranderingen?

Kijk voor meer informatie op www.ey.nl

Partners in Sport

ERNST & YOUNG
Quality In Everything We Do

De raad kan ook besluiten een eigen onderzoek te starten naar het gevoerde beleid (artikel 155) en hiervoor een externe partij benaderen. De uitbesteding van het onderzoek heeft vaak te maken met de omvang van het onderzoek in relatie tot de beschikbare capaciteit van de rekenkamer.

Het college van burgemeester en wethouders

Menigmaal is het gemeentelijke apparaat, als het gaat om de mate van bereikte efficiëntie dan wel effectiviteit, object van onderzoek door adviesbureaus of interne onderzoek- en evaluatie-instanties. Deze onderzoeken vallen, anders dan bij een onderzoek van de rekenkamer, onder de regie van het college of de raad. Het college heeft minder grip op de toetsende rol van de rekenkamer. Het ligt daarom voor de hand te veronderstellen dat bepaalde onderzoeken van de rekenkamer met argwaan zullen worden bekeken.

De beschikbare functies

Het college heeft verschillende functies tot haar beschikking om op een actieve wijze onderzoek te initiëren en daarmee invulling te geven aan '213a onderzoek'. Te denken valt hierbij aan het bureau statistiek, de afdeling beleidsevaluatie, de afdeling interne controle en de afdeling collegeonderzoek.

De afdeling statistiek, vooral voorkomend in de grotere gemeente, houdt zich bezig met het evalueren van beleid, terwijl de afdeling collegeonderzoek gericht is op doelmatigheid- en effectiviteitonderzoek. Daarnaast zijn er in de lijn ingebouwde feedbackmogelijkheden zoals peer reviews, self assessments van het management en de periodieke managementrapportages.

Naast de interne mogelijkheden wordt ook traditioneel veel gebruikgemaakt van de externe accountant en in mindere mate van de inzet van externe onderzoekers.

De rekenkamer(functie) zelf

Lokale rekenkamers dienen in beginsel zoveel als mogelijk te steunen op de resultaten van onderzoeken die door deze interne functies van de gemeente zijn bereikt. De lokale rekenkamer zal door haar onafhankelijke positie en de openbaarheid van haar onderzoeksrapporten in zekere mate als competitief voor het functioneren van de bestaande interne onderzoeksfuncties worden gezien. De mate van onafhankelijkheid, de beschikbare kennis en de ervaring zijn bepalend voor het succes van elke onderzoeksfunctie en dus ook voor de rekenkamer. Het succes van de rekenkamer is vooral af te meten aan de gedane verbetersuggesties om de kwaliteit van beheersing verder te verbeteren en de acceptatie en implementatie van de verbetersuggesties door het college en de ambtelijke leiding.

Rekenkamers en horizontaal toezicht

In dit artikel is vanuit de bestaande governancestructuur bij gemeenten aandacht geschonken aan de rol van de lokale rekenkamer. Deze rol staat momenteel stevig ter discussie omdat er veel verschillen bestaan in de effectiviteit van deze rekenkamers. Ondanks daarop gerichte wettelijke maatregelen zijn er in de praktijk veel verschillen te constateren tussen de rekenkamers. Daarbij gaat het zowel om de structuur, de taakstelling, de samenstelling en de kwaliteit van de bemensing als het feitelijk functioneren in termen van objectkeuze, onderzoeksaanpak en kwaliteit van rapporteren.

Ook zijn er verschillen in de wijze waarop rekenkamers steunen op de inrichting van de gemeentelijke organisatie, in casu de wijze waarop het horizontaal toezicht binnen de gemeente is georganiseerd. Een rekenkamer zou bijvoorbeeld beter kunnen functioneren als men rekening houdt met de getroffen maatregelen van interne controle en andere toetsing- en onderzoeksactiviteiten binnen gemeenten.

In de praktijk blijkt bijvoorbeeld dat rekenkamers procesaudits uitvoeren, terwijl deze eigenlijk onder de noemer van artikel 213a thuishoren. De rekenkamer zou zich meer moeten kunnen focussen op de meer beleidsmatige vraagstukken en hoe deze na de politieke besluitvorming worden geëffectueerd door de verschillende afdelingen van de gemeente.

Afsluiting

In het kader van toezicht op het gemeentelijk handelen is in dit artikel de rol van de lokale rekenkamer behandeld. Te constateren valt dat colleges het kennelijk nog steeds moeilijk vinden om de raad transparantie te bieden door verantwoording af te leggen over de realisatie van overeengekomen beleid. Deze raad neemt op haar beurt te weinig initiatief om het college en het ambtenarenapparaat te activeren en te bewerkstelligen dat zij adequaat wordt geïnformeerd over de voortgang in de beleidsrealisatie. Met andere woorden, er ligt voor de lokale rekenkamer nog een mooie taak in het verschiet. Die taak kan echter alleen succesvol worden uitgevoerd als de lokale rekenkamer zodanig is gepositioneerd en kwalitatief is toegerust dat zij in het gemeentelijk bestel de haar toe te meten toezichtfunctie kan realiseren.

In een volgend artikel wordt nader ingegaan op de discussie die momenteel in Nederland wordt gevoerd over de toegevoegde waarde, de bemensing en de onderzoeksaanpak van de rekenkamers.

Arie Molenkamp (l) is organisatieadviseur, auteur en opleider. Hij is verbonden aan de EMIA-opleiding aan de Universiteit van Amsterdam. Ronald Jansen werkt bij KPMG Advisory nv binnen een groep die zich richt op met Internal Audits, Risk & Compliance Services.

Managen van IA in dynamische tijden: meer doen met minder

De huidige economische omstandigheden leiden bij veel organisaties tot teruglopende omzetten en stevige druk op de kosten. Uit recente studies blijkt dat ook de budgetten van Internal Audit onder druk staan, waarbij de vraag welke toegevoegde waarde Internal Audit nu eigenlijk levert, sterker wordt. Dit artikel gaat in op de ontwikkelingen die in diverse studies[1] naar voren komen en geeft aangrijpingspunten voor internal auditors en kunnen als basis voor een actieplan dienen.

Drs. A. Man CIA

Naast de huidige economische omstandigheden is ook nieuwe regelgeving in aantocht, is riskmanagement zeker in grote organisaties vaak niet eenduidig belegd, blijkt het omgaan met 'emerging risks' in de praktijk lastig en blijft het gebruik van data-analyse en mogelijkheden van ERP-pakketten bij Internal Audit beperkt. Al deze ontwikkelingen hebben invloed op het werkpakket van de internal auditor. Kortom, de internal auditor moet meer doen met minder.

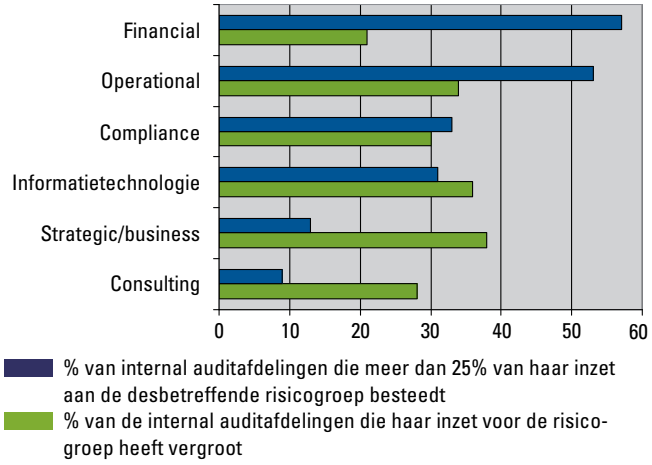
Noodzaak tot efficiencyverbetering

Onderzoek uit 2009 onder internal auditors in de VS toont aan dat de helft van de respondenten verwacht dat het internal auditbudget voor 2009 gelijk zal blijven, terwijl een derde een reductie verwacht. Respondenten uit Fortune 500-organisaties zijn nog negatiever: 51 procent gelooft dat er een medium tot hoog risico is dat de economische situatie tot een extra budgetreductie voor Internal Audit zal leiden. Uit onderzoek in het Verenigd Koninkrijk komt een iets positiever beeld naar voren: 21 procent verwacht een daling in budget en 29 procent verwacht dat het budget hetzelfde zal blijven. Dit onderzoek is gedaan binnen de bank- en kapitaalmarktsector. Cijfermateriaal ondersteunt dus de gedachte dat internal auditmanagers nog meer zullen moeten werken aan het vaststellen én uitdragen van de toegevoegde waarde van hun afdeling door efficiënter, slimmer en sneller te gaan werken.

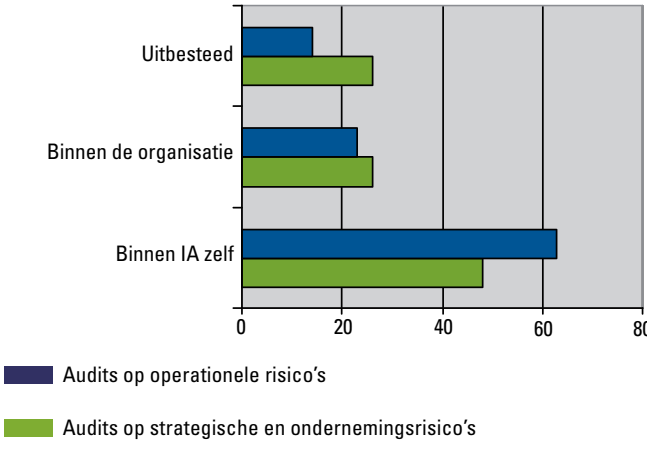
Afstemmen op de bedrijfsdoelstellingen

Ondernemingsrisico's[2] staan tegenwoordig in een scherper daglicht, zeker voor organisaties die buiten de landsgrenzen opereren. Risico's zijn toegenomen, maar ook meer uiteenlopend van aard. Emerging risks, die gezien ervaringen in het verleden lastig te voorspellen zijn, komen alomvattend tevoorschijn in diverse markten en economieën. Deze 'kleine-kans-grote-impact-risico's' met imperfecte informatie en ingewikkelde onderlinge afhankelijkheden manifesteren zich exponentieel binnen een korte tijdspanne. Het is noodzakelijk voor een proactieve internal auditfunctie om zich meer te richten op dit soort risico's en daarmee op veranderende prioriteiten en omstandigheden van het management. Uit meerdere onderzoeken komt naar voren dat er een verschuiving moet optreden van nadruk op risico's in de financiële rapportage naar risico's die de aandeelhouderswaarde kunnen ondermijnen. Strategische risico's en ondernemingsrisico's blijken dan ook een veel grotere bedreiging op te leveren voor de aandeelhouderswaarde dan operational, compliance of financiële risico's. Dit geldt met name voor grote organisaties, zoals FTSE 100- of Fortune 500-ondernemingen. Uit onderzoek komt naar voren dat strategische en ondernemingsrisico's goed zijn voor 60 procent van de afname in aandeelhouderswaarde, operationele risico's voor 20 procent, financiële risico's voor 15 procent en compliancerisico's voor 5 procent.

Als we dit tegen de tijdsbesteding van Internal Audit aanhouden dan blijkt dat het lastig is om de focus aan te passen aan daar waar het grootste risico ligt. Slechts 13 procent van de respondenten in het 2009-onderzoek gaf aan dat zij minstens een kwart van hun tijd aan strategische en ondernemingsrisico's besteden (zie *figuur 1*). Er is dus voor veel internal auditafdelingen nog een flinke stap te maken.



