# AUDIT MAGAZINE

VAKBLAD VOOR DE INTERNAL AUDITOR

NUMMER 1 2016 JAARGANG 15

**Thema: DATA**

Interview met Jacob Kohnstamm | De komst van de datacratie
Belangrijke ontwikkelingen in de privacywetgeving | Ken je klassiekers

# Refreshing Advise
# Internal Audit 3.0

When looking at the business environments of our clients, we have noticed some severe challenges. Business conditions have become more complex and unpredictable, whilst information technology available is rapidly developing, leading to big data volumes and even new digital business models. Boards are reconsidering their top priorities, seeking for new business opportunities and managing the risks they are facing. In these uncertain times, there is a need for a partner who can provide assurances and assistance in their responses to a continuously evolving environment.

Our aim is to take our internal audit services and fundamentally make a difference to the organisations we partner with. We reframed the internal audit methodology and now have a different perspective and approach. We believe that getting insights into data using advanced data analytic techniques can assist organisations in achieving real outcomes and impact from internal audit.

By applying a different way of thinking we achieve a paradigm shift in internal audit. Adding new skills, tools, and techniques substantially improves the focus and effectiveness of the Internal audit function and will radically change the required effort put in at each stage of the internal audit methodology.

Internal Audit 3.0 will lead to several advantages: increased relevance and insights into high risk populations and value areas, better targeting and more coverage.

For more information, please contact Deloitte Risk Services,

**Wim Eysink**
+31 (0) 651 417 099
weysink@deloitte.nl

**Rob de Leeuw**
+31(0) 652 048 367
rdeleeuw@deloitte.nl



Deloitte.

COLOFON

**Audit Magazine wordt uitgebracht namens het Instituut van Internal Auditors Nederland (IIA Nederland) en de Stichting Verenigde Operational Auditors (SVRO).**

Bijdragen kunnen worden gemaild aan:
auditmagazine@iia.nl

**Redactie**
Drs. Laszlo Nagy EMIA RO (voorzitter)
Naeem Arif RO EMIA
Ir. Gezina Atzema RO
Sander Diks CIA
Drs. Nicole Engel-de Groot RA
Drs. Margot Hovestad RO
Drs. Huub van Hout RA CIA
Jip Olieroock MSc RO CIA
Björn Walrave RO CIA

Nederland
**E-mail**
auditmagazine@iia.nl
**IIA Nederland**
Burgemeester Stramanweg 102A, 1101 AA Amsterdam
Postbus 22657, 1100 DD Amsterdam
tel.: 088-0037100
iia@iia.nl, www.iia.nl

SVRO
Stichting Verenigde Operational Auditors
Burgemeester Stramanweg 102A, 1101 AA Amsterdam
Postbus 22657, 1100 DD Amsterdam
iia@iia.nl, www.iia.nl

**Bureauredactie**
Ria Harmelink Journalistieke Producties

**Uitgever**
VM uitgevers, Gees Wymenga
info@vm-uitgevers.nl
tel.: 035-6462623

**Vormgeving**
ViaMare grafisch ontwerp, Marijke Maarleveld

**Druk**
Senefelder Doetinchem

**Advertenties en abonnementen**
IIA Nederland, Postbus 22657, 1100 DD Amsterdam
tel.: 088-0037100
iia@iia.nl (zie ook de website: www.iia.nl).

IIA-leden ontvangen Audit Magazine uit hoofde van hun lidmaatschap gratis. Andere geïnteresseerden kunnen losse nummers en/of een abonnement gratis aanvragen bij het IIA.

Audit Magazine verschijnt vier maal per jaar.


ISSN: 1570-856X



# Data: het nieuwe goud?

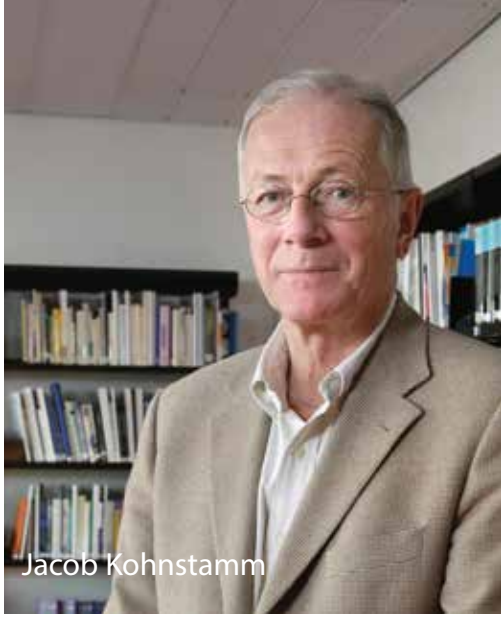
We trappen het jaar 2016 af met een nummer dat in het teken staat van data. Een onderwerp dat in toenemende mate in de zeer warme belangstelling staat van commerciële partijen als marketeers, kredietbeoordelaars en verzekeraars, overheid en toezichthouders. En aan dit rijtje kunnen we internal auditors moeiteloos toevoegen.

Data kregen het predicaat 'het nieuwe goud' in een uitzending van Zembla (2 december 2015). Overduidelijk werd deze omschrijving gebruikt vanwege het grote geld dat verdiend wordt met de handel in data. Maar zijn data ook voor internal auditors het nieuwe goud? Welke kansen biedt het gebruikmaken van data auditors, wat kunnen we met data-analyse en hoe kunnen we in ons werk het toenemende belang van data nog beter tot zijn recht laten komen? In dit nummer wordt in verschillende artikelen ingegaan op deze vragen. Bieden data niet zozeer kansen maar vormt het toenemende belang vooral een bedreiging voor onze beroepsgroep? Maakt de geautomatiseerde verwerking van data ons beroep straks misschien wel overbodig? Uit de antwoorden op de stellingen blijkt dat we ons hierover nog niet al te veel zorgen maken!

Er kleven overduidelijk risico's aan het opslaan van gegevens en het gebruik van data. De media berichten met grote regelmaat dat er sites gehackt zijn en gegevens van klanten of gebruikers 'op straat liggen'. De lijst met incidenten van de afgelopen jaren is ellenlang. Dit roept de vraag op of we ons voldoende bewust zijn van deze risico's en van alle privacyregels. Wat kunnen we als auditors doen om de privacy te waarborgen binnen onze organisaties? Dat de zorg voor de privacy van persoonsgegevens een achilleshiel is, blijkt wel uit het interview met Jacob Kohnstamm van de Autoriteit Persoonsgegevens (voorheen het College bescherming persoonsgegevens). Daarnaast vindt u in deze editie onder meer een zeer lezenswaardig interview met Ronald Prins, directeur bij Fox-IT, een artikel over de meldplicht bij datalekken en tips om als auditor bij te dragen aan de weerbaarheid van de organisatie tegen cybercrime.

De redactie heeft met veel plezier en energie gewerkt aan dit eerste nummer van 2016. We hopen dat u met net zo veel plezier dit nummer zult lezen!

De redactie van *Audit Magazine*

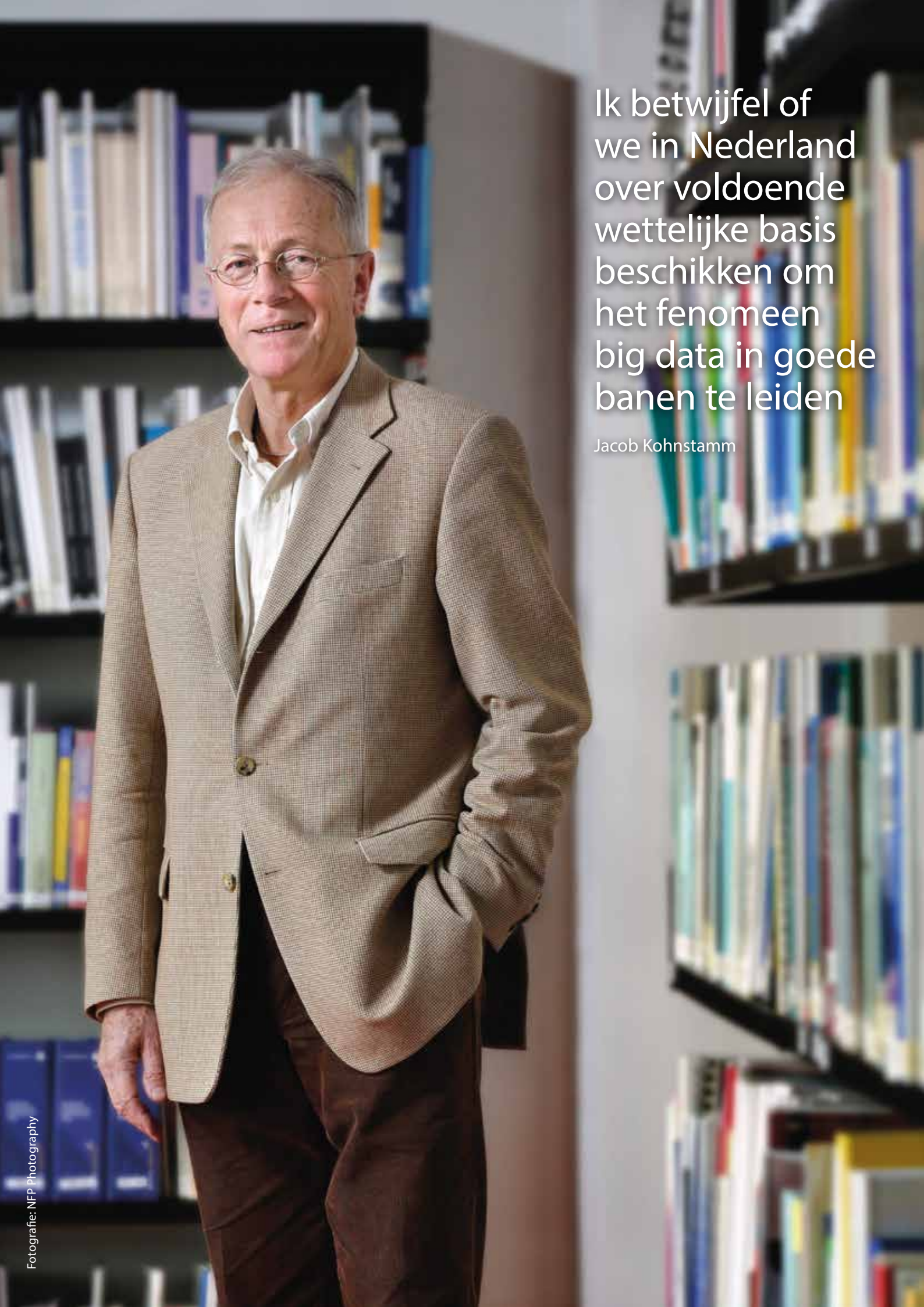

Jacob Kohnstamm

# THEMA: DATA





## Rubrieken



# Ik betwijfel of we in Nederland over voldoende wettelijke basis beschikken om het fenomeen big data in goede banen te leiden

Jacob Kohnstamm

Fotografie: NFP Photography

Sander Diks CIA
Jip Olieroock MSc RO CIA



*Audit Magazine* sprak met Jacob Kohnstamm, voorzitter van de Autoriteit Persoonsgegevens, voorheen het College bescherming persoonsgegevens, over nut en noodzaak van het beschermen van persoonsgegevens, big data en over de veranderingen in het privacylandschap. Ook de rol van internal auditors kwam aan bod.

# Bescherming van persoonsgegevens begint aan de **tekentafel**

## Over...

Jacob Kohnstamm is sinds 2004 voorzitter van de Autoriteit Persoonsgegevens. Van 2010 tot 2014 was hij ook voorzitter van de Artikel 29-werkgroep. Dit onafhankelijke en raadgevende orgaan bestaat uit de verzamelde Europese privacytoezichthouders. Daarnaast was hij van 2011 tot 2014 voorzitter van het executive committee van de International Data Protection and Privacy Commissioners Conference. Na diverse jaren als advocaat trad hij in 1981 namens D66 toe tot de Tweede Kamer en in de periode 1982-1986 bekleedde hij tevens het partijvoorzitterschap van D66. Hij was staatssecretaris van Binnenlandse Zaken van 1994 tot 1998. Van 1999 tot 2004 was hij lid van de Eerste Kamer.

**Als introductie voor de lezers van Audit Magazine: wat doet de Autoriteit Persoonsgegevens?**

"De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens, waaronder de Wet bescherming persoonsgegevens (Wbp) en adviseert over nieuwe regelgeving. Sinds 1 januari van dit jaar heeft het College bescherming persoonsgegevens een andere naam: Autoriteit Persoonsgegevens.
Met betrekking tot het houden van toezicht maakt de Autoriteit Persoonsgegevens een onderscheid in het realiseren van zogenoemde alternatieve interventies en het uitvoeren van meer diepgaande onderzoeken. Een alternatieve interventie is het bellen of aanschrijven van een bedrijf of organisatie wanneer de Autoriteit Persoonsgegevens een tip ontvangt over een (mogelijke) overtreding van de privacyregelgeving. De diepgaande onderzoeken ter plaatse vinden met name bij de meer ernstige overtredingen plaats en dienen volgens de regels van de Algemene Wet Bestuursrecht te worden uitgevoerd."

**Kunt u een paar voorbeelden noemen van wapenfeiten van de Autoriteit Persoonsgegevens?**

"De Autoriteit Persoonsgegevens heeft in samenwerking met de zusterorganisatie in Canada onderzoek gedaan naar WhatsApp. Het onderzoek richtte zich op het gegeven dat wanneer iemand de app downloadt, WhatsApp voor de dienstverlening ook toegang kreeg tot de mobiele telefoonnummers van niet-gebruikers in het elektronisch adresboek van de gebruiker. WhatsApp heeft inmiddels een aantal maatregelen genomen die waarborgen dat WhatsApp de telefoonnummers van niet-gebruikers alleen verwerkt om gebruikers met elkaar in contact te brengen en niet voor andere doelen.

Soms kunnen interventies van de Autoriteit Persoonsgegevens zeer snel effect hebben. Een voorbeeld hiervan betreft de ING die enige tijd geleden het plan lanceerde om de betalingsgegevens van klanten te vermarkten. Hierbij heeft de Autoriteit Persoonsgegevens, evenals de minister van Financiën, De Nederlandsche Bank en enkele Tweede Kamerleden, snel laten weten tenminste grote vraagtekens te zetten bij dit plan, met als gevolg dat het plan vooralsnog niet tot uitvoering is gebracht."

**Hebben we met ons ongebreideld gebruik van social media, het op allerlei plekken achterlaten van onze persoonsgegevens op internet en het klakkeloos accepteren van gebruikersvoorwaarden, ons recht op privacy niet een beetje verspeeld?**

"De gedachte dat men enkel vrijwillig informatie afstaat klopt niet. Het achterlaten van digitale voetsporen is bijna inherent aan het moderne leven, ook zonder dat je daar een keuze in kunt maken. Wanneer een medewerker met zijn OV-chipkaart naar kantoor gaat, voor het werk websites bezoekt en communiceert via zijn smartphone, worden tal van databases van nieuwe informatie voorzien. Dit gaat doorgaans ongemerkt. Dit kan een individu eigenlijk niet tegengaan. De enige mogelijkheid om dit te voorkomen is te kiezen voor een kluizenaarsbestaan. Dit laatste is natuurlijk een absurde gedachte, zeker omdat de bescherming van jouw persoonsgegevens een grondrecht is.
Microsoft heeft ooit eens aan enkele medewerkers gevraagd de tijd in kaart te brengen die zij nodig hadden om de verschillende privacyvoorwaarden waar zij als gebruiker mee werden geconfronteerd woord voor woord te lezen. Dit kwam uiteindelijk neer op ongeveer 76 dagen per jaar! Dat kun je in redelijkheid van niemand vergen. Daarom heeft de samenleving voor het doen naleven van het grondrecht ook goede wetgeving, een goede consumentenorganisatie en een sterke toezichthouder nodig."

## 'Privacy by design' is nodig om naleving van de Wbp te waarborgen

**Is de Autoriteit Persoonsgegevens voldoende uitgerust om deze toezichthoudersrol te kunnen vervullen?**

"De omvang van de Autoriteit Persoonsgegevens is zeker veel te beperkt. Een positieve ontwikkeling is wel dat de Autoriteit Persoonsgegevens per 1 januari 2016 een boetebevoegdheid heeft gekregen. Omdat wij sinds die datum boetes mogen uitschrijven is de naam dan ook veranderd in Autoriteit Persoonsgegevens. De boetebevoegdheid is echt nodig omdat een bedrijf nu nog weinig (financieel) risico loopt bij mogelijke overtreding van de Wbp. De prikkel ontbreekt om als bedrijf zelf toe te zien op strikte naleving. Ik verwacht dat met het verkrijgen van de nieuwe bevoegdheid de Wbp meer serieus zal worden genomen en beter zal worden nageleefd."

**Wat zijn de grootste risico's van big data? En biedt big data ook kansen?**

"Big data biedt zeker ook kansen. Denk bijvoorbeeld aan het inzetten van big data voor detectie en bestrijding van epidemieën. De mogelijkheden zijn enorm, maar eigenlijk staat het fenomeen big data nog in de kinderschoenen. Het probleem is dat de kern van de wetgeving en het doel van big data strijdig met elkaar lijken te zijn. De Wbp mikt op 'surprise minimalization' terwijl 'surprise maximalization' juist inherent is aan het inzetten van big data. De Wbp stelt onder meer dat er bij gebruik van gegevens altijd een duidelijk vooraf overeengekomen doel moet zijn vastgesteld (ofwel geen verrassingen waar de data voor wordt gebruikt). Bij big data is juist sprake van een zoektocht naar nieuwe mogelijkheden en toepassingen, die lang niet altijd vooraf zijn bepaald. Hierbij speelt natuurlijk de vraag in hoeverre individuen nog in staat zijn om vooraf 'explicit and informed consent' te geven wanneer zij hun data afstaan: het is immers niet te overzien waarvoor en op welk moment hun data gebruikt gaat worden. Overigens betwijfel ik of we in Nederland momenteel over voldoende wettelijke basis beschikken om het fenomeen big data in goede banen te leiden."

**U sprak en schreef al eerder over digitale predestinatie. Wat houdt dit in en waarom is het onwenselijk?**

"Met digitale predestinatie doel ik op de ontwikkeling dat mensen op basis van hun doen en laten online bepaalde profielen krijgen toebedeeld, die vervolgens bepalend zijn voor de wijze waarop zij worden gezien en behandeld. Het zogenoemde 'profiling'. Mensen worden ingedeeld in profielen zonder dat ze daarvan op de hoogte zijn, zonder dat zij weten wat de consequenties van de profielen voor hen zijn, laat staan hoe zij daar verandering in kunnen brengen. Dit blijkt in de praktijk niet alleen effecten te hebben op de reclameboodschappen die mensen ontvangen, maar bijvoorbeeld ook op de aard van de informatie die zoekmachines opleveren. Mensen kunnen zich daardoor minder vrij ontplooien en worden belemmerd in hun keuzevrijheid. Ik ben daar een sterk tegenstander van."

**Wat zijn de grootste dilemma's en uitdagingen voor organisaties als het gaat om bescherming van persoonsgegevens en privacy?**

"Voor bedrijven bestaat het risico dat bij het ontwikkelen van nieuwe producten en diensten er onvoldoende rekening wordt gehouden met de Wbp. Er ontbreekt dan iemand met gedegen kennis van de Wbp aan de ontwerptafel, met het risico dat achteraf moet worden vastgesteld dat een eerste release niet voldoet. De vervolgens noodzakelijk door te voeren aanpassingen pakken altijd duur uit. Bedrijven doen er dus goed aan om waarborgen in te bouwen dat de Wbp bij de ontwikkeling van nieuwe producten of diensten voldoende serieus wordt genomen. 'Privacy by design' is nodig om naleving van de Wbp te waarborgen.

Een van de grootste problemen bij de Wbp is dat de gevolgen van het niet naleven van deze wet voor gewone mensen vaak totaal onzichtbaar zijn. Als je in een auto rijdt met slechte remmen en het gaat mis dan zijn de gevolgen en de ernst direct duidelijk. Schort het in de naleving van de Wbp dan is het nog maar de vraag of een consument of burger kan zien of weten dat zijn grondrecht op bescherming van persoonsgegevens is geschonden."

**Is er momenteel niet sprake van een overkill aan wet- en regelgeving op privacygebied? En werkt dit niet verlammend of is het juist bittere noodzaak?**

"In beginsel hebben we goede wetgeving die de tand des tijds redelijk heeft doorstaan. De nieuwe Europese verordening over gegevensverwerking is bovendien een stap in de goede richting die er daarenboven voor zorgt dat er gelijke regels zullen komen in alle EU-lidstaten. De principes uit de thans geldende wetgeving zijn overigens per saldo in de nieuwe EU-wetgeving overeind gebleven.
Wij horen wel eens de kritiek dat de wetgeving te abstract is. Wettelijke formuleringen moeten echter altijd 'techniekonafhankelijk' blijven. Je kunt immers niet continu de wetgeving aan technologische ontwikkelingen blijven aanpassen. Wel is de verwachting dat de toekenning van de boetebevoegdheid ertoe gaat leiden dat er meer tegen de Autoriteit Persoonsgegevens geprocedeerd zal gaan worden. Dit leidt dan tot toenemende jurisprudentie en daar is in de rechtspraktijk dringend behoefte aan. Jurisprudentie maakt de wetgeving meer concreet en dit geeft bedrijven en consumenten handvatten."

**Kijken jongere generaties anders tegen privacy aan? Is er in dat opzicht sprake van een generatiekloof?**

"Ik kom nog wel eens op middelbare scholen en daar is er altijd wel iemand die roept dat-ie niets te verbergen heeft. Wanneer ik vervolgens vraag of zijn of haar ouders ook lid zijn van hun Facebook-vriendenclub is het antwoord van diegene 'daar niet aan te moeten denken'. De informationele zelfbeschikking speelt voor iedereen en lijkt redelijk los te staan van leeftijd. Ongetwijfeld zijn er verschillen per generatie maar in de kern heeft iedereen behoefte om een bepaalde controle te hebben en te houden over de informatie die wordt gedeeld met anderen."

**Welke rol hebben internal auditors als het gaat om privacy en bescherming van persoonsgegevens binnen organisaties?**

"Per 1 januari 2016 is de meldplicht datalekken van kracht. Dit houdt in dat zodra sprake is van een datalek, dit door betreffende organisatie moet worden gemeld bij de Autoriteit Persoonsgegevens en in bepaalde gevallen ook aan burgers en consumenten. Internal auditors doen er goed aan om zich inhoudelijk te verdiepen in de meldplicht datalekken om vervolgens te toetsen of de eigen organisatie voldoende waarborgen heeft ingebouwd om succesvol aan deze meldplicht te kunnen voldoen. De aanwezigheid van een plan om datalekken te voorkomen en om adequaat te reageren op een datalek zou in organisaties aanwezig moeten zijn en auditors zouden hier op kunnen toetsen. Het geven van invulling aan de meldplicht zou voor de bedrijven een vanzelfsprekendheid moeten worden.
Verder zouden internal auditors erop toe kunnen zien dat bij de ontwikkeling van nieuwe producten en diensten voldoende rekening met de Wbp wordt gehouden. Dit vergt enerzijds de aanwezigheid van voldoende kennis aan de tekentafel en anderzijds het voldoende serieus nemen van de wet in de dagelijkse praktijk van de organisatie."

**Hebt u ten slotte nog een advies aan de beroepsgroep als het gaat om privacy en bescherming van persoonsgegevens?**

"In algemene zin wil ik wijzen op het gezegde 'denkt aleer gij doende zijt en doende denkt dan nog'. Zorg er nu voor dat er voldoende kennis van de Wbp is en voorkom dat vertrouwen wordt geschaad. Internal auditors zouden deze uitgangspunten, mits relevant voor het auditobject, heel goed een plek kunnen geven in hun audits." <<

Drs. Rolf Bruins

De toename en impact van data zijn disruptief voor organisaties. In het nirwana van de toekomstbestendige organisatie – de datacratie – staan data-analyse, flexibiliteit en leren centraal. Dit hyperbeweeglijke organisatietype, waarin voorspelbaarheid van de toekomst op basis van data een van de grootste uitdagingen is, vereist een systematische en onafhankelijke werkwijze van de auditfunctie.

# De komst van de **datacratie**

Er wordt steeds meer gepubliceerd over de 'quantified self', 'quantified workplace' en 'quantified consumer'. Alles wordt quantified. Het grote doel van deze quantifiedbeweging is te begrijpen *waarom* mensen doen wat ze doen. Het waarom van menselijk gedrag ligt besloten in de feitelijke interactiepatronen. Technologie stelt ons in staat deze patronen bloot te leggen, te analyseren en er beslissingen op te baseren. We bevinden ons inmiddels middenin het interactietijdperk. We nemen daarmee afscheid van de voorliggende periode, het transactietijdperk. Hierin was het mogelijk om via formele transacties, bijvoorbeeld het afsluiten van een verzekering of het scannen van de boodschappen, te achterhalen wat consumenten deden. Dit heeft doorgaans weinig voorspellende waarde en is voor bedrijven voor toekomstige acties minder interessant. In het interactietijdperk zijn we steeds beter in staat wisselwerkingen met en tussen consumenten te kwantificeren waardoor enorme hoeveelheden data ontstaan die met behulp van algoritmes real-time geanalyseerd kunnen worden, met als doel het voorspellen en verzilveren van zakelijke kansen.

**Achtergrond interactietijdperk**

Het interactietijdperk heeft zijn basis in het 'internet of humans' (het gebruik van social media op internet zoals wij het nu kennen) en het daarop voortbordurende 'internet of things'. Door het toenemende gebruik van digitale toepassingen laten we (vaak onbewust) een schat aan data achter. Deze kunnen op een slimme manier worden 'gedolven' en opgeslagen in gegevenspakhuizen. De schatting is dat er de afgelopen twee jaar tien keer zoveel gegevens zijn vastgelegd dan in de gehele geschiedenis daarvoor.[1]

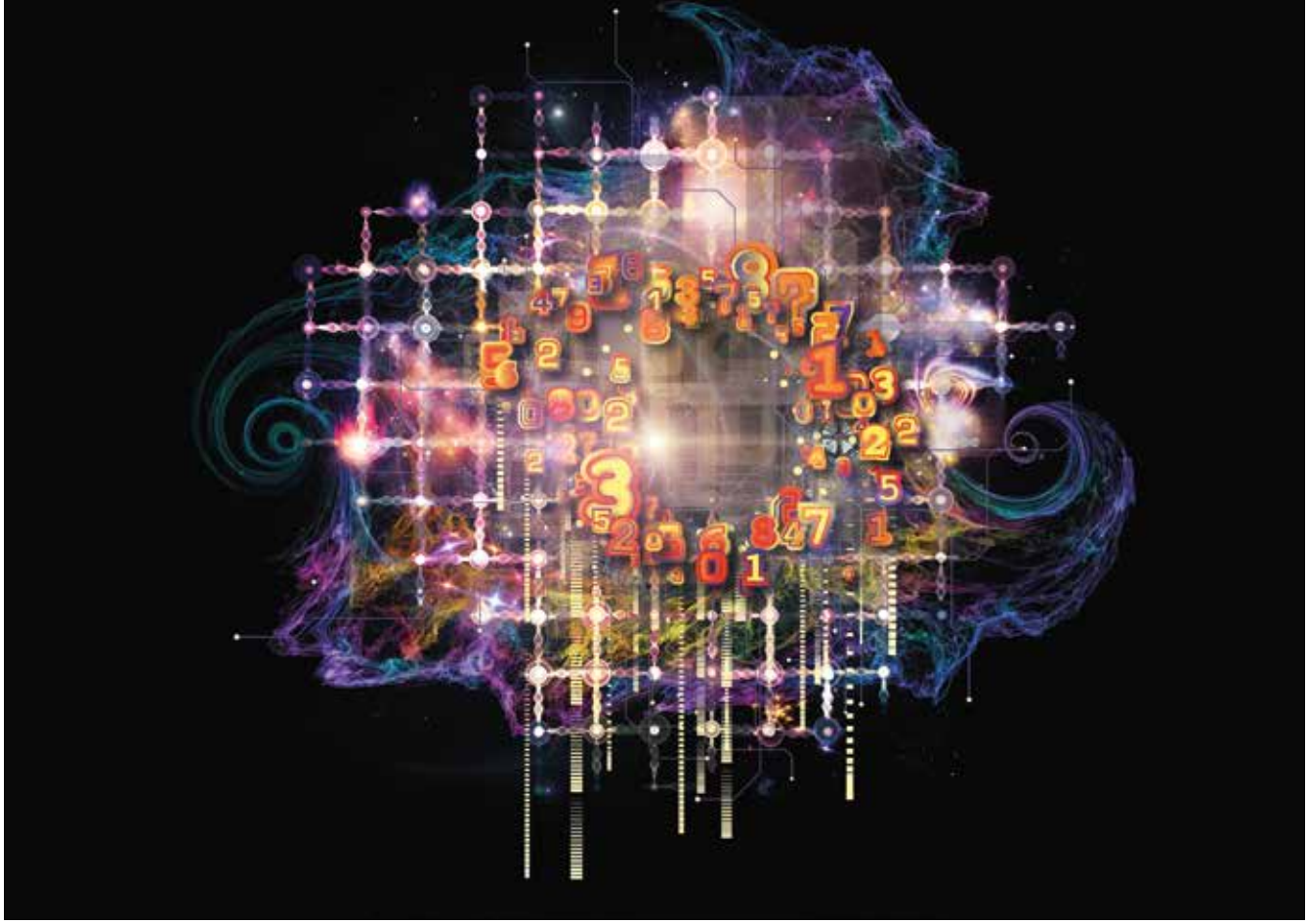
Met deze schatting laat de toekomst zich op dit punt niet moeilijk raden. Het sec verzamelen van data levert echter niets op. Het is juist de kunst om deze via data-analyse op een slimme manier te koppelen aan andere data. De analyse van aanschaf van een product wordt interessanter op het moment dat dit gegeven wordt gekoppeld aan voorkeuren op basis van eerder bezochte websites of aankopen die in het verleden zijn gedaan. Op die manier ontstaat een basis voor inzichten die we daarvoor niet hadden. Hiermee tekent de organisatie-evolutie zich af die mede een impuls krijgt in het hoger beroeps- en universitair onderwijs met studies als business analytics en allerlei varianten daarop.