Figuur 1. Internal auditinzet per risicogroep (Bron: PwC 2009 #1)



Figuur 2. Verdeling inzet medewerkers (in procenten) (Bron: PwC 2009 #1)

Nieuwe aanpak voor kennismanagement en bezetting

Dat binnen Internal Audit essentiële stappen nodig zijn om de toegevoegde waarde van de functie te vergroten, mag voldoende duidelijk zijn. Maar het zou kunnen dat het realiseren van veranderingen belemmerd wordt door een gebrek aan kennis van de internal auditstaf van de genoemde risicogroepen en aan een gebrek aan ervaring en vaardigheden om al deze risicogroepen te doorgronden. Helaas is de perceptie dat Internal Audit de business niet begrijpt, dat zij zich slechts richt op details en daarmee meer last dan lust is, nog steeds bon ton bij bestuur en management. Maar misschien is dat ook wel echt zo. Het antwoord zal ook liggen in andere keuzen bij het rekruteren van medewerkers, gekoppeld aan een significante verbetering van kennismanagementvaardigheden.
Internal Audit zal attractief moeten zijn voor toptalent en zal de kennis van de primaire bedrijfsprocessen bij haar medewerkers moeten versterken.
Een substantieel deel van de internal auditstaf blijkt minder dan vijf jaar ervaring te hebben. En als we hieraan koppelen dat in grotere organisaties de afgelopen jaren veel aandacht is besteed aan Sarbanes Oxley-werkzaamheden, dan is duidelijk dat deze generatie bijsturing behoeft om de nieuwe realiteit en nadruk op bedrijfsbrede risico's anders dan gericht op financiële rapportages of compliance, serieus vorm te geven.

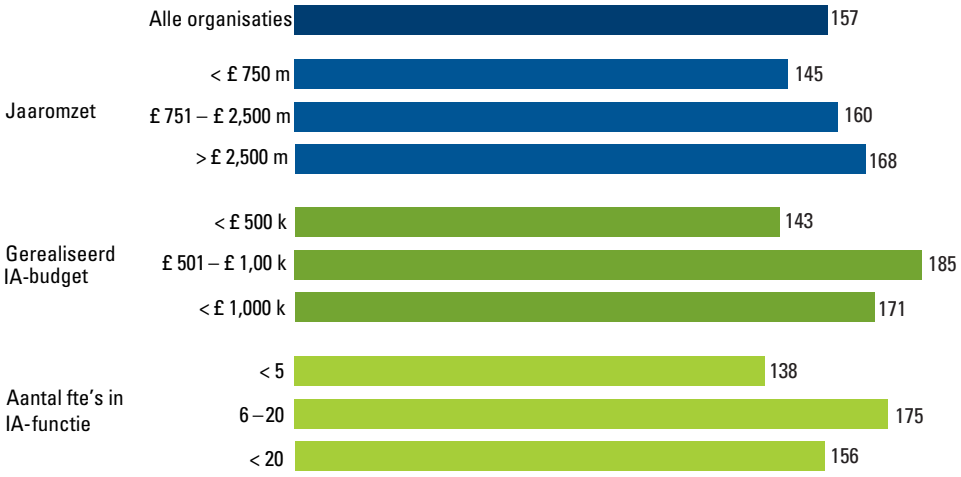
Chief Audit Executives en auditmanagers hebben gewoonlijk gedegen kennis van de markt en branch, (senior) auditors gewoonlijk beduidend minder:
- 79% van CAE's heeft acht jaar of meer ervaring;
- 59% van de managers heeft acht jaar of meer ervaring;
- 27% van de auditors heeft minder dan drie jaar ervaring;
- 31% van de auditors heeft drie tot vijf jaar ervaring;
- 25% van de auditors heeft vijf tot acht jaar ervaring;
- 17% van de auditors heeft acht jaar of meer ervaring.

De inzet van externe expertise is verschillend per risicogroep (zie *figuur 2*).

Meer aandacht voor ERP-systemen en data-analyse

In zijn algemeenheid zal het gebruik van technologie in tijden van economische teruggang een belangrijk middel zijn voor kostenreductie en productiviteitsverbetering. Dit levert voor Internal Audit echter een aantal implicaties op. In de eerste plaats omdat weinig auditors echt voorbereid zijn om in geautomatiseerde omgevingen te auditen met kennis van de systemen enerzijds en het gebruikmaken van datgene wat systemen aanleveren anderzijds. Verder geldt dat bedrijfsprocessen en de onderliggende technologieën continu evolueren, waardoor bestuur en management in toenemende mate verwachten dat Internal Audit zekerheid zal kunnen geven over deze systemen en technologie, gebruikmakend van geautomatiseerde controlomgevingen en continuous auditing tools.[3] Het omarmen van technologie op alle niveaus zal Internal Audit ertoe brengen dat zij haar toegevoegde waarde steeds meer in door technologie gedreven organisaties kan bewijzen, gekoppeld aan een toenemende productiviteit. Auditors spenderen gemiddeld 157 dagen per jaar aan auditing; dat is een bruto productiviteit van rond de 62 procent (zie *figuur 3*). Dat moet omhoog kunnen.
Uit het 2009-onderzoek blijkt dat de kennis over de technologie en automatisering binnen de organisatie bij niet-IT-auditors (gedefinieerd als auditors die minder dan 75 procent van hun tijd besteden aan IT-audits) niet groot is:

Internal Audit zal attractief moeten zijn voor toptalent en zal de kennis van de primaire bedrijfsprocessen bij haar medewerkers moeten versterken



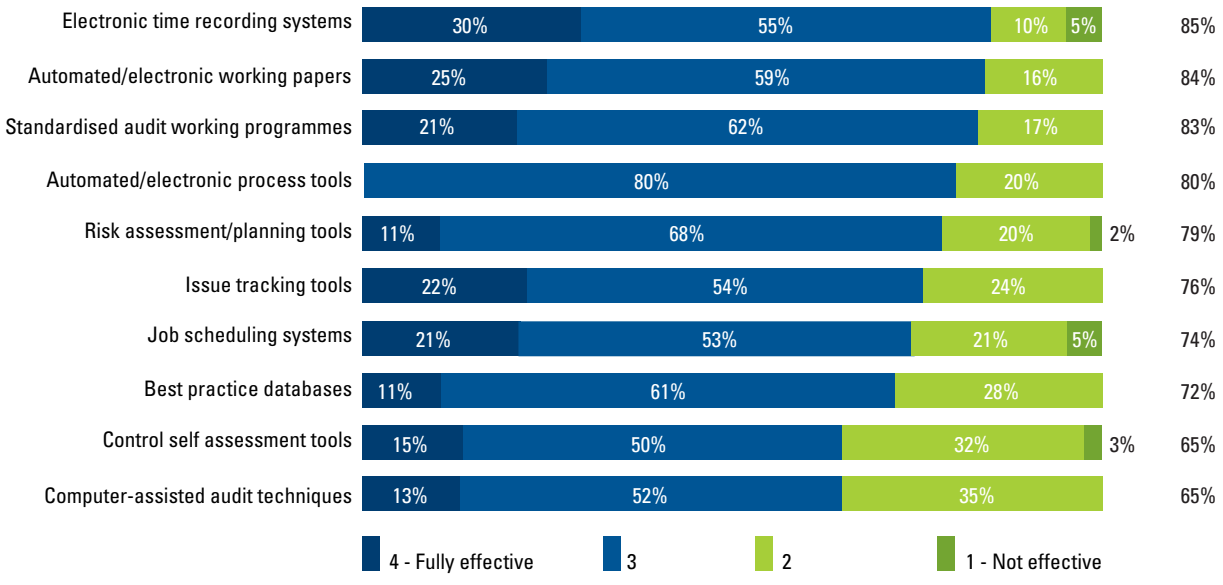
Figuur 3. Gemiddeld aantal 'auditdagen' per auditor naar omvang van de organisatie (Bron: PwC 2009 #3)

- 49% geeft aan dat minder dan een kwart van de auditors van de auditafdeling ervaring heeft in het gebruiken van de ERP-systemen van de organisatie om rapportages te genereren of om te navigeren door het systeem;
- 65% geeft aan dat minder dan een kwart ervaring heeft om aanbevelingen te doen met betrekking tot het gebruik van ERP-systemen (bijvoorbeeld: welke processen zouden geautomatiseerd kunnen worden, hoe kan het systeem beter geconfigureerd worden?);
- 75% geeft aan dat minder dan een kwart ervaring heeft in het gebruik van systemen of live datafeeds om performance- of risico-indicatoren te monitoren;
- 87% geeft aan dat minder dan een kwart ervaring heeft in het onderhoud en gebruik van governance, risk & compliancesystemen.

Er zijn meerdere strategieën beschikbaar om de ervaring en deskundigheid omtrent IT-audit te verhogen. Driekwart van de respondenten uit het 2009-onderzoek geeft aan in ieder geval de basiskennis met betrekking tot het begrip van technologische risico's en het auditen daarvan bij de internal auditstaf te willen verhogen. Ruim tweederde geeft aan ook meer geavanceerde tooling te willen aanschaffen om deze risico's af te dekken alsmede meer gebruik te willen maken van externe deskundigen. Ruim de helft geeft aan te kiezen voor een organisatorische aanpassing, waarbij internal auditors met IT-vaardigheden opgenomen worden in de auditpool, uitgezonderd een kleine groep IT-specialisten, die zal fungeren als een support centre. De helft van de respondenten geeft aan meer ervaren IT-auditors te willen inzetten, het aantal relevante certificeringen binnen de IT-auditors te willen verhogen of simpelweg de ratio IT-auditors/niet-IT-auditors te willen vergroten. Een derde van de respondenten geeft aan IT-specialisten zonder auditachtergrond te willen inzetten (zie *figuur 4*).

Meten performance van Internal Audit

Het is voor veel internal auditors lastig om hun daadwerkelijke toegevoegde waarde helder en concreet zichtbaar te maken voor het auditcomité, het management en andere belanghebbenden. En juist in tijden van neergang is het nog belangrijker om dit wel te kunnen. Kengetallen afkomstig uit betrouwbare bronnen zullen interne belanghebbenden en klanten helpen om de werkzaamheden van Internal Audit goed te kunnen waarderen. Maar het blijkt



Figuur 4. Waardering die internal auditors geven aan managementtools die zij gebruiken (Bron: PwC 2009 #3)

dat er binnen de internal auditbranche geen duidelijk eensluidende mening heerst over hoe de effectiviteit en toegevoegde waarde van Internal Audit te meten en te communiceren. Slechts 58 procent van de respondenten van het 2009-onderzoek geeft aan heldere kengetallen te hebben gedefinieerd. Toch blijkt dat er niet echt grote overeenstemming in het veld is over het gebruik van kengetallen. Slechts 17 procent van de respondenten meldt het gebruik van het aantal uitgevoerde audits, 15 procent rapporteert de kwalificaties of opleidingsniveaus van de staf, 14 procent rapporteert het percentage gerealiseerd auditplan en 13 procent rapporteert klanttevredenheid. En dit waren de grote getallen. Ook rapporteert maar een minderheid van de internal auditfuncties dit soort kengetallen aan het auditcomité: 28 procent rapporteert ze jaarlijks en 26 procent tijdens elke audit comittee meeting. En 5 procent rapporteert het nooit!