**Stadia van organisatie-evolutie**

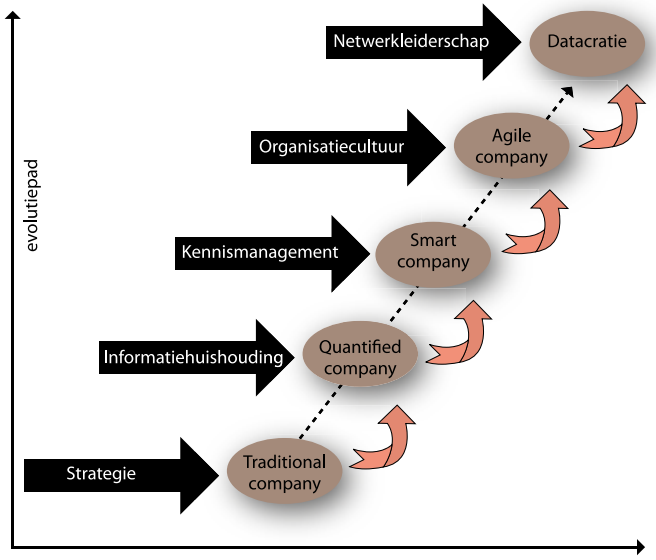
Er zijn vier fasen die een organisatie moet doorlopen om sustainable of toekomstvast te kunnen zijn.

**Fase 1. *Van traditional naar quantified***

Veel organisaties bevinden zich in stadium 1, wat ik de traditional company noem. De structuren, werkwijzen, competenties en informatiehuishouding zijn als traditioneel te kenmerken. Vooral het ontbreken van schaalbaarheid van deze aspecten



is kenmerkend voor traditionele organisaties. Een belangrijke keuze voor de traditionele organisatie om verder te evolueren is strategisch van aard en omvat de vraag of er daadwerkelijk ingezet wordt op een datagedreven toekomst.
De transitie naar een quantified company markeert in feite de overgang van het werken met een database naar 'data-driven-werken'. Hierbij is het cruciaal om de informatiehuishouding op orde te hebben. Aan de basis van de quantified company staat een duidelijke informatiebehoefte. Deze behoefte is gebaseerd op datgene wat de organisatie ook daadwerkelijk kan beïnvloeden zoals kosten, opbrengsten en kwaliteit. Need-to-knowinformatie krijgt altijd voorrang op nice-to-knowinformatie.




**Figuur 1.** De 4 fasen om te komen tot datacratie

**Fase 2.** ***Van quantified naar smart***
In een volgende fase naar de smart company wordt expliciet aandacht besteed aan het ontdekken van interactiepatronen. Door deze te herkennen, hier data van af te 'tappen' om er vervolgens interessante patronen uit af te leiden, ontstaat kennis die de organisatie smart maken. Het is hierbij van belang om te onderkennen dat er drie soorten interacties zijn, te weten interacties buiten de organisatie (bijvoorbeeld fora en gemeenschappen op social media), interacties met de organisatie (stakeholders communiceren met of over de organisatie) en interacties binnen de organisatie (communicatiepatronen van medewerkers onderling).
Door data uit deze interacties af te tappen en met elkaar te combineren via algoritmes ontstaan inzichten die we via de traditionele wegen van gesprekken, rapporten of intuïtie nooit hadden kunnen krijgen. In de smart company is de functie van datawetenschapper die samenwerkt met (data)gedreven medewerkers cruciaal. Data zijn hier inmiddels de 'raison d'être' van de organisatie geworden. Zoals eerder aangegeven, spelen Hogescholen en Universiteiten hier met hun opleidingsaanbod reeds op in.

**Fase 3.** ***Van smart naar agile***
De smart company zet naast menselijk kennismanagement ook in op 'deep learning', ook wel 'machine learning' genoemd, waarbij systemen of software zelf kunnen leren dankzij slimme algoritmen. Deze blijken in de praktijk bijvoorbeeld al beter dan oncologen te zijn in het herkennen van borstkanker op medische scans, zijn effectiever in het opsporen van plagiaat in werkstukken van studenten en kunnen twee keer beter verkeersborden herkennen dan mensen. Smart companies zijn in staat om het leren van medewerkers te combineren met het leren van algoritmen zodat ze elkaar kunnen versterken. Een voorbeeld van een agile company qua werkwijze en cultuur is

het Nederlandse bedrijf Springest. Springest, een onafhankelijke vergelijkingssite voor opleidingen en trainingen, baseert zich op holacratische principes en kent bijvoorbeeld geen top down management.[2] De hiërarchische lagen met teams en managers zijn vervangen door gelijkwaardige cirkels waarin de rollen van de medewerkers centraal staan. Dit alles draagt bij aan de agility van de organisatie.

Smart werken is een voorwaarde om snel en flexibel te kunnen opereren. In de eerste plaats komen concurrenten niet alleen van links of rechts maar komen ze inmiddels ook uit de lucht vallen zoals bij Airbnb en Uber het geval was. In de tweede plaats moeten kansen worden gepakt als ze zich voordoen of als ze door de organisatie gecreëerd worden. Kodak heeft bijvoorbeeld vanuit de eigen R&D-gelederen indertijd zelf de mogelijkheden voor digitale fotografie ontwikkeld maar deze kans niet benut omdat het de corebusiness te veel zou kannibaliseren. Kodak is inmiddels geen speler meer die ertoe doet omdat ze onvoldoende 'agile' was.

Mentale beweeglijkheid in combinatie met schaalbaarheid van mensen, middelen en werkwijzen is in een agile-organisatie een must. Hier passen niet langer snelheidsbeperkende maatregelen in de vorm van hiërarchieën, protocollen, beleidsplannen en andere door/doodgeformaliseerde zaken. Deze traditionele managementreflex van beheersbaarheid wordt vervangen door de reflex van het snel kunnen leren van nieuwe omstandigheden. Het reeds opgetuigde kennismanagement in de fase van de smart company is een belangrijk middel voor de agile company. Ook om het leren binnen de organisatie te faciliteren. Leren wordt de dominante cultuur. De werkplek wordt een samenwerkplek waar tevens samen gedacht en geleerd wordt. Technologie ondersteunt dit.

**Fase 4.** ***Van agile naar datacratie***

De datacratie kunnen we zien als het organisatorische equivalent van het boeddhistische nirwana en vertegenwoordigt de hoogste staat die door de organisatie bereikt kan worden. Het is zoals gezegd de toekomstbestendige organisatie die haar data structureel analyseert, die flexibel is en leert. Alle elementen van de evolutionaire voorlopers zijn hierin zichtbaar en met elkaar verbonden. Er wordt data-driven gewerkt en gedacht, data worden uit de verschillende interactiepatronen afgetapt en geanalyseerd en de principes van agility behoren tot de cultuur van de organisatie. In een cultuur van agility gaan mensen en hun onderlinge interactie boven processen en tools, werkende methoden zijn belangrijker dan allesomvattende documentatie, samenwerking met de klant gaat boven

contractonderhandelingen en het inspelen op verandering is belangrijker dan het volgen van een plan.[3]
De basisarchitectuur van de datacratie is van eenzelfde soort als die van internet. Het is een netwerk van netwerken. Een belangrijk kenmerk van netwerken is het ontbreken van centrale sturing. Een organisatie is deelnemer aan het netwerk en kan zichzelf niet als eigenaar van een netwerk aanwijzen. Het is onder omstandigheden (bijvoorbeeld door het bezit van financiële middelen, superieure kennis of onderhandelingsmacht) hoogstens mogelijk om (tijdelijk) de rol van netwerkregisseur te vervullen. Door het ontbreken van centrale sturing wordt het ontwikkelen van netwerkleiderschap steeds belangrijker. Een organisatie kan alleen deel uitmaken van een netwerk indien het meetbaar in staat is om toegevoegde waarde te bieden. Een organisatie die geen waarde toevoegt is in managementtermen waardeloos en zal niet overleven.
Een belangrijk kenmerk van de datacratie is dat het bestuurd wordt door data. Dit in tegenstelling tot een democratie waarin het 'volk' bestuurt. Data heeft geen behoefte aan macht. Mensen wel. Machtsmisbruik wordt daarmee tot een minimum beperkt. Het kan wel optreden indien een lid van het netwerk beschikt over superieure inzichten omdat het kan beschikken over grote hoeveelheden superieure data. In dat geval kan het andere partijen afhankelijk maken. Echter, de overstap van (leden van) het netwerk naar een andere 'databroker' is in deze tijden snel gemaakt.
Iedere evolutie heeft zijn eigen singulariteit. Dit is een situatie waar de normale regels of wetten niet meer geldig zijn of niet meer toegepast kunnen worden. De datacratie kunnen we als een organisatorische singulariteit beschouwen. Het vindt zijn oorsprong in de strategische erkenning van het feit dat de organisatie daadwerkelijk data-driven zal moeten worden.

**Nieuwe dimensies**
Het doorlopen van de verschillende evolutiefasen zal voor organisatie en medewerkers uitdagend zijn. Gedreven medewerkers zullen met data en data-analyse met nieuwe dimensies in het werk te maken gaan krijgen. De humanresourcesafdeling zal haar focus moeten verleggen naar het zoeken en opleiden van datagedreven medewerkers met persoonlijke flexibiliteit en leervermogen als belangrijkste kwaliteiten.
Momenteel zien we nog geen uitgesproken voorbeelden van bedrijven waarin alle aspecten van de datacratie vertegenwoordigd of met elkaar verbonden zijn. Het grootste modeconcern ter wereld, Inditex, met fast-fashionmerken als Zara en Bershka, is een duidelijk voorbeeld van een quantified company. Het moederbedrijf heeft reeds in een vroeg stadium ingezet op waardecreatie met behulp van data. Met het uitgekiende quick-responssysteem kan het sneller en goedkoper dan haar concurrenten nieuwe collecties ontwikkelen en in de winkels aanbieden, met minimale voorraden.

**Werken in de datacratie, wat betekent dat?**
Wat betekent de transformatie in de richting van de datacratie nu voor de internal auditor? Even terug naar het interactietijdperk. Het volgen van en interveniëren op de drie eerder genoemde interacties (buiten de organisatie, met de organisatie en binnen de organisatie) vormt de kern van de werkwijze van de datacratie. Dat kan alleen als er relevante data afgetapt kunnen worden uit interacties om daarmee toekomstige interacties te voorspellen. De focus van de internal auditor verschuift daarmee van controles achteraf, kenmerkend voor het transactietijdperk, naar forecasting.
De kwaliteit van voorspellingen hangt een-op-een samen met de kwaliteit, hoeveelheid en relevantie van de interactiedata. Het monitoren van deze aspecten ligt voor een belangrijk deel bij auditors. Bovendien is het essentieel dat de algoritmes kloppen die de data transformeren naar patronen. Ook hier ligt een uitdaging voor de auditfunctie. Hier komen datawetenschappelijke kennis en vaardigheden om de hoek kijken. In termen van paradigma zal de auditfunctie in de datacratie niet meer gezien worden als een functie die zich richt op het achteraf toetsen en analyseren, maar als borging van de voorspellende kwaliteiten van de organisatie. Dat kan alleen bereikt worden indien auditors in staat zijn data-driven te leren en te denken en over de vaardigheid beschikken om deze snel en flexibel op te schalen. Dat is de vaardigheid om samen met anderen te kunnen werken door ook samen te denken en samen te leren, en dat in de context van netwerken.
Een data-driven wereld waarin de focus ligt op het voorspellen van de toekomst op basis van data vraagt een andere visie op auditing. In termen van een metafoor zal de auditor de situatie op de weg steeds minder beoordelen via de achteruitkijkspiegel maar vooral door door de voorruit te kijken. Een richting die al eerder is ingezet met de eisen aan de relevantie van data naast betrouwbaarheid. Deze verdere ontwikkeling vereist een datacratisch perspectief op de wereld, een perspectief waarbij hoogwaardige datakwaliteit een voorwaarde is voor de succesvolle organisatie van de toekomst. Mogelijk zal de pendulum weer meer richting gegevensgericht auditen gaan al blijven de processen rondom de data natuurlijk even zo belangrijk. <<

## De focus op het voorspellen van de toekomst op basis van data vraagt een andere visie op auditing

**Noten**
1. Klous en Wielaard (2014).
2. Zie ook het boek *Holacracy* van Brian Robertson, de grondlegger van dit fenomeen.
3. Zie ook het Agile Manifest.

Rolf Bruins is breinexpert, hbo-docent, auteur van artikelen en lesboeken, spreker en eigenaar van het opleidingsbureau Management Class.
info@managementclass.nl

FSV
RISK ADVISORY


info@fsvriskadvisory.nl
www. fsvriskadvisory.nl

# Winst is een beloning voor het nemen van risico's

**Een goed rendement vraagt dan ook om helder zicht op risico's en om goede maatregelen om risico's te beheersen. Wie dat optimaal in de vingers heeft, neemt een voorsprong op de concurrentie. Dat is waar FSV Risk Advisory elke dag mee bezig is bij een breed scala van organisaties.**

We opereren op drie terreinen met een sterke onderlinge verbinding:

- Internal Audit, waaronder **Quality Assessment Review & Support**
- Risk Management, waaronder Control Framework Improvement
- Financial Management

Onze ervaren professionals werken met u samen binnen deze drie 'lines of defence'. Uitgangspunt in onze dienstverlening is het Governance Risk Control model waarin de lines of defence met elkaar verbonden zijn.

Meer weten? Bel ons op nummer 0418 57 96 89, of bezoek onze website:

**www.fsvriskadvisory.nl**

# De lezer over DATA

*Audit Magazine* legde via de website en het lezerspanel de lezer vijf stellingen voor over data. In totaal reageerden 75 lezers.

Data is een begrip waar je tegenwoordig als auditor onmogelijk omheen kunt. Data is alom vertegenwoordigd, het wordt overal om ons heen gebruikt en opgeslagen. Zo bewaren bedrijven als Google gegevens over je zoekopdrachten en je telefoon registreert ook allerlei gegevens. Aan het gebruik en de opslag van data kleven naast grote kansen ook grote risico's. Het waarborgen van de privacy van de gebruikers is bijvoorbeeld een belangrijk aandachtsgebied voor veel organisaties. Een aandachtsgebied met vele dilemma's zoals ook wel blijkt uit het interview met Jacob Kohnstamm, voorzitter van de Autoriteit Persoonsgegevens. Wat mogen en kunnen organisaties wel en niet doen met de verzamelde data? Hoe worden deze gegevens beveiligd? En wat doe je als het verkeerd gaat? Zoals afgelopen zomer toen een vreemdgangerssite werd gehackt en de gegevens van miljoenen klanten 'op straat' lagen.

Kunnen dit soort incidenten worden voorkomen door meer regels en richtlijnen? Een meerderheid (68%) denkt dat dit niet de oplossing is. Een veelgehoorde opmerking is dat privacywet- en regelgeving een verlammende werking heeft op organisaties. Hier zijn de meningen over verdeeld. Bijna de helft van de respondenten (49%) is het hier mee oneens en 32% is het hiermee eens.

De hoeveelheid data groeit snel en is vaak complex en ongestructureerd. Big data wordt desalniettemin gezien als het nieuwe goud voor bedrijven met schier oneindige mogelijkheden. Terecht? Over de vraag of big data een hype is die weer overwaait waren de lezers duidelijk: nee, big data is geen hype antwoordde 88%. Big data is relevant voor de werkzaamheden van auditors maar hebben wij voldoende kennis en kunde om hier goed gebruik van te maken en om erover te kunnen oordelen of is een auditspecialisatie noodzakelijk? 48% van de respondenten denkt dat er een nieuwe auditspecialisatie zal ontstaan vanwege de grote relevantie van big data. Werk aan de winkel dus voor onze opleiders!

Een ruime meerderheid (82%) denkt dat wij als auditor nog steeds nodig zijn binnen een organisatie ondanks de komst van big data-analyse. Terwijl vergelijkbare beroepsgroepen in een onderzoek van de wetenschapper Carl Frey en Michael Osborne in de Top-10 staan van beroepen die overbodig worden in verband met automatisering. Ontkennen we de kracht van big data of zien wij ons wellicht in een andere rol?

Wij danken de respondenten voor het beantwoorden van de stellingen!

**één**

Er zijn meer regels en richtlijnen nodig om het aantal incidenten ten aanzien van informatiebeveiliging verder terug te dringen

| | |
|---|---|
| 1. Helemaal mee eens | 5% |
| 2. Mee eens | 12% |
| 3. Neutraal | 15% |
| 4. Mee oneens | 52% |
| 5. Helemaal mee oneens | 16% |

**twee**

De wet- en regelgeving omtrent privacy heeft een verlammende werking op organisaties

| | |
|---|---|
| 1. Helemaal mee eens | 5% |
| 2. Mee eens | 27% |
| 3. Neutraal | 19% |
| 4. Mee oneens | 41% |
| 5. Helemaal mee oneens | 8% |

**drie**

Big data is een hype die wel weer overwaait

| | |
|---|---|
| 1. Helemaal mee eens | 3% |
| 2. Mee eens | 1% |
| 3. Neutraal | 8% |
| 4. Mee oneens | 55% |
| 5. Helemaal mee oneens | 33% |

**vier**

De relevantie van big data is zo groot dat hier een nieuwe auditspecialisatie uit voortkomt

| | |
|---|---|
| 1. Helemaal mee eens | 15% |
| 2. Mee eens | 33% |
| 3. Neutraal | 17% |
| 4. Mee oneens | 32% |
| 5. Helemaal mee oneens | 3% |

**vijf**

Het huidige werk van de auditor wordt door de komst van big data analyse grotendeels overbodig

| | |
|---|---|
| 1. Helemaal mee eens | 1% |
| 2. Mee eens | 13% |
| 3. Neutraal | 4% |
| 4. Mee oneens | 47% |
| 5. Helemaal mee oneens | 35% |

Drs. Piet Goeyenbier RE RA RO

Door ontwikkelingen, zoals e-commerce, apps, big en open data en 'internet of things', nemen de risico's voor de privacy toe. Het Nederlandse en het Europese parlement spelen op deze ontwikkelingen in met nieuwe wetgeving. 1 januari 2016 werd de meldplicht datalekken van kracht en later volgt de Algemene Verordening Gegevensbescherming (AVG). NOREA ontwikkelde een nuttig hulpmiddel in de vorm van een Privacy Impact Assessment (PIA).

# Belangrijke ontwikkelingen in de **privacywetgeving**

Medio 2015 is de meldplicht datalekken aangenomen en is de ingangsdatum van deze wet vastgesteld op 1 januari 2016. Hiermee is aan de Wet bescherming persoonsgegevens (Wbp) een meldplicht voor inbreuken op beveiligingsmaatregelen voor persoonsgegevens toegevoegd. Met de meldplicht datalekken wordt beoogd de gevolgen van een datalek voor de betrokkenen zoveel mogelijk te beperken en hiermee een bijdrage te leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

**Meldplicht**

De meldplicht datalekken schrijft voor dat de verantwoordelijke voor de verwerking van persoonsgegevens bij een datalek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, een melding moet doen bij de toezichthouder, de Autoriteit Persoonsgegevens (AP), maar ook de betrokkene(n) moet informeren. Deze meldplicht geldt voor alle verantwoordelijken voor de verwerking van persoonsgegevens, zowel in de private als publieke sector. Als er geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete, opgelegd door de AP. In dit kader heeft met deze wetsuitbreiding ook een uitbreiding van de bevoegdheid van de AP tot het heffen van bestuurlijke boetes plaatsgevonden.

Met de inwerkingtreding van de wetsaanpassing is de naam van het College bescherming persoonsgegevens (CBP) gewijzigd in Autoriteit Persoonsgegevens. Met deze nieuwe naam komt de uitbreiding van de bestuurlijke bevoegdheid van de toezichthouder beter tot uitdrukking. De AP heeft eind september 2015 in concept richtsnoeren aangereikt over de nadere invulling van de meldplicht datalekken. De AP geeft verder aan dat zij begin 2016 met een formulier en een website komt zodat dan de meldingen ook daadwerkelijk plaats kunnen vinden.

Concreet betekent de uitbreiding van de Wbp het volgende: de verantwoordelijke voor de verwerking van persoonsgegevens dient de AP onverwijld in kennis te stellen van een inbreuk op de beveiliging die leidt tot (een) aanzienlijke (kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Ook dient de verantwoordelijke de betrokkene(n) te informeren (art. 34a). In artikel 34a is de wijze waarop invulling moet worden gegeven aan deze meldplicht nader uitgewerkt. Bij het niet of onvoldoende invulling geven aan het voorgaande kan de AP een bestuurlijke boete opleggen van 10% van de omzet van de betreffende organisatie. Het maximumbedrag van deze bestuurlijke boete is € 810.000 (dit was onder de oude wetgeving € 4500).

Het moge duidelijk zijn dat het opleggen van een bestuurlijke boete naast de financiële gevolgen ook de nodige negatieve gevolgen heeft voor de reputatie van de betreffende organisatie.

**Privacy officer**

Naast de meldplicht is nog een belangrijke verandering voor de privacywetgeving aanstaande, de vervanging van de Wbp door de AVG. Dit betreft een Europese verordening die directe werking heeft in de Europese lidstaten. Voor overheid en bedrijfsleven houdt deze nieuwe verordening in dat expliciet aandacht moet worden geschonken aan het onderwerp

privacy door bijvoorbeeld het inrichten van privacybeleid en het beschikken over een privacy officer. Het doel hiervan is zorgdragen dat een individu zijn rechten op het gebied van privacy ook daadwerkelijk kan effectueren.
Voor een organisatie leidt de meldplicht datalekken tot de volgende drie vragen:

- Beschikt de organisatie over registraties met privacygevoelige persoonsgegevens waarvoor zij verantwoordelijk kan worden gesteld?
- Worden met de betreffende persoonsregistratie(s) risico's gelopen op het gebied van datalekken?
- Indien zich onverhoopt een datalek voordoet is dan het proces van ontdekking, melding en oplossing in voldoende mate ingericht?

**Privacy Impact Assessment (PIA)**
Met de PIA heeft NOREA in een hulpmiddel voorzien waarmee een organisatie kan inventariseren in welke mate privacy bij een persoonsregistratie van belang is en of er toereikende maatregelen zijn getroffen. Voor overheidsorganisaties is het uitvoeren van een PIA verplicht. De rijksoverheid heeft hiervoor een eigen PIA ontwikkeld. Hier wordt verder ingegaan op de PIA die ontwikkeld is door NOREA.
Allereerst kan een organisatie een quickscan PIA uitvoeren met een 'privacychecker' (beschikbaar via internet). Via tien vragen wordt dan vlot inzicht verkregen of het uitvoeren van een PIA zinvol is. Is dit het geval, dan kan de PIA worden uitgevoerd (per persoonsregistratie) aan de hand van de vragenlijst die is opgenomen in het NOREA-document. Een praktische werkwijze is om dat gezamenlijk te doen met een aantal betrokkenen (zoals de verantwoordelijke voor de persoonsregistraties, de privacy officer en de bewerker). Door de discussie van deze betrokkenen ontstaat een breder en gedeeld beeld. Het vastleggen van de onderbouwing van de antwoorden is belangrijk voor later (onderhoudbaarheid en overdracht). De internal auditor kan in dit proces bijvoorbeeld een rol vervullen op het gebied van het toezien op de kwaliteitsborging.
De onderdelen van de PIA vragenlijst (NOREA):
1. Het type project.
2. De gegevens.
3. Betrokken partijen.
4. Verzamelen van gegevens.
5. Gebruik van gegevens (inclusief verstrekken).
6. Bewaren en vernietigen van gegevens.
7. Beveiliging.

Door het uitvoeren van de PIA worden de eerste twee van de hiervoor genoemde drie vragen beantwoord. Een toereikend informatiebeveiligingsplan kan (voor de betreffende persoonsregistratie) inzicht bieden in de getroffen beveiligingsmaatregelen (de opzet). Om daadwerkelijk zicht te krijgen op de risico's die samenhangen met de persoonsregistratie, de getroffen beheersmaatregelen en mogelijke datalekken, zou een onderzoek uitgevoerd moeten worden naar de opzet, het bestaan en de werking van het beheer en de beveiliging van

## Als er geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete

de betreffende persoonsregistratie. Het komt overigens vaak voor dat de verwerking van de persoonsregistratie (of delen daarvan) door een serviceorganisatie plaatsvindt (de bewerker). Door middel van een bewerkersovereenkomst moeten dan de eisen en de plichten van de verantwoordelijke worden doorvertaald naar de betreffende dienstverlener.
De derde vraag, het proces van ontdekking van het datalek tot melding (en de registratie van die meldingen), is niet geadresseerd in de PIA-vragenlijst. Zo'n proces moet door iedere organisatie worden ingericht, waarbij wel aangesloten kan worden op de aanwezige procedures op het gebied van melden van incidenten en calamiteiten.

**Te treffen acties**
Nadat door middel van analyse is vastgesteld dat de Wbp en de meldplicht datalekken relevant zijn, dient de organisatie de relevante processen en beheersingsmaatregelen te inventariseren, te optimaliseren en te borgen. Ook dienen de bewerkersovereenkomsten te worden aangepast zodat de bewerker (de serviceorganisatie) eventuele datalekken zo spoedig mogelijk meldt bij de verantwoordelijke organisatie. Hierdoor kan deze invulling geven aan de wettelijke meldplicht en de bijbehorende vereisten, zoals de registratie van incidenten en calamiteiten.
Maatregelen in het kader van de meldplicht datalekken:
1. Benoem de verantwoordelijke(n) voor de registratie.
2. Pas de bewerkersovereenkomsten aan.
3. Pas het incident- en calamiteitenproces aan.
4. Zorg voor een meldprocedure (datalekprotocol).
5. Zorg van registraties van de gedane meldingen.

Naast de inrichting moet ook een meldprocedure (of datalekprotocol) worden ingericht. Zo'n meldprocedure kan uit de volgende stappen bestaan:
- Intern melden, registreren en analyseren van een incident.
- Vaststellen of sprake van een datalek is.
- AP informeren en deze melding registreren.
- Betrokkenen informeren en deze melding registreren.
- Oplossen datalek.
- Evalueren.

Zolang er nog geen heldere regels zijn die voorschrijven wanneer wel en niet gemeld moet worden, kunnen de volgende vuistregels worden gehanteerd:
- Hoe zou u geïnformeerd willen worden als het uw eigen persoonsgegevens betreft?
- Bij twijfel melden!