Aangrijpingspunten voor actieplan

Hierna volgt kort een vijftal aangrijpingspunten waar internal auditfuncties mee aan de slag zouden moeten om de functie klaar te maken voor de toekomst:

- Het internal auditproces onder de loep nemen (werken aan efficiency, verleggen van de focus naar strategische en ondernemingsrisico's, verbeteren kennismanagement, aanpassen bezetting).
- Opstellen en communiceren van duidelijke kengetallen (om zodoende de toegevoegde waarde te concretiseren en zichtbaar te maken).
- (Mede) sturing geven aan de veranderende beleving van risicomanagement (denk aan het identificeren en managen van emerging risks, continue risicoanalyse en dynamisch auditplan, zekerheid verstrekken over de ERM-functie).
- Technologie omarmen (de IA-staf naar ERP-boot camp, dataanalysefase expliciet toevoegen in auditmethodologie, maximaliseren gebruik automated controls, gebruiken interne en externe IT-expertise).
- Aandacht voor bemensing (denk aan niet-financiële beloningscomponenten, herijking bemensing van (senior)managementposities, toptalent blijven uitdagen, bouwen aan talent leadership, werken aan trainingcurriculum, samenstelling team qua achtergrond (audit- of organisatiekennis)).

Arjan Man is principal manager bij PricewaterhouseCoopers Advisory en verantwoordelijk voor de Internal Audit Services Groep voor de financiële sector. Daarvoor was hij werkzaam binnen NYSE Euronext, waar hij verantwoordelijk was voor IT, financial en operational audit in Europa en daarvoor bij KPMG Management Consulting, waar hij zich onder meer bezighield met operational audit en ERM.

Noten

1. Dit artikel is grotendeels gebaseerd op de resultaten van een onderzoek uitgevoerd in het vierde kwartaal van 2008 onder 700 internal auditors, waarvan 88 procent chief audit executive (CAE), internal audit director of manager is. Daarnaast is 69 procent van de respondenten werkzaam in organisaties met een omzet groter dan een miljard dollar. Zie ook www.pwc.com/internalaudit en de literatuurlijst.
2. In het Engels: business risk.
3. Zie ook *Audit Magazine,* december 2008.

Literatuur

- *Business upheaval: internal audit weighs its role amid the recession and evolving enterprise risks*, PricewaterhouseCoopers LLP, 2009.
- *Managing in a downturn: driving efficiencies and value from internal audit*, PricewaterhouseCoopers LLP, 2009.
- *Keeping pace with demand? Driving efficiencies and value from Internal Audit*, PwC LLP, 2009.
- *KPMG's 2009 IT Internal Audit Survey: The status of IT audit in Europe, the Middle East and Africa*, KPMG International, 2009.
- *An opportunity for transformation: how internal audit helps contribute to shareholder value*, PricewaterhouseCoopers LLP, 2008.
- *Internal Audit 2012: A study examining the future of internal auditing and the potential decline of a controls-centric approach*, PricewaterhouseCoopers LLP, 2007.

IIA Congres: 'Auditors on the beach'

De weergoden waren de auditors goed gezind dit jaar. Terwijl het in grote delen van Nederland regende, ontmoetten de bezoekers van het IIA Jaarcongres 2009 elkaar onder schitterende weersomstandigheden in het Circustheater in Scheveningen om inspiratie op te doen voor het komende jaar. Een verslag.

Drs. H.A. Mulders RA RC
Drs. D.L. Stabel RE CIA

Een duik in de kredietcrisis

Dat de inspiratie niet op voorhand werd aangereikt, bleek al bij de eerste mainstreamsessie toen Willem Middelkoop (journalist en vooral bekend als marktcommentator bij RTL Z) achter de katheder ging staan en welhaast als een profeet orakelde over de door hem voorspelde kredietcrisis en de nog grotere rampspoed die hij de komende jaren verwacht.

De belangrijkste oorzaak van de kredietcrisis, aldus Middelkoop, is de wereldwijde 'schuldenbubble' en de ongebreidelde groei van de handel in niet-begrepen derivaten. Hij gaf aan dat het huidige financiële systeem in feite al is ingestort en alleen nog door de steun van overheden in stand gehouden wordt. Hij voorspelt dat alle banken uiteindelijk genationaliseerd zullen worden en dat zal blijken dat de 'toverstaf van Obama (het ruime monetaire beleid – red.) niet meer is dan een geschilderde dorre tak'. Voor de auditor in de zaal was er gelukkig ook nog een geruststellende boodschap: "Zorg dat u een specialisme hebt, want voor goede mensen is er altijd een baan."

Cut the crap!

Middelkoop liet de deelnemers in verwarring en twijfel achter. Hij voorspelde nog meer onheil, maar bood geen oplossing om aan de misère te ontsnappen. Gelukkig was daar Angélique Schmeinck (een van de twee vrouwelijke meesterkoks van Nederland) om de vertwijfelde auditors te laten inzien dat met inspiratie grenzen verlegd kunnen worden. Schmeinck probeerde de auditor ervan bewust te maken dat inspiratie de mogelijkheid biedt om het onmogelijke te realiseren. Daarbij moeten we niet schizofreen zijn als het om ideeën gaat; we laten ons vaak tegenhouden door het bedenken van redenen waarom iets niet kan lukken. Concreet voor de auditor betekent dit bijvoorbeeld het uitstellen van het oordeel: oordeel niet te snel, maar neem waar en wordt getuige van de beleving. Schmeinck illustreerde haar verhaal aan de hand van de verwezenlijking van haar inspiratie: het realiseren van een restaurant in een hete luchtballon.

De creatieve auditor

Een van de bij te wonen substreamsessies werd verzorgd door Karl Raats (partner bij het Centrum voor de Ontwikkeling van het Creatief Denken). In een vermakelijk en interactief uur werd met een aantal oefeningen duidelijk gemaakt dat het voor een auditor

Het congres bestond uit mainstream (plenaire) sessies en substream (parallelle) sessies. De mainstreamsessies hadden vooral de kredietcrisis als rode draad. De substreams (waarvan er een aantal in dit artikel besproken wordt) gingen in op een drietalonderwerpen: risicomanagement & audit, de auditprofessional en lessons learned & nieuwe ontwikkelingen.

belangrijk is om meer creativiteit in zijn werk aan te brengen. Zodoende kan hij zijn boodschap veel beter overbrengen. Hoog tijd om minder met de linkerhersenhelft en meer met de rechterhersenhelft te doen is dan ook zijn devies. Het is zaak, aldus Raats, dat de auditor ook eens positief kijkt naar de materie en zichzelf vaker afvraagt wat wél goed gaat binnen het auditobject. Door dit zelfs sterk te overdrijven zouden wel eens hele zinvolle inzichten kunnen ontstaan en creatieve innovaties vanzelf naar boven kunnen komen drijven.

Project auditing, een mistig gebied voor auditors?

Hans Cleton (managing partner bij ACS) wist als doorgewinterde projectmanager al vrij vroeg in zijn parallelsessie de aandacht te trekken met een aantal ontluisterende opmerkingen als: “Ik heb een vreselijke hekel aan projectaudits” en: “Projectaudits zijn irritant en van weinig toegevoegde waarde”. Gelukkig veranderde de toonzetting van deze sessie al vrij snel en werd het een constructieve bijeenkomst waarin Cleton duidelijk maakte hoe wél toegevoegde waarde geleverd kan worden in projectaudits. Naar zijn idee kan er op basis van de Balanced Change Card op een zinvolle manier een projectaudit uitgevoerd worden. Dit model kent vier perspectieven waarbij de auditor vast dient te stellen of in het project gezorgd is voor:

1. tijdige aanpassingen aan veranderde behoeften;
2. hechte veranderteams;
3. duidelijke spelregels;
4. resultaatgerichte inspanningen.

Zijn boodschap is dat auditors van projecten de inhoud van het auditobject niet dienen te schuwen, samen dienen te werken met projectmanagers en ook aandacht dienen te schenken aan sociale aspecten.

Soft controls, van kustwateren naar open zee

Inge van der Meulen (zelfstandig consultant) gaf een toelichting op haar betrokkenheid binnen VERA bij de ontwikkeling van een model om soft controls inzichtelijk te maken. Een belangrijke boodschap in haar verhaal was dat de keuze van onderzoeksmethodieken veelal afhankelijk zijn van de affiniteit c.q. achtergrond van de auditor. Het is zaak dat men zaken durft los te laten en open staat voor andere invalshoeken ofwel disciplines. Van der Meulen heeft een achtergrond in sociale wetenschappen en benadert soft controls in sterke mate vanuit de wereld van ethiek en integriteit. Samen met auditors met diverse achtergronden creëerde ze een multidisciplinaire aanpak. Deze verschuiving vanuit een monodisciplinaire aanpak brengt onzekerheden met zich mee, maar biedt ook nieuwe mogelijkheden en perspectieven. Het traject is tijdrovend en intensief: eerst pootjebaden alvorens de open zee in te gaan.

Maarten van Rossum, is de kust in zicht?

Hoogtepunt van de dag was een zeer animerend en onderhoudend optreden van Maarten van Rossum. Deze historicus gaf zijn visie op de oorzaken van het ontstaan van de kredietcrisis vanuit een historisch perspectief. In tegenstelling tot Middelkoop is Van Rossum van mening dat de toekomst volledig open is. Niemand kan voorspellen op welke wijze zaken zich zullen gaan ontwikkelen. Er is sprake van een collectief gebrek aan kennis van de toekomst.

Van Rossum vindt dat de kredietcrisis niet als een verrassing kwam. Deze is namelijk in belangrijke mate veroorzaakt door het marktdogmatisme dat sinds eind jaren zeventig zijn intrede heeft gedaan. Marktdogmatisme wordt gekenmerkt door de opvatting dat markten in staat zouden zijn om oplossingen voor maatschappelijke problemen te creëren. Daarnaast leidt het marktdogmatisme tot het versoepelen en/of verdwijnen van relevante regelgeving. Naast het marktdogmatisme zijn ook de intrede van het computertijdperk, de hedge funds en de CMO (collateralized mortgage obligation) belangrijke oorzaken, aldus Van Rossum.

Arie Molenkamp Award

In een interactieve sessie, waarbij de vier genomineerden voor de Arie Molenkamp Award (AMA) in gesprek gingen met de deelnemers van het congres, werd de inhoud bediscussieerd van de referaten van de recentelijk afgestudeerde Executive Masters of Internal Auditing. Tijdens deze discussie bleken alle genomineerden een onderwerp gekozen te hebben dat verder gaat dan een traditionele beschouwing van het vakgebied. Geert-Jan Krol deed onderzoek naar business IT-alignment. Remco Bosma schreef een referaat over wie de assurance levert over het mvo-jaarverslag. Maarten Hoornweg verrichtte onderzoek naar auditparadigma’s en

Foto’s: Marc van Heugten





Jolanda van der Burg onderzocht ter afsluiting van haar opleiding het fenomeen objectiviteit onder auditors. De prijs ging dit jaar naar Van der Burg. Zij volgde haar opleiding aan de Universiteit van Amsterdam. Van der Burg werd geroemd om de wetenschappelijke kwaliteit van haar referaat en mocht daarom de AMA-bokaal in ontvangst nemen.

Beachdaten

De eerste dag van het congres werd op het strand van Scheveningen afgesloten. Terwijl de zon langzaam onderging, konden de deelnemers speeddaten met de experts van het Institute van Internal Audit Nederland. Velen gebruikten deze sessie om onder het genot van een drankje en een hapje van de barbecue weer eens bij te praten met vakgenoten.