**De rol van Internal Audit**
Zoals al is aangegeven heeft de aangepaste privacywetgeving consequenties voor de organisatie. Door het uitvoeren van een PIA kan de organisatie nagaan of kwetsbaarheden voorkomen bij persoonsregistraties. Is dit het geval, dan dient de organisatie in actie te komen om te voldoen aan de eisen van de nieuwe privacywetgeving. Internal Audit kan hierbij verschillende rollen vervullen. Zij kan de organisatie bewust maken van de (komende) wetswijzigingen zodat de organisatie daar tijdig op kan anticiperen (de signalerende rol). Tijdens het analyse- en het implementatieproces van de beheersingsmaatregelen kan zij de rol vervullen van facilitator dan wel toezicht houden op de kwaliteitsborging van het proces. Na de implementatie kan Internal Audit een audit uitvoeren naar de nieuwe processen. Daarnaast kan de internal auditor ook een onderzoek uitvoeren naar de kwaliteit van het beveiligingsstelsel. <<

## Relevante websites

- http://www.norea.nl/norea/actueel/nieuws/presentatie+pia.aspx
- https://cbpweb.nl/nl/over-privacy/persoonsgegevens/beveiliging-van-persoonsgegevens#faq
- http://www.cip-overheid.nl
- http://www.IBDgemeenten.nl
- http://privacychecker.eu/nl
- http://www.justitia.nl/privacy/

Piet Goeyenbier is auditmanager bij de Auditdienst Rijk (ADR) van het ministerie van Financiën. Hij is lid van de Commissie Professional Practices van IIA Nederland. Verder is hij als extern deskundige betrokken bij de AITAP (post-master IT-auditopleiding) aan de Amsterdam Business School (UvA).
p.j.m.goeyenbier@minfin.nl

Dit artikel is geschreven op persoonlijke titel.

# Nieuw redactielid

**Jip Olieroock**
Sinds kort ben ik lid van de redactie van *Audit Magazine*. Graag maak ik van deze gelegenheid gebruik om mijzelf te introduceren. Nadat ik bij diverse organisaties heb gewerkt (waaronder de Lage Landen Vendorlease en KPMG Management Services) kwam ik bij mijn huidige werkgever voor het eerst echt in aanraking met het auditvak. Dit is de Dienst Justitiële Inrichtingen (DJI) van het ministerie van Veiligheid & Justitie. Toen ik hier in dienst trad was dat bij de afdeling Interne Controle, vervolgens ontwikkelde deze afdeling zich naar een internal auditafdeling met een bredere scope. Deze transitie vormde voor mij aanleiding mijn kennis op auditgebied verder te ontwikkelen. Dit heb ik gedaan door onder meer de opleidingen tot CIA en RO te volgen. Momenteel ben ik als senior auditor binnen DJI verantwoordelijk voor vraaggestuurde audits.
Ik ben om meerdere redenen enthousiast over mijn deelname aan de redactie. Zo houd ik mij graag bezig met vraagstukken die aan het vakgebied zijn gerelateerd. Daarbij gaat mijn interesse met name uit naar sturing en beheersing, en ben ik altijd nieuwsgierig naar wat in specifieke situaties echt werkt om de organisatiedoelstellingen te realiseren. Daarnaast ben ik erg geïnteresseerd in onderzoekgerelateerde methoden & technieken en modellen die het instrumentarium van de internal auditor verder verrijken. Ik vind het leuk om via mijn redactiewerkzaamheden een kijkje in de keuken te krijgen bij andere internal auditafdelingen. Ik kijk er dan ook naar uit om mij in te zetten voor dit mooie vaktijdschrift! <<

Nederland **VAN HET BESTUUR**

Vincent Moolenaar, voorzitter van het IIA, over het thema van dit nummer: big data.

# Data:
# auditors, deliver on your promise!

Het is al weer een tijd geleden dat ik de Rotterdamse collegebanken verliet. Toentertijd leerde je in het eerste jaar (of was het al op de middelbare school?) dat je drie productiefactoren had: land, arbeid en kapitaal. Een snelle check op internet (bij het jarige Wikipedia) leert dat er nog steeds slechts wordt gesproken over dezelfde drie productiefactoren. Schoorvoetend vermeldt de site dat ondernemerschap soms ook tot de productiefactoren wordt gerekend. Daarnaast stelt de encyclopedie van de 21e eeuw dat er een discussie gaande is over de mogelijkheid om kennis als productiefactor te beschouwen. Toe maar! Ik zal Wikipedia er wel niet mee halen, maar ik zou hier toch een pleidooi willen houden voor data als productiefactor. Wat mij betreft is data een meer primaire factor dan kennis, die ik beschouw als een bewerking van data. Ter vergelijking: arbeid wordt toch ook beschouwd als een productiefactor in plaats van bijvoorbeeld een competentie of een vaardigheid?

Hoe het ook zij, data is voor veel organisaties van cruciaal belang voor de bedrijfsvoering en het behalen van bedrijfsdoelstellingen. En als auditors weten wij dat in zo'n situatie de met data gemoeide risico's scherp in ons auditvizier moeten staan. In veel gevallen zal dat ook zo zijn, al is het vaak het domein van IT-auditors. Overigens veelal uitstekend opgeleide of gecertificeerde (via NOREA, ISACA) professionals, die ik elke IAF zou aanbevelen. Ik zou er sterk voor willen pleiten dat dergelijke IT-auditspecialisten veel gezamenlijk optreden met hun operational auditcollega's in integrated audits. Immers, belangrijke delen van het control framework van organisaties bestaan uit een samenstel van zowel handmatige als geautomatiseerde controls. Een gezamenlijke aanpak is dus onmisbaar. In mijn eigen IAF hebben we dat ook op die wijze vormgegeven door een combinatie van reguliere integrated audits naast gespecialiseerde audits.

Er schuilt ook een 'bedreiging' in de wijze waarop IAF's data meenemen in hun audits. Dit hangt deels samen met een belofte die onze professie al heel lang doet en die maar heel beperkt uit de verf komt. Toen ik in 2002 mijn eerste schreden in het internal auditvak zette werd ik al vrij snel tegemoet getreden door vertegenwoordigers van allerhande consultants die mij oplossingen aanboden die variaties waren op het thema computer assisted audit techniques (CAAT). Ruim tien jaar later heb ik opnieuw een poging laten doen om 'data mining' onderdeel te laten worden van onze auditaanpak. Ik moet zeggen dat de resultaten zeer mager waren. Relatief hoge kosten waren gemaakt maar resulteerden in een bescheiden oogst. Mijn persoonlijk motto is: 'deliver on your promises' (en natuurlijk heb ik ook op dit punt opnieuw goede voornemens moeten maken tijdens de jaarwisseling!).

CAAT is een belofte die ons vakgebied al lang maakt, maar waarvan het werkelijke resultaat in mijn beperkte waarneming achterblijft bij de verwachtingen. In een wereld waarin dagelijks wordt gesproken over big data en zelfs de aanstelling van chief data officer in plaats van de inmiddels al traditionele chief information officer, moeten we echt nog een tandje bijzetten. Ik hoop dat in deze editie ook positieve verhalen over het gebruik van computer audittechnieken aan bod komen, want die zullen er ook in ruime mate zijn. En ik hoop echt dat ons mooie vakgebied in algemene zin deze belofte zo spoedig mogelijk volledig zal nakomen.

Drs. Alex Hoogteijling RE CISA MBCI

# Datamanagement in relatie tot BCM

Bij datamanagement in relatie tot bedrijfscontinuïteitsmanagement (BCM) wordt al gauw gedacht aan het maken van back-ups en het herstellen van data. Binnen BCM speelt datamanagement echter een veel grotere rol en kan het zelfs worden ingezet om calamiteiten te voorkomen.

Het BCM-proces richt zich op het versterken van het weerstandsvermogen en de veerkracht van organisaties ter voorbereiding op bedreigingen die de bedrijfsvoering kunnen verstoren, zoals brand, ICT-uitval of stroomstoring. In dit managementproces worden continuïteitsbedreigingen geïdentificeerd en wordt de impact hiervan op de bedrijfsvoering geanalyseerd. Dit leidt, afhankelijk van onder andere de risicobereidheid van een organisatie, tot de implementatie van continuïteitsmaatregelen (preventief, detectief, repressief en/of correctief) om bijvoorbeeld de kans op verstoringen en de gevolgen hiervan te verlagen of de verstoringsduur te verkorten.
Enkele voorbeelden van continuïteitsmaatregelen zijn het implementeren van een noodstroomvoorziening, het documenteren en testen van noodprocedures en het redundant (dubbel) uitvoeren van ICT-systemen. Of dergelijke maatregelen afdoende zijn dient periodiek te worden beoordeeld via management reviews en internal audits. Bevindingen uit dergelijke controles zouden idealiter moeten leiden tot correctieve maatregelen op het gebied van bedrijfscontinuïteit.

**Dataverslaving**
Aangezien organisaties in toenemende mate afhankelijk zijn van ICT en informatie, is het niet meer dan logisch dat continuïteitsmaatregelen zich ook richten op de beschikbaarheid van betrouwbare informatie in geval van een calamiteit. Vroeger beperkte dit zich tot het maken van een back-up van slechts een selectie van data op een tape (onder andere vanwege de kostprijs van tapes en de lange tijdsduur voor het maken van back-ups). Deze tapes werden niet eens altijd dagelijks extern opgeslagen. Het terugplaatsen van data werd bovendien slechts sporadisch getest.
In het huidige tijdperk van virtualisatie en cloud computing is er nauwelijks meer een drempel om data real-time op meerdere plaatsen tegelijk op te slaan. Zelfs voor particulieren is dit routine geworden dankzij diensten als iCloud, OneDrive en Dropbox.
Wij beschouwen het tegenwoordig als vanzelfsprekend dat wij overal en altijd bij onze data kunnen. Je zou zelfs kunnen stellen dat wij hier verslaafd aan zijn geraakt. Zodra zich hierin ook maar even een verstoring voordoet weten we ons geen raad. We schakelen dan massaal over naar een afwachtende modus totdat de ICT-problemen weer zijn verholpen. Creativiteit om toch het werk op een alternatieve wijze voort te zetten is dan vaak ver te zoeken.
Men is zelfs zo gewend geraakt aan digitale informatie-(verwerking) dat het terugvallen op 'papieren workarounds' in veel gevallen ondenkbaar is geworden. Zo is bij verzekeraars het claimafwikkelingsproces en de verzekerdenadministratie tegenwoordig in hoge mate gedigitaliseerd. Informatie zoals polissen, claimaanvragen, klantendossiers en claimbeoordelingscriteria zijn vaak niet eens meer op papier beschikbaar. Bij ICT-uitval of andersoortige verstoring waarbij deze data tijdelijk ontoegankelijk is ligt de gehele bedrijfsvoering stil, wat vervolgens voor een enorme improductiviteit zorgt. Daar komt nog eens de schade als gevolg van omzetderving, negatieve publiciteit en eventuele claims voor het niet of te laat nakomen van afspraken bovenop. Dit probleem doet zich niet alleen voor bij dienstenleveranciers, maar ook bij productiebedrijven. Het primaire productieproces valt bij veel bedrijven al snel stil als informatie over bijvoorbeeld bestelorders, productieplanningen en voorraden niet beschikbaar is.

**Crisismanagementdata**
Niet alleen voor het continueren van de bedrijfsvoering zijn organisaties in grote mate afhankelijk van informatietoegang, maar ook voor het managen van de calamiteit zelf en de crisiscommunicatie hieromtrent. Het tijdsaspect speelt daarbij een belangrijke rol. In het eerste uur direct na een calamiteit dienen namelijk meteen al belangrijke besluiten te worden genomen. Ook verwachten stakeholders zoals medewerkers, klanten, businesspartners en media direct geïnformeerd te worden. Informatie die hiervoor benodigd is wordt vaak gebundeld in een bedrijfscontinuïteitsplan. Zo'n bedrijfscontinuïteitsplan bevat onder meer gedocumenteerde noodprocedures, recovery (herstel) procedures, workaroundformulieren, crisiscommunicatieprotocollen, contactgegevens van belangrijke stakeholders (waaronder toeleveranciers) en checklists voor specifieke crisisscenario's.
Dergelijke informatie dient in geval van een calamiteit natuurlijk wel beschikbaar te zijn. Hier moet Internal Audit bijzonder alert op zijn. Het komt namelijk nogal eens voor dat een bedrijfscontinuïteitsplan verloren gaat in de calamiteit of dat de digitale versie alleen benaderbaar is voor een beperkt aantal personen dat vanwege de calamiteit hier niet direct bij kan. Dit is een beetje te vergelijken met het maken van een back-up, maar deze in dezelfde ruimte bewaren als de primaire databestanden.

**Voorkom datalekkage**
Tijdens calamiteiten zijn organisaties kwetsbaarder voor fouten en misbruik waardoor zich, bovenop de bestaande crisissituatie, nieuwe ongewenste gebeurtenissen kunnen voordoen. Denk daarbij aan diefstal van laptops, USB-sticks of complete servers met bedrijfs-, privacy, of medisch gevoelige informatie uit een bedrijfspand dat is getroffen door een brand. Dat bedrijfskapitaal (waaronder data) verloren is gegaan als gevolg van de calamiteit is op zich al een ramp. Hier biedt een schadeverzekering in sommige gevallen echter nog enige pijnverlichting. Maar als vertrouwelijke dossiers ineens op straat liggen, dan heb je als organisatie toch het een en ander uit te leggen. Dit is dan een crisis bovenop een crisis.
In een bedrijfscontinuïteitsplan dienen dus instructies te zijn opgenomen rondom het beveiligen van een getroffen vestiging zodra overheidshulpdiensten de locatie hebben verlaten. Denk daarbij aan het plaatsen van hekken, het inzetten van beveiligers en het veiligstellen van informatiedragers (digitaal en papier). Internal Audit dient vast te stellen of

## In perioden van verstoringen moeten internal auditors alert zijn op data integriteitsissue

dergelijke instructies in het bedrijfscontinuïteitsplan zijn opgenomen. Helemaal mooi zou het zijn als internal auditors ten tijde van een calamiteit ook ingezet worden om het crisisteam scherp te houden en te checken of alle instructies ook worden nageleefd.
De internal auditor kan bij een calamiteit er bijvoorbeeld op toezien dat informatiedragers die ogenschijnlijk als verloren beschouwd kunnen worden, niet argeloos bij het grofvuil worden geplaatst. Het is namelijk goed mogelijk dat de data hierop nog door gespecialiseerde salvagebedrijven kan worden hersteld. Indien dit niet meer het geval is dient de informatiedrager definitief te worden vernietigd zodat eventueel misbruik hiervan ook echt niet meer mogelijk is.
Het risico op ongewenste verspreiding van data doet zich overigens niet alleen direct na een calamiteit voor. Ook in de daaropvolgende periode waarin noodproductie- en herstelactiviteiten plaatsvinden bestaat dit risico. Tijdens een noodproductie- of uitwijksituatie ontbreekt het namelijk vaak aan adequate informatiebeveiligings- en controlemaatregelen. Ook wordt gewerkt volgens noodprocedures waarmee niet iedereen even bekend is. Dit alles leidt tot een verhoogde kans op procedurele fouten, onjuiste of onvolledige informatieverwerking, beveiligingsincidenten door misbruik van de situatie en mogelijk zelfs lekken van informatie of diefstal hiervan.

Van belang is dat een organisatie zich bewust is van dergelijke risico's en hieraan in het bedrijfscontinuïteitsplan ook aandacht besteedt. Hier is weer een belangrijke controlerende rol voor de internal auditor weggelegd. Zo dient bij een tijdelijke verruiming van bevoegdheden erop toegezien te worden dat hier geen misbruik van wordt gemaakt. Dit zou bijvoorbeeld het geval kunnen zijn bij het versneld inkopen van vervangende bedrijfsmiddelen waarbij bepaalde controlestappen uit de reguliere inkoopprocedure worden overgeslagen. Bij terugkeer naar de business-as-usualsituatie, moet een organisatie dergelijke brede bevoegdheden weer inperken, workaroundprocedures beëindigen en controls weer heractiveren.

**Nazorg datamanagement**
Bij herstel van data en terugkeer naar de reguliere gang van zaken dient nog wel goed gecheckt te worden of alle data ook juist en volledig zijn hersteld. Naast technische verificatie hiervan is een gebruikersacceptatietest geen overbodige luxe. Internal Audit zal in perioden waarin zich verstoringen

hebben voorgedaan alert moeten zijn op data-integriteitsissues. Indien toch data verloren is gegaan, is reproductie hiervan wellicht mogelijk via andere bronsystemen, papieren dossiers, poststukken en e-mails. In een uiterst geval zal een organisatie ook gegevens opnieuw moeten opvragen bij businesspartners of klanten.
Overigens dient niet alleen de recovery van primaire data te worden geverifieerd maar ook die van instellingen rondom toegangsbeveiliging, logging, functiescheiding, et cetera. Onder tijdsdruk kan het namelijk gebeuren dat vergeten wordt de standaard inlogcredentials van een 'admin' account van een nieuw aangeschafte server aan te passen. Ongeautoriseerde personen zouden zich zo toegang kunnen verschaffen en ongewenste handelingen kunnen verrichten waaronder het aanpassen van beveiligingsinstellingen, datadiefstal, sabotage en het bewerken van transacties.
Na herstel van systemen en data zal een eventuele achterstand in de informatieverwerking moeten worden weggewerkt. Informatie die tijdens de crisissituatie als workaround tijdelijk is vastgelegd op papieren formulieren of spreadsheets, dient overgezet te worden in de herstelde bedrijfsapplicaties. Dit is een foutgevoelig proces dat ook nog eens verstoord kan worden doordat gebruikers weer hun reguliere werkzaamheden in de applicaties uitvoeren. De kans op conflicten of dubbele invoer wordt hierdoor vergroot. Idealiter zou eerst de informatie volledig moeten zijn bijgewerkt voordat de applicatie wordt vrijgegeven voor gebruik. Het is denkbaar dat dit geduld niet altijd kan worden opgebracht.

**Inzet big data bij BCM**
Datamanagement bij BCM is niet alleen belangrijk met het oog op herstellen, verwerken en beveiligen van informatie, maar het kan ook worden ingezet bij het bestrijden van calamiteiten. Vooral ICT-verstoringen kunnen hierdoor worden beperkt. Door het analyseren van data afkomstig van verschillende sensoren en early warning systems, kan nog tijdig worden ingegrepen indien bijvoorbeeld een harde schijf dreigt te crashen of een server oververhit dreigt te raken. In de praktijk wordt al volop gebruiktgemaakt van dergelijke analyses voor het inplannen van onderhoud aan apparatuur en technische installaties.
Voor het voorkomen van andere type verstoringen wordt big data op dit moment nog niet of nauwelijks ingezet, terwijl hier toch wel degelijk mogelijkheden voor zijn. Denk bijvoorbeeld aan productieverstoringen als gevolg van problemen bij een toeleverancier. Een brand bij een leverancier is lastig voorspelbaar, maar veel andere problemen hebben een langere aanloopperiode waarvoor soms ook data beschikbaar is. Denk daarbij aan financiële problemen bij een leverancier, het niet kunnen leveren vanwege een boycot, levering vanuit een conflictgebied of staking door personeel. Door analyse van data uit diverse bronnen (nieuwsberichten, kredietbeoordelaars, betalingsgedrag uit eigen administratie) kan een organisatie dergelijke problemen bij toeleveranciers mogelijk eerder zien aankomen.
Ervaringsgegevens van verstoringen die zich hebben voorgedaan kunnen ten slotte worden gebruikt voor het verder verbeteren van analyses zodat organisaties de kans op toekomstige verstoringen nauwkeuriger kunnen inschatten.

**Conclusie**
Datamanagement en de rol van Internal Audit hierin is van essentieel belang voor bedrijfscontinuïteitsmanagement. Zowel in de voorbereiding op calamiteiten als de afwikkeling daarvan. Indien men hier steken laat vallen dan kan dat resulteren in een crisis bovenop een crisis. Het gaat daarbij om meer dan alleen het tijdelijk niet beschikbaar zijn van vitale data. Denk bijvoorbeeld aan het lekken van bedrijfs-, privacy, of medisch gevoelige informatie doordat informatiedragers na een calamiteit niet zijn veiliggesteld of beveiligingsinstellingen niet juist zijn geconfigureerd op uitwijkapparatuur. Tijdens crisissituaties is er bovendien een verhoogde kans op procedurele fouten, onjuiste/onvolledige informatieverwerking en misbruik van de situatie.
Internal Audit zou bij het implementeren van bedrijfscontinuïteitsmanagement de beheersmaatregelen rondom dergelijke datamanagementrisico's moeten beoordelen. Tijdens een daadwerkelijke calamiteit kunnen zij het crisisteam ondersteunen door te verifiëren of recovery van data en configuraties correct heeft plaatsgevonden en of afgesproken noodprocedures met bijbehorende controls daadwerkelijk worden nageleefd. <<

## Big data kan ook worden ingezet bij het bestrijden van calamiteiten

Alex Hoogteijling is directeur en consultant bedrijfscontinuiteit bij Hoogteijling Management Consultancy. Hij is specialist op het gebied van business continuity management. alexhoogteijling@bcmspecialist.nl

# Elke voordeur wordt wel een keer opengebroken als er maar voldoende tijd is

Ronald Prins

Fotografie: NFP Photography

Jip Olieroock MSc RO CIA
Drs. Laszlo Nagy EMIA RO



*Audit Magazine* sprak met Ronald Prins, medeoprichter en chief technology officer van Fox-IT, over 'cyber security', 'internet of things', 'red teaming' en tips voor de internal auditor.

# De **uitdagingen** van **cyber** security

**Wat zijn de laatste relevante ontwikkelingen op het gebied van data en welke gevaren spelen daarbij?**
"Een ontwikkeling die een enorme impact op de samenleving heeft betreft internet of things. Hiermee bedoel ik dat meer en meer alledaagse zaken met internet worden verbonden. Denk bijvoorbeeld aan de 'slimme' energiemeters, inbraakbeveiligingsapparatuur en thermostaten. Hoewel het aansluiten van alledaagse dingen op internet oneindig veel nieuwe kansen en mogelijkheden oplevert, brengt het ook gevaren met zich mee. Systemen kunnen immers gehackt worden en (privacy)gevoelige informatie kan worden ontvreemd. Dit geldt niet alleen voor particulieren maar ook voor organisaties. Naast het stelen van informatie bestaan er ook fysieke gevaren in die zin dat de besturing van buitenaf kan worden overgenomen. Denk bijvoorbeeld aan het hacken van air-traffic-controlsystemen of van sluizen, gemalen en bruggen. Deze laatste categorie is de laatste jaren al meerdere malen in het nieuws geweest omdat was aangetoond dat het overnemen van dergelijke systemen soms kinderlijk eenvoudig was. Naast internet of things zie je ook een trend dat teneinde de veiligheid te vergroten, steeds meer kritische handelingen worden geautomatiseerd. In dergelijke gevallen wordt getracht het menselijk falen uit te sluiten door de mens als schakel uit de besturing te halen. Denk bijvoorbeeld aan de treinmachinist. Op het moment dat door menselijk falen een ernstig ongeluk plaatsvindt, is een eerste reactie vaak om de operatie verder te automatiseren. Met het oplossen van safetyproblemen worden dan vaak weer securityproblemen geïntroduceerd. De kans op een ongeluk wordt dan weliswaar verkleind maar tegelijkertijd ontstaan er weer nieuwe en externe dreigingen vanwege de kwetsbaarheid van systemen."

**Hoe gaan we binnen Nederland met dergelijke gevaren om?**
"Nederland loopt op het gebied van technologische ontwikkelingen en toepassingen graag voorop. Kijk bijvoorbeeld naar de digitalisering van het betalingsverkeer. Nederlandse banken lopen op dit gebied ten opzichte van bijvoorbeeld de Belgische banken echt voorop. We realiseren ons echter niet voldoende dat de consequentie hiervan is dat we door vallen en opstaan pas leren wat goede (preventieve) controls zijn. Door vooruitstrevend te zijn begeven we ons ook op onontgonnen terreinen met de consequentie dat we op het gebied van de beheersing eigenlijk continu achter de feiten aan lopen. In wezen is het een proces van 'trial and error'. Naarmate steeds meer zaken worden verbonden met internet ontstaan er derhalve ook steeds meer risico's: we weten

## Over...

Ronald Prins is directeur en medeoprichter van Fox-IT (1999). Hij studeerde technische wiskunde aan de TU Delft en specialiseerde zich daarna als cryptograaf. Bij het Nederlands Forensisch Instituut was hij werkzaam als wetenschappelijk onderzoeker. In het kader hiervan heeft hij vele (cryptografische) beveiligingen doorbroken waar de politie tegenaan liep bij het uitvoeren van hun rechercheonderzoeken.

Fox-IT richt zich op het voorkomen, onderzoeken en beperken van de meest serieuze cyberdreigingen met innovatieve oplossingen voor met name overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven. Het in 1999 opgerichte bedrijf heeft als missie het leveren van technische en innovatieve bijdragen voor een veiligere samenleving. Bij Fox-IT werken ruim 150 beveiligingsexperts.

immers dat nagenoeg elk systeem te hacken is. Indien vitale infrastructuur wordt verbonden met internet moet men zich goed realiseren dat de mogelijkheid ontstaat dat er ernstige ongelukken kunnen plaatsvinden.
Vitale infrastructuur zou dan ook niet van internet afhankelijk moeten worden gemaakt. De overheid heeft echter nu juist in het kader van de privatisering steeds meer relevante taken overgedragen aan de markt. Denk bijvoorbeeld aan energiebedrijven, telecom en financiële instellingen. Hierdoor is de besluitvorming over het beveiligingsvraagstuk van deze organisaties ook uit handen gegeven.
De Nederlandse overheid zou ten aanzien van organisaties van nationaal belang veel meer moeten eisen op het gebied van de beveiliging. In Groot-Brittannië bijvoorbeeld zijn ze hier al een stuk verder mee. Daar heeft de overheid circa vijf bureaus gecertificeerd om de beveiliging van organisaties te beoordelen en te helpen verbeteren. De Britse overheid verplicht organisaties met voor de samenleving relevante functies vervolgens om met een van deze vijf gecertificeerde bureaus in zee te gaan om de beveiliging op orde te krijgen en te houden. Dit is zelfs via wetgeving geregeld. Op een dergelijke wijze zou de Nederlandse overheid ook moeten opereren. De Nederlandse overheid zou ten aanzien van cruciale organisaties meer dan nu een regierol moeten pakken. Van dergelijke organisaties mag ook worden verwacht dat zij hun systeembeveiliging continu monitoren, net zoals nu real time wordt gecheckt of bijvoorbeeld de Russen het Nederlandse luchtruim betreden. Een inbraak op een vitaal systeem, al dan niet in opdracht van een ander land, kan immers veel schade berokkenen. Hierbij geldt dat inbreken een aantrekkelijke optie is omdat het tegen lage kosten, zonder slachtoffers aan eigen kant en relatief anoniem kan worden uitgevoerd. Let wel, de incidenten die wij op dit gebied in de krant lezen zijn slechts het topje van de ijsberg!"

**Fox-IT richt zich onder meer op cyber security. Wat treffen jullie aan als jullie bij bedrijven binnenkomen?**
"Als wij bij bedrijven binnenkomen is het vaak vanwege incidenten. Wij treffen dan vaak teleurgestelde IT-medewerkers aan die in de veronderstelling waren dat ze de beveiliging op orde hadden. Vaak denkt de board dit ook omdat er immers wordt geaudit. Ons beeld is dat er nog regelmatig een groot gat zit tussen de wijze waarop een auditafdeling de beveiliging toetst en de werkelijke weerbaarheid tegen aanvallen van buitenaf. Dit is ook een erg lastig fenomeen om grip op te krijgen. Kijk maar naar de harde les die is geleerd bij de hack van DigiNotar, een van de meest geaudite organisaties in Nederland.
Vaak vindt beoordeling van de beveiliging plaats door te kijken naar de aanwezige beheersmaatregelen. Het beoordelen van de werking van dergelijke maatregelen is echter lastig. Dit valt te vergelijken met het testen van brandbeveiliging. Om echt vast te kunnen stellen of de organisatie voldoende weerbaar is tegen brand, zou je iets in de fik moeten steken! Er kan dus eigenlijk geen sluitend uitsluitsel worden gegeven over het in de praktijk daadwerkelijk in control zijn. Een dienst die wij hieromtrent leveren is red teaming. Red teaming betreft het samen met de opdrachtgever selecteren van de meest onwenselijke scenario's op het gebied van cyber security, om vervolgens met een team te proberen het systeem te hacken en betreffende scenario's te realiseren. Terwijl de inbraakpogingen worden ondernomen, wordt gekeken of de opdrachtgeversorganisatie tijdig de aanvallen weet te detecteren en hier adequaat op weet te reageren. Dergelijke testen zijn relevant omdat het enkel steunen op preventieve maatregelen in de praktijk onvoldoende is gebleken. Om de beveiliging goed te regelen is het met name belangrijk dat een mechanisme is opgezet om 'security breaches' tijdig te signaleren: elke voordeur wordt immers wel een keer opengebroken als er maar voldoende tijd is. Het testen van de werking van een dergelijk detectiemechanisme is de enige 'thermometer' die daadwerkelijk aan kan geven of de beveiliging van de systemen op orde is. Eigenlijk zouden auditors erop aan moeten sturen dat de organisatie af en toe red teaming uitvoert of laat uitvoeren. Dit levert inzicht in de sterkten en zwakten van de beveiliging en biedt concrete punten ter verbetering van de beheersing."