Windkracht 9

Dag twee van het congres begon met ruime aandacht voor de Rijksauditdienst. Bernard ter Haar (plv. thesaurier-generaal bij het ministerie van Financiën en tevens directeur van de directie Financiële Markten) en Dion Kotterman (algemeen directeur van de Rijksauditdienst), die een dag eerder door Fred Steenwinkel als nieuw IIA-groepslid was verwelkomd, gingen in op de ontwikkelingen binnen de rijksoverheid, de impact van de kredietcrisis op de werkzaamheden van het ministerie van Financiën en de rol van de internal auditor hierbij. Bijzondere fenomenen als saboterende projectmedewerkers en de politieke omgeving waarbinnen een rijksauditor moet manoeuvreren, kwamen uitgebreid aan de orde. Dat dit telkens weer leidt tot grote vaktechnische uitdagingen en een belangrijke maatschappelijke functie voor de auditor van de rijksoverheid werd overduidelijk.

Risicomanagement en luie managers!

Jan Driessen (partner bij KPMG Internal Audit, Risk & Compliance Services) ging in op risicomanagement in relatie tot ondernemerschap. Uit onderzoek van KPMG blijkt dat veel bestuurders risicomanagement als een last zien en niet goed in staat zijn de voordelen die risicomanagement kan bieden, te materialiseren. Driessen gaf aan dat de performancemeting van risico's daarom verbeterd moet worden. Dan kan namelijk de 'cost of control' afgezet worden tegen de 'cost of risk' en per saldo een zinvolle afweging gemaakt worden van wat wel en wat geen aandacht verdient binnen risicomanagement.
Daarnaast werd in deze sessie stilgestaan bij de kwaliteit van risicomanagement tijdens de kredietcrisis en wat op grond van het KPMG-onderzoek is misgegaan. Driessen sloot zijn lezing af door in te gaan op de vraag 'hoe nu verder?' Hij betrok in zijn antwoord een aantal sociale aspecten door te benadrukken dat er meer aandacht moeten komen voor mensen, vertrouwen, moraliteit en cultuur.

Bob Hoogenboom, bouw je mee aan luchtkastelen?

Bob Hoogenboom (bijzonder hoogleraar Politiestudies en Veiligheidsvraagstukken aan de Vrije Universiteit van Amsterdam) prikkelde de internal auditors met een aantal uitdagende stellingen. Daarbij ziet hij zich als wetenschapper als de hedendaagse hofnar die de gevestigde orde kan bekritiseren met opmerkingen en suggesties die buiten de gangbare normen vallen. De kern van zijn betoog richtte zich op de eigen onderwereld die in de publieke en private sector is ontstaan en het feit dat de internal auditor zijn focus daar niet op heeft gericht. De zogenoemde onderwereld heeft betrekking op onregelmatigheden die zich binnen de onderneming (en in sommige gevallen tussen ondernemingen) afspelen, zoals werknemers die stelen van de baas, het manipuleren van onderzoeksresultaten, kartelvorming en 'cooking the books'. Fraude speelt zich af op alle niveaus binnen de onderneming. Volgens Hoogenboom staat de 'white collar crime' niet op de maatschappelijke agenda en vinden de fraudeurs zichzelf ook niet crimineel. Hoogenboom constateert dat binnen het bedrijfsleven een alternatief systeem is ontstaan voor het omgaan met onregelmatigheden. Denk bijvoorbeeld aan het buiten de publiciteit houden, het hanteren van afkoopsommen en 'gouden handdrukken'. Door het gebrek aan focus vanuit Internal Audit op deze vorm van onregelmatigheden meent Hoogenboom dat de internal auditor een bijdrage levert aan het in stand houden van dit luchtkasteel. Hij onderbouwt dit met zijn stelling dat slechts een miniem aantal van de ontdekte fraudes in de voorbije jaren door (internal) audits zijn ontdekt.

Powerboaten

Na de ochtendsessies werd er aan het strand uitgewaaid met een goed verzorgde lunch waarbij voor de liefhebbers een unieke powerboatervaring was weggelegd.

The future of finance, een zonnige toekomst

Het seminar werd afgesloten met een inspirerende lezing van trendwatcher Adjiedj Bakas. Bakas staat bekend om zijn visionaire beelden. Ook hij ging in op de kredietcrisis en de oorzaken, maar nam vooral de tijd om verder te kijken. Veel verder. Als het gaat om de vraag hoe financiële instellingen verder moeten, schroomt Bakas niet om onconventionele denkbeelden te uiten. Hij geeft aan dat financiële astrologie en bedrijfsastrologie populairder zullen worden dan ooit en dat de huidige crisis mede veroorzaakt is door het cocaïnegebruik onder een belangrijke groep medewerkers en beslissers van financiële instellingen die daardoor onverantwoorde risico's namen.

Tot slot

Ter afsluiting keek dagvoorzitter Peter van der Geer terecht terug op een succesvol congres: veel inspirerende sprekers, geïnteresseerde deelnemers, betrokken sponsors en natuurlijk fantastisch zomerweer aan zee. Alles – behalve het weer – te danken aan de enthousiaste inzet van de vele vrijwilligers die het voor het IIA mogelijk maken een dergelijk succesvol evenement te organiseren.

Rick Mulders is senior auditmanager bij Robeco. Dennis Stabel is managing partner bij linQtree Advisory Services. Beiden zijn als redacteur verbonden aan *Audit Magazine*.

In de rubriek ‘de estafettecolumn’ schrijft een auditprofessional op persoonlijke titel een stuk over een onderwerp dat hem of haar bezighoudt, irriteert of verbaast. Dit op uitnodiging van de columnist uit het vorige nummer van *Audit Magazine*, om daarna zelf het stokje weer door te geven. Dit keer **Guus van Gameren**, hoofd Internal Audit PGGM.

Beheersen van risico’s: sprookje of realiteit?

De afgelopen maanden heeft één thema op ieders lippen gelegen: de (krediet)crisis. Er is veel over gesproken of de crisis te voorzien was en hoe je het voor de toekomst kunt voorkomen. Onder het motto ‘homo eruditio’ proberen we door allerlei inspanningen te verhinderen dat we in de toekomst opnieuw in een dergelijke situatie terechtkomen.

Binnen de organisaties waarin we werkzaam zijn is het voorkomen van een dergelijke gebeurtenis aan de orde van de dag. De oplossing die vaak wordt gehoord is dat riskmanagers andere, meer betrouwbare, voorspellingen gaan doen. Bij sommige organisaties was de crisis zelfs aanleiding om de riskmanagementfunctie te versterken of te introduceren. De bestuurders van deze organisaties geven hier eigenlijk mee aan nog niet goed te begrijpen waar het om gaat. Immers, niet de riskmanagementfunctie is verantwoordelijk voor het gedrag binnen de organisaties, maar het bestuur zelf. Dat zij een ‘voorspeller’ zien in de riskmanager is een misvatting. Hooguit inventariseren riskmanagers de risico’s waarna ze zelf inschattingen (kans, gevolg) toevoegen. Al wat zij meer zeggen te zijn in dit kader komt dicht in de buurt van sprookjes. Leuk om te horen, maar niet realistisch!

Sprookjes vertellen en auditing hebben op het eerste oog weinig gemeen. Misschien is een overeenkomst alleen te vinden in het gegeven dat velen denken het te kunnen en weinigen het resultaat van hun inspanning boeiend kunnen overbrengen. Als ik een sprookje lees wil ik het graag geloven omdat het zo mooi klinkt en dus luister ik met plezier naar een goede verteller.

Enige tijd geleden las ik in *Audit Magazine* (december 2008) een sprookje over ‘De nieuwe kleren van de keizer’. Een leuk verhaal dat ik nog kende uit mijn jeugd. Na de woorden ‘tot zover’ ging het echter nog even door. De sprookjesverteller van dit artikel meent dat auditors moeten toegeven dat risico’s complexer zijn geworden, zelfs ‘zo complex dat niemand ze meer kan begrijpen’. Echter, hiermee dienen wij niemand. Een vergoelijking van het gebeurde door een overdrachtelijk ‘jij kon het niet helpen, je begreep het immers niet’ lijkt me geen goede insteek om verder te komen. Welk signaal geven we af aan het management als we zeggen dat we het als auditprofessie niet snapten, of nog sterker, dat de risico’s zo complex zijn dat ook zij als management het niet snapten?

Feit is dat de risico’s niet complexer zijn geworden in de betekenis van moeilijker. Wel hebben we steeds meer risico’s gestapeld in onze businessproposities. De handelingen van het management zijn daardoor risicovoller, door bewuste of soms zelfs door onbewuste acties. In beide gevallen is dat de verantwoordelijkheid van het management.
Als auditors dienen we ons wel de vraag te stellen of wij voor deze businessproposities met meer risico afdoende hebben gewaarschuwd. Een operational auditor die zijn functie goed verstaat zal dit zeker hebben gedaan.

Graag draag ik het stokje over aan Wiebe Blok, hoofd Audit Woonzorg Nederland.

Eerlijke waardering

Dale Carnegie • Zo maakt u vrienden en goede relaties • Omega Boek • ISBN 9060575253

R.J. Klamer

Een van de meest aangename sprekers waar ik ooit naar heb mogen luisteren, prof. Steven B. Sample, stelde dat je bij de keuze welk boek je zou moeten lezen, je vooral moet laten leiden door de leeftijd van het boek. Zijn redenering was even simpel als logisch. Als een oud boek nog steeds gelezen wordt zal het wel goed zijn, dan zullen er wel wetenswaardige of wijze dingen in staan. Als gevolg van die redenering beval hij ons aan om de Bijbel, de Koran en Machiavelli te lezen. Alle drie, hoewel geheel verschillend, toch buitengewone boeken.

Hoewel *Zo maakt u vrienden…* van Dale Carnegie niet direct in dezelfde categorie valt, is het wel een oud boek dat steeds maar weer opnieuw wordt uitgegeven. De eerste druk is nota bene van 1936. Hoewel het boek weliswaar gedateerd is, staan er natuurlijk voorbeelden en helden in die ons nu, ruim zeventig jaar later, niet zoveel meer zeggen. Maar de inhoud is sprankelend gebleven. Leerzaam voor iedereen die veel met mensen om moet gaan. Met talloze tips en aanwijzingen – zij het soms wat ouderwets geformuleerd.

Het boek bestaat uit vier delen; de grondbeginselen van het omgaan met anderen, manieren om jezelf bemind te maken, hoe je anderen tot jouw standpunt kunt bekeren en, wees een leidersfiguur…
Elk hoofdstuk wordt afgesloten met een stelregel. In het boek aangeduid als ‘grondbeginsels’, maar dat vind ik wat overdreven. Toch is er een aantal zeer lovenswaardige stelregels. In het derde deel wordt in een nogal lang betoog aangetoond dat het heel zinvol is om ‘respect te tonen voor de opvatting van de ander’. Zeg nooit: ‘Je zit er naast!’ (pag. 168). Het hoofdstuk daaropvolgend sluit af met de stelregel: ‘Als je het mis hebt, geef het dan vlug en nadrukkelijk toe’ (pag. 177). Gevolgd door: ‘Pak het op een vriendelijke manier aan’ (pag. 187) en: ‘Zorg dat je gesprekspartner van het begin af aan je woorden moet beamen’ (blz. 194).
Nog afgezien van de wijsheid waarvan deze regels blijk geven, denk ik dat, gezien de tijd (1936!), deze opmerkingen toen nogal nieuw waren. Niet om ze te denken, dat doen we al eeuwen, maar wel om dit soort regels in een cursus en een boek te verwoorden. Ik denk dat Carnegie met dit boek de grondlegger is geweest van het positieve denken. De ideeën van Norman Peale zijn feitelijk een vervolg op de toen ingeslagen weg.