**Wat zouden organisaties dan moeten doen?**
"Organisaties kunnen veel minder doen om zich te bewapen tegen aanvallen dan ze zelf denken. Het is ontzettend moeilijk

voor een doorsnee bedrijf om een IT-securityfunctie neer te zetten waarmee je werkelijk in control kunt zijn. Denk bijvoorbeeld aan de analogie van een huis. Net als bij een bedrijf beveilig je je huis omdat je niet wilt dat er wordt ingebroken. Er bestaat echter geen slot dat niet geopend of omzeild kan worden. Het huis is dan ook niet enkel beveiligd door het slot, maar ook door het gegeven dat er zicht van derden op staat, bijvoorbeeld de buren of voorbijgangers, en omdat er altijd sprake is van een pakkans. Deze laatste elementen zijn in de digitale wereld echter niet of zeer beperkt aanwezig.
Organisaties zouden maatregelen moeten nemen die gericht zijn op de terreinen preventie, detectie en respons. Hierbij geldt dat bedrijven het uiteindelijk met de detectie en respons zullen moeten winnen. Denk aan het eerder genoemde

beveiliging goed in te richten betreft het gegeven dat de 'end users' toch nog altijd een zwakke schakel vormen. Je kunt als bedrijf veel investeren in awareness, maar bij een phishingaanval hoeft maar een medewerker erin te trappen en de hacker is binnen. De end user blijft in dit opzicht altijd een lastig te tackelen probleem. Binnen onze organisatie testen wij ook onze eigen beveiliging. Als we hierbij phishing mails inzetten dan blijkt er altijd wel iemand te zijn die erin trapt, terwijl je nergens op het gebeid van de beveiliging meer 'paranoïde' medewerkers vindt dan bij ons!
Het zijn overigens met name de grotere spelers die voldoende oog hebben voor de noodzaak om een goede beveiliging neer

## Met het oplossen van safetyproblemen worden vaak security problemen geïntroduceerd

detectiemechanisme. Preventie alleen zal zonder detectie en respons nooit voldoende zijn omdat juist uit de praktijk van detectie en respons kan worden geleerd wat goede preventieve maatregelen zijn. Hierbij geldt dat met het continu ontwikkelen van nieuwe systemen en applicaties de 'goede preventieve maatregelen' ook steeds in ontwikkeling zijn.
Wanneer we echter teruggrijpen op de eerdergenoemde vitale systemen in de samenleving dan zal het voor iedereen duidelijk zijn dat het via 'trial and error' tot stand komen van preventieve controls een erg onprettige gedachte is. Het voelt niet lekker als er mogelijk mensenlevens op het spel staan. Organisaties doen er dan ook goed aan om te werken aan de bouw van een platform waarbinnen security een serieuze functie is met voldoende budget en instrumenten om de security te monitoren en, naargelang de situatie, tijdig bij te sturen. Het inzetten van red teaming is hierbij een goed middel om te testen of bijsturing noodzakelijk is."

**U geeft aan dat het lastig is om de security voldoende goed te organiseren. Wat maakt dit zo moeilijk?**

"Om de beveiliging goed te kunnen organiseren heb je als organisatie technologie, intelligence en de juiste mensen nodig. De technologie vergt investeringen waar organisaties lang niet altijd bereid toe zijn. Intelligence kan worden aangeschaft maar het moet voor een groot deel ook intern worden ontwikkeld en worden gecultiveerd. Dit staat in nauw verband met de derde factor: de juiste mensen. Als organisatie heb je 'skilled professionals' nodig om over de beveiliging te waken. Om van skilled professionals te kunnen spreken moet je mensen hebben die over de juiste en actuele kennis en vaardigheden beschikken. Om hiervan te kunnen spreken is het noodzakelijk dat deze medewerkers in hun dagelijkse praktijk frequent met beveiligingsincidenten worden geconfronteerd. Het lastige is dat lang niet alle soorten organisaties vaak genoeg met incidenten worden geconfronteerd, waardoor de ontwikkeling van de eigen medewerkers op dit onderwerp achterblijft. Daarbij geldt dat skilled professionals ook graag daar willen werken waar ze zich in het heetst van de strijd kunnen wagen. Een doorsnee organisatie is lang niet altijd interessant genoeg en het is daardoor moeilijker om over eigen skilled professionals te beschikken.
Een ander punt dat het in de praktijk lastig maakt om de te zetten en ook nog eens in staat zijn dit goed te organiseren. Het zijn juist de kleine en middelgrote organisaties die doorgaans onvoldoende in staat zijn om de security goed te organiseren."

**Welke tips hebt u voor internal auditors?**

"In de eerste plaats: hecht niet te veel waarde aan ISO-certificeringen en vinklijstjes. Fox-IT heeft zelf ook ISO-certificeringen en procedurele maatregelen zoals wachtwoordbeheer. Maar als wij red teaming op onze eigen organisatie toepassen komen altijd wel zwakheden boven water. Enkel het gebruik van dergelijke procedurele instrumenten is onvoldoende. Wij hebben ervaren dat er een enorm gat bestaat tussen dergelijke beheersinstrumenten en wat eigenlijk noodzakelijk is om security van systemen en organisaties echt te waarborgen.
Een andere tip betreft het altijd kritisch in de gaten houden van de gehanteerde scope. Wanneer wij met auditafdelingen praten merken wij dat de internal auditors allemaal rapporten van bijvoorbeeld penetratietesten opvragen, maar dan komt het nog wel eens voor dat door de beperkte gehanteerde scope de toegevoegde waarde erg of zelfs te beperkt is. Je kunt bijvoorbeeld penetratietesten op een SAP-systeem loslaten, maar dit biedt weinig garanties als de credentials via een inbraak op de Eldat-server gemakkelijk kunnen worden verkregen. Een vergelijkbare ervaring hadden wij bij de controle van de toegangsbeveiliging met detectiepoortjes. De organisatie had bij het beoordelen van de veiligheid het onderliggende systeem buiten de onderzoeksscope gelaten. Dat systeem bleek nu juist erg gemakkelijk binnen te dringen.
Ten slotte zijn er best wel wat mooie proefsoftwarepakketjes te verkrijgen. Auditors doen er goed aan eens een dergelijk pakket te proberen om wat testen te doen en vervolgens te kijken of deze terugkomen op de incidentenrapportages van de eigen organisatie. Wel even vooraf rugdekking regelen natuurlijk!" <<

Ari Davies
Ivo Noppen MSc

Een groot deel van de informatiebeveiliging van processen en de operatie draait om compliance. Compliance is nuttig maar uiteindelijk moet informatiebeveiliging worden gezien als een groter geheel.

# Informatiebeveiliging - buiten de geijkte paden treden

Bij het beschermen van informatie is de relatie tussen de interne auditfunctie (IAF) en het securityteam van een organisatie interessant. Beide zijn belast met een gelijksoortige taak: het beschermen van de (informatie van de) organisatie. De onafhankelijke IAF is verantwoordelijk voor toetsing en het afdwingen van compliancevereisten. Het securityteam streeft naar dezelfde doelen maar is ook operationeel verantwoordelijk voor de informatiebeveiliging. Een spanningsveld, omdat het securityteam door de operationele verantwoordelijkheid per definitie op een minder onafhankelijke manier de toetsing van de informatiesystemen kan inrichten dan de IAF.
In de organisatie draait informatiebeveiliging vaak om de volgende vraag: zijn het streven naar compliance en de activiteiten die we ondernemen voor informatiebeveiliging genoeg of zouden we nog aanvullende activiteiten moeten ondernemen? Deze vraag manifesteert zich bijvoorbeeld als volgt:

- We zijn compliant aan raamwerk X, hebben onze controlemaatregelen getest op basis van risicoanalyses en daarnaast voeren we penetratietests uit op IT-infrastructuur en applicaties. Maar zijn we hiermee wel veilig?
- We hebben monitoring en incident response ingeregeld. Maar is het wel afdoende getest en hoe zou het verantwoordelijke team reageren in geval van een daadwerkelijke aanval?
- Begrijpen we echt wat een aanvaller in onze omgeving kan doen en hoe hij een aanval zou uitvoeren?

**Informatiebeveiliging versus computerbeveiliging**
Om deze vragen te beantwoorden moet eerst worden bekeken wat informatiebeveiliging betekent wanneer dit begrip wordt afgezet tegen computerbeveiliging. Organisaties en hun medewerkers dienen zich te realiseren dat informatiebeveiliging over meer gaat dan alleen computerbeveiliging. Computerbeveiliging kan organisaties op een vals spoor van veiligheid zetten: 'zo lang onze infrastructuur en systemen veilig zijn, is onze organisatie veilig'. *Figuur 1* op pag. 30 laat het verschil zien tussen informatiebeveiliging en computerbeveiliging.
De fundamentele elementen van informatiebeveiliging, de 'drie-eenheid van informatiebeveiliging' omvatten de volgende elementen:

- Cyber gaat over de online wereld, internet, intranet en alle andere computernetwerken.
- Fysiek gaat over ongeautoriseerde toegang tot fysieke locaties. Denk hierbij aan gebouwen of serverruimten. Daarnaast betreft het veiligheid van de personen in deze locatie.
- De mens gaat over de sleutelrol die zij speelt in het behandelen van informatie binnen organisaties. Ook de mens is kwetsbaar voor aanvallen, zoals de 'social-engineeringaanval', waarbij een aanvaller het vertrouwen van de persoon probeert te misbruiken om informatie te verkrijgen of zich ergens toegang toe te verschaffen. Vaak is dit de meest genegeerde en verkeerd begrepen link die de fysieke en cyberwereld aan elkaar bindt.

Computerbeveiliging omvat slechts een van de hiervoor genoemde basiselementen. Het gaat hier over maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen binnen IT-infrastructuren of -systemen. Maatregelen gericht op de techniek dus. Informatiebeveiligingsbeleid is vervolgens het beleid binnen een organisatie die de drie basiselementen omzet in controls.

**Palet aan opties**

De harde realiteit is dat aanvallers zichzelf niet beperken tot het misbruiken van technische kwetsbaarheden in de IT-infrastructuur en -systemen. Aanvallers combineren alle aspecten van de 'drie-eenheid van informatiebeveiliging' om hiermee het pad te bepalen van de minste weerstand om de organisatie binnen te komen.

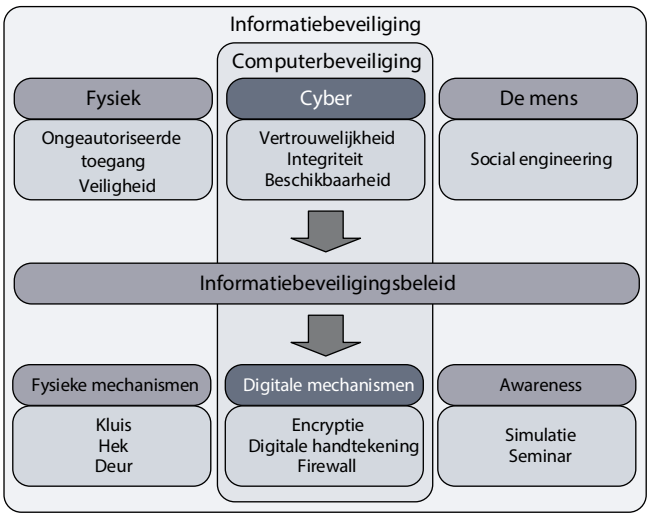
Dit betekent dat een aanvaller de keuze heeft uit een groot palet aan opties. Hij kan bijvoorbeeld gebruikmaken van het fysieke element aangevuld met het menselijke: zonder pasje achter iemand aanlopen door een geopende deur ('tailgating') en zich voordoen als een werknemer om zijn doelen te bereiken.

Uiteraard bestaan er verschillende manieren om toegang te krijgen tot een organisatie via het fysieke en menselijke element. Het meest voorkomende voorbeeld van misbruik van het menselijke element is social engineering en het zenden van phishing mails. Deze mails hebben tot doel het slachtoffer te manipuleren zodat deze zich schikt naar de wensen van de aanvaller. Om hierin te slagen gebruikt de aanvaller psychologische stimulansen, zoals complimenten, beloningen en zelfs angst. Een andere methode op het snijvlak van het fysieke en menselijke element is 'USB baiting'. Hierbij plaatst een aanvaller op strategische locaties binnen en buiten de organisatie USB-sticks of andere media waarop malware (kwaadaardige software) geïnstalleerd is. Doel is dat een slachtoffer de media in een computer laadt en de infectie verder verspreidt binnen het bedrijf.

**Casus – Haven van Antwerpen**

De laatste jaren hebben we verschillende voorbeelden gezien van succesvolle aanvallen door het combineren van de elementen cyber, fysiek en menselijk. Zo was er een aanval op de haven van Antwerpen door drugskartels. Met als doel drugs in te voeren op de Europese markt wierf het drugskartel hackers om in de systemen te komen waarmee ladingen, douanewerkzaamheden en de haveninfrastructuur worden beheerd. De aanvallers begonnen in dit scenario met het uitvoeren van simpele social-engineeringaanvallen om ervoor te zorgen dat medewerkers malware installeerden. Op het moment dat de malware werd ontdekt door de organisatie en extra beveiligingsmaatregelen werden geïnstalleerd, veranderden de aanvallers hun werkwijze. Door zich fysieke toegang te verschaffen tot het bedrijfsterrein konden de aanvallers keyloggingapparatuur (apparatuur die elke toetsaanslag registreert) direct aan de computers hangen. Tevens konden de

## Begrijpen we echt wat een aanvaller in onze omgeving kan doen en hoe hij een aanval zou uitvoeren?




**Figuur 1.** Verschil tussen informatiebeveiliging en computerbeveiliging

aanvallers vanaf afstand via een draadloze verbinding een verbinding met het netwerk van de haven leggen. Een simpele en efficiënte oplossing vanuit het oogpunt van de aanvallers, die zo geen last meer hadden van de verscherpte aandacht op de extern bereikbare infrastructuur. De aanvallers zaten immers direct op het interne netwerk van de haven.

**'Red teaming'**

De voorbeelden uit de praktijk laten zien dat informatiebeveiliging fysiek, cyber en de mens omvat, omdat ook aanvallers van deze elementen misbruik maken. Dit betekent dat bestaande maatregelen zoals compliance assessments, raamwerken en zelfs penetratietesten, met een nieuwe vorm van beveiligingstests moeten worden aangevuld. Een nieuwe vorm van beveiligingstests wordt 'red teaming' genoemd, een term die oorspronkelijk uit de militaire wereld komt, net zoals vele andere termen binnen de informatiebeveiliging.

Beveiliging betekent altijd het een stap voor zijn van dreigingen en de daaraan gelieerde risico's. Daarnaast betekent veiligheid het begrijpen van de mogelijke bestaande dreigingsscenario's. Maar belangrijker nog is het begrijpen van het onbekende, het nog niet bedachte en dat waarvan niemand dacht dat het mogelijk was. Dit betekent dat we tests moeten uitvoeren die de 'known known' (compliance, frameworks) en 'known unknown' (penetratietesten) complementeren.

Binnen de informatiebeveiliging staat red teaming voor een aanpak waarin het management van een organisatie en het uitvoerende team van ethische hackers (red team) vooraf samen een lijst 'kroonjuwelen' van de organisatie vaststelt. Het is de taak van het red team om te komen tot een aanpak gebaseerd op scenario's die aanvallers zouden kunnen gebruiken om de kroonjuwelen te bemachtigen. Hierbij worden ook enkele doelen ('flags') vastgelegd die een mogelijke rol kunnen spelen in het verschaffen van toegang, bijvoorbeeld het verkrijgen van toegang tot een bepaald gebouw, of toegang tot systemen in het netwerk.

Het red team neemt vervolgens al deze informatie mee in een project waarin de scenario's worden uitgevoerd in de vorm van een gecontroleerd incident. Een red-teamingproject bestaat uit de volgende fasen:

**Fase 1.** ***Verzamelen van publieke informatie en verkenning***

Het red team, dat eigenlijk als aanvaller fungeert, probeert in deze fase een zo compleet mogelijk beeld op te bouwen van de organisatie met behulp van openbare bronnen waarmee een succesvolle aanval kan worden uitgevoerd op de gebieden cyber, fysiek en menselijk.

**Fase 2.** ***Fysieke toegang en social engineering***

Door gebruik te maken van fysieke aanvalstechnieken zoals 'lock picking' (het openen van sloten zonder gebruik te maken van de sleutel) en social-engineeringaanvallen zoals phishing, probeert het red team bij de organisatie in te breken en iets achter te laten waardoor ze zich in een volgende stap gemakkelijker toegang kunnen verschaffen. Bijvoorbeeld door het plaatsen van een stuk hardware zoals een WiFi access point of een key-logger, waarmee alle toetsaanslagen worden vastgelegd. Bij phishing hebben we het meestal over malware waarmee het red team vanaf internet toegang kan krijgen tot de computer.

**Fase 3.** ***Onderzoek en uitbreiden van de initiële toegang***

In de vorige fase heeft het red team zich succesvol toegang verschaft tot de organisatie via een geplaatst stuk hardware of software. Het doel is vervolgens de toegang binnen de organisatie te vergroten zodat, zelfs als de initiële toegang wordt verloren, het red team nog steeds een ingang heeft binnen de organisatie.

Omdat het red team zich in deze fase reeds toegang heeft verschaft tot het interne netwerk van de organisatie, zal het netwerk ook worden onderzocht en in kaart worden gebracht om de juiste weg te kunnen bepalen naar de vastgestelde doelen. Wie zijn de belangrijkste medewerkers? Waar bevinden zich de meest kritieke databases? Hoe werken betalingstransacties en waar bewaart de organisatie haar intellectueel eigendom?

**Fase 4.** ***Escalatie en eindspel***

Dit is de laatste en mogelijk meest kritieke fase van een red-teamingproject omdat de meeste doelen zullen worden bereikt. Alle voorgaande fasen waren een opstap naar deze kritieke fase en het red team is nu bezig met het vinden van kwetsbaarheden, hacken en het binnendringen van systemen binnen de IT-infrastructuur om de vooraf gestelde doelen te bereiken. Onder de radar blijven vliegen is in deze fase minder belangrijk dan in de voorgaande fasen omdat het red team het 'geluidsniveau' langzaamaan zal moeten opschroeven. Dit is niet alleen om de doelen te kunnen bereiken, maar belangrijker nog om de capaciteiten van het monitoring en incident responseteam van de organisatie te kunnen evalueren. Wanneer de gestelde doelen zijn behaald is de (optionele) laatste stap het gecontroleerd exfiltreren van de bemachtigde gegevens en het zoveel mogelijk opruimen van het bewijs van hun aanwezigheid.

Na deze vier fasen is het tijd voor een terugkoppeling met de organisatie, aangevuld met bijvoorbeeld het organiseren van een workshop waarin kennis wordt gedeeld over het oplossen van de kwetsbaarheden en het toepassen van verbeteringen binnen de organisatie.

Samengevat is red teaming:

1. Een poging de verschillende elementen, cyber, fysiek en menselijk, samen te brengen met het doel realistische feedback te krijgen over de volwassenheid van de informatiebeveiliging van een organisatie.
2. Het is niet alleen een middel om de bestaande beveiligingsmaatregelen binnen de organisatie te testen, maar ook om inzicht te krijgen in hoe verschillende interne teams, afdelingen of derde partijen omgaan met 'gecontroleerde incidenten'.
3. Red teaming verleent ondersteuning aan andere teams die onderzoeken doen gedreven door intelligence, zoals de incident response, monitoring en crisismanagementteams. Als je een dief wilt vangen moet je immers als een dief leren denken.

**Conclusie**

Voor de IAF bieden de geijkte paden van compliance en frameworks niet langer genoeg zekerheid dat de organisatie en haar gegevens veilig zijn. Daarom is het belangrijk te zoeken naar nieuwe, holistische en innovatieve manieren waarop organisaties hun kwetsbaarheden kunnen analyseren.

Tests gericht op alle elementen van informatiebeveiliging – bijvoorbeeld red teaming – kunnen een organisatie meer zekerheid bieden over de werking van hun maatregelen tegen cybercriminaliteit. Dit biedt een realistisch inzicht in de tekortkomingen van het informatiebeveiligingsbeleid en vooral ook de implementatie daarvan. Hiermee kunnen maatregelen getroffen worden om het vertrouwen in de beveiliging van de kroonjuwelen van de organisatie te verbeteren.

Tevens heeft de IAF een unieke positie als onafhankelijk bewaker van de organisatie en haar data. Vanuit deze positie heeft zij de mogelijkheid de organisatie te verbeteren en hiermee kunnen bestaande initiatieven zoals compliance en control testing worden aangevuld met bijvoorbeeld red teaming. Deze exercities kunnen – door de grote impact en zichtbaarheid van een dergelijk project – een grote impuls vormen om een organisatie weerbaarder te maken tegen cybercriminaliteit. <<

Ari Davies is senior manager en teamleider van Deloitte red teaming operations. Met zijn internationale ervaring binnen de security- en veiligheidssector heeft hij brede kennis opgedaan van de werkwijze van aanvallers en de beveiliging hiertegen.

Ivo Noppen is junior manager en houdt zich binnen Deloitte bezig met red teaming operations en penetratietesten. Naast het aansturen van teams voert hij voornamelijk red-teamingopdrachten uit waarbij hij onder andere het technische infrastructuurvlak bestrijkt.

Kim Gunnink MA

# Ken je **klassiekers**

Hoe verhoog je als organisatie je cyberweerbaarheid? Tips voor de auditor.

De werknemers op de redactie van TV5 Monde zagen het voor hun ogen gebeuren: de Twitteraccounts werden overgenomen, vervolgens de Facebookpagina en daarna de andere social-mediapagina's van het bedrijf. Op hetzelfde moment werden de tv-uitzendingen verstoord. De oorzaak? In de avond van 8 april 2015 werd het Franse televisiestation gehackt. Ruim 18 uur lang waren de websites van de nieuwssite onbereikbaar en gingen de tv-zenders op zwart. De directeur van het tv-station stelde dat er sprake moest zijn van een 'buitengewoon zware cyberaanval', want 'we hebben zeer sterke firewalls die we recent hebben laten controleren en toen waren ze in orde'.

**Overmacht of niet?**

Veel mensen voelen mee met deze directeur. Wanneer een organisatie sterke preventieve IT-maatregelen treft om aanvallers buiten de deur te houden, moet er sprake zijn van overmacht – althans, zo is de gedachte. De directeur maakt echter twee klassieke fouten met zijn uitspraak. Preventieve maatregelen – zoals een recent geüpdatete firewall – kunnen niet uitsluiten dat cyberaanvallers een organisatie schade berokkenen. Detectiemethoden, een goede respons en doordachte herstelmaatregelen zijn een noodzakelijke aanvulling. Ook zijn maatregelen voor IT-systemen of bij het ICT-departement onvoldoende om te garanderen dat een organisatie weerbaar is tegen cyberdreigingen en over de veerkracht beschikt om te herstellen na een geslaagde aanval. Cyber is meer dan alleen IT: mensen, processen en communicatie moeten ook onderdeel zijn van de cyberweerbaarheidsmaatregelen die een organisatie treft. Door als auditor bewustzijn te creëren op deze twee punten draag je bij aan een integraal cyberweerbaarheidsbeleid binnen de organisatie waarvoor je werkt.

**Een cyclus van preventie, detectie, respons en herstel**

Het nemen van preventieve maatregelen stond tot in de jaren negentig gelijk aan veilig zijn. Rond de millenniumwisseling realiseerde men zich echter dat ongeacht hoe sterk de preventieve maatregelen zijn, iedere organisatie op een zeker moment gehackt wordt. En als dat gebeurt, kun je er maar beter klaar voor zijn. Dus kwam detectie in zwang: hoe eerder een aanvaller wordt opgemerkt hoe minder schade hij kan toebrengen. Inmiddels leeft het besef dat preventie en detectie ook niet zaligmakend zijn. Er is immers altijd sprake van (enige) schade, ongeacht het tijdsbestek waarbinnen een succesvolle aanval ontdekt wordt. Dat betekent dat er respons- en herstelmaatregelen klaar moeten liggen om effectief met de gevolgen van een geslaagde aanval om te gaan. Om het herstel te voltooien is het belangrijk dat de situatie wordt geëvalueerd en dat de lessen die daaruit voortkomen, worden gebruikt om de gehele keten met veerkrachtvergrotende maatregelen te versterken. Dit kan bijvoorbeeld door het aanpassen van trainingen voor medewerkers, het updaten van detectiesystemen en het aanscherpen van herstelprocedures.

**Cyber is meer dan IT**

Auditors spelen een belangrijke rol bij het helpen voorkomen dat hun organisatie in dezelfde valkuil trapt als de directie van TV5 Monde. Uitdragen dat een organisatie voor haar eigen veiligheid bredere maatregelen moet treffen dan het sluiten van de poorten, is slechts een eerste stap. Cyber is immers veel meer dan IT alleen. Om de cyberweerbaarheid en de veerkracht van een organisatie te vergroten moeten er maatregelen getroffen worden in vier categorieën. Een daarvan is zeker IT, maar minstens zo belangrijk zijn mensen, processen en communicatie. Auditors kunnen stimuleren dat er in hun organisatie ook in deze laatste drie categorieën op een bewuste manier met cyberrisico's wordt omgegaan.

**Menselijk vlak**

Op het menselijke vlak zijn cultuur en bewustzijn bepalende factoren als het gaat om cyberweerbaarheid. Zo is het van groot belang dat het bestuur en senior management van een


organisatie cyberrisico's begrijpen, het belang van informatiebeveiliging erkennen en de relevantie ervan uitdragen naar de medewerkers. Dit uit zich onder meer in regelmatig terugkerende, gerichte bewustwordingstrainingen voor medewerkers op alle niveaus, inclusief het hoger management.
Bewustzijn van cyberrisico's onder de eigen medewerkers vergroot niet alleen de bescherming van de organisatie doordat mensen bijvoorbeeld minder snel in een phishing mailtje trappen, maar ook omdat het de tijd verkort tot een aanval ontdekt wordt. Het is daarbij belangrijk dat er een positieve meldcultuur bestaat in de organisatie: mensen moeten aangemoedigd worden om melding te maken van een mogelijk risico en moeten niet bang hoeven te zijn voor een reprimande omdat ze per ongeluk een verkeerde bijlage hebben geopend.

**'Security by design'**
Bewust omgaan met cyberrisico's in organisatieprocessen verkleint de kans op een geslaagde aanval en kan tevens de impact van een aanval beperken als deze wél slaagt: security by design. Intern kun je daarbij denken aan het inrichten van een proces waarbij alle hard- en software en de netwerkinstellingen van een organisatie periodiek grondig getest worden aan de hand van relevante veiligheidsstandaards. Ook kan ervoor worden gezorgd dat het aanvalsoppervlak zo klein mogelijk is: beperk het aantal punten dat een aanvaller kan gebruiken om de systemen binnen te dringen en waarlangs informatie naar buiten kan worden gesmokkeld. Het dusdanig beperken van systeemtoegangsrechten dat alleen degenen voor wie vanuit operationeel oogpunt systeemtoegang noodzakelijk is, is hier een voorbeeld van.
Security by design heeft ook betrekking op relaties met ketenpartners. Het komt namelijk niet zelden voor dat cyberaanvallers een derde partij als kruiwagen gebruiken om binnen te dringen bij hun uiteindelijke doelwit. Dit kan ver gaan: een notoir voorbeeld is de hack van de Amerikaanse supermarktketen Target eind 2013, waarbij de aanvallers nota bene via de aircoleverancier van de keten door wisten te dringen tot de point-of-salesystemen en vandaar uit de gegevens van meer dan 40 miljoen credit- en debitkaartgebruikers wisten te stelen.
Rekening houden met cyberrisico's tijdens bijvoorbeeld de onderhandelingen over servicecontracten met een derde partij maakt duidelijk waar verantwoordelijkheden en aansprakelijkheden liggen en vergemakkelijkt de communicatie als er sprake is van een aanval.

**Communicatie**
Ook vanuit communicatieoogpunt moet een organisatie rekening houden met cyberrisico's. Als er bekend is wat er op welk moment aan wie gecommuniceerd moet worden wanneer een cyberaanval ontdekt is, kan de schade ingedamd worden. Informatie delen met zowel de eigen medewerkers als externe belanghebbenden zoals relevante autoriteiten, klanten, ketenpartners en media is cruciaal. Door deze betrokkenen te informeren, kunnen verdere verspreiding van de aanval, speculatie over wat er gaande is en eventuele paniekreacties onder klanten beperkt worden.
De communicatie moet wel goed overdacht zijn. Zo werd een van de medewerkers van TV5 Monde voor een interview naar aanleiding van de hiervoor genoemde hack gefilmd in zijn kantoor. Al snel ging er echter meer aandacht uit naar de wand achter hem dan naar wat hij te vertellen had: op de wand hingen namelijk diverse A4-tjes met wachtwoorden voor social media accounts van het tv-station… <<

Kim Gunnink werkt bij De Nederlandsche Bank en verdiept zich als beleidsmedewerker in cyberdreigingen ten aanzien van de financiële sector en het betalingsverkeer.

Walter Swinkels

# Gaat het nu **echt** gebeuren…

Het onderwerp data is een treffend onderwerp voor het nieuwe jaar, want dit onderwerp heeft fundamentele impact op de invulling van de internal auditfunctie (IAF) in de toekomst.

Volgens publicaties van externe partijen op het web is het leveren van toegevoegde waarde als IAF onmogelijk zonder data analytics en continuous monitoring en auditing. Daarbij is het interessant te constateren dat diezelfde externe partijen deze methoden zelf niet standaard hanteren. Blijkbaar is het toch niet zo gemakkelijk als het lijkt. Echter, de IAF is de externe auditfunctie al ver ontstegen. In de nieuwe IIA-principes is dit ook een van de kernprincipes: 'Internal Audit is insightful, proactive, and future-focused'. Hierin past de strategische keuze van de IAF om in te springen op de fundamentele transformatie die in de economie plaatsvindt door digitalisatie, oneindige connectiviteit en globalisatie, toch?

Ondernemingen en IAF's die vooruit denken, maken al jaren gebruik van data-analyticsmethoden. Maar er is nog veel werk te doen; er zijn ook veel ondernemingen en IAF's die in een soort 'competency trap' zitten. Vaak is er sprake van een totale ontkenning van de noodzaak om te veranderen ofwel het onvermogen om te veranderen naar de volgende internal auditconfiguratie. Mogelijk is het in dit kader interessant te onderzoeken of verbanden bestaan tussen de mate van verandering en transformatie van ondernemingen versus de internal auditfunctie transformatie binnen die ondernemingen.

Laat mij een voorspelling doen. Wellicht vindt u het op dit moment nog ondenkbaar. Mogelijk verklaart u mij zelfs voor gek. Maar ik zie de volgende ontwikkelingen rondom de impact van data op de samenstelling en werkzaamheden van IAF in de nabije toekomst:

1. Handmatig, transactiegerelateerd auditwerk gaat vanaf 2016 in hoger tempo geautomatiseerd worden. Dit heeft impact op de werkzaamheden en samenstelling van de IAF die steeds meer data-analisten, maar ook geschiedkundigen en natuurkundigen bevat die data kunnen interpreteren. Data uit systemen krijgen is een kant van het verhaal, er iets mee doen is een andere!

2. Innovatieve ondernemingen benoemen steeds vaker psychologen met een RO-titel – ze komen daarvoor uit de hele wereld naar Nederland – als Chief Audit Executive vanwege het toenemende belang van analytisch denken, het kunnen werken met een breder pallet van methoden en technieken en focus op gedragsrisico's binnen alle lagen van een onderneming.

3. Vanwege diepgaander inzicht in afwijkingen in transacties en datapatronen kan de IAF meer onderbouwd een statement geven over de mate van in control zijn van een onderneming. Dit internal audit statement wordt ook meer expliciet in jaarverslagen opgenomen vanwege de behoefte van externe partijen aan proactieve en toekomstgerichte informatie.

Het gaat nu echt gebeuren, er is geen weg terug.

Walter Swinkels is partner bij CPI. Hij is tevens verbonden aan het Executive Internal Audit Program van de Universiteit van Amsterdam.

Marco de Jong

Iedereen heeft de boodschap inmiddels begrepen: big data biedt auditors fantastische mogelijkheden. Maar welke stappen moet je zetten om de vruchten ervan te kunnen plukken? Hoe moet je beginnen? En welke valkuilen moet je vooral vermijden?

# Tips om te starten met **big data** & **analytics**

## 1. Begin!

Als je erover blijft nadenken begint iemand anders er wel mee. Ik zou zeggen: 'begint eer ge bezint' in plaats van andersom. We hebben er genoeg over nagedacht, laten we nu eens wat gaan doen. Niet in het wilde weg, zonder enig plan, maar wel gewoon theorie om gaan zetten naar praktijk.

## 2. Houd het klein

Droom gerust groot, maar zet kleine stappen. Accepteer dat 10% beter ook beter is. Als je eerst gaat nadenken over hoe je 100% beter kunt worden, heb je over twee jaar nog niets bereikt. Er zijn geweldige nieuwe mogelijkheden, maar je kunt niet van 0 naar 100. Ga op kleine schaal eens proberen om wat bescheiden verbeteringen met data te realiseren. Richt je op zichtbare en meetbare (tussen)resultaten. Auditors zijn bij uitstek in staat data te analyseren want dat zijn professionals met een overkoepelend beeld, analytische vaardigheden én een onafhankelijke positie binnen de organisatie. Dat zijn drie belangrijke aspecten die van waarde kunnen zijn bij het benutten van big data binnen organisaties. Auditors moeten dan wel bereid zijn de neiging te onderdrukken om alles 100% perfect te willen hebben voor ze ergens aan beginnen.

## 3. Denk holistisch

De grootste winst van de nieuwe mogelijkheden van big data is dat je alles met elkaar kunt verbinden; afdelingen, systemen, producten, klanten, et cetera. Binnen de telecom hebben ze bijvoorbeeld het 'cost-to-serveconcept' geïntroduceerd. Daarmee kunnen zij vanuit de daadwerkelijke operatie kijken wat voor 'touch points' ze met de klant hebben: hoe vaak hij belt met de klantenservice, wat zijn betaalgedrag is, hoe hij zijn abonnement gebruikt, hoe hij is binnengekomen, hoe lang hij klant is, waar hij woont en werkt, welke telefoon hij gebruikt, et cetera. Wanneer je de data van al die invalshoeken bij elkaar brengt krijg je opeens een hele andere kijk op de kosten en omzet van die klant.
In die veelheid van gezichtspunten liggen mogelijkheden. Alleen al door data te integreren en in context te bekijken, krijg je gegarandeerd verrassende nieuwe inzichten. Waar auditors nu typisch naar kijken zijn dwarsdoorsnedes van populaties en daarbinnen met name naar de uitzonderingen die het meest in het oog springen. Dat is een zeer beperkte toepassing van de beschikbare data. Een rijke analysecontext rondom het onderzoeksonderwerp helpt om nieuwe inzichten op te doen en maakt bijvoorbeeld analyse van gedrag mogelijk. Een weloverwogen risico-inschatting op basis van nieuwe feiten.

## 4. Automatiseer

Door meer context in de analyses mee te nemen, ben je in staat veel beter het verhaal achter de processen en cijfers te vatten. Door analyses op basis van wiskundige modellen en algoritmes geautomatiseerd tot stand te laten komen, hoeft dat niet zo veel tijd te kosten als vroeger. Dit biedt auditors de kans om hun analytische vaardigheden beter in te zetten. Als je dan vervolgens op basis van die inzichten operationele zaken beter kunt onderzoeken, blijft er veel meer tijd over voor de natuurlijke adviesfunctie.

## 5. Houd een open blik

Bijna iedereen begint een onderzoek met de vraag: wat wil je weten? Alleen, als we goed zouden zijn in het bepalen van wat we willen weten hadden we dit artikel niet nodig gehad. Probeer dus niet alle vragen voorafgaand aan het onderzoek te formuleren. De echt interessante inzichten bedenk je niet van tevoren, die worden duidelijk vanuit de verzamelde informatie.


Iedereen lijkt bang voor een wereld waarin niets meer veilig is en waarin iedereen laat zien wat ze allemaal te weten kunnen komen. Dat angstbeeld lijkt me onterecht, want je bent er toch zelf bij? Je kunt toch bijsturen? Je moet nieuwsgierig zijn bij dit soort onderzoeksmethoden, anders moet je er überhaupt niet aan beginnen.

### 6. Werk iteratief

Durf fouten te maken, zorg alleen dat je snel van je fouten leert. Kies dus voor flexibiliteit, zowel in mensen als in tooling. Hoewel deze tip misschien het simpelst klinkt is hij in de praktijk het lastigst vorm te geven. Bestaande structuren binnen organisaties rondom jaarplannen, thema-audits, budgetten, IT-investeringen, et cetera, werken in de praktijk recht tegen dit principe in. Een noodzakelijke voorwaarde voor succes is een research- en developmentcultuur. Het liefst binnen de hele auditafdeling, maar op zijn minst binnen het team dat met big data aan de slag gaat.

### 7. Kies de juiste mensen

Verzamel talent om je heen. Vind de mensen die over de kennis en kunde beschikken om je verder te helpen. Kijk goed wat je al in huis hebt en onderzoek wat je nog mist. Wees niet bang om met mensen samen te werken die heel anders kijken en denken. Al die verschillende gezichtspunten helpen juist bij het samenstellen van data en bij het bedenken van mogelijke invalshoeken voor de analyses.

### 8. Kies de juiste tools

Als je een tijdje aan het pionieren bent geweest, heb je een beter beeld van wat je voor de onderzoeken nodig hebt. Wees je ervan bewust dat wanneer je kiest voor een specifieke softwareoplossing je voor een aantal mogelijkheden kiest en andere mogelijkheden juist uitsluit. Je kunt bijvoorbeeld een onderscheid maken tussen exploratieve analyses en concluderende analyses. Voor dat eerste type analyse wil je een data- of procesminingoplossing hebben waarmee je iedere vraag die je ter plekke bedenkt kunt beantwoorden. Het liefst op een visuele manier en in een bepaalde context. Als je concluderende analyses wilt heb je juist een statistisch onderbouwende tool nodig. Denk er dus heel goed over na wat je wel en wat je niet wilt en schaf dan pas een tool aan.

### 9. Kijk niet alleen naar binnen

Staar je niet blind op je eigen organisatie, kijk ook eens verder. Vraag aan anderen met welke vragen zij zitten en welke oplossingen zij gevonden hebben. Doe inspiratie op bij andere organisaties en wees creatief. Mogelijk bestaat er een kant-en-klare oplossing. Je hoeft niet alles zelf te ontdekken. Wees niet alleen maar bang dat anderen er met je idee vandoor willen, maar deel inzichten en probeer juist als onderdeel van het netwerk te groeien. Met co-creatie en symbiose kun je een heel eind komen.

### 10. Neem de tijd om inzichten te absorberen

Wanneer je in de onderzoeksfase genoeg te weten bent gekomen kun je ook even stoppen. Er is niets zo vervelend als allerlei nieuwe inzichten hebben maar niets kunnen concluderen. Veel auditors moeten wennen aan bottom-upinzichten. Waar we in het verleden op basis van deelwaarnemingen processen in kaart brachten krijgen we nu alle uitzonderingen ongefilterd terug. Het vergt een nieuwe evaluatiemethode om hier als auditor effectief mee om te gaan. Het is van groot belang deze ontdekkingsreis samen met de auditee aan te gaan.

Onderzoekstrajecten worden idealiter niet door analisten alleen gedaan. Voeg altijd iemand met inhoudelijke kennis van zaken vanuit de operatie aan het team toe om de consequenties van de nieuwe inzichten in te kunnen schatten. Ook agility speelt een belangrijke rol bij onderzoekstrajecten. Je moet het auditplan en de evaluatie wel aan kunnen passen op basis van de ontdekkingen die je doet en dat is vaak niet eenvoudig als je iets al jaren op dezelfde manier doet. Daar moet je bij zulke trajecten heel goed over nadenken. Stel dat je alles te weten kunt komen, op welke manier beïnvloedt dat de evaluatie en hoe kom je tot een conclusie? <<

Marco de Jong is opgeleid als RA, met een achtergrond bij EY, hij heeft ervaring opgedaan als SAP consultant en adviseur. De laatste vier jaar werkt hij nauw samen met Data Scientists, eerst vanuit Data to Insight en in 2015 startte De Jong samen met Jan de Roos Experience Data. www.experiencedata.nl

Dit artikel is een bewerking van een artikel dat eerder in de *FM Magazine* special *Big Data & Analytics* is gepubliceerd.

Ir. Gezina Atzema RO
Ellen Couwenberg MSc

Wat betekent het gebruik van grote hoeveelheden data voor het bestuur en organisaties? Hoe verloopt de interactie tussen het gebruik van informatietechnologie en het sociale systeem? *Audit Magazine* sprak hierover met hoogleraar Publieke Innovatie Albert Meijer.

# **Cijfers** vertellen nooit het hele **verhaal**

**Vanwaar uw interesse voor datagestuurde organisaties?**
"Ik werk graag op het grensvlak van wetenschap en samenleving. In het bijzonder wat nieuwe technologische ontwikkelingen betekenen voor de menselijke praktijken. Vanuit mijn profileringsleerstoel richt ik me op de 'slimme stad', hoe de stad door de komst van allerlei IT-ontwikkelingen verandert als publiek-politiek systeem. Alles en iedereen in de stad creëert informatie en gebruikt die ook. Ik noem dat de datafication van de stad. Op het gebied van informatietechnologie zie ik aan de ene kant een 'optimistische lijn' over de mogelijkheden die ontstaan door de beschikbaarheid van heel veel data die door publieke organisaties, bedrijfsleven en burgers worden verzameld. Denk aan toepassingen als transparantie van toezicht of voor burgerparticipatie. Aan de andere kant heb je een 'onheilslijn' die zich vooral zorgen maakt over zaken als privacy, het verdwijnen van het geheugen van de overheid, et cetera. Beide lijnen hebben geen gelijk maar wel een functie omdat ze onze aandacht vestigen op mogelijkheden en risico's van nieuwe technologieën.
Met empirisch onderzoek wil ik de interactie tussen technologische en sociale systemen zichtbaar maken en laten zien wat er nu echt gebeurt. Een mooi voorbeeld van een interactie is het gebruik van e-mail in een bureaucratische organisatie. Hoe e-mail wordt gebruikt reproduceert hoe de organisatie in feite werkt, het is als een spiegel. Tegelijkertijd verandert e-mail ook de communicatie, door e-mail ontstaan er veel meer netwerkverbanden in de organisatie."

**Hoe goed kunnen we de werkelijkheid in kaart brengen met data?**
"Overheid, bedrijven en burgers creëren allerlei datastructuren die als het ware een laag vormen over een stad. Data hebben een hele grote hardheid, maar je moet dat toch zien als de illusie van beheersing. Het gaat er ook om hoe je met de data werkt. De fictie dat we de werkelijkheid kennen door data wordt alleen maar sterker. Een gevaar bij de analyse van datasets is dat het je ontgaat dat er veel complexere relaties zijn dan in data worden gesuggereerd. Techniek modelleert nu eenmaal sociale systemen en doet dat op een vrij 'arme' manier. Je kunt bijvoorbeeld winkels in kaart brengen, maar een winkel is vaak het middelpunt van allerlei sociaal gedrag, het is niet alleen een plek waar je spullen koopt. Een complex sociaal systeem kun je nooit in cijfers verpakken. Het gaat steeds om het verhaal achter de data. Het beeld dat we van de werkelijkheid creëren doet geen recht aan de werkelijke menselijke interacties.
Modellering is heel erg gericht op het temmen van irrationaliteit, maar daarmee maken we de wereld niet ineens rationeel. Ik begrijp de angst dat we de hele wereld gaan bevriezen in datasystemen die op een gezaghebbende manier zeggen hoe de werkelijkheid eruit ziet, waarbij de relationele, menselijke aspecten worden verwaarloosd. Dave Eggers beschrijft dat mooi in zijn roman *The Circle*, een wereld waarin alles wordt gemeten en volledig transparant is. Geheimen zijn niet toegestaan, terwijl een geheim bijvoorbeeld een relationeel nut heeft en belangrijk is voor je identiteit, maar dat soort patronen zit niet in die modellen."

## Over...

Prof. dr. Albert Meijer is sinds mei 2015 hoogleraar op het vakgebied Publiek Management, in het bijzonder Publieke Innovatie bij het departement Bestuurs- en Organisatiewetenschap (USBO) van de Universiteit Utrecht. Zijn onderzoek richt zich op innovatieprocessen in de publieke sector met daarbij specifiek aandacht voor de 'slimme stad'.

# Mijn angst is dat we de wereld gaan bevriezen in data-systemen

Albert Meijer

Foto: Marike van Pagée

**Auditors zijn van nature vooral gefocust op risico's. Hoe kijkt u aan tegen de risico's van verzameling van grote hoeveelheden data in de publieke sector?**

"Het missen van kansen wordt door auditors vaak niet als risico gezien, terwijl dat met het oog op de 'opportunity costs' natuurlijk wel is. Mijn indruk is dat auditors geen opportunity costs meten. Maar los daarvan, we staan echt aan het begin van een nieuw tijdperk, met 'internet of things', met nieuwe risico's rond het gebruik van data. De hoeveelheid data zal steeds meer toenemen.

Technologisch lijkt dataverzameling altijd een goed ding, we kijken later wel wat we ermee doen. Mijn telefoon registreert bijvoorbeeld continu mijn bewegingen en kan mij op basis van die unieke patronen identificeren. Maar het brengt risico's met zich mee op het gebied van privacy, bedreigingen in de sfeer van criminaliteit en oorlogsvoering en op het gebied van afhankelijkheid van systemen. Privacy, een beter woord is in dit verband wellicht de term 'data-autonomie', komt onder druk te staan. Maar we zijn niet helemaal machteloos. Toezichthouders als het CBP hebben zelf ook steeds slimmere manieren om toezicht te houden. Data-autonomie moet centraler komen te staan. Zo ontvangt de Belastingdienst op dit moment informatie over je bankgegevens zonder dat je daar expliciet toestemming voor hebt gegeven. Dat is toch een rare constructie, mijn bank heeft immers een zakelijke relatie met mij. Denkbaar is om in plaats daarvan te werken met een instrument als een datakluis waar de burger zelf eigenaar van is en waarbij je toestemming kunt geven, bijvoorbeeld aan de Belastingdienst, om je bankgegevens te mogen inzien.

De vraag is ook hoe lang verstrekte data gebruikt mogen worden. Data die lang bewaard blijven kunnen een andere betekenis krijgen in een andere context. Een verloopdatum is misschien wel een goed idee. Bij archieven heb je ook vernietigingstermijnen. Bij bedreigingen in de sfeer van criminaliteit en oorlogsvoering valt mij op dat het bewustzijn bij bedrijven over de kwetsbaarheid van aanvallen van digitale systemen heel laag is. Bij de afhankelijkheid van systemen is het risico, als gevolg van bijvoorbeeld cybercrime, dat bedrijfsprocessen niet meer kunnen draaien en dat daardoor het hele proces van een bedrijf of organisatie stil komt te liggen. De afhankelijkheid van data is enorm. Denk maar eens aan systeemproblemen bij de politie, dat er politietaken uitvallen of gegevens over verdachte personen niet bereikbaar zijn, dan kun je niet functioneren."

**Op welke manier kan audit gebruikmaken van grote hoeveelheden data?**

"Het auditvak kan versterkt worden door nieuwe technologieën. Maar hoe ver wil je daarin gaan? Een risico – ook een filosofisch risico – is dat we bepaalde patronen gaan ondersteunen, bijvoorbeeld het voorkomen van corruptie, en andere menselijke (sociale) patronen, bijvoorbeeld informele afstemming, verdringen. Een betere insteek is om het als auditors met elkaar te hebben over wat we met de technologie willen en ons niet beperken tot beschikbare technologische mogelijkheden gebaseerd op een arm beeld van sociale interacties.

Belangrijk is hoe je beelden van de werkelijkheid weergeeft. Kun je dit het best weergeven in getallen of in verhalen? Als auditor ligt het accent in het vakmanschap misschien meer op getallen, maar toch ook in het interpreteren van de getallen in een verhaal. In datalogica wordt dat laatste vaak ontlopen, bijvoorbeeld bij schoolkaarten van de onderwijsinspectie waarbij een interpretatie van de getallen ontbreekt. Het gaat er juist om dat je een betekenisvol verhaal kunt geven aan de data! Het gaat om de combinatie van inhoudelijke expertise en (big-)dataexpertise. De interessante kennis ontstaat op het grensvlak van die twee expertises." <<

Prof.dr. Jacques de Swart MBA
Dr. Jan Wille FRM
Drs. Michael Zuur EMIA

# Data analytics volgens het **push-leftprincipe**

Data analytics bieden vele mogelijkheden voor de innovatie van het werk van internal auditors, maar de praktijk leert dat die nog onvoldoende benut worden. Dit artikel bespreekt hoe het push-leftprincipe internal auditors helpt om data analytics te positioneren in hun werk.

De toegenomen belangstelling voor data analytics leidt tot hoge verwachtingen en mogelijkheden, ook voor internal auditors. De situatie lijkt een beetje op big data: iedereen heeft het erover, maar (bijna) niemand gebruikt het nog. We noemen drie soorten verwachtingen.

**1 – Kwantificering**

De toegevoegde waarde van internal auditors blijft moeilijk te duiden, zeker als zij in operational audits de risico's in een proces als laag inschatten en later toch blijkt dat de procesbeheersing serieuze tekortkomingen kent. Tegelijkertijd begrijpt iedereen dat internal auditors niet alles kunnen zien. Zeker als het gaat om grote processen, zou het dan niet mogelijk zijn om op basis van allerlei sporen die processen tegenwoordig achterlaten in systemen aangevuld met extra waarnemingen, op zijn minst de onzekerheid in de beoordeling van de internal auditor te kwantificeren?

Ook wordt de internal auditor geacht zijn unieke onafhankelijke positie en toegang tot databronnen om te zetten in op feiten gebaseerde observaties waar de organisatie op kan acteren. Niet alleen de interne maar in toenemende mate ook externe data, kloppen elke dag weer op zijn deur met de brutale boodschap: misschien bevatten wij wel toegevoegde waarde waardoor de organisatie beter in staat zal zijn haar doelen te verwezenlijken.

Deze combinatie maakt de vraag of internal auditors ook kwantitatief kunnen duiden wat hun toegevoegde waarde is – inclusief de kans dat zij in hun beoordeling iets over het hoofd zien – op termijn onvermijdelijk.

**Casus Pensioenverzekeraar**

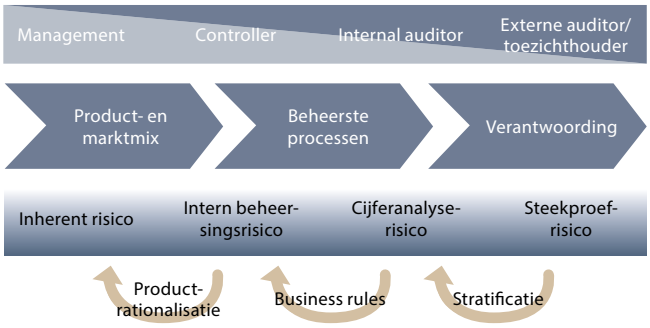
In het kader van haar toezichtsproject Quinto vroeg de DNB een aantal pensioenverzekeraars om inzicht te geven in de juistheid van de aanspraken in de administratie. De vraag die hierbij centraal stond was: krijgt de deelnemer waar hij/zij recht op heeft? Een slimme data-analyse van de internal auditor toonde aan welke mutaties in welke systemen het meest foutgevoelig waren en hierdoor nader bekeken dienden te worden door middel van een steekproef. Met name voor complexe tailor-made pensioenproducten bleek het herleiden van de mutaties in aanspraken naar pensioencontracten een ingewikkelde en arbeidsintensieve klus. De steekproef toonde verder aan dat de tailor-made pensioenproducten veel handmatig werk opleverden en dat dit tot veel foute mutaties leidde. Het inzicht in de controle-inspanning en foutgevoeligheid van deze complexe tailor-made producten overtuigde het management van het nut en de noodzaak van productrationalisatie en vormde daarmee een waardevol hulpmiddel in de besluitvorming over de te voeren productportfolio. In termen van figuur 1 in dit artikel: het risico dat aanspraken niet kloppen werd deels gemitigeerd door het inherente risico te verkleinen.

**2 – Effectiviteit**
Aan goedkope rekenkracht is in de meeste organisaties geen tekort. En anders is er nog de cloud die deze – tegenwoordig ook veilig – kan leveren. Algoritmes worden slimmer. Brondocumenten die vroeger nog handmatig uit hard-copy archieven moesten worden gelicht zijn steeds vaker integraal elektronisch beschikbaar. Dit roept zeker vanuit een data driven organisatie de vraag op of daarmee de werkzaamheden van de internal auditor effectiever kunnen worden en meer waarde kunnen toevoegen. Dit maakt de internal auditor die nog dagen spendeert aan het vangen van de complexe wereld in de twee dimensies van zijn spreadsheet (rijen en kolommen) zonder toegang tot die slimme algoritmes op zijn minst onrustig, want hij weet zelf ook wel dat voor data analytics geldt dat excelleren iets anders is dan Excel leren. Om te excelleren is meer nodig.

**3 – Data driven audit**
Steeds vaker baseren toezichthouders zich op uitgebreide data-extracties om hun oordeel te bepalen, zonder daarbij uitgebreid aandacht te besteden aan de inrichting van de processen die ten grondslag liggen aan de opgevraagde gegevens. Een voorbeeld hiervan is het uitvragen van 'loan tapes' tijdens de asset quality reviewexercitie door de ECB. Ook bij externe auditors wordt data steeds meer gebruikt bij het geven van goedkeurende verklaringen. Een voorbeeld hiervan zijn de data-analyses in het kader van de ISA 240-richtlijn (frauderichtlijn). Als toezichthouders en externe auditors zich minder richten op het proces roept dit de vraag op wie eventuele bevindingen terugvertaalt naar lacunes in het proces of de beheersmaatregelen. Tijd om aandacht te geven aan wat we het push-leftprincipe noemen.

**Push-left data analytics als antwoord op uitdagingen**
We zullen nu eerst het push-leftprincipe in beknopte vorm uitleggen en daarna toelichten hoe dit principe elk van de drie uitdagingen het hoofd biedt. Voor de volledige uitleg verwijzen wij naar het MAB-artikel uit 2013, waarin we het push-leftprincipe hebben geïntroduceerd.
*Figuur 1* visualiseert het push-leftprincipe. Het product van de vier risico's is, net als in het audit risk model, de kans dat een verantwoording een fout groter dan de controletolerantie van de auditor bevat. Boven de risico's staat de keten van besluiten die deze risico's beïnvloeden: de partijen die invloed uitoefenen op deze keuzen staan bovenaan. Van links naar rechts neemt de invloed van het management af terwijl die van de interne en externe auditors en toezichthouders juist toeneemt.