Ik heb mijzelf tijdens het lezen van het boek vaak betrapt op het maken van mentale notities in de zin van ‘dat moet ik onthouden, dat kan ik goed gebruiken in die situatie’. Vooral de positieve benadering sprak mij erg aan. Ik ben meestal geneigd de confrontatie aan te gaan en duidelijkheid te geven en te verlangen. In sommige gevallen lijkt het er wel erg dik bovenop te liggen, toch heeft Carnegie mij ervan overtuigd dat het geen manipulatie is maar oprechte belangstelling en oprechte waardering. Immers, alle andere vormen van overdreven positief gedrag merken we direct en ervaren we als onecht.

Het vierde deel van het boek gaat over leiderschap. Het denken over leiderschap is de afgelopen zeventig jaar natuurlijk behoorlijk geëvolueerd. De basis blijft echter nog altijd hetzelfde: ‘Zorg dat de ander met plezier datgene doet wat u voorstelt’ (pag. 287). Dat lijkt manipulatie maar is het niet. Het toont aan dat het de verantwoordelijkheid van de leider is om te zorgen voor plezier in het werk. En daarover is inmiddels een mooi aantal boeken geschreven. En deze boeken laten hun sporen na bij echte leiders die om die reden dan ook heel erg gewaardeerd worden.

Ik realiseer me meer en meer dat de methode om de wereld te verbeteren door bij jezelf te beginnen, daadwerkelijk meer effectief is dan enig andere methode. En om die reden zal ook dit boek een belangrijke plaats krijgen in mijn boekenkast. Gewoon om af en toe eens aan terug te denken. Waarbij vooral de tweede stelregel van het eerste deel mij veel deed: ‘Laat uw waardering blijken: eerlijk en oprecht’. Het zoeken naar een oprecht positief oordeel is vaak lastiger dan het vinden van kritiekpunten. Toch is dat eerste vele malen effectiever. En daar gaat het om.

Renze J. Klamer is management consultant bij Sentle bv (www.sentle.nl)
Duinvoet 8, 8242 RB Lelystad,
0320-231280,
✉ klamer@sentle.nl

Deze keer de overstap van **Edward Roozenburg**. Sinds 1 april jl. werkt hij bij de Sociale Verzekeringsbank als adviseur concerncontrol en organisatieontwikkeling. Tot die tijd was hij werkzaam bij de Algemene Rekenkamer.

Het werk bij de Sociale Verzekeringsbank vertoont een paar grote verschillen met het werk bij de Algemene Rekenkamer. “Ik ben bijvoorbeeld meer betrokken bij de implementatie van adviezen die voortkomen uit mijn audits”, zegt Edward. “Ik werk samen met mijn directe collega’s die geen auditor zijn, maar veranderdeskundige of controller. De auditrapporten werk ik zelfstandig uit. Wat dat betreft bepaal ik nu meer in mijn eentje hoe mijn werk eruitziet dan in mijn vorige baan. Binnen de Algemene Rekenkamer sprak ik namelijk veel met teamgenoten over de onderzoeksrichting en de uitvoering ervan.”

Implementatie

De betrokkenheid bij de implementatie van adviezen is opmerkelijk. “Meestal leggen auditors adviezen neer in de hoop dat er vervolgens iets mee gebeurt. Maar nu ben ik zelf betrokken bij het proces van implementatie.” Toch probeert Edward wel de nodige afstand te bewaren tot dit proces, aangezien de onafhankelijkheid van zijn functie anders in het geding kan komen. “Ik moet voorzichtig te werk gaan. Aan de ene kant moet ik afstand bewaren van de implementatie van het advies en aan de andere kant moet ik helpen de adviezen zo goed mogelijk te implementeren. Het is een kwestie van balanceren en goed het evenwicht bewaren. Dat maakt het spannend. Waar de grens precies ligt, ga ik nog ontdekken.”

Edward doet audits over allerlei onderwerpen binnen de Sociale Verzekeringsbank. “De audits zijn niet zozeer operationeel of financieel, maar hebben een algemeen karakter. Het gaat wel altijd over de vraag of de zaken goed georganiseerd zijn. Ook lever ik ‘program assurance’. En soms adviseer ik de raad van bestuur zonder dat daar een uitgebreid en systematisch onderzoek aan ten grondslag ligt.” De onderwerpen die Edward bij de Sociale Verzekeringsbank onderzoekt, hebben met name betrekking op interne aangelegenheden. Onderzoeken bij de Algemene Rekenkamer hadden vaak direct betrekking op maatschappelijke issues, zo laat hij weten. “Bij de Algemene Rekenkamer onderzocht ik de resultaten en effectiviteit van het rijksbeleid en verder onderzocht ik of de ministeries goed georganiseerd waren.”

> “Het is een kwestie van balanceren en goed het evenwicht bewaren”

Overzicht

Edward kijkt positief terug op zijn vorige baan. “Het was interessant werk. Onder andere vanwege het brede werkveld. De onderzoeken hadden betrekking op alle beleidsterreinen binnen het Rijk. Daardoor heb ik me in de meest uiteenlopende maatschappelijke issues verdiept. Ook alle organisatorische aspecten kwamen daar aan bod: beheersing, financiën, organisatiestructuur, efficiency, doelmatigheid, doelrealisering en bedrijfsvoering. Verder heb ik daar meegekregen op wat voor manier een onderzoek daadwerkelijk meerwaarde kan hebben.”

Na een mooie tijd bij de Algemene Rekenkamer vond Edward het tijd om ergens anders een kijkje in de keuken te nemen. “Op die manier houd ik mezelf wakker. Bovendien is het erg leerzaam. In een andere organisatie kom je voor een deel dezelfde, maar ook weer andersoortige problemen tegen. Daardoor krijg ik een goed overzicht en weet ik uiteindelijk precies welke problemen overal voorkomen en welke specifiek zijn voor een bepaalde sector.”

Disciplines

Wat Edward vooraf het meest aansprak in zijn nieuwe functie is de brede insteek. “De meeste van mijn naaste collega’s op deze afdeling zijn geen auditors maar verandermanager of controller. Vanuit deze afdeling proberen we vanuit drie disciplines (audit, control en organisatieverandering) de organisatie te verbeteren.” Tot dusver zijn de verwachtingen over zijn nieuwe baan uitgekomen. “Ik hoopte op een afdeling terecht te komen waar ik veel zelfstandigheid zou hebben in mijn werk. Dat is zeker het geval. Het zoeken naar nuttige samenwerking met de collega’s die niet als auditor werkzaam zijn, is interessant. Verandermanagers hebben namelijk vaak een andere kijk op de wijze waarop aanbevelingen uit audits moeten worden uitgevoerd. Verder zijn ze vaak goed op de hoogte van allerlei belemmeringen in de organisatie. Door een goede samenwerking tussen de verschillende

disciplines kunnen adviezen uiteindelijk optimaal geïmplementeerd worden."

Succes

Op de vraag of zijn nieuwe baan een zeer bewuste stap was in zijn loopbaan antwoordt hij: "Gedeeltelijk. Ik vond het tijd om ergens anders te gaan kijken. Het maakte mij in eerste instantie niet veel uit waar dat zou zijn." Maar inmiddels weet Edward voor zichzelf dat hij het leuk vindt om met verschillende disciplines samen te werken. Bovendien heeft hij door deze overstap een beter beeld gekregen van de mogelijkheden binnen het auditvak. Hij beschouwt zijn overstap als een succes wanneer zijn aanbevelingen zijn geïmplementeerd en de organisatie haar doelstellingen beter realiseert.

Hoe ziet Edward zichzelf in professionele zin over vijf tot tien jaar? "Het lijkt me interessant om betrokken te zijn bij het vormen en samenstellen van een onderzoeksteam, waarbij vanuit zeer uiteenlopende disciplines, en dus vanuit een breed perspectief op de organisatie, gewerkt wordt aan organisatieverbetering. Het nuttig inzetten van deze verschillende disciplines trekt mij. Bovendien heeft het samenbrengen van verschillende disciplines volgens mij een meerwaarde voor een organisatie."

De romantische boekhouder

Gerrit Zalm • Balans • ISBN 9789050188838 • € 19,50

Zoon van een kolenboer. Oud-directeur van het Centraal Planbureau. Met twaalf jaar de langstzittende minister van Financiën ooit. Naamgever van de Zalmnorm en de Zalmsnip. Leermeester van Wouter Bos, drager van de trotse bijnaam 'Il Duro'. Voormalig PvdA-lid en oud-fractievoorzitter van de VVD in de Tweede Kamer. Liefhebber van flipperkasten die Nederland de euro bracht. Joviaal maar deskundig, vriendelijk doch gevreesd.

Gerrit Zalm, een fenomeen. In dit boek geeft hij, als een van de hoofdrolspelers in de Nederlandse politiek van de afgelopen twintig jaar, voor het eerst openheid van zaken. *De romantische boekhouder* is het levendige verslag van zijn loopbaan in de ambtenarij en politiek. Openhartig vertelt hij over het reilen en zeilen op het ministerie van Financiën, de samenwerking met de overige ministers, zijn turbulente tijd als VVD-leider en zijn rol als vice-premier. Zalm gunt de lezer een blik achter de coulissen van 'Europa' en ook pijnlijke zaken gaat hij niet uit de weg: de kwestie Hirsi Ali; de perikelen rond Rita Verdonk en de val van het eerste kabinet-Balkenende. Bovendien geeft hij verrassende achtergronden bij de financiële crisis die de wereld op dit moment teistert.

Kwaliteitsmanagement en interne auditing

Bernadette van Pampus • Boom onderwijs • ISBN 9789047301073 • € 22,00

Kwaliteitsmanagement is het doorlopend verbeteren van interne processen. Regelmatig moet worden getoetst of het systeem nog doeltreffend is of dat er verbeteringen nodig zijn. De interne audit is een onderzoek om zwakke plekken in het kwaliteitsmanagementsysteem op te sporen.

In *Kwaliteitsmanagement en interne auditing* komt aan de orde hoe het proces van de interne audit verloopt, wat verwacht kan worden van de auditor en wat er gebeurt met de resultaten. Het boek bevat verder praktische tips en suggesties om een auditsysteem op te zetten en te onderhouden. Talloze praktijkvoorbeelden laten zien wat de winsten, maar ook wat de valkuilen van een interne audit kunnen zijn.

Bankroet – Hoe Fortis al zijn krediet verspeelde

Stefaan Michielsen, Michaël Sephiha • LannooCampus • ISBN 9789020983241 • € 19,95

Dit boek vertelt het verbijsterende verhaal van de internationale kredietcrisis, die van Fortis een van de belangrijkste slachtoffers maakte. De trotse financiële groep werd helemaal ontmanteld, de aandeelhouders bleven geruïneerd en gefrustreerd achter. Aan de hand van unieke getuigenissen van de belangrijkste hoofdrolspelers reconstrueren twee economische journalisten van *De Tijd* deze dramatische gebeurtenissen uit het najaar van 2008 en het voorjaar van 2009. Ze leggen de oorzaken bloot van de onthutsende fragiliteit van Fortis voor de financiële crisis, gaan na waarom niemand de ramp zag aankomen en waarom het management van Fortis niet bij machte was de desastreuze afloop te voorkomen.