Data analytics maken het de internal en external auditor mogelijk om elk van de vier risico's te kwantificeren. Waar dit niet mogelijk is schrijft het voorzichtigheidsbeginsel een risico van 100% voor. Slimme statistische modellen op diverse databronnen zorgen voor nieuwe mogelijkheden voor de kwantificering van met name het inherente risico, het interne beheersingsrisico en het cijferanalyserisico. Zie de *kaders* voor voorbeelden. Met deze vier risico's kan de auditor het risico dat hij een tot een verkeerd oordeel komt kwantificeren.
Het push-leftprincipe betekent dat een auditor start aan de rechterkant (steekproef/cijferanalyse) en op basis hiervan kijkt naar het interne beheersingsrisico om dan stil te staan bij het inherente risico. Vaak zullen audits precies andersom gaan. Starten met het inschatten van inherente risico. Dan kijken naar processen, het beoordelen van interne beheersingsmaatregelen om te eindigen bij een steekproef (van links naar rechts).
Echter, de belangrijkste meerwaarde van het push-leftprincipe volgt als we juist van rechts naar links gaan. De internal auditor kan elke bevinding (bijvoorbeeld uit een steekproef) die hij zelf doet gebruiken om de zekerheid links van hem te vergroten. Als we rechts beginnen betekent dit dat hij gevonden fouten in zijn steekproeven gebruikt bij zijn cijferanalyses. Inzichten uit de cijferanalyses en steekproeven kunnen leiden tot business rules die in de interne beheersing van de processen kunnen worden ingebed. Geconstateerde




**Figuur 1.** Het push-leftprincipe

**Casus Uitkeringsinstantie**
De interne accountantsdienst van een uitkeringsinstantie slaagt erin om de rechtmatigheidscontrole voor een bepaald type uitkering jaarlijks te vernieuwen door steeds meer elektronische data te betrekken zodat steeds minder criteria voor rechtmatigheid door middel van steekproeven gecontroleerd hoeven te worden. Daarnaast organiseert zij jaarlijks een risk & control self assessment workshop met de eerste en tweede lijn. De uitkomsten van die workshop worden gebruikt om business rules aan te scherpen en de massa slimmer te stratificeren op foutgevoeligheid. Foutgevoelige strata worden intensiever gecontroleerd, hoewel er ook nog beperkte controlewerkzaamheden in de minst risicovolle deelmassa plaatsvinden. Gevonden fouten worden vertaald in nog slimmere stratificaties voor de controle van volgend jaar. De eerste en tweede lijn voelen zich gewaardeerd omdat hun kennis optimaal wordt ontsloten. Er ontstaat een cultuur waarin niet langer jaar-in-jaar-uit hetzelfde controleprotocol wordt afgedraaid, maar waarin het de ambitie is om het controleprotocol elk jaar wéér slimmer te maken. Waar gevonden fouten eerder als een ramp werden beschouwd omdat ze niet in een geïsoleerde massa werden gevonden en dus al snel opbliezen tot een ontoelaatbare fout, worden ze nu juist verwelkomd omdat hun extrapolatie naar het geheel beperkt is maar ze wel handvatten bieden om nog slimmer te stratificeren. Een gevulde koek voor iedereen die een fout vindt!

zwakheden in de interne beheersing die zo worden ontdekt, kunnen leiden tot aanbevelingen tot productrationalisatie ter verlaging van het inherente risico, zodat delen van de interne controle overbodig worden. Een dergelijke aanbeveling is de ultieme push left. Hoe verder naar links de aanbeveling doorwerkt hoe hoger doorgaans ook de toegevoegde waarde. Het bovenstaande wordt aangegeven met de drie push-leftpijlen onder de figuur.

Binnen de organisatie bevindt de internal auditor zich rechts in de keten, terwijl hij via zijn controlemix wel de risico's in de hele keten in kaart brengt. Hij heeft dus de mogelijkheden om een beweging naar links te initiëren. Op basis van de bevindingen van de toezichthouder of de externe auditor krijgt hij vanuit rechts ook nog eens goede ideeën voor steekproeven en cijferanalyses in zijn schoot geworpen. Naast het afgeven van gekwantificeerde zekerheid als daar aanleiding toe is initieert hij zo ook verbeteringen in zijn organisatie. Dit zijn de op feiten gebaseerde observaties waar de organisatie op kan acteren en waarvoor de internal auditor meer waardering zal oogsten en meer waarde zal kunnen toevoegen. Hij doet dit primair als continue verbeteraar van zijn eigen organisatie en pas secundair als verbeteraar van de auditprocessen.
Kortom, het push-leftprincipe zorgt ervoor dat de internal auditor zijn onzekerheid kwantificeert, steeds effectiever werkt maar vooral ook continu verbetering aanjaagt binnen zijn organisatie. Last but not least, zijn werk wordt er een stuk interessanter door en eventueel koudwatervrees voor data analytics zal snel omslaan in enthousiasme en kansen! <<

Jacques de Swart is als partner verantwoordelijk voor de data-analyticsafdeling van PwC Advisory. Daarnaast is hij hoogleraar toegepaste wiskunde aan Nyenrode Business Universiteit. De Swart heeft een passie voor organisaties helpen door de pracht en kracht van wiskunde te ontsluiten.

Jan Wille is senior manager binnen de data-analyticsafdeling van PwC Advisory. Hij richt zich op risicomodellering, hoofdzakelijk binnen de financiële sector. Wille studeerde econometrie en promoveerde op onderzoek naar de toepassing van statistische expertsystemen binnen de accountantscontrole.

Michael Zuur is senior manager binnen de data-analyticsafdeling van PwC Advisory. Hij richt zich op risk & compliance modelling (RCM) in de financiële sector, ofwel op het gebruik van kwantitatieve methoden als data-analyses, steekproeven en risicomodellering om klanten te helpen om te gaan met (nieuwe) toezichthouders vereisten. Zuur heeft een achtergrond in de econometrie en een executive master in Operational en Internal Auditing.

Ir. Gezina Atzema RO



In deze rubriek stelt *Audit Magazine* vijf vragen aan een CAE. Deze keer aan Marian Meeuwsen, CAE van Concern Auditing gemeente Rotterdam.

# Vijf vragen aan...

één

**Hoe ziet uw afdeling eruit qua taak- en samenstelling?**

"Concern Auditing Rotterdam is een jonge afdeling: we bestaan drie jaar, de medewerkers zijn jong van geest en we kijken op een jeugdige, nieuwsgierige wijze naar het auditvak. De afdeling bestaat uit circa 22 mensen met een zeer diverse achtergrond: van bestuurskundige, historicus, EDP-auditor, jurist tot accountant. Wat ons bindt is passie voor de stad Rotterdam en de drive om de gemeentelijke organisatie beter te laten presteren. Wij voeren onze audits uit voor het college van B&W en het management van de gemeente Rotterdam. De audits zijn heel divers. Zo toetsen wij de efficiency, effectiviteit en de kwaliteit van de interne beheersing van processen, systemen, projecten, programma's en organisatieonderdelen. We bekijken of de opzet in orde is, of men op de goede weg is en achteraf of de beoogde doelen zijn bereikt. Concern Auditing levert daarmee een bijdrage aan een betere beheersing van de risico's, het anticiperen op kansen (op concernniveau) en aan het realiseren van de doelen van de gemeente Rotterdam."

twee

**Op welke manier werkt u samen met de business en de tweede lijn?**

"Ons motto is: audits leiden tot verbetering. We staan graag naast de business. Kijken objectief mee en stellen de kritische en soms lastige vragen. Zo maken we blinde vlekken zichtbaar, zetten we de organisatie aan het denken en stellen vanzelfsprekendheden ter discussie. We delen onze kennis en waarnemingen. Focus is: wat kan er richting de toekomst beter? We kijken niet graag achteruit, maar zijn meer gericht op de toekomst. Dat betekent dat we samen met de business komen tot oplossingen, ieder vanuit de eigen rol en verantwoordelijkheid."

**Over...**

Marian Meeuwsen RA RC is hoofd van Concern Auditing van de gemeente Rotterdam.

drie

**Hoe ziet u het vak in de komende jaren ontwikkelen?**

"Het vak gaat gelijke tred houden met de ontwikkelingen om ons heen. Dus meer IT-driven audits tijdens de uitvoering van projecten en programma's en niet achteraf. Ik zie een verbreding over alle aspecten van de organisatie. Hiermee bedoel ik dat de werkzaamheden zich niet beperken tot de bedrijfsvoering, maar zich ook richten op de primaire activiteiten van de gemeente. Daar horen wat ons betreft ook onderzoek naar bijvoorbeeld het systeem van integriteit en doelmatigheidsonderzoeken bij. De opmerking van Leen Paape in *Audit Magazine* van juni 2015: 'Ik heb geleerd mijn rug recht te houden', spreekt mij daarbij zeer aan."

vier

**Welke verandering zou u zelf graag zien in het vak?**

"Ik verwacht en hoop dat de lijn die wij bij Concern Auditing hebben ingezet, zich doorzet. Niet te rigide vasthouden aan normenkaders maar kijken hoe wij met audits kunnen bijdragen aan het behalen van de doelstellingen van de gemeente. Dat vraagt soms om een onorthodoxe aanpak en je nek uitsteken. Maar als dat lukt, geeft dat erg veel voldoening."

vijf

**Waar gaan we u in de toekomst nog tegenkomen?**

"Zeker in Rotterdam! Een mooie stad om met en voor te kunnen werken. Een stad die blijft verrassen en zich blijft vernieuwen. De werkwijze van de gemeente Rotterdam is vaak onorthodox en trendsettend. Dat wordt weerspiegeld in de skyline van de stad met iconen als de Markthal en De Rotterdam. Laatst is daar het Timmerhuis aan toegevoegd. Dat blijft boeien en biedt elke keer weer een ander perspectief. Kortom, daar wil je zijn en gezien worden."

Hans Nieuwlands RA CIA CGAP CCSA

# Zakelijk **inzicht** en andere **essentiële** competenties

Het IIA Global Internal Audit Competency Framework (het raamwerk) is een instrument dat de competenties omschrijft die nodig zijn om aan de eisen van het International Professional Practices Framework (IPPF) te voldoen. Dit om het beroep van internal auditor naar behoren uit te voeren.

Gevraagd naar de belangrijkste competenties van internal auditors noemen internal auditors zelf vaak het voldoen aan beroepsstandaarden, een kritische instelling, goede communicatieve vaardigheden en expertise op het gebied van interne controle. De klanten van de internal auditfunctie (IAF) zoals de raad van bestuur, het senior management en de auditcommissie zijn het daar niet altijd mee eens en vinden het hebben van zakelijk inzicht en overtuigingskracht en samenwerking zeker zo belangrijk. Daarnaast is een goed begrip van verbetering en innovatie belangrijk. In dit artikel ga ik dieper in op de laatst genoemde competenties omdat ik denk dat het goed is voor internal auditors om zich af te vragen of ze deze voldoende hebben ontwikkeld.

**Richtlijnen vanuit het IIA**

Het IIA heeft richtlijnen uitgevaardigd op het gebied van de noodzakelijke competenties. Standaard 1210 *Vakbekwaamheid* stelt dat internal auditors de kennis, vaardigheden en overige competenties moeten hebben om de hun opgedragen werkzaamheden te kunnen uitvoeren (zie *figuur 1*). De IAF als geheel dient deze competenties te hebben of te verwerven om al hun taken naar behoren te kunnen uitvoeren. In de Common Body of Knowledge Study (CBOK) is onderzoek gedaan naar de tien kerncompetenties van internal auditors. Op basis van de uitkomsten ontwikkelde The Institute of Internal Auditors Inc. het Global Internal Audit Compentency Framework (raamwerk).

Dit artikel gaat dieper in op een aantal competenties die minder uitvoerig zijn behandeld in de IPPF, te weten: zakelijk inzicht, overtuigingskracht & samenwerking en verbetering en innovatie. Dit zijn de competenties waar stakeholders de nadruk op leggen en die vanuit een traditionele auditopleiding naar mijn mening niet altijd voldoende worden belicht.


**Figuur 1.** Structuur van het competentieraamwerk en de samenhang van de onderdelen ervan. (©2013 IIA Inc.)

**Competentie: zakelijk inzicht**
Bij het evalueren van uitgevoerde audits wordt vaak de opmerking geplaatst dat internal auditors te weinig oog hebben voor de zakelijke afwegingen die het management maakt. Natuurlijk zijn auditors geen ondernemers, maar het is goed om de essentiële elementen van het ondernemerschap te begrijpen. Daar hoort een winststreven bij, waarbij bewust risico's worden gelopen om de doelstellingen te behalen binnen gegeven (budgettaire) beperkingen. Auditors lopen tegen ondernemersrisico's aan die niet worden afgedekt. Op grond daarvan worden vaak aanbevelingen gedaan aan het management. De implementatie van de verbeterpunten die de auditor aanreikt zijn echter niet altijd economisch te verantwoorden. In het bespreken van de risico's en mogelijke verbeterpunten dient de auditor open te staan voor het standpunt van het management en bereid te zijn een dialoog aan te gaan.
Gebruikers van de auditrapporten verwijten de internal auditor regelmatig dat deze de 'business' niet begrijpt. Gebrek aan kennis van de branche, van de organisatie of van de producten of services ondermijnen het gezag van de internal auditor. Dit geldt in het bijzonder voor organisaties waar hoogopgeleide andere disciplines werken. Het is daarom van groot belang dat internal auditors hun zakelijk inzicht vergroten en zich waar nodig laten adviseren door experts bij het uitvoeren van de audits.

## Verandering roept weerstand op, dat is niet anders bij verbetervoorstellen die een auditor doet

Het raamwerk noemt als competenties omtrent zakelijk inzicht specifiek:
- Verdiep je in de missie, strategie en doelstellingen van het bedrijf.
- Neem kennis van de risico's waaraan de organisatie is blootgesteld.
- Houd rekening met de organisatiecultuur.
- Neem kennis van de branche, inclusief relevante regelgeving.
- Begrijp relevante macro- en micro-economische factoren en de impact ervan op de organisatie.
- Heb kennis van relevante, mondiale ontwikkelingen.

- Heb kennis van relevante, internationale wet- en regelgeving.
- Evalueer gehanteerde kwaliteitsmanagementsystemen.
- Beoordeel de mate waarin de organisatie steunt op IT en de daarbij behorende risico's.
- Begrijp kostprijsberekeningen, financiële rapportages en managementrapportages.

**Competentie: overtuigingskracht & samenwerking**
Het is van groot belang dat internal auditors hun boodschap kunnen 'verkopen'. Verandering roept immers weerstand op en dat is niet anders bij verbetervoorstellen die een auditor doet. De auditor en de auditee zijn onderdeel van dezelfde organisatie en dragen allebei bij aan het bereiken van de bedrijfsdoelstellingen; ze hebben echter beiden een andere rol. De auditor moet zijn gesprekspartner met argumenten ervan kunnen overtuigen dat verbetering noodzakelijk is en enkel in uitzonderingsgevallen escaleren. Dit is in het belang van beide partijen en daarmee uiteindelijk ook in het belang van de organisatie.
De samenwerking tussen het management en de auditor dient altijd constructief te zijn en concreet te worden ingevuld. Zo kan er bijvoorbeeld samen worden gezocht naar een oplossing voor een onderkend probleem. Nadat de internal auditor zijn zorgpunt heeft toegelicht kan de manager met een verbetervoorstel komen, waarbij beide partijen gezamenlijk vaststellen of dit de juiste oplossingsrichting is. Zo'n gezamenlijke aanpak kan leiden tot een snellere implementatie dan wanneer de auditor een (suboptimale) oplossing voorstelt. Samenwerking kan ook in breder en langduriger verband plaatsvinden, zoals bij projecten. Het is dan zaak om te zorgen dat de onafhankelijkheid en objectiviteit van de auditor niet in het gedrang komt.

Enkele aandachtspunten uit het raamwerk wat betreft overtuigingskracht en samenwerking:
- Wees je bewust van de impact van je eigen interpersoonlijke stijl op die van anderen.
- Gebruik onderhandelingsvaardigheden bij conflicten.
- Zoek de balans tussen diplomatie en assertiviteit.
- Bouw effectieve, strategische partnerschappen.
- Toon veerkracht in moeilijke situaties door weerstand weg te nemen en vervolgens constructief samen te werken.
- Stuur met invloed, persoonlijke overtuiging en sensitiviteit en niet op basis van macht.
- Onderken je eigen beperkingen en vraag om advies en ondersteuning waar nodig.

**Competentie: verbetering & innovatie**
Internal auditors komen vaak met voorstellen voor de verbetering van de governance, risk management & control van organisaties. Sommige bevindingen kunnen leiden tot beperkte wijzigingen, terwijl andere mogelijke impact hebben op organisatiebrede processen, systemen of projecten. Veranderingen leiden vaak tot weerstand. De auditor dient een goed begrip te hebben van de processen die bijdragen aan een succesvolle verandering waar het gaat om de implementatie van aanbevelingen.

Dit onderdeel van het raamwerk richt zich vooral op de CAE. Een selectie:
- Ondersteun doorlopende verbetering en innovatie en ondersteun anderen daarbij.
- Ontwikkel een visie hoe veranderingen kunnen worden geïmplementeerd in de organisatie.
- Lever een significante bijdrage aan de veranderstrategie van de organisatie.
- Moedig anderen aan om innovatieve ideeën voor te stellen en geef positieve feedback om deze ideeën verder uit te werken.
- Onderken en adresseer risico's gerelateerd aan verandering in audits. <<

## Meer weten

Het volledige raamwerk kunt u vinden op http://bit.ly/iiaIACF

Hans Nieuwlands is directeur van IIA Nederland.

Esther van Liempt MSc RA

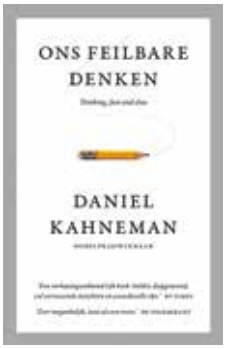
# Op uw **gevoel** afgaan. Is dat **slim**?

Psycholoog en Nobelprijswinnaar Daniel Kahneman beschrijft in *Ons feilbare denken* ogenschijnlijk onuitputbare inzichten, kennis en ervaringen die hij de laatste decennia heeft opgedaan ten aanzien van oordeels- en besluitvorming. 'Hebben mensen goede intuïties op het punt van statistiek?', is een van de eerste vragen geweest die Kahneman zichzelf (samen met Amos Tversky) heeft gesteld. In het boek onderwerpt hij u veelvuldig aan oefeningen waarbij vaak snel en dus op basis van intuïtie gereageerd dient te worden. Voorts laat hij u ervaren dat relevante statistische gegevens bijna altijd over het hoofd gezien worden. De volgende oefening is daar een voorbeeld van: denk na over de letter K. Komt deze letter vaker voor als eerste letter of als de derde letter van een woord?
Het is veel gemakkelijker om op woorden te komen die met een bepaalde letter beginnen, dan op woorden die diezelfde letter in de derde positie hebben. Derhalve denken de meeste respondenten dat de letter K vaker als eerste letter voorkomt. Echter, het tegengestelde is waar, de letter K komt in de derde positie vaker voor.

De resultaten van zijn onderzoeken en experimenten beschrijft Kahneman in vijf delen. In het eerste deel worden de twee hoofdpersonen van ons brein beschreven, te weten het automatische en intuïtieve systeem 1 en het rationele en bewuste systeem 2. Het tweede deel houdt zich bezig met het raadsel waarom het zo moeilijk is om statistisch te denken. Deel drie gaat in op de beperkingen van ons denkvermogen. Het vierde deel beschrijft een dialoog met de economie over het maken van inschattingen en nemen van besluiten. Ten slotte wordt in het laatste deel de dominantie van systeem 1 beschreven, wat maakt dat we onjuiste beslissingen kunnen nemen op basis van herinneringen zonder rekening te houden met de (slechte) ervaringen die we daarbij hadden.

Kahneman heeft met dit boek bedoeld een beeld van de werking van onze geest te schetsen dat berust op ontwikkelingen in de cognitieve en sociale psychologie. Door het lezen van dit boek zult u begrijpen waarom u aan loterijen meedoet terwijl u weet dat de kans dat u de hoofdprijs wint ongelooflijk klein is. Of waarom u in drukke perioden afstapt van een dieet en te veel geld uitgeeft aan impulsaankopen. Kahneman schetst tal van dergelijke eyeopeners en creëert daarmee een enorme bewustwording voor het feit dat we geneigd zijn te overschatten hoeveel we van de wereld begrijpen en tegelijkertijd de rol van het toeval in gebeurtenissen behoorlijk onderschatten.

Voor auditors kan dit boek erg interessant maar tegelijkertijd ook confronterend zijn vanwege de biases die bestaan in onze oordeelsvorming. Door het lezen van dit boek komt u erachter hoe onze oordeelsvorming werkt en gaat u wellicht objectieve oordeelsvorming in een nieuw daglicht zien. Het vermogen om beoordelingsfouten te herkennen en te begrijpen kan door het lezen van dit boek versterkt worden. Het voorkomen van deze fouten is echter, in ieder geval volgens de theorie van Kahneman, niet mogelijk. Wel zult u op basis van de opgedane inzichten van Kahneman eerder herkennen dat sprake is van een situatie waarbij mogelijk een foutief oordeel gegeven of beslissing genomen zal worden. Op uw gevoel afgaan is daarbij vaak niet slim.




**Ons feilbare denken**
**Thinking, fast and slow**
DANIEL KAHNEMAN
Business contact
ISBN 9789047006473
€ 12,50 (paperback)

Esther van Liempt is senior auditor bij CZ. Daarnaast is zij betrokken bij de opleiding tot registeraccountant aan de Universiteit van Tilburg als corrector en scriptiebegeleider.

Dr. Arno Nuijten RE CIA

In dit artikel wordt op een verhalende manier verteld over het onderzoek dat bij Erasmus School of Accounting & Assurance (ESAA) is verricht rondom de vraag waarom mensen wel of niet geneigd zijn om te luisteren naar risicowaarschuwingen van de internal auditor. In het bijzonder wanneer het spannend wordt, zoals bij complexe op hol geslagen ICT-projecten. Er wordt een analogie gelegd met een vakantiereis naar Spanje met de internal auditor op de bijrijdersstoel.

# De internal auditor op de **bijrijdersstoel** bij complexe ICT-projecten

In de beroepspraktijk van de internal auditor kan soms de volgende, bijna wanhopige, vraag opkomen: waarom wordt er niet geluisterd naar mijn indringende en onderbouwde waarschuwingen over risico's die de organisatie loopt? In een tijd waarin veel geschreven wordt over de rol, de positionering en de bijdrage van internal auditors, lijkt dat een relevante vraag. Als namelijk op cruciale momenten niet geluisterd wordt naar de waarschuwingen van internal auditors, dan is dat toch een indicator ten aanzien van de effectiviteit van de interne auditfunctie binnen een organisatie?
Nog pijnlijker wordt het als waarschuwingssignalen van de internal auditor lange tijd terzijde worden geschoven, waardoor het risicovolle gedrag in de organisatie alleen maar toeneemt. En als dan uiteindelijk (veel te laat) hardhandig een eind komt aan op hol geslagen projecten of risicovol gedrag, vraagt de omgeving zich af: hoe heeft het zover kunnen komen? En waar was Internal Audit?
Het lijkt alsof mensen in de organisatie niet willen luisteren naar waarschuwingen. Woorden als 'ego' en 'alfamannetjes' dienen zich al snel aan. Wie zich echter werkelijk in de vraag verdiept waarom er soms niet geluisterd wordt, weet dat het antwoord niet zo simpel ligt.

**Doof voor risicowaarschuwingen**
Natuurlijk beperkt dit fenomeen van 'risicodoofheid' zich niet tot de risicowaarschuwingen van internal auditors. Ook in andere situaties zijn mensen soms geneigd om waarschuwingen in de wind te slaan. Er zijn voorbeelden te over, van politiek tot voetbalclubs. Vaak leidt dit achteraf tot verwijten aan degenen die doof waren, soms meerdere keren. Het is dus niet alleen een relevant maar ook een gevoelig onderwerp. Een verwijtend vingertje naar diegenen die doof bleken voor risicowaarschuwingen is op voorhand slechts een deel van het verhaal. Doofheid voor dergelijke signalen kan namelijk iedereen overkomen. Voorbeelden uit het verkeer kunnen dit soort fenomenen goed duiden, velen zullen ze namelijk herkennen, bij zichzelf of in hun directe omgeving.

Een voorbeeld: een paar jaar geleden moest de bumper van mijn auto vanwege parkeerschade vervangen worden. De schadehersteller vertelde dat opvallend veel bumpers met schade van die parkeersensoren hadden (net als die van mij). Blijkbaar voelen mensen zich met die dingen zo zeker dat, bijvoorbeeld bij haast, de aandacht verslapt en de waarschuwingspiep pas wordt gehoord ná de botsing. Of er wordt achteraf vol overtuiging beweerd dat hij – deze keer – niet op tijd gepiept heeft. We hebben het hier over een soort schijnzekerheid waardoor we de aandacht verliezen voor waarschuwingssignalen. Het voorbeeld laat zien dat er bij doofheid niet per se sprake is van onwil, maar dat het ook te maken kan hebben met verminderde gevoeligheid voor waarschuwingssignalen als gevolg van wat we begrensde rationaliteit noemen. We zijn minder rationeel dan we denken.

**Complexe ICT-projecten als psychologisch mijnenveld**

Door de ESAA wordt onderzoek gedaan naar besluitvorming in complexe ICT-projecten, iets waar veel internal auditors mee te maken hebben. Juist door die complexiteit mogen we een dergelijk project gerust als een psychologisch mijnenveld beschouwen. In het bijzonder richt het onderzoek zich op complexe ICT-projecten die een eigen leven zijn gaan leiden en schijnbaar niet meer gestopt of bijgestuurd kunnen worden.

Grote ICT-projecten hebben typische kenmerken: ze zijn vaak erg complex, gericht op de lange termijn, gaan gepaard met grote belangen, ze kosten veel, veel mensen zijn er bij betrokken en hebben er een mening over, ze herbergen vaak technologische onzekerheid en staan onder druk van buiten. Ook is de voortgang moeilijk waar te nemen, bijvoorbeeld in vergelijking met het bouwen van een huis. Natuurlijk zijn er vele andere soorten projecten die dezelfde kenmerken vertonen, maar het lijkt geen toeval dat juist grote ICT-projecten de naam hebben om op hol te slaan en onderweg de rode seinen voorbij te stevenen. Er gaat veel geld en energie verloren wanneer ze te laat of helemaal niet bijgestuurd worden, ook al is het doel van het project (de onderliggende businesscase) al lang uit beeld verdwenen.

Juist door deze stapeling van afhankelijkheden, veranderlijkheid, onzekerheden en ambiguïteit is het onmogelijk om puur verstandelijk beslissingen te nemen waarbij opties en keuzen worden gewogen op hun consequenties. Mensen zijn nu eenmaal begrensd in hun vermogen om alle relevante informatie te verwerken. Daarom schiet ons rationele systeem in deze situaties tekort en maakt plaats voor ons ervaringssysteem. Op basis van eerdere ervaringen richten we onze aandacht op belangrijke zaken en laten ons leiden door vuistregels, heuristieken en intuïtie.

Bij complexe projecten zoeken we daarom juist de projectleider die in het verleden heeft bewezen zijn aandacht te kunnen richten op de zaken die nodig zijn om projecten tot een goed einde te brengen. En daarom zal die projectleider geneigd zijn om mensen om zich heen te verzamelen met wie hij dezelfde ervaringen heeft opgebouwd in eerdere projecten. Dit ervaringssysteem neemt ons bij de hand in het lopende project. De andere kant van de medaille van dit ervaringssysteem is dat het ons in sommige situaties ook bij de neus kan nemen, doordat al onze aandacht gevangen wordt door factoren die onze waarnemingen en inschattingen verstoren.

Hier dient het psychologisch mijnenveld zich aan, denk daarbij aan het eerdergenoemde voorbeeld van de parkeerschade. De meest ervaren projectleiders zijn het meest kwetsbaar voor dergelijke verstorende invloeden: onze ervaringen gaan met onze waarneming aan de loop.

**Over op hol slaande projecten en de vakantie naar Spanje**

Het gezin zit al uren in de auto, onderweg naar de camping in het zuiden. Na 900 kilometer in de hitte geeft de bijrijder de chauffeur op stevige toon het dringende advies om op de volgende parkeerplaats te stoppen en een camping voor de nacht

te zoeken. Maar de chauffeur ziet het advies vooral als een verwijt en hoort in gedachten al de hoon op het eerstvolgende familiefeestje. Gevolg: de chauffeur stampt juist nog wat harder op het gaspedaal, scheurt de parkeerplaats voorbij en de stemming in de auto is te snijden. Het doel van de reis, een prettige vakantie, is inmiddels allang achter de horizon verdwenen.
Er zitten in dit voorbeeld wat kenmerken die ook terugkeren bij grote ICT-projecten die in zwaar weer dreigen te komen en die het psychologisch mijnenveld illustreren.

**Alle focus op het dashboard – doelsubstitutie**
Zo gauw mensen intensief met een complexe taak aan de slag gaan die hen uitdaagt of anderszins bezighoudt, wordt automatisch alle aandacht gefocust op het volbrengen van die taak. Zodra de chauffeur in het voorbeeld in de auto is gestapt op weg naar het zuiden, verdwijnt het doel van de reis, een plezierige vakantie, naar de achtergrond. Alle aandacht is nu gericht op het afronden van de reis zelf en wordt opgeslokt door de klok, de kilometers en de benzinemeter. Dit fenomeen wordt 'doelsubstitutie' genoemd: de vakantie als doel maakt plaats voor het doel om de reis af te ronden.
Bij complexe projecten zien we hetzelfde gebeuren. Zodra het project van start is gegaan, belandt de businesscase (het bestaansrecht en doel van het project) in de onderste la en alle aandacht wordt opgeslokt door de metertjes op het dashboard en de kilometers in de vorm van kleurenrapportages, tijdschema's en opleverdata, %-complete indicatoren, voortschrijding in de kosten en eventuele budgetoverschrijdingen.



De businesscase als doel heeft plaats gemaakt voor het project als doel en alle aandacht wordt opgeslokt om deze klus te klaren. En juist doordat alle aandacht wordt opgeslokt door de kilometerteller en metertjes op het dashboard hebben mensen nauwelijks in de gaten hoe makkelijk hun ervaringssysteem daarmee op het verkeerde been gezet kan worden. Hier dienen zich de volgende psychologische mijnen aan.

***We zien wat we verwachten***
De eerste psychologische mijn die we nu tegenkomen heet cognitieve dissonantie, in dit verband ook wel aangeduid als 'zelfbevestiging'. Onze aandacht wordt opgeslokt door datgene dat we verwachten te zien en dat bevestigt wat we van tevoren al dachten of vermoedden. Dat is geen moedwillige actie, maar ons ervaringssysteem maakt ons juist gevoelig voor signalen die eerdere ervaringen, indrukken of vooroordelen bevestigen en onderstrepen. De ervaren projectleider is gevoelig voor informatie die zijn ervaringen in voorgaande projecten bevestigt, maar hij is tamelijk ongevoelig voor gebeurtenissen die daarvan afwijken. Zijn mooie track record zit hem wat dat betreft in de weg. Zoals de ervaren chauffeur op weg naar Spanje zich zal laten leiden door zijn eerdere succeservaringen.

***De metertjes op het dashboard sturen beslissingen***
Omdat ons waarnemingssysteem zo gefocust is op het dashboard van het project, kunnen wij ook gemakkelijk op het verkeerde been gezet worden door subtiele wijzigingen in de metertjes op dat dashboard. Een presentatie die de aandacht vestigt op een vorm van verlies of achterstand leidt er onbewust toe dat wij meer de neiging krijgen tot risicozoekend gedrag. Een presentatie die de aandacht richt op een vorm van voorsprong of winnen leidt ertoe dat we juist meer de neiging hebben tot veilige en risicomijdende keuzen. Als de aandacht in hoge mate wordt gericht op de verlieskant van een risicovol project zijn we dus juist geneigd om door te blijven gaan met een risicovol avontuur.
We zien dit ook terug als een soort casinogedrag bij projecten, waarbij keer op keer 'ingezet' wordt als gevolg van het zogenaamde 'sunk-costeffect': 'Dit project heeft al zoveel gekost dat we niet meer kunnen stoppen'. Doordat onze aandacht wordt opgeslokt door het verlies vanwege de reeds gemaakte projectkosten, neemt het commitment toe om te volharden in de voortzetting van het project. En naarmate we verder in deze fuik terechtkomen wordt de aantrekkingskracht om door te gaan steeds sterker.

***Het completioneffect***
Een andere psychologische mijn wordt gevormd door het zogenaamde completioneffect: de rapportages roepen het beeld op dat het project voor 90% gereed is. Door de beeldvorming dat we er 'bijna zijn' blijven we bereid om de investeringen te doen in 'de laatste stap'. We zouden dit kunnen typeren als een soort afmaakgedrag. Meer dan eens blijkt een dergelijk project op 90% te blijven hangen en niet de afronding te benaderen.

***Schijnzekerheid maakt zich van ons meester***
Een ander mijnenveld heeft te maken met 'illusion of control' ofwel een soort van schijnzekerheid. Daarbij hebben wij het gevoel dat we een hogere mate van controle hebben over een situatie dan dat we feitelijk hebben. Wij zijn derhalve geneigd

om onszelf vaardigheden toe te dichten op basis van waargenomen patronen en daaruit ontstane verwachtingen: 'Ik heb al drie keer een zes met mijn dobbelsteen gegooid toen het nodig was, dus nu gaat me dat vast nog een keer lukken'. Als speler schudden we vol overtuiging de dobbelsteen en blazen er een keer op alvorens te werpen, alsof wij met dit dobbelsteengedrag als ritueel onze kans op succes kunnen sturen.
Er zijn vele factoren van invloed op het gevoel van controle (perceived control) die wij ondervinden in een situatie. De zichtbare aanwezigheid van allerlei controls brengt met zich mee dat betrokkenen de perceptie hebben meer controle over de situatie te hebben. En het interessante is dat mensen geneigd zijn om in zo'n situatie meer risico's te nemen en mogelijk zelfs roekeloos gedrag te gaan vertonen.
De stap richting het ICT-project in ons voorbeeld is niet moeilijk te maken. Bij aanvang was gedetailleerd beschreven wat de uitkomst van het project moest worden. Op deskundige wijze was opgetekend hoe de processen, systemen, gegevens en techniek er aan het einde van het project zouden uitzien. Ook was uitvoerig beschreven hoe de reis daar naartoe zou gaan plaatsvinden en was een beproefde projectmethode gekozen. De ervaren projectleider wist sowieso al wat ons te wachten zou staan want hij had immers al vaker met dit bijltje gehakt. Al deze factoren dragen bij aan een gevoel van zekerheid dat de uitkomst behaald gaat worden en de situatie onder controle is. Niet in het minst heerst dit gevoel bij de projectleider zelf.

**De internal auditor op de bijrijdersstoel**
In het psychologisch mijnenveld van de bestuurder op weg naar Spanje introduceren wij nu iemand op de bijrijdersstoel die zich met de bestuurder en zijn reis gaat bemoeien en risicowaarschuwingen afgeeft. De variabele die we daaraan toevoegen is dat deze bijrijder gezien kan worden als meewerkend partner of als een tegenstander die de tekortkomingen van de bestuurder blootlegt. Vaak hebben bestuurder en bijrijder een historie met elkaar. Ook al is de inhoud van de boodschap hetzelfde, ons waarnemingssysteem filtert de boodschap door het beeld dat we van de boodschapper hebben.
Uit het ESAA-onderzoek blijkt dat het beeld van de bijrijder als partner of als tegenstander van invloed is op de neiging om naar die waarschuwing te luisteren. Ook is vastgesteld dat er een wisselwerking is met de eerdergenoemde factoren van ons psychologisch mijnenveld: namelijk 1) de manier waarop de boodschap wordt gepresenteerd, in termen van winst of verlies en 2) de mate van het gevoel van controle die de bestuurder meent te hebben.

**Implicaties voor de praktijk van internal auditors**
Wat betekent dit onderzoek voor de praktijk van internal auditors in het algemeen en als bijrijder bij complexe ICT-projecten in het bijzonder?
Allereerst blijkt dat strategisch partnerschap loont voor internal auditors om gehoord te worden op de momenten dat het echt spannend wordt. Opgemerkt moet worden dat de rol van operationeel partner (als internal auditor operationele werkzaamheden verrichten in projecten) op dergelijke momenten juist averechts kan werken: dus als bijrijder onderweg de boterhammen smeren voor de bestuurder helpt bepaald niet op momenten dat je je met de reis gaat bemoeien.
Ook blijkt uit het onderzoek dat het verstandig is waarschuwingen niet, zoals internal auditors gewend zijn, negatief in termen van verliezen/tekortkomingen te presenteren: 'je haalt de planning niet', 'je voldoet niet aan je norm', et cetera. Focus op verliezen zet mensen er namelijk toe aan om risico's te blijven nemen. Dit kan juist doofheid voor risicowaarschuwingen in de hand werken.
Verder is het voor internal auditors van belang om een beeld te hebben van de 'perceived control' van de bestuurders van een ICT-project en schijnzekerheid op te merken bij de ervaren projectleider en projecten die zijn overladen met plannen, rapportages en procedures. Het psychologisch mijnenveld toont zich in signalen van opmerkelijk gedrag (denk aan gedrag van een overmoedige chauffeur in de auto of het eerder genoemde dobbelsteengedrag) en in kenmerkend woordgebruik, maar ook de timing van de boodschap is van belang.[1]
Samen met andere partijen, verricht ESAA vervolgonderzoek naar deze en andere factoren om doofheid voor risicowaarschuwingen te begrijpen en daarmee een bijdrage te leveren aan de effectiviteit van internal auditors in de praktijk. En hebt u er op uw werk niets aan, dan hebt u er misschien plezier van op vakantie. <<

## Focus op verliezen zet mensen ertoe aan om risico's te blijven nemen

**Noot**
1. Benschop, Nuijten en Van der Pijl, 'Het beeld achter de woorden', *M&O*, nr. 4, pag. 59-75, 2015.

Arno Nuijten is sinds 2012 wetenschappelijk directeur van de opleiding IT-Auditing & Advisory aan de Erasmus School of Accounting & Assurance en als onderzoeker verbonden aan de vakgroep Gedragseconomie. Hij is ruim 25 jaar werkzaam in diverse functies in internal auditing en IT-auditing alsmede in (interim-)management op het gebied van ICT-projecten.

Dit artikel is een verhalende weergave van het proefschrift van Arno Nuijten: *Deaf Effect for Risk Warnings – A causal examination applied to information systems projects*.

Ingrid Laurier Msc. RO

Risicoperceptie verschilt per individu. Dit heeft te maken met de mate van risicoaversie. We weten dat dit verschil op individueel niveau bestaat, maar bestaat het ook tussen verschillende afdelingen of functionarissen in een organisatie? Bestaat er bijvoorbeeld verschil in risicoperceptie tussen de internal auditor en de auditee? En zo ja, waar wordt dit verschil door veroorzaakt?

# Verschil in **risicoperceptie**

Veel economische theorieën zijn gebaseerd op het uitgangspunt dat mensen rationeel handelen. In de realiteit blijkt dat mensen in veel situaties juist irrationeel handelen. De 'expected utility theory' gaat ervan uit dat mensen rationeel handelen en altijd kiezen voor de optie met de hoogste verwachte waarde (gewogen gemiddelde waarde). Kahneman en Tverskey (1997) hebben aangetoond dat dit niet juist is. Zij deden onderzoek naar het irrationeel gedrag van mensen als het gaat om het nemen van beslissingen met onzekerheid (ofwel met een risico) en introduceerden de 'prospect theory'.
Uit hun onderzoek blijkt dat mensen ook op het gebied van het nemen van risico's irrationeel handelen (bias); mensen vinden het veel erger om iets te verliezen dan dat zij het waarderen om iets te winnen. Daarnaast zullen de meeste mensen sneller kiezen voor de zekere optie in plaats van de onzekere optie. Dit noemen zij 'loss aversion of risk aversion'. Kahneman en Tverskey (1997) hebben, naast het feit dat de mens over het algemeen risicoavers zijn, ook aangetoond dat de mate van risicoaversie kan verschillen per persoon. Een voorbeeld. Welk van de volgende twee opties zou u kiezen?

A. U doet mee aan een loterij waarbij u 25% kans heeft om € 30.000 te winnen en 75% kans heeft om € 0 te winnen.
B. U doet mee aan een loterij waarbij u 20% kans heeft om € 40.000 te winnen.

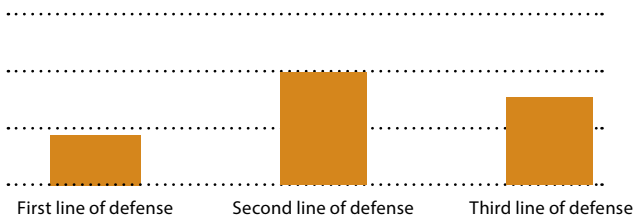
Uit onderzoek van Kahneman en Tverskey (1997) blijkt dat de meeste individuen kiezen voor de meer zekere optie A, terwijl de verwachte waarde van optie B € 500 hoger ligt.

**Verschil risicoperceptie internal auditor en auditee**
In het kader van mijn internal auditopleiding aan de UvA in Amsterdam onderzocht ik of de mate van risicoaversie van de internal auditor verschilt van die van de auditee. Door middel van een enquête heb ik de mate van risicoaversie gemeten van 310 medewerkers, verdeeld over verschillende three-lines-of-defensefuncties van één grote Nederlandse financiële instelling. De drie partijen binnen het three-lines-of-defenseprincipe zijn in het onderzoek als volgt gedefinieerd: de eerste line of defense zijn de salesfuncties, de tweede line of defense zijn functies als risk management en compliance en de derde line of defense is de interne auditfunctie (IAF). Uit het onderzoek blijkt dat de gemiddelde medewerker risicoavers is. Daarnaast zijn medewerkers in de eerste line of defense het minst risicoavers en medewerkers in de tweede line of defense het meest risicoavers. De mate van risicoaversie van de medewerkers in de derde line of defense ligt hier tussenin (zie *figuur 1*). Statistische toetsing wijst uit dat dit verschil tussen de verschillende lines of defense significant is.

**Oorzaken: demografische achtergrond en context**
Waar komt dit verschil vandaan? In welke mate speelt de demografische achtergrond van medewerkers, zoals geslacht, leeftijd, opleidingsniveau en inkomen een rol? En is de context, zoals de heersende cultuur, doelstellingen van een afdeling of de positie die iemand binnen een afdeling heeft, een factor? Regressieanalyses laten de volgende significante relaties zien:

- de mate van risicoaversie stijgt naarmate men ouder wordt;
- de mate van risicoaversie daalt naarmate het inkomen stijgt;
- de mate van risicoaversie stijgt naarmate het opleidingsniveau stijgt;
- de context (cultuur/line of defense) is van invloed op de mate van risicoaversie.

Dit betekent dat naast demografische achtergrond (leeftijd, inkomen, opleidingsniveau), context ook een belangrijke factor is die van invloed is op de mate van risicoaversie. Voorts blijkt dat vrouwen binnen de onderzochte organisatie niet




**Figuur 1.** Verschil in risicoaversie tussen three-lines-of-defensefuncties

significant meer risicoavers zijn dan mannen. Interessant, aangezien onderzoek uitgevoerd op grote populaties in (verschillende) landen juist aantoont dat vrouwen meer risicoavers zijn dan mannen (Byrnes, Miller en Schafer, 1999). Mogelijk kan hiervoor een verklaring worden gevonden in het aannamebeleid van de betreffende organisatie of in de heersende cultuur die een bepaalde type vrouwen en mannen aantrekt.

### Invloed op oordeelsvorming

Zowel de demografische achtergrond als de context spelen een rol bij hoe wij als mens in het leven staan. Zij bepalen onze normen waarden. Het model van McDavid and Hawthorn (2006) laat zien dat normen en waarden, maar ook kennis en ervaring, invloed hebben op onze oordeelsvorming (zie *figuur 2*). Dat betekent dat een bias zoals risicoaversie hierop van invloed zou kunnen zijn. Dit is voor ons als internal auditors van belang, aangezien wij dagelijks oordelen over risicobeheersing. Om met de bias risicoaversie om te kunnen gaan is het allereerst van belang dat internal auditors accepteren dat deze bias bestaat. Bovendien zijn er verschillende technieken om deze bias te verminderen, zoals:

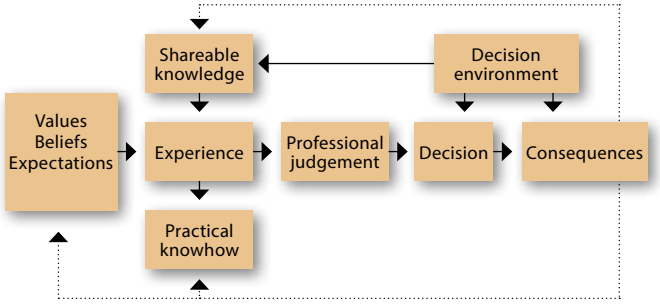
- elkaar wijzen op het feit dat je het probleem ook op een andere manier kunt zien;
- duidelijke criteria bepalen op basis waarvan je een oordeel geeft;
- een duidelijk proces implementeren om tot je uiteindelijke oordeel te komen (Soll et al, 2013).

### Overige inzichten

Uit het onderzoek blijkt dat internal auditors zich bewust moeten zijn van de bias risicoaversie, daar het invloed heeft op de oordeelsvorming. Daarnaast is er nog een aantal andere inzichten voortgekomen uit het onderzoek. Het inzicht in de verschillen in risicoperceptie tussen de internal auditor en auditee stelt ons in staat om hier in de communicatie met de auditee rekening mee te houden en er begrip voor te tonen. Dit kan ertoe leiden dat discussies in het auditproces en afstemming van bevindingen efficiënter verlopen en de kans op escalatie vermindert.

Nu blijkt dat context naast demografische achtergrond een belangrijke invloed heeft op de mate van risicoaversie van een afdeling, is het van belang dat de juiste omgevingsfactoren worden gecreëerd, zoals cultuur en doelstellingen, die passen bij de gewenste mate van risicoaversie. Dit is een aandachtspunt voor de internal auditfunctie zelf, maar kan ook een belangrijk punt zijn dat de internal auditor nadrukkelijker kan meenemen als belangrijke soft contol in advies en assuranceopdrachten.

Het onderzoek geeft verschillende nieuwe inzichten van verbanden tussen risicoperceptie enerzijds en demografische achtergrond en context anderzijds. Meer onderzoek is nodig om deze verbanden in een bredere context aan te kunnen tonen; binnen de financiële sector maar ook binnen andere sectoren. Dit onderzoek geeft op dit moment een indicatie dat verschillen in risicoperceptie bestaan en dat er factoren zijn zoals de bias risicoaversie die onze oordeelsvorming beïnvloeden. Deze indicatie stelt internal auditors in staat zich bewust te zijn van het bestaan van de bias risicoaversie en kan daarmee helpen het dagelijks werk goed uit te voeren. <<




**Figuur 2.** Model professional judgment
(Bron: McDavid and Hawthorn, 2006, p. 454-455)

## Meer weten...

Meer informatie is te vinden in het scriptiedocument *Differences in risk attitudes among the three lines of defense parties within a bank*, dat is op te vragen bij de Universiteit van Amsterdam (Amsterdam Business School).

**Literatuur**


- Byrnes, J., Miller, D. en W. Schafer, 'Gender Differences in Risk Taking: A Meta-Analysis', *Psychological Bulletin*, 125, 1999, p. 367-383.
- Kahneman, D. en A. Tversky, 'Prospect Theory: An Analysis of Decision under Risk', *Econometrica*, 47:2, 1979, p. 263-292.
- McDavid, J.C. en L.R.L. Hawthorn, *Program Evaluation and Performance Measurement: An Introduction to Practice*, London: Sage publications, 2006.


Ingrid Laurier is senior auditor bij ABN Amro, met als aandachtsgebied risk management & strategy. Zij studeerde in september 2014 af voor het Executive Internal Auditing Program aan de Universiteit van Amsterdam. Voor haar afstudeerscriptie onderzocht Laurier het verschil in risicoperceptie tussen de internal auditor en de auditee.

Drs. Sam Huibers EMIA RO CRMA
Drs. Jeroen Bolluijt CISA CISSP CPPD Prince2 P

# De **evolutie** van project auditing

Naar verwachting zullen wereldwijd de uitgaven aan kapitaalintensieve en infrastructurele projecten meer dan verdubbelen en toenemen tot $ 9 biljoen in 2025. Uit onderzoek blijkt dat vanaf 2002 30% van alle projecten mislukt. Aan de hand van het door ons in 2015 uitgevoerde wereldwijde onderzoek verkennen we de oorzaken hiervan en zetten uiteen wat een interne auditor kan doen om de slagingskans van projecten te vergroten.

Vanwege toenemende interesse in project auditing is in 2015 een wereldwijd onderzoek uitgevoerd in navolging van de enquête over trends in project auditing in Nederland (Huibers en Walrave, 2013). De doelstelling van dit wereldwijde benchmarktonderzoek is inzicht verkrijgen in de trends en ontwikkelingen met betrekking tot project auditing en in de wijze waarop auditfuncties hierop kunnen inspelen. Auditors verspreid over 22 sectoren en 43 landen namen aan het onderzoek deel. Aan de hand van vijf thema's de voornaamste uitkomsten van het onderzoek.

**Thema 1. *Trends***
Uit de resultaten blijkt dat respondenten verwachten dat het aantal projecten toeneemt (62%) en dat deze tegelijkertijd ook steeds gecompliceerder worden (76%) (zie *figuur 1*). 90% van de respondenten geeft aan dat de interne auditfuncties (IAF's) waarvoor zij werkzaam zijn inmiddels ook project audits uitvoert.

**Thema 2. *Selectie van projecten***
Doordat er meer projecten zijn dan auditcapaciteit, is het aantal projecten dat geaudit kan worden beperkt. Het is dus van belang de juiste audits te selecteren op basis van de juiste criteria. Op die manier kan de toegevoegde waarde van de project audits gemaximaliseerd worden. In de praktijk blijkt echter vaak geen gestructureerde werkwijze te worden gehanteerd om audits te selecteren. De helft van de project audits komt tot stand op basis van ad-hocverzoeken van het senior management (30%) of de raad van commissarissen (19%) (zie *figuur 2*).

**Thema 3. *De rol van de auditor in projecten***
We onderzochten drie typen rollen die interne auditors op legitieme wijze zouden kunnen vervullen in projecten, al dan niet met randvoorwaarden (Huibers, 2010 en 2013) (zie *figuur 3*):

- Assurancerollen: de interne auditor voert onafhankelijke evaluaties uit op de projectbesturing en controls (bijvoorbeeld het op de juiste wijze toepassen van de projectmethodologie en het evalueren van het ontwerp en de effectiviteit van de projectproducten).
- Adviserende rollen: de interne auditor gebruikt zijn professionele kennis om het project te adviseren maar is niet direct betrokken bij de uitvoering van het project (bijvoorbeeld door middel van het geven van advies over het opzetten van het project en door op te treden als deskundige of coach).
- Participerende rollen: de interne auditor heeft een actieve rol in het project (bijvoorbeeld bij het documenteren van controls of het faciliteren van risk assessments).

Adviserende en participerende projectrollen zijn legitieme rollen die alleen door de auditor vervuld kunnen worden indien aan bepaalde randvoorwaarden wordt voldaan. De belangrijkste van deze randvoorwaarden is dat de auditor geen eindverantwoordelijkheid over het project mag hebben. Dit geldt voor alle fasen van het project: vanaf het bepalen van de risicobereidheid bij aanvang van het project tot het uiteindelijke implementeren van de resultaten in de organisatie. De rol van de auditor verschuift van de meer traditionele assurancerol naar een rol waarin de auditor meer als proactieve partner in projecten naar voren treedt. Terwijl het bieden van zekerheid door middel van projectevaluaties een basisrol van interne auditors blijft, blijkt uit het onderzoek dat veel interne auditors ook adviserende rollen vervullen (85%) en, in mindere mate, participeren in projecten (20%). Uit de enquête blijkt daarnaast dat de audits niet

alleen aan het eind van het project worden uitgevoerd, maar in alle fasen van de projectcyclus. De interne auditor kan op deze wijze wellicht meer waarde aan het project toevoegen.

**Thema 4. *Prestatie***

In het algemeen beoordelen interne auditors hun eigen prestaties op het gebied van projectauditing als goed. 81% van de respondenten beoordeelt de prestaties met betrekking tot de assurancerollen als goed of zelfs uitstekend, 72% beoordeelt de prestaties in het kader van adviserende rollen ook als zodanig (zie *figuur 4*). De score daalt naar 44% voor participerende rollen. De positieve zelfreflectie van interne auditors steekt schraal af tegen de magere slagingsfactoren van projecten: 30% van alle projecten faalt.

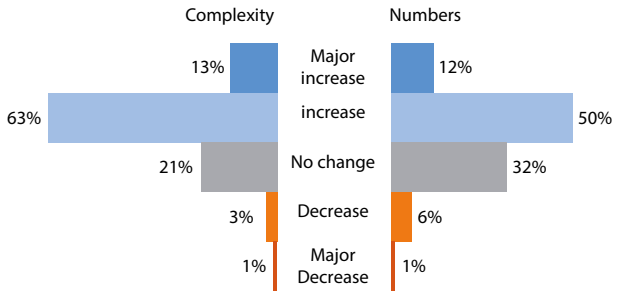
**Thema 5. *Methoden***

Uit het onderzoek blijkt dat auditwerkprogramma's die momenteel veelal gebruikt worden vaak niet voldoende geschikt zijn om complexe projecten te beoordelen. Dit is mede te verklaren doordat deze in hoge mate gebaseerd zijn op het toetsen van de naleving van het toepassen van een projectmethodologie (bijvoorbeeld Prince2). Met name de minder ervaren interne auditors baseren hun oordeel daarbij op de vaststelling of de betreffende projectbeheersmaatregelen al dan niet zijn geïmplementeerd. Deze benadering kan averechts werken, de auditor kan mogelijk blind worden voor de daadwerkelijke risico's. Te veel nadruk leggen op de naleving van de methodologie kan het projectrisico dus juist verhogen!

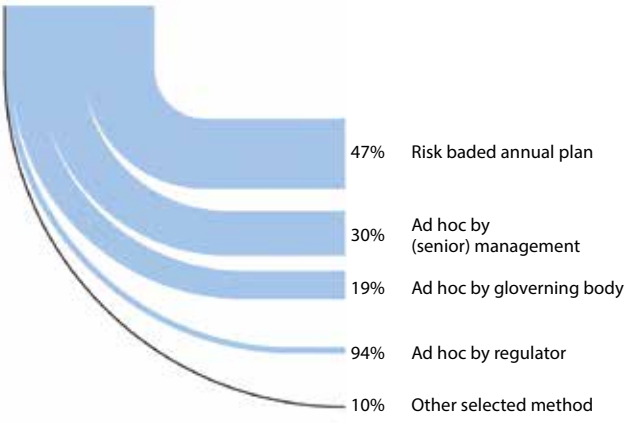
De minder tastbare elementen blijven vaak onderbelicht. Denk bijvoorbeeld aan het vaststellen of de projectmanager over de juiste competenties beschikt, of het managementteam een eenduidige visie op het project heeft en of iedereen er voldoende bij betrokken is. Met andere woorden, er zou een beter begrip moeten komen voor de sociale dynamiek en individuele gedragingen binnen projecten. In de praktijk lijken ervaren projectauditors de tekortkomingen van de raamwerken die ze gebruiken vaak te compenseren door te vertrouwen op hun professionele oordeel. Het gebrek aan geschikte raamwerken creëert op deze wijze een afhankelijkheid van individuen en beperkt de flexibiliteit en capaciteit van auditfuncties.

**Aanbevelingen voor de auditor**

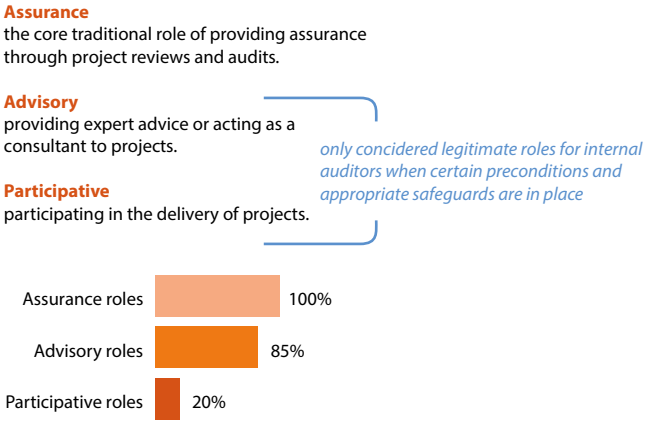
De slagingskans van projecten zal niet drastisch veranderen. Het onderzoek wijst namelijk uit dat zowel het aantal projecten als de moeilijkheidsgraad van projecten alleen maar gaat toenemen. Bovendien evalueren IAF's hun prestaties met betrekking tot project audits zelf als goed. De positieve zelfreflectie van interne auditors steekt schraal af tegen de magere slagingsfactoren van projecten. Wellicht is goed niet goed genoeg?