Het resultaat is een indringend relaas – van dag tot dag en uur tot uur – over de wanhopige zoektocht om Fortis en het bankensysteem overeind te houden. Een sage over de ontstellende machteloosheid van bestuurders, regering en aandeelhouders om greep te krijgen op de crisis.

H. Nieuwlands RA CIA CGAP CCSA*

De ethiek van een zelftoetsende accountant

Onlangs heeft een Engelse beursonderneming (Rentokil) besloten vanwege financiële redenen zowel de jaarrekeningcontrole als ook de internal auditfunctie uit te besteden aan één accountantskantoor (KPMG). Dit heeft geleid tot een discussie onder de leden van het Instituut van Internal Auditors (IIA) of dit ethisch acceptabel is.
Waar is deze discussie op gebaseerd? Het NIVRA heeft een ethische code geaccepteerd waarin staat dat de externe accountant zijn onafhankelijkheid niet in gevaar mag brengen. Indien dit wel gebeurt, is er sprake van onethisch gedrag.

Wat is nu precies het gevaar? Een externe accountant dient te beoordelen in welke mate hij gebruik wil maken van het werk van de Internal Audit Dienst (IAD). Daartoe dient hij de kwaliteit van de IAD te beoordelen. Van oudsher is de IAD een interne dienstverlener die onderdeel uitmaakt van de organisatie.
Wanneer nu de jaarrekeningcontrole en de IAD zijn ondergebracht bij hetzelfde accountantskantoor ontstaat het gevaar van een zelftoets. De kans bestaat dat de controlerend accountant een ontoereikende evaluatie doet van de werkzaamheden van de IAD, die door collega's van hetzelfde kantoor zijn uitgevoerd. In het geval van Enron heeft dit ertoe geleid dat Enron en het accountantskantoor Andersen niet meer bestaan.

De SEC heeft naar aanleiding daarvan deze combinatie verboden bij bedrijven die aan de New York Stock Exchange zijn genoteerd. Bij de meest recente herziening van de Nederlandse corporate governancecode in 2008 heeft het IIA aangedrongen op het verplicht stellen van een IAD voor beursgenoteerde ondernemingen. Dit is door de commissie Frijns overgenomen in de vorm van een Best Practice. Bij het ontbreken van een IAD evalueert de auditcommissie van de raad van commissarissen (RvC) de situatie en rapporteert daarover in het verslag van de RvC in de jaarrekening. De code vermeldt ook dat niet-controlewerkzaamheden van de externe accountant, zoals het uitbesteden van een IAD, moeten worden goedgekeurd door de RvC.
Gezien het hiervoor genoemde is het IIA van mening dat de RvC uiterst terughoudend moet zijn in het goedkeuren van de uitbesteding van de IAD-functie aan een kantoor dat tevens de externe jaarrekeningcontrole uitvoert.

* is directeur van het Instituut van Internal Auditors

Audit Clients that are Public Interest Entities
290.200
In the case of an audit client that is a public interest entity, a firm shall not provide internal audit services that relate to:
a. a significant part of the internal controls over financial reporting;
b. financial accounting systems that generate information that is, separately or in the aggregate, significant to the client's accounting records or financial statements on which the firm will express an opinion; or
c. amounts or disclosures that are, separately or in the aggregate, material to the financial statements on which the firm will express an opinion.

(Bron: Code of Ethics for Professional Accountants, IFAC, June 2009)

290.196
Internal audit services involve assisting the audit client in the performance of its internal audit activities. The provision of internal audit services to an audit client creates a self-review threat to independence if the firm uses the internal audit work in the course of a subsequent external audit. Performing a significant part of the client's internal audit activities increases the possibility that firm personnel providing internal audit services will assume a management responsibility. If the firm's personnel assume a management responsibility when providing internal audit services to an audit client, the threat created would be so significant that no safeguards could reduce the threat to an acceptable level. Accordingly, a firm's personnel shall not assume a management responsibility when providing internal audit services to an audit client.

(Bron: Code of Ethics for Professional Accountants, IFAC, June 2009)

290.198
To avoid assuming a management responsibility, the firm shall only provide internal audit services to an audit client if it is satisfied that:
a. the client designates an appropriate and competent resource, preferably within senior management, to be responsible at all times for internal audit activities and to acknowledge responsibility for designing, implementing, and maintaining internal control;
b. the client's management or those charged with governance reviews, assesses and approves the scope, risk and frequency of the internal audit services;
c. the client's management evaluates the adequacy of the internal audit services and the findings resulting from their performance;
d. the client's management evaluates and determines which recommendations resulting from internal audit services to implement and manages the implementation process; and
e. the client's management reports to those charged with governance the significant findings and recommendations resulting from the internal audit services.

(Bron: Code of Ethics for Professional Accountants, IFAC, June 2009)

Auditors in het buitenland

Johan Hundertmark werkte in Nederland en Saoedi-Arabië. Tegenwoordig vertoeft hij in Australië. Hij beschrijft, op persoonlijke titel, zijn ervaringen met 'cultuur en leiderschap' in den vreemde. "Ik kan het iedereen aanbevelen om over de grens te kijken."

J. Hundertmark

Ik werk in Sydney, Australia als director/country head Group Audit Australia & New Zealand voor Deutsche Bank in welke hoedanigheid ik ook lid ben van het managementteam voor de regio Azië en Pacific. Daarvoor heb ik voor ABN Amro gewerkt in Nederland en in Saoedi-Arabië.
De Nederlandse cultuur kennen we natuurlijk allemaal en aangezien ik er zelf in ben opgegroeid, heeft het mij zwaar beïnvloed. Zowel in positieve als in negatieve zin. De Nederlandse pragmatische insteek en de non-autoritaire cultuur maken dat we heel gemakkelijk ingang krijgen en eenvoudig geaccepteerd worden door andere culturen. Dat heeft ons in de historie als handelsreizigers in staat gesteld om met alle landen te handelen.
Daartegenover staat de reeds genoemde onbedoelde directheid en onze consensuscultuur die internationaal ook wel als zacht en weinig doortastend gezien wordt. Die innertie in besluitvorming en het gebrek aan doortastendheid is in het boek *De Prooi* van Jeroen Smit goed beschreven. Aan de andere kant heb ik gemerkt – ogenschijnlijk in tegenspraak hiermee – dat de structuur in de vorm in het voormalige ABN Amro sterk hiërarchisch was, veel meer dan ik nu bij Deutsche Bank ervaar.

In Australië komen dames op teenslippers binnen om deze onder hun bureau te verwisselen voor hoge hakken

Teenslippers op kantoor

De stap naar Australië was voor mij vooral een keuze om, na de teloorgang van ABN Amro in de oude vorm, mijn internationale carrière voort te zetten. Iets waartoe mijn vrouw en ik al langer geleden besloten hadden. De Australische cultuur was mij redelijk onbekend, ook al heeft iedereen het beeld van strand, surfen en laid-back. Mijn conclusie na één jaar is dat er inderdaad een sterke strandcultuur is en ja, er wordt veel gebarbecued. En de teenslippers worden werkelijk óveral gedragen, zelfs op kantoor. De dames komen op teenslippers binnen om deze onder hun bureau te verwisselen voor hoge hakken. Met het arbeidsethos is echter niets mis: er wordt hier verschrikkelijk hard gewerkt.

De Australische cultuur in de werkomgeving van mijn huidige werkgever is lastig te betitelen, omdat het een mengeling is van het Duitse Rijnlandse Model en het Angelsaksische Model. Modellen zijn op zich geen culturen, aangezien er een groot verschil bestaat tussen respectievelijk de Franse en de Duitse cultuur. Toch worden beide betiteld als Rijnlands. In de Australische werkelijkheid van Deutsche Bank betekent dit relatief platte organisaties met een no-nonsensecultuur en korte lijnen, op non-autoritaire basis.
Dat betekent echter niet dat de Nederlandse directheid hier werkt, evenmin als dat, om volstrekt andere redenen, in Saoedi-Arabië werkte. Wat wij in Nederland als directheid betitelen wordt in beide culturen niet zelden als te direct ervaren. Ik ontdekte dat in Saoedi-Arabië al heel snel en zag pas nadien in dat wat wij in Nederland als normaal zien, in het geheel niet de standaard omgangsvorm is in andere delen van de wereld.
Het leidinggeven in drie totaal verschillende culturen heeft me geleerd dat leiderschap in Australië en Saoedi-Arabië vooral als richtingbepalend wordt gezien. Het moet de (nieuwe) organisatie vormgeven. In Nederland wordt de leider nooit gezien als meerdere maar als primus inter pares die de veranderingen alleen kan realiseren door daarvoor een zo groot draagvlak te creëren binnen de organisatie. Omdat ik niet gewend ben zelf zo tegen een leider aan te kijken zag ik pas later in welke impact mijn beslissingen en uitlatingen hebben op niet-Nederlandse medewerkers.

Stammenstructuren

Het verschil tussen man en vrouw is in Australië nihil, nog kleiner dan in Nederland, en geheel anders dan in Saoedi-Arabië. In vergelijking met de Australische cultuur zijn zowel de Nederlandse als de Saoedische cultuur geheel verschillend. Te beginnen met de Saoedische Wahabi-cultuur. Deze cultuur is gevormd door de strengste interpretatie van de islam en kent een absolute scheiding in het dagelijks leven tussen man en vrouw. Man en vrouw werken niet of nauwelijks direct met elkaar samen en hun werkomgevingen zijn strikt van elkaar gescheiden. Deze cultuur doordrenkt het gehele leven en dus ook de manier waarop je als hoofd Internal Audit je collega's aanstuurt.

De aansturing is in deze sterk masculiene omgeving nogal directief. Men verwacht dat je de antwoorden hebt op alle problemen en vraagstukken. Wel praten de Saoedische mannen graag over de problemen en het goed voorbewerken van de belangrijkste stemmingmakers is van belang. Hier geldt dat de formele organisatie van beperkt belang is omdat de stammenstructuren en familieposities in de Saoedische samenleving nog altijd de dominante structuur zijn. Ergo, de informele familie- en stammenposities ten opzichte van het koningshuis bepalen binnen ieder instituut, dus ook de bank, uiteindelijk het gezag.

Vooringenomenheid

Na ruim drie jaar in twee verschillende landen kan ik iedereen aanbevelen om ook zo'n stap te maken. Het leert je inzien met welke vooringenomenheden je als Nederlander gewend bent geraakt te handelen. Deze zijn vanzelfsprekend in Nederland, maar niet in het buitenland. Steeds minder ben ik ervan overtuigd dat er alleen maar een Rijnlandse en Angelsaksische (audit) cultuur bestaat. Elk land heeft juist een eigen unieke cultuur die bepaald wordt door zaken als historie, religie, en regionale invloeden. De academische grondslagen voor auditors zijn uiteraard grotendeels hetzelfde, maar de werkomgevingen zijn verschillend per land zonder dat daar een andere grote gemene deler voor kan worden gedefinieerd dan die van Hofstra met de onderverdeling tussen de masculiene en feminiene culturen.