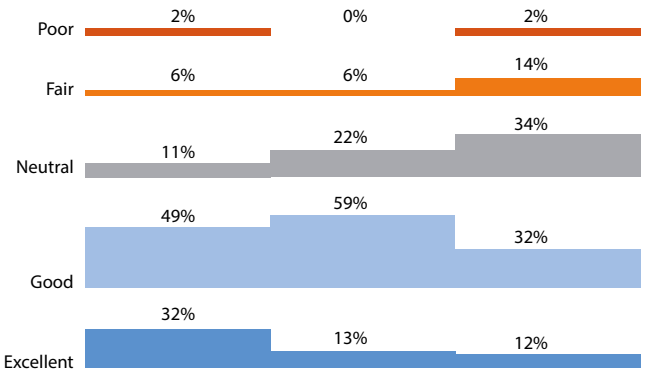

**Figuur 1.** De verwachte trend in het totale aantal projecten en complexiteit voor de komende een tot twee jaar
(Bron: Huibers, MIC, 2015)




**Figuur 2.** De wijze waarop audits worden geselecteerd voor projecten
(Bron: Huibers, MIC, 2015)




**Figuur 3.** De rollen van de auditor in projecten
(Bron: Huibers, 2010 en 2013)




**Figuur 4.** Huidige prestaties van de auditfunctie in elk type projectrol
(Bron: Huibers, MIC, 2015)

De afgelopen jaren hebben auditfuncties meer en meer projectaudits in hun auditplan opgenomen, mede als reactie op het toenemend aantal verzoeken vanuit het management. Ook zijn de auditfuncties naast het bieden van assurance steeds meer een proactieve rol in projecten gaan vervullen. Verder raakt de interne auditor steeds vaker in een vroegtijdig stadium bij projecten betrokken. Op basis van het onderzoek kunnen we interne auditors drie hoofdaanbevelingen doen:

1. Volg een systematische aanpak voor de identificatie van projecten die in aanmerking komen voor een audit. Wacht niet alleen op de ad-hocverzoeken van het senior management.
2. Richt je tijdens een project audit naast de harde aspecten van de projectmethodiek ook op de zachte aspecten, zoals tone at the top en effectief verandermanagement.
3. Probeer al in een vroegtijdig stadium betrokken te zijn bij een project. Als interne auditor kun je op deze wijze meer waarde aan het project toevoegen.

Uit de discussies binnen de klankbordgroep blijkt dat veel interne auditors niet over de juiste gereedschappen beschikken om de genoemde zachte factoren te evalueren. Ook is behoefte binnen het vakgebied aan handvatten voor een systematische selectie van projectaudits. <<

## Meer weten…

Het volledige rapport is verkrijgbaar via de website van IIA Nederland.

**Literatuur**


- Huibers, S.C.J., Bolluijt, J., Nan Tie, B. en N. Coleman, *The Evolution of Project Auditing*, 2015 Global Benchmark Study, Management Innovation Centre, 2015. Download on the IIA NL site.
- Huibers, S.C.J. en B. Walrave, *Trends in Project Auditing, voor wie wacht komt alles steeds te laat*, oktober 2013.
- Huibers, S.C.J., 'The Role(s) of the Auditor in Projects: Proactive Project Auditing', Taylor and Francis, *American Journal EDPACS,* 2013, (www.iia.nl).
- Huibers, S.C.J., Rol(len) van de (IT-)auditor in projecten, *Handboek EDP Auditing*, 5313 – Informatiesystemen, uitgave 43, juni 2012, Alphen aan den Rijn, Kluwer, 2012.
- Huibers, S.C.J., Hartog, P., Michel, P., Boogers, L., Van der Nat, G., Webbers, D. en N. Verburg, Het Instituut van Internal Auditors Nederland *(IIA), Project Auditing, Handvatten voor de Internal Auditor*, IIA Nederland, www.iia.nl/sitefiles/project-auditing.pdf, 2010.



Sam Huibers is lid van het Management Team Global Audit van Heineken International. Hiervoor werkte hij in diverse internationale functies in het bedrijfsleven als MT-lid van werkmaatschappijen, intern adviseur en projectmanager van grote internationale projecten. Hij is tevens vast lid van de Commissie Professional Practices van het IIA NL en verbonden aan de postmaster auditopleiding van de Universiteit van Amsterdam. Hij voert onafhankelijk onderzoek uit op het gebied van project auditing.

Jeroen Bolluijt is verbonden aan het Management Innovation Centre (MIC). Daarvoor werkte hij als projectmanager in diverse grote projecten.

Dit artikel is op persoonlijke titel geschreven.

Björn Walrave RO CIA

# Dedoose

De gefundeerde theoriebenadering ('grounded theory') is een onderzoeksstrategie die nog niet erg vaak door auditors wordt toegepast. Bij deze vorm van kwalitatief onderzoek stelt de auditor geen normenkader op aan de hand waarvan hij toetst en strikt genomen mag dus ook niet van een audit worden gesproken. Toch kan deze vorm van onderzoek erg waardevol zijn voor een organisatie. Zo kunnen met behulp van deze methode complexe situaties, zoals de oorzaken van het falen van een project, worden onderzocht.[1] Bij deze vorm van onderzoek is een zorgvuldige en navolgbare werkwijze van groot belang. Hierbij kan Dedoose goed van pas komen.

**Intuïtief**

Dedoose is een online softwareprogramma dat op dezelfde manier werkt als andere zogenaamde computer assisted qualitative data analysis software (CAQDAS). De gebruiker kan media, zoals spreadsheets, tekst, video en audio importeren en vervolgens coderen en analyseren, waardoor verborgen patronen kunnen worden gevonden.
Dedoose is gebruikersvriendelijk en intuïtief. Vooral auditors die ervaring hebben met kwalitatief onderzoek zullen geen moeite hebben snel vertrouwd te raken met de software. Via het menu kunnen eenvoudig codes en descriptoren worden beheerd, media worden geïmporteerd en gecodeerd en diverse analyses worden uitgevoerd. Indien gewenst kunnen zelfs de uitkomsten van een surveyonderzoek in zijn geheel worden geïmporteerd, waarbij codes en descriptoren automatisch worden aangemaakt. Het importeren van pdf-bestanden wordt vooralsnog niet ondersteund. Dergelijke bestanden dienen eerst handmatig te worden omgezet naar een ander formaat (zoals .txt of .docx). Dedoose kent naast voorgenoemde functies een handige memofunctie, waarbij memo's kunnen worden gekoppeld aan codes, descriptoren en media(fragmenten).

**Ondersteuning**

Gebruikers kunnen in Dedoose als een team aan een project werken. De projectmanager kan individuele gebruikersrechten toekennen en gebruikers kunnen met elkaar chatten en via de memofunctie met elkaar communiceren. Dedoose biedt ondersteuning primair via e-mail en daarnaast via telefoon en social media. Ondersteuning wordt daarnaast geboden in de vorm van vele instructiefilmpjes en er kan veel informatie worden teruggevonden in een uitgebreide online handleiding.
Data worden online (in de cloud) beveiligd opgeslagen en er wordt dagelijks een back-up van gemaakt. Supportmedewerkers van Dedoose hebben echter toegang tot de data, tenzij gekozen wordt voor de gratis optie projectspecifieke encryptie. Data kunnen bovendien worden geëxporteerd en lokaal worden opgeslagen.
Een licentie voor Dedoose kost, afhankelijk van het aantal gebruikers in een groep, tussen de $ 8,95 en $ 12,95 per maand en is daarmee zeer goedkoop in vergelijking met andere, wellicht meer bekende CAQDAS, zoals ATLAS.ti en MAXQDA. Indien gewenst kan één gebruiker de licentiekosten voor het hele team betalen.

Kortom, Dedoose is een volwaardige, gebruikersvriendelijke en prijstechnisch zeer interessante CAQDAS. Geschikt voor zowel de auditor die met onderzoek volgens de gefundeerde theoriebenadering wil gaan beginnen als voor de auditor die er al jarenlang ervaring mee heeft!

**JA**

- Online softwareprogramma (SAAS), dus wereldwijd te gebruiken
- Gebruikersvriendelijk en intuïtief
- Gebruikers kunnen als een team aan een project werken
- Prima ondersteuning via e-mail, telefoon en social media
- Instructiefilmpjes en een uitgebreide online handleiding
- Data-encryptie en back-up
- Zeer goedkoop in vergelijking met andere CAQDAS

**NEE**

- Het importeren van pdf-bestanden wordt vooralsnog niet ondersteund

**Noot**

1. Zie voor een uitgebreide behandeling van een vorm van gefundeerde theoriebenadering, te weten learning history-onderzoek: Meulen, I. van der en J. Otten, 'Behavioural auditing: Het onderzoeken van gedrag in organisaties 2', *Audit Magazine 2014* (2), p. 34-37.

Björn Walrave is eigenaar van Auditability. Daarnaast is hij senior auditor bij CZ en redactielid van *Audit Magazine*. Hij traint, doceert, spreekt en publiceert regelmatig over aan audit gerelateerde onderwerpen.
bjorn.walrave@auditability.nl

Naeem Arif RO EMIA

# Sander Weisz:

# "Internal auditor '**ont-dekt**' zaken voor het management"

In de rubriek Passie voor het vak spreekt *Audit Magazine* met mensen die een belangrijke bijdrage hebben geleverd aan de ontwikkeling van het vak internal auditing. Deze keer Sander Weisz, corporate director Internal Auditing bij USG People.

**Hoe kwam u in aanraking met het vak internal auditing?**
"Ik werkte bij het ministerie van Justitie (1996) en een collega, Frans Rijkschroeff, had zich opgegeven voor een post-hbo-opleiding operational auditing. Onbekend met dat vakgebied las ik de folder van de Haagse Hogeschool door en dacht: dat ga ik ook doen. Samen met Frans ben ik toen bij Arie Molenkamp in de schoolbanken gekomen. Ik was altijd al geïnteresseerd in de beheersing en besturing van organisaties, dit werd versterkt tijdens mijn studie Economie. De beschouwende en enthousiaste wijze waarop Arie lesgaf was voor mij een verademing: het gaf inzicht en overzicht. Inzicht in waar besturing en beheersing over gaat en in het auditen daarvan. Ik ben na de afronding van die opleiding voor Arie gaan werken bij KPMG en ben vervolgens de postmaster RO-opleiding gaan doen."

## Over...

Sander Weisz vervulde auditfuncties bij VluchtelingenWerk, het ministerie van Justitie, KPMG en KPN. Op dit moment werkt hij bij USG People waar hij zich richt op risicomanagement en auditing. Weisz vervulde verschillende bestuursfuncties bij de SVRO en het IIA, beginnend met de fusie tussen de VRO en het IIA en eindigend als voorzitter van het IIA. Daarnaast geeft hij sinds 1998 (parttime) trainingen en opleidingen op het gebied van auditing, risicomanagement, leidinggeven en control.

**U hebt een brede staat van dienst. Wat vindt of vond u het leukst om te doen?**
"Auditing heeft veel leuke facetten, en als ik terug kijk dan zie ik vele jaren van auditingplezier. Wat ik het leukst vind is om met een paar collega's te brainstormen over hoe we iets gaan onderzoeken: wat is nu de vraag en wat is de vraag achter de vraag, wat willen wij daarvan onderzoeken, hoe zetten wij dat onderzoek op? Et cetera. Ik vind het fijn om tijdens zo'n sessie vaktechnisch de degens te kruisen en gezamenlijk creatief naar oplossingen te zoeken. Samen iets creëren wat je vooraf nooit zelf had kunnen bedenken, dit natuurlijk naast de lol en het plezier van het brainstormen zelf."

**Wat maakt het vak zo mooi?**
"Je 'ont-dekt' zaken voor het management en brengt risicovolle kwesties over het voetlicht waardoor het management inzicht krijgt in datgene waar verbeterpotentieel zit. En je doet dat door te onderzoeken en te analyseren. Dit geheel maakt auditing voor mij mooi. De verscheidenheid aan onderzoeken die je uitvoert en de diversiteit aan omgevingen waarin je opereert maken auditing ook boeiend en afwisselend."

**Hoe ziet u het vak zich ontwikkelen de komende jaren?**
"Zoals velen kan ik hierop antwoorden met: alles wat te maken heeft met verdere toepassing van IT en de psychosociale vakgebieden, of het nu gaat om (IT-)beveiliging of de culturele en sociale context van een organisatie. Maar we mogen niet vergeten wat dit betekent voor de voor mij belangrijke basisvraag van internal auditing: doen wij als organisatie de goede dingen? Deze vraag vormt de continue en tijdloze toegevoegde waarde van internal auditing.



# Ontdek je vakgebied. Begrijp goed wat de kern van auditing is, waarvoor wij op aarde zijn, wat onze rol is

Sander Weisz

Ondanks de vaktechnische ontwikkelingen blijft onze taak om het topmanagement de spiegel voor te houden als het gaat om de sturing en beheersing van de organisatie zodat de juiste zaken op het juiste moment worden geadresseerd. De aard van de werkzaamheden van internal auditing kunnen drastisch veranderen, maar de basisfunctie blijft gelijk."

**Welke verandering zou u graag zien in het vak?**

"Er wordt al veel ontwikkeld voor ons vakgebied, meer en meer worden theorieën en methoden uit andere vakgebieden gebruikt voor het opzetten en uitvoeren van audits. Dit is iets waaraan elke auditor een bijdrage kan leveren. Daarnaast zou ik willen dat ons vakgebied nog effectiever wordt in het overbrengen van onze boodschap. Het beste onderzoek of het mooiste rapport heeft geen toegevoegde waarde als het management niet daadwerkelijk nadenkt over het door ons gerapporteerde. Alleen als wij op de juiste wijze communiceren wat wij willen overbrengen komt de boodschap aan. Tevens is het van belang om bewust om te gaan met ons gedrag binnen de organisatie en de effecten daarvan. Mijn inschatting is dat onze toegevoegde waarde verder verbetert als wij aan dergelijke punten nog meer aandacht besteden."

**Wat doet u het liefst wanneer u niet met het vak bezig bent?**

"Wat is er anders dan? Nee, flauwekul. Ik vind het fijn om in mijn vrije tijd te wandelen, te sporten (cardiofitness, Tai Chi) en soms vind ik het lekker om eens rustig een boek te lezen of een film te kijken. En dit samen doen met mijn vriendin en kinderen maakt het ideaal. En ik denk dat ik ga starten met gitaarles. Niet dat ik talent heb, maar het lijkt me leuk om te doen."

**Wat is uw advies aan de nieuwe generatie auditors?**

"Mijn advies is eigenlijk een open deur: ontdek je vakgebied. Begrijp goed wat de kern van auditing is, waarvoor wij op aarde zijn, wat onze rol is. Ga er dan vervolgens creatief en met een rechte rug mee aan de slag. Blijf bijleren en laat je coachen (zowel vaktechnisch als persoonlijk). Promoot ons vakgebied door het uitvoeren van relevante en goed uitgevoerde audits en verrijk het met nieuwe invalshoeken. Creëer die relatie met je stakeholders waardoor je gesprekspartner bent, zodat je de grootste kans hebt dat je boodschap wordt gehoord. En geniet bovenal van datgene wat je doet." <<

# VERENIGINGSNIEUWS

## Brochure financiële auditors

Aan ondernemingen in de financiële sector in Nederland worden veel eisen gesteld, gebaseerd op (inter)nationale wet- en regelgeving, toezichtwet- en regelgeving voor bepaalde bedrijfstakken en codes voor corporate governance. Met dit toegankelijke, breed toepasbare overzicht van de beginselen voor ondernemingsbesturing, organisatie-inrichting en risicobeheersing, kan de inzichtelijkheid in de eisen worden vergroot en de naleving ervan worden verbeterd.
http://bit.ly/iia-boor


## Kom ook naar de ALV

De laatste Algemene Ledenvergadering van IIA Nederland vond plaats in november 2015. Zie daarvoor http://bit.ly/ALV05112015. De eerstvolgende ALV vind plaats op 26 mei 2016. Voorafgaand aan de ALV is er een gastspreker met een inspirerend verhaal. Kijk voor meer informatie op http://bit.ly/ALV26052016.

## IIA feliciteert de geslaagden

**Nieuwe RO's:** Noushin Baghbani Arzanagh, Jantien te Bokkel, Ruud Bousché, Wilbert van den Brink, Erwin Cubuk, Gertjan Dekker, Kezban Gürpinar, Sjon van der Kleij, Annelies Reijne, Jac van de Schoor en Fong-Chi Wai.

**Nieuwe CIA's:** Rosabelle Anne Bandola, Chris Barbiers, Patrick Beekhuizen, Brechtje Brugman, Radmila Cosic-Pantelic, Jos Dijkhof en Tanya Maas.

**Nieuwe CCSA:** Nicole Huijbrechts.

**Nieuwe CRMA's:** Nicole Huijbrechts en Ronald Davidsz.

**Nieuwe IAP:** Mehul Chandra


## IIA Congres 2016: Explore, Discover, Experience

We verwelkomen u graag op het IIA Congres op 9 en 10 juni 2016 in Zeist. Met het thema Explore, Discover, Experience informeren en vermaken wij u twee dagen lang.

Wat biedt het IIA Congres 2016?
- Interessante keynote speakers als Larry Harrington, Bob Hirth en Margiet Sitskoorn.
- Een prikkelende paneldiscussie met Marcel Pheijffer, Margot Scheltema en Hans Wijers, geleid door Jort Kelder.
- Boeiende presentaties van de chief audit executives van onder andere Airbus, ING, Seadrill en Sanoma.

Schrijf u in vóór 1 april met vroegboekkorting en zorg dat u erbij bent!
http://bit.ly/congres2016

## Europees Academisch Congres

Het Europese Academische Congres voor Internal Audit en Corporate Governance vindt plaats van 6 tot 8 april 2016 in de Erasmus School of Accounting & Assurance in Rotterdam. Professor Mark Beasley presenteert de keynotepresentatie: Opportunities and Challenges for Internal Audit in Risk Oversight. Inschrijven is mogelijk tot 29 maart. Kijk voor meer informatie op http://bit.ly/IACG2016.

## Bestuurswisselingen

Tijdens de laatste ALV traden Carlo Bavius en Michel Vlak af. Het bestuur bedankt beide heren voor hun jarenlange inzet. Willem van Loon, CAE van Triodos Bank, trad toe tot het bestuur. Wij wensen hem veel succes in deze functie.

ESAA Erasmus School of Accounting & Assurance

## Diploma-uitreiking

Op 12 november jl. was er een gezamenlijke diploma-uitreiking van de postmasteropleidingen Internal Auditing & Advisory en IT-Auditing & Advisory. De studenten kregen hun diploma uit handen van Ron de Korte RA RE RO CIA en dr. Arno Nuijten RE CIA CISA. Namens de studenten bedankte Maikel de Maertelaere (alumnus ITAA) de opleidingen voor hun onderwijs en ondersteuning. Ter afsluiting sprak namens het curatorium drs. Fred Ruoff RO CIA de aanwezigen toe. In totaal hebben 17 IAA- en ITAA-studenten in oktober en november 2015 hun slotexamen afgelegd.

**IAA**

• Fleur Lamers | Uncovering psychological causes of escalating commitment: Integrating warning indicators in project auditing • Sammy-Jo Liefveld | Uncovering psychological causes of escalating commitment: Integrating warning indicators in project auditing

**ITAA**

• Ferry van der Ende | Van Wbp naar EPV. Kansen IT-auditor inzake hernieuwing privacy recht • Maikel de Maertelaere | Van Wbp naar EPV. Kansen IT-auditor inzake hernieuwing privacy recht • Jaco Struik | Van Wbp naar EPV. Kansen IT-auditor inzake hernieuwing privacy recht • Joan Tjin-A-Tsoi | Management control van human factor bij informatieveiligheid • Jaap van Bruchem | Van nuttig naar noodzaak. De adoptie van process mining • Ahmed Fadlaoui | Gevolgen van de Europese privacy verordening voor het gebruik van clouddiensten • Steven de Haard | XBRL. Casestudy naar FRIS-validaties van XBRL instances binnen XBRL-enabled softwaretoepassingen • Johan Kattestaart | Process Mining. Van toegevoegde waarde voor de jaarrekeningcontrole? • Edwin Valstar | Onderzoek de mogelijkheden om inzicht te krijgen in de kwaliteit van een IT productieomgeving • Caroline Joannes | Enterprise Mobility Security Standard • David van der Kleij | ITGCs en data-analyse in de jaarrekeningcontrole • Matthijs den Haan | ITGCs en data-analyse in de jaarrekeningcontrole • Delil Akdeniz | Beveiliging van Android devices • Shaief Abdoel Gafoer | Beveiliging van Android devices • Marieta Vermulm | What are the effects of using information technology controls to influence deviant behavior in an organization?

---

Universiteit van Amsterdam

**Amsterdam Business School**

## EIAP

Het Executive Internal Auditing Programme (EIAP), de opleiding tot Register Operational auditor (RO), is een parttime programma voor ambitieuze internal auditors aan de Universiteit van Amsterdam. Het verwerven van de internationaal erkende CIA-titel is geïntegreerd in het eerste jaar. Voor RA's, RE's en RC's is er een versneld programma dat de mogelijkheid biedt om in een tot anderhalf jaar RO te worden.

## Nieuwe modules: Risk management & compliance

Het is mogelijk de collegereeks Risk management & compliance als losse module te volgen. De module start op 5 februari en kent zeven bijeenkomsten van drie uur. De kosten voor de collegereeks bedragen € 1500. Met het volgen van deze collegereeks zijn 21 PE-punten te behalen. Zie voor meer informatie: eiap@uva.nl of 020-5255327.

## Nieuwe cyclus CIA-training

In het voorjaar van 2016 vinden de eerstvolgende trainingen plaats ter voorbereiding op het CIA-examen. De gehele training beslaat zeven avonden van 18.30 tot 21.00 uur. U kunt de gehele training volgen, maar u kunt zich desgewenst ook inschrijven voor individuele onderdelen (I, II of III). De training wordt verzorgd door drs. R.G.M. Bartelink RO CIA EMIA CCSA CGAP. Voor meer informatie, zie de website www.uva.nl/eiap.

## Nieuwe alumni

Op vrijdag 27 november 2015 vond de uitreiking plaats van de RO-diploma's. Wij feliciteren alle afstudeerders nogmaals van harte met het behaalde resultaat en wensen hen succes in hun verdere carrière!

• Erwin Cubuk | Een studie naar de persoonlijkheidskenmerken van auditors • Jeroen Lans | De afwezige IAD binnen de bouwnijverheid • Annelies Reijne | Een geslaagde verandering. Referentiemodel om de effectiviteit van veranderingsprocessen bij nieuwe taken van gemeenten te auditen • Thalia Weidema | Een studie naar persoonlijkheidskenmerken van internal auditors in relatie tot informatiezoekgedrag • Debby van der Meulen-De Jong | Fraude(bewustzijn) en internal auditing • Stijn Felius | De IIA standaarden en de toegevoegde waarde van de kleine auditfunctie; een perspectief op de IIA kwaliteitstoets • Jack Mills | The impact of big data on the organizational risk landscape • Fong-Chi Wai | Persoonlijkheidskenmerken van mannelijke en vrouwelijke internal auditors

## Interesse

Wilt u een boost geven aan uw carrière? Bezoek onze website www.abs.uva.nl en start de uitdagende opleiding op 1 september of 1 februari. U kunt ook contact opnemen per e-mail eiap@uva.nl of per telefoon 020-5254020.

Drs. Willem van Loon RA CIA

# Vertel eens een **verhaal**

Steeds meer mensen hebben het over databeveiliging en zijn vol van beschikbaarheid, integriteit en vertrouwelijkheid van data. Wereldwijd worden miljarden geïnvesteerd in beveiliging van databases, infrastructuren en dataverbindingen zoals WiFi en 3G/4G. Hele beroepsgroepen leven ervan. Data recovery, uitwijkfaciliteiten en cybersecurityoplossingen zijn big business. En ook wij als internal auditor besteden er, zakelijk gezien, veel tijd en energie aan.

Waar IT-oplossingen juist zouden moeten zorgen voor meer tijd en vrijheid lijkt het wel of de extra aandacht voor databeveiliging in die externe omgeving leidt tot minder aandacht voor de databeveiliging in onze eigen interne omgeving. Ja letterlijk, die in ons hoofd! Hoeveel tijd en aandacht besteden we aan het onderhouden, verrijken en analyseren van de gegevens in onze hersenen, toch ook een soort database? Hebben we er wel eens bij stilgestaan dat ook daar een datacrash kan plaatsvinden of een geheugenschijf corrupt raakt? Dat we maar 10% van onze hersencapaciteit gebruiken is een fabeltje; het is veel meer, dus als er iets misgaat kan dat grote gevolgen hebben. De opslag van data in onze hersenen is gevoelig. Een crash zit in een klein hoekje en toch besteden we daar verdraaid weinig tijd aan. Tegen een stroomstoring zijn de meeste IT-afdelingen wel opgewassen. Je moet er voor onze eigen dataopslag niet aan denken, maar toch gebruiken onze hersenen zo'n 20% van alle energie die het lichaam opwekt.

Eind vorig jaar kwam Walt Disney/Pixar met de animatiefilm *Inside out*. Een kinderfilm over een jong meisje dat met haar ouders verhuist naar een andere stad. Over hoe hersenen werken, emoties de overhand nemen en (kern)herinneringen worden gemaakt en verdwijnen. Zoals veel kinderfilms verplichte kost voor volwassenen. Er zitten zoveel diepere lagen in dat het bijna beter werkt dan welke cursus dan ook. Vooral: zorg voor herinneringen en het levend houden van je eigen belevingen. Misschien is dat wel de sleutel om te werken aan de beveiliging van onze eigen data, ons geheugen, onze ervaringen en belevenissen. Deze zullen we aandacht moeten geven. Keer op keer, om ervoor te zorgen dat ze niet onderin het bakje met herinneringen komen. Met het gevaar dat ze, na in onbruik geraakt te zijn, verdwijnen op de grote hoop van uitgedroogd en vergeten verleden. Met het devies 'alles wat je aandacht geeft, groeit', pleit ik er van harte voor om weer verhalen aan elkaar te gaan vertellen. Dat is voor sommigen misschien onwennig. Zeker in een op het individu georiënteerde maatschappij als de onze. Je zult elkaar ervoor moeten opzoeken, putten uit eigen herinneringen en er moeite voor moeten doen om de eigen ervaringen om te zetten in een aansprekend verhaal. Een met een pakkende boodschap waar mensen rijker van worden en dat vervolgens wordt doorverteld, waarna het weer anderen aan het denken zet.
Bijkomend voordeel is dat door elkaars verhaal te horen er nieuwe ideeën ontstaan, we elkaars capaciteiten kunnen gebruiken om creatieve oplossingen te verzinnen voor issues en problemen waar we mee zitten, privé, sociaal en zakelijk.

Zo zorg je dus niet alleen voor je eigen back-up; je hoort immers misschien je eigen verhaal na verloop van tijd van een ander weer terug. Je zorgt ook voor dataverrijking door te delen en maakt eigenlijk gebruik van data-analyse om inconsistenties in je eigen gedachtepatroon te identificeren – en corrigerende maatregelen te nemen. In de IT-gedreven wereld vinden we dataverrijking, analyse en databeveiliging heel normaal. Na jaren van individualisering van onze maatschappij wordt het weer tijd elkaar op te zoeken en te zorgen voor de eigen verrijking. Graag daag ik je uit. Zorg voor je eigen back-up en vertel een verhaal.

Willem van Loon is als docent en examinator verbonden aan het Executive Internal Audit Program van de Universiteit van Amsterdam. Daarnaast is hij hoofd Internal Audit van Triodos Bank nv en bestuurslid van IIA NL.

AUDIT PEOPLE

# INTERIM
# WERVING & SELECTIE
# TRAINEESHIP
# ADVIES EN BEGELEIDING

INFO@AUDITPEOPLE.NL • WWW.AUDITPEOPLE.NL • 085-2733025

# Turning data from insights into value

Data is voor de internal auditfunctie een onmisbare brandstof. En de hoeveelheid beschikbare data groeit exponentieel. Maar data is op zichzelf waardeloos. Pas als data wordt omgezet in relevante inzichten ontstaan er mogelijkheden om waarde voor de organisatie te creëren. Daarbij is het van belang dat risico's adequaat worden beheerst.

KPMG adviseert onafhankelijk en deskundig, maakt risico's beheersbaar en zorgt ervoor dat data waarde creëert voor uw business. Nu en in de toekomst.

**Contact**


Bart van Loon
KPMG Internal Audit,
Risk & Compliance Services
T: +31 (0)20 656 7796
E: vanloon.bart@kpmg.nl

Maurice op het Veld
KPMG Data & Analytics
T: +31 (0)10 453 4214
E: ophetveld.maurice@kpmg.nl


**kpmg.nl**

KPMG