Voor iedereen die overweegt een stap over de grens te maken heb ik een tip: weet hoe culturen in elkaar zitten en weet hoezeer de formele organisatie van de informele organisatie verschilt. Beide zijn van groot belang om snel en effectief aan de slag te kunnen gaan.

Johan Hundertmark (38) werkt in Australië als director/country head Group Audit Australia & New Zealand voor Deutsche Bank. Voorheen was hij werkzaam voor ABN Amro Bank als senior vice president in Nederland en als hoofd Internal Audit voor de ABN Amro-dochteronderneming Saudi Hollandi Bank in Saoedi-Arabië. Hij schreef dit artikel op persoonlijke titel. Hij is getrouwd en heeft drie kinderen in de leeftijd van zeven, vier en drie jaar.

Rapport Review of Internal Audit Ahold nv

Begin juli 2009 werd door Jan Driessen van KPMG het rapport *Review of Internal Audit Ahold nv* aan het internal auditmanagement overhandigd. De review vond plaats in de daarvoor liggende maanden. Leden van het audit committee, de board en management van Ahold nv zijn geïnterviewd en de auditmethodologie, de auditsystemen, de afdelingsstructuur en de uitgevoerde audits zijn door het onderzoeksteam beoordeeld. Met de beste rating volgens de IIA Standards en een hoge waardering volgens de onderzoeksmethodiek van KPMG, is de review een groot succes geworden.

Joop Brakenhoff, Chief Audit Executive: "Een erkenning voor de vele investeringen die we de afgelopen jaren in de internal auditfunctie hebben gedaan met grote steun van de raad van bestuur en de raad van commissarissen van Ahold."

De bijeenkomst werd bijgewoond door Joop Brakenhoff en Erik Boon (beiden van Ahold Internal Audit) en Jan Driessen, Willem van Loon en Wim van Hazendonk (het onderzoeksteam van KPMG).

Activiteitenkalender 2009

Oktober

7-8-9 Training Auditor-in-charge. Tools and techniques
8 Seminar Verbeter de effectiviteit van uw oordeelsvorming door dr. Bob van Kuijck RA RC
13-14 Training Fraudedetectie en -onderzoek
14 GAIN Round Table – Financials: follow-up en risk assessment van audit findings
15 Presentatie Studierapport 'Samen nog sterker'
15-16 RO Masterclas RO/EMIA-titel anno 2009
20-21 Training Enterprise risk management: an introduction
28 Seminar Alignment Audit, een bijzondere vorm van auditen compliance en integriteit

November

2-3 Training Introductie SAP Internal Control Auditing
4-5 Training Creativiteit, onmisbaar voor auditors
5 Seminar Toezicht en audit bij de (lokale) overheid door Arie Molenkamp RO
5 GAIN-middag 2009
10-11 Training Control self assessment: an introduction
17-18 Training Auditen van soft controls
19 Seminar Auditing soft controls door prof. dr. Muel Kaptein en drs. Rick Mulders RA RC

December

2-4 Training Introductie in IT-auditing
8-9 Training Beginning auditor tools and techniques
15-16 Training Beginning auditor tools and techniques
14-15 Training Auditen van projecten
15-16 Seminar Strategisch risicomanagement

Voor een actueel overzicht van onze activiteiten verwijzen wij u naar onze website www.iia.nl.

SVRO bestaat 12,5 jaar

Vijftien jaar geleden, op 7 juli 1994, is de VRO opgericht. Op 8 januari 2009 is de VRO omgezet in een stichting, de SVRO. In de eerste vijf jaar is een financieel onafhankelijke vereniging met een sterke verbondenheid met haar leden opgebouwd. Vaktechnisch gezien is daarbij het fundament gelegd voor een management driven internal auditbenadering naar het Angelsaksisch model. In Nederland was dat toen nieuw. Daarnaast is het register voor Operational Auditors opgezet. Een van de successen van de laatste vijf jaar is de samenwerkingsovereenkomst met IIA Nederland.

Diploma-uitreiking CIA

Op 22 juni jl. vond de CIA-diploma-uitreiking plaats op het bureau van het IIA in Naarden. Dit is de eerste uitreiking sinds IIA inc. is overgegaan op de automatisering en uitbesteding van de CIA-examens. IIA Nederland is van plan een aantal malen per jaar een persoonlijke uitreiking te verzorgen. Voorheen was het mogelijk om slechts twee maal per jaar examen te doen. Nu is het voor studenten mogelijk om het hele jaar door examen te doen.
Wil je je opgeven voor een examen? Aanmelden kan via m.rose@iia.nl.

Diploma-uitreiking CIA te Naarden

Rapport Commissie Maas

Naar aanleiding van het rapport van de Adviescommissie Toekomst Banken heeft het IIA een reactie gestuurd naar de Nederlandse Vereniging van Banken. Het IIA stelt dat de rol van de interne auditdienst rondom de governance binnen de bank sterker en explicieter benoemd dient te worden. In het rapport zou namelijk onvoldoende recht worden gedaan aan de functie die een interne auditdienst kan vervullen bij het verbeteren van de governance en het riskmanagement zoals dat bij de banken ingevuld wordt. De rol van de interne auditdienst blijft in het rapport onderbelicht, zo meent het IIA. Het IIA wijst erop dat voor een goede governance en een effectieve risicobeheersing een nauw samenspel tussen alle actoren die betrokken zijn bij de governance van de bank, noodzakelijk is. De Commissie Maas heeft inmiddels aangegeven dat Internal Auditing ten onrechte niet meegenomen is in het rapport. In een nieuw te schrijven Code zal er wel aandacht aan de functie worden besteed.

Trainingen

Op 7, 8 en 9 oktober 2009 vindt de training 'Auditor-in-charge: tools and techniques' plaats. Als u promotie hebt gemaakt en erachter bent gekomen dat het leidinggeven aan een audit toch iets anders is dan er zelf een uitvoeren, dan is deze cursus geschikt voor u. Tijdens de cursus wordt ingegaan op het aansturen van auditwerkzaamheden, effectief delegeren, projectmanagement, planningstechnieken en timemanagement. Door middel van cases en discussievormen zullen enkele vaardigheden worden geoefend. Meer informatie vindt u op www.iia.nl.

Nieuw initiatief: Commissie Individuele Dienstverlening

Vanuit de leden van het IIA is het initiatief gekomen om een nieuwe commissie in het leven te roepen. Deze commissie gaat de belangen vertegenwoordigen van de zelfstandigen onder de leden. De doelstelling is het werkgebied van deze IIA-leden in de breedte een actief kader te geven. Dit initiatief heeft onlangs de steun van het bestuur gekregen. De naam van de commissie luidt: Commissie Individuele Dienstverlening.
Eén van de initiatieven zal zijn om een portal voor zelfstandigen te faciliteren op de website van IIA Nederland. Daarnaast zullen vanuit de commissie bijeenkomsten georganiseerd worden. De kick-off van de commissie staat gepland op 8 oktober aanstaande. Iedereen die met de commissie en collegazelfstandigen behoeften en wensen wil delen is welkom. Houd voor meer informatie de website van IIA in de gaten.

Seminars

Op 8 oktober 2009 wordt het seminar 'Verbeter de effectiviteit van uw oordeelsvorming' gehouden. In dit seminar ligt de nadruk op de verbetering van de effectiviteit van de oordeelsvorming van auditors. Met name in deze tijden van onzekerheid en snelle veranderingen wordt waarde gehecht aan het oordeel van auditors. Een auditor tracht de lezer van een auditrapport te overtuigen en moet derhalve effectief zijn. In een interactief seminar behandelt Bob van Kuijck de do's en don'ts in relatie tot gedegen oordeelsvorming. Meer informatie vindt u op www.iia.nl.

Op 19 november 2009 vindt het seminar 'Auditing soft controls' plaats. Het niet functioneren van hard controls wordt als een van de belangrijkste oorzaken beschouwd van beursfraudes, boekhoudschandalen en rechtmatigheidsfouten bij de overheid zoals die de laatste jaren aan het licht zijn gekomen. Volgens Muel Kaptein zijn echter de normen en waarden, de handel en wandel en de cultuur van organisaties op zijn minst even belangrijke factoren. Goed gedrag van mensen is niet te waarborgen door louter systemen, procedures en gedragscodes. Het gaat om betrokkenheid, goede intenties en een juiste omgang met druk. In hoeverre vormen soft controls een (integraal) onderdeel van de werkzaamheden van de internal auditor? In een interactief seminar behandelen Muel Kaptein en Rick Mulders aan de hand van korte presentaties en casestudies het onderwerp soft controls. Meer informatie vindt u op www.iia.nl.

UNIVERSITEIT VAN AMSTERDAM

Buluitreiking

Twee keer per jaar organiseert de EMIA-opleiding een buluitreiking, een in het voorjaar en een in het najaar. Op 15 mei jl. ontvingen de volgende studenten hun bul:

- Jerzy Bloemberg
- Ilona de Haas
- Wouter Jonker
- Joshua Tange
- Marlinde Westland
- Leander Wolterbeek
- Peter Draijer
- Daan Hartman
- Hugo Jacobs
- Johan Laan
- Pieter Poelstra

Wij feliciteren de studenten van harte met het afronden van de EMIA-opleiding.

Toolkit 'Trust Rules'

De Amsterdam MBA (onderdeel van de Amsterdam Buisiness School) en KPMG hebben een toolkit met lesmateriaal ontwikkeld met de naam 'Trust Rules'. Deze toolkit is ontwikkeld voor hogescholen, universiteiten en business schools om studenten al tijdens hun opleiding kennis te laten maken met de onderwerpen integriteit, cultuur, leadership en ethiek. Hiermee willen de Amsterdam Business School (ABS) en KPMG een bijdrage leveren aan de ontwikkeling van een waardesysteem voor toekomstige managers. Het lesmateriaal zal wereldwijd ter beschikking worden gesteld en is uitvoerig in de praktijk getest, onder meer in de vorm van een tweedaagse pilot workshop die april jl. is gegeven aan de studenten van de Amsterdam MBA. In navolging van deze workshop hebben prof.dr. Edo Roos Lindgreen (ABS en KPMG), dr. Willemijn van Dolen (ABS) en drs. Martijn de Kiewit (KPMG) een eendaagse workshop gegeven aan een groep van achttien studenten van de NYU Schack School of Real Estate. Het succes van de workshop mag blijken uit het feit dat de ABS en KPMG direct zijn uitgenodigd om volgend jaar weer een workshop te geven aan de New York University.

Aanscherping en afronding

Met de feedback uit beide workshops wordt de toolkit de komende tijd verder aangescherpt en afgerond. In de Amsterdam MBA zal de workshop vanaf het volgend academisch jaar een verplicht onderdeel worden van het Amsterdam Leadership Programme. Verder wordt een uitrol naar andere ABS-programma's op dit moment bekeken. De EMIA-opleiding zal de toolkit in het programma opnemen.

Arie Molenkamp Award

Tijdens het IIA congres, op 15 juni jl, ontving Jolanda van der Burg de Arie Molenkamp Award (AMA) voor haar referaat 'Objectiviteit: een subjectief begrip?'In het tijdschrift *Finance & Control* is inmiddels een uitgebreid artikel naar aanleiding van het referaat van Jolanda van den Burg verschenen, met een verwijzing naar het volledige referaat in de Finance & Control-base. Ook een artikel naar aanleiding van het referaat van Remco Bosma, een van de genomineerden voor de AMA, getiteld 'Wie levert de assurance over het MVO-jaarverslag?' kunt u vinden in het tijdschrift *Finance & Control.*

ERASMUS UNIVERSITEIT ROTTERDAM

Gastcollege Jules Muis

Vrijdag 19 juni jl. gaf 'good governance-auteur' Jules Muis een gastcollege aan de Erasmus Universiteit Rotterdam. Muis gaf, op speciaal verzoek van de studenten, zijn visie op de kredietcrisis en de (gewenste) rol van auditors. Omdat met dit college het tweede jaar op een feestelijke manier werd afgesloten, waren de collega's en bazen van onze studenten ook uitgenodigd.
Muis startte met het geven van een groot compliment aan de opleiding: ons curriculum zag hij als voorbeeld voor alle auditopleidingen. Als aanvulling op de literatuurlijst beval hij Machiavelli's *Il Principe* aan.

Carrière
Muis startte zijn carrière als interne accountant bij Philips en was onder andere voorzitter van het NIVRA, controller van de Wereldbank en Chief Internal Auditor van de Europese Commissie. Op dit moment woont hij in Washington. Eigenlijk had hij cartoonist willen worden, maar het is er nooit van gekomen. Nu geeft hij op een andere manier de werkelijkheid gecomprimeerd weer. Zo ook de kredietcrisis. Na een analyse van de oorzaken van de kredietcrisis, de invloed van de accountant en de rol van de internal auditor kwam ook de voorspelbaarheid van de crisis aan de orde. Muis gaf daarbij zijn eigen analyse uit 2004 toen hij van mening was dat het met de huizenmarkt in Amerika niet zo door kon gaan, het geld te goedkoop was en niemand voldoende begreep van de derivatenhandel. Veel kleine risico's kunnen één grote worden.
Was de crisis dan voorspelbaar geweest? Muis vraagt het zich hardop af en is van mening dat met de ogen open de crisis voor 80 procent voorspelbaar was geweest. Maar niemand pakte de signalen op dat er iets niet klopte en zo herhalen crises zich in de geschiedenis. Niets menselijks is ons vreemd!

Massaal falen
In de discussie Balkenende-Bos is hij het eens met Balkenende dat de oorzaak van de crisis 'man-made' is en niet door de systemen is ontstaan. Bovendien zijn alle calamiteiten voorafgegaan door goedkeurende verklaringen van accountants!
Ondanks SOx en COSO faalde de financiële sector massaal. Met de hard controls alleen kom je er dus niet. De menselijke factor is erg belangrijk. Aan de zaal vol auditors vraagt Muis waar de auditors waren met de kredietcrisis. De zaal blijft erg stil. Gelukkig voor de toehoorders geeft Muis aan dat je als individu de crisis niet kunt tegenhouden. Ten alle tijden blijft het echter wel belangrijk wat je, als het er op aan komt, met je deskundigheid doet: gebruiken of misbruiken?

Bijzondere audits maken het auditberoep nog boeiender

Dr. J.R. van Kuijck*

In lijn met het thema van deze editie van *Audit Magazine* passeren hier drie verschillende actuele onderwerpen de revue. Ieder met een specifieke dimensie. Onderwerpen die zich lenen voor bijzondere audits die het beroep van auditor nog boeiender maken dan het al is.

Complexe problematiek

Een tijd geleden werd je nog voor gek verklaard als je het denkbaar achtte dat overheden bankroet zouden kunnen gaan. De huidige financiële crisis zet alles op zijn kop en laat ons terugdenken aan de jaren dertig van de vorige eeuw of zelfs de 18e eeuw. Met de IOU (I owe you) van Arnold Schwarzenegger, gouverneur van Californië, zijn we inderdaad terug in de 18e eeuw. In die tijd voerde men Continentals in, een vergelijkbare schuldbekentenis. Maar hoe is het met de Continentals afgelopen? Niet zo goed. De Continentals verloren destijds vrij snel hun waarde. Zo ontstond ook het Amerikaanse gezegde 'not worth a continental'. Zou dit ook het lot zijn van de IOU's van de 'Golden State' Californië met miljarden dollars schuld? De IOU's werden al verhandeld via internet en banken hebben aangegeven ze niet te accepteren. Een bijzondere audit naar het uitgifteproces en de waarde van deze waarde(loze)papieren zou interessant zijn.

Ambiguïteit in normering

Per 1 september 2009 is de beloningscode voor tv-presentatoren bij de publieke omroep ingevoerd. De exorbitante inkomens van presentatoren boven de Balkenende-norm waren reden voor de Tweede Kamer om deze code in te voeren. Er is heel wat publiciteit geweest bij de eerste presentatie van de code, met veel kritiek op de gesignaleerde 'lekken'. Het blijkt dat presentatoren met eigen productiebedrijven en/of meerdere werkgevers in omroepland in feite buiten schot kunnen blijven. De code vormt namelijk geen belemmering voor presentatoren als Niehe, Tensen, Pauw & Witteman, De Leeuw of Felderhof om toch hoge inkomens te verwerven. Rik Felderhof lacht tevreden vanuit zijn eigen villa in Tanzania of betaalde werkadres 'Villa Felderhof' in Zuid-Frankrijk. Een audit naar de compliance met de code is een boeiend gegeven. Zal de Nederlandse publieke omroep of overheid opdracht geven tot een dergelijke audit? Hoe zouden we als auditors zo'n audit inrichten? Nemen we de feitelijke code als uitgangspunt? Of is de intentie van de opstellers van de code de norm?

Deskundigheid

In Nederland is een ware hype ontstaan om auto's aan te schaffen die energiezuinig en milieuvriendelijk zijn. Gedreven door voordeeltjes in de belastingsfeer kopen vele Nederlanders hybride auto's en kleine auto's. Maar zijn die auto's wel zo zuinig als wordt beweerd? Eerder dit jaar is onderzoek gedaan naar de kwaliteit van het door fabrikanten opgegeven brandstofverbruik en de CO_2-uitstoot van auto's. Naar nu blijkt voeren fabrikanten in laboratoria de metingen uit volgens de zogenaamde ECE+EUDC-testcyclus. Deze metingen geven een beter resultaat dan in de realiteit ooit kan worden gerealiseerd.
Nog een voorbeeld. Wat te denken van de feiten inzake de elektrische auto. Overheden en energieleveranciers investeren sterk in het positieve imago van de elektrische auto. Maar is die wel zo milieuvriendelijk? Uit nader onderzoek blijkt dat de huidige generatie Lithium-ion accu's zeer milieubelastend is. Pas als er een doorbraak wordt bereikt met bijvoorbeeld de condensatortechnologie zal de elektrische auto de auto op fossiele brandstoffen definitief verdringen. Als auditor steun je in audits vaak op deskundigen en hun oordelen. Maar zijn het wel experts? Zijn de onderzoeken wel goed uitgevoerd? Zie er maar eens achter te komen als schijn bedriegt en je steunt op vermeende experts of keurmerken die achteraf twijfelachtig blijken te zijn.

Wat kan het vak van auditor toch *bijzonder* boeiend zijn!

* Geniet thans van een sabbatical en gebruikt deze periode voor het uitvoeren van onderzoek en het schrijven van een boek (vankuijck.bob@hetnet.nl).

Ask how Protiviti is helping clients use the new IIA standards to create organizational value.

The new IIA International Standards for the Professional Practice of Internal Auditing (*Standards*) took effect in January. These *Standards* require improvements to IT governance, use of data analysis techniques, fraud risk management and records retention programs. Do you know how the *Standards* affect your organization? Are you using them as an opportunity to create value? At Protiviti, we recently held several online seminars for more than 2,000 internal audit leaders to help them understand the revisions. We are helping our clients use the *Standards* to make their internal audit functions more effective and efficient. Could you be doing the same? Ask how by visiting **protiviti.nl**, calling **020 346 04 00** or emailing **contact@protiviti.nl** today.

Powerful Insights. Proven Delivery.™

PRINCIPAL PARTNER

protiviti®
Risk & Business Consulting.
Internal Audit.

It's all about pushing the right buttons.

right

Carrière maken een kwestie van een druk op de juiste knop? Niet dus, dat weet jij inmiddels ook wel. Carrière maken vergt heel wat meer. Ambitie, gedrevenheid. Vakkennis. Passie voor je vak. Sociale kwaliteiten. En natuurlijk: talent. Maar groeien, vooruit komen, jezelf ontwikkelen – het vraagt nog meer: een omgeving waarin je talenten ook werkelijk tot hun recht kunnen komen. Waarin veelbelovende professionals als jij herkend worden en de ruimte krijgen om hun knowhow, hun gevoel voor het vak en affiniteit met klanten voortdurend te scherpen. Een omgeving zoals Deloitte dus.

Deloitte is met ruim 6.000 medewerkers en kantoren in heel Nederland de grootste organisatie op het gebied van Belastingadvies, Accountancy, Consultancy en Financieel Advies. ERS houdt zich bezig met dienstverlening voor ondernemingen, gericht op de controle van de processen en de IT-architectuur achter de cijfers. Dat betekent het signaleren, analyseren, beoordelen en managen van risico's. Variërend van boardroom-risico's op strategisch niveau tot technische risico's op netwerkniveau, zowel in een adviserende als controlerende rol. Buitengewoon uitdagend en afwisselend werk voor ambitieus talent. Voor iemand als jij dus!

Voor Deloitte Enterprise Risk Services zoeken we wo-ers met een bedrijfskundige of IT-gerelateerde studie en werkervaring vanaf 3 jaar. Met interesse in een van de volgende werkgebieden:

IT-Auditors
Specialisten die zich bezighouden met onderzoek naar de kwaliteit van de beheersing van IT-risico's en vraagstukken op het gebied van Corporate en IT Governance.

Applicatiespecialisten
Consultants die betrokken zijn bij het adviseren, controleren en implementeren van control frameworks en beveiliging van ERP-applicaties (SAP, Oracle, JD Edwards, Peoplesoft).

Security-specialisten
Professionals die adviseren over complexe security-systemen en bijbehorende processen (beveiliging, netwerken, hacking, privacy) en deze controleren en implementeren.

Data-specialisten
Je richt je o.a. op fraudedetectie in databestanden; ondersteuning bij accountantscontrole m.b.v. data-analyse; econometrische modelbouw en research om specifieke klantvraagstukken op te lossen; conversie en opschoning van data in IT-systemen als SAP, Oracle, JD Edwards.

Softwarespecialisten
Je ontwerpt en bouwt internettoepassingen met de nieuwste Microsoft-technologie. En je werkt in een multidisciplinair team van specialisten aan web-oplossingen om Deloitte en haar cliënten te ondersteunen.

Riskconsultants/internal auditors
Je werkt aan opdrachten op het gebied van enterprise-wide risk management en internal audit, die je in multidisciplinaire teams uitvoert bij onze grote internationale klanten.

Deloitte biedt je een ruime mate aan afwisseling en uitstekende doorgroeimogelijkheden. Internationale trainingen, postdoctorale opleidingsmogelijkheden, een informele werksfeer: dat is typisch Deloitte. We vragen veel van je, maar geven je ook veel ruimte. Meer weten over onze vacatures binnen ERS of solliciteren? Ga dan naar onze website www.careers.deloitte.com. Je kunt ook contact opnemen met Mina Bahaj, telefoonnummer 020 - 454 74 34, e-mail: mbahaj@deloitte.nl.

Deloitte.

Audit . Tax . Consulting . Financial Advisory.

TreasuringTalent.com