# AUDIT MAGAZINE

VAKBLAD VOOR DE INTERNAL AUDITOR
NUMMER 4 2018 JAARGANG 17

THEMA
Complexe technologie

## Remaining relevant in a fast moving organisation

Blockchain:

## waar staan we na tien jaar?

## Wat vinden robots van COBIT?

# IIA Quality Assessment Review

## veel ervaring
## veel toegevoegde waarde

FSV
RISK ADVISORY

www.fsvriskadvisory.nl

**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 naar
auditmagazine@iia.nl

**Redactie**
Björn Walrave RO CIA (voorzitter)
Naeem Arif EMIA RO
Sander Diks CIA
Liane van Eerde MSc
Drs. Nicole Engel-de Groot RA
Petra Hamm-van Bodegraven MSc CPsA
Drs. Margot Hovestad RO
Drs. Huub van Hout RA CIA
Bas de Jong MSc RA
Drs. Laszlo Nagy EMIA RO
Jip Olieroock MSc RO CIA
Raymond Wondergem MSc RO
Drs. Paul van der Zwan EMIA RO

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 Register 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**
De Nederlandse Associatie (DNA)
Miranda de Haan
info@denederlandseassociatie.nl
tel.: 030-2271677

**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. Andere geïnteresseerden kunnen losse nummers en/of een abonnement aanvragen bij het IIA.

Audit Magazine verschijnt vier maal per jaar.


ISSN: 1570-856X



# Complexe technologie

Internet of things. Of je het nu wilt of niet, iedereen krijgt ermee te maken. Dit geldt voor jezelf, maar ook in je rol als internal auditor. Het is koffiedik kijken met welke snelheid de technologie zich ontwikkelt. De wet van Moore gaat uit van een exponentiële groei. Dat houdt in dat de technologische vooruitgang elke twee jaar verdubbelt. En dus zal nieuwe technologie met een duizelingwekkende vaart het leven van mensen, organisaties en daarmee ook de internal auditor, beïnvloeden.

Maar hoe kun je je als internal auditor voorbereiden op de impact van technologie? Hoe kun je zorgen dat je organisatie niet belandt in het rijtje Kodak en Nokia, organisaties die niet aanhaakten bij de nieuwe technologie? Een belangrijke vraag die de internal auditor de organisatie moet stellen is in welke mate de organisatie in staat is om mee te bewegen met de technologische ontwikkelingen en de veranderende vraag van de klant. Daarnaast zal de internal auditor enige kennis moeten hebben van de technologische ontwikkelingen. De auditor hoeft geen early adopter te zijn, maar moet wel mee kunnen praten over onderwerpen als robotica en blockchain en weten welke nieuwe audit tools bruikbaar zijn. En durft de auditor het aan om procesbeschrijvingen en projectplannen los te laten omdat de organisatie agile werkt en zich verlaat op stand ups en meet ups?

Internet of things biedt oneindig veel mogelijkheden. Het zorgt voor gemak, zoals het wijzen van de snelste route in een zelfrijdende auto. Maar het heeft ook een keerzijde. Identiteitsfraude, hacken en ransomware zijn vervelende bijeffecten waar je als persoon en organisatie mee te maken krijgt. Het is noodzakelijk om weerbaar te zijn en te kunnen anticiperen. Privacy is belangrijk. Google en Facebook verzamelen, gevraagd en ongevraagd, data om deze vervolgens commercieel in te zetten. Zijn wij hier voldoende op voorbereid? Daarnaast krijgen organisaties te maken met de nieuwe privacywetgeving.

Kost dit de internal auditor hoofdbrekens? Natuurlijk niet, deze uitdagingen maken het vak alleen maar leuker. Het vergt wel flexibiliteit en de wil om zichzelf te ontwikkelen. Internal auditor innoveer ook zelf, hoe leuk is dat! Ook leuk is dat *Audit Magazine* drie nieuwe redactieleden welkom heet: Petra Hamm-van Bodegraven, Liane van Eerde en Bas de Jong.

Wij wensen u veel leesplezier!

De redactie van *Audit Magazine*

# THEMA: Complexe technologie


NFP Photography

## Remaining relevant in a fast moving organisation

Relevant zijn en blijven als internal auditafdeling in een beursgenoteerde onderneming als Adyen, is een uitdaging. Anthony Latelle, hoofd van de IAF van de payment service provider, vertelt over zijn ervaringen. **Pag. 6**

## Blockchain: waar staan we na tien jaar?

Welke 'reis' hebben we de afgelopen tien jaar op de technologieladder gemaakt? Over tokens, distributed ledgers, DLT en audit-by-design. **Pag. 12**

## Stairway to digital heaven

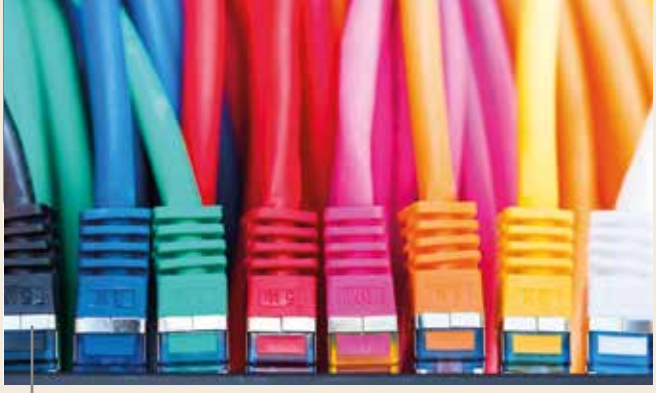
De cyberrevolutie is onverbiddelijk en voltrekt zich in hoog tempo. Dat brengt ook cyberrisico's met zich mee. In dit artikel een handzame aanpak voor de beheersing hiervan. **Pag. 46**

## "Ik zie de auditor in de toekomst meer in netwerken functioneren"

Peter Hartog is sinds afgelopen juni manager Vaktechniek binnen IIA Nederland. Een nieuwe functie, een nieuw geluid? **Pag. 42**

## "Mijn missie is om van elk event een succes te maken"

Die opdracht geeft Annemiek van Raalten, eventmanager bij IIA Nederland, zichzelf bij ieder event. **Pag. 52**



## “Het is nog niet te laat”

Marc van Heese, partner bij ARC People, vertelt over de innovatie van de auditfunctie en hoe we deze toekomstbestendig kunnen houden. **Pag. 16**

## Het belang van risicomanagement voor de Nederlandse FinTech

Risicomanagement is een belangrijke factor als het gaat om het slagen – denk aan Tikkie van ABN AMRO – of falen van een FinTech. **Pag. 20**

## Staat blockchain al in het auditplan 2019?

Het lijkt erop dat blockchain bedrijfsprocessen en businessmodellen gaat veranderen. Kan de auditor deze technologische ontwikkeling negeren? **Pag. 24**

## “Er is een groot verschil tussen uitvinden en innoveren”

Innovatie is als een doolhof, maar er zijn routes om hier succesvol uit te komen. Dat zegt Gijs van Wulfen, schrijver, innovatie-autoriteit en keynote speaker. **Pag. 54**


## Wat vinden robots van COBIT

Robotics process automation (RPA) doet in steeds meer organisaties haar intrede. Over de nieuwe uitdagingen en RPA-specifieke risico’s. **Pag. 28**


## Beheersing van de technologie voor een rondje om de aarde

Franco Ongaro is directeur Technology, Engineering and Quality en hoofd van ESTEC, waar complexe technologische ruimtevaartprojecten worden gerealiseerd. *Audit Magazine* in gesprek met hem over hoe een complex project te beheersen. **Pag. 32**

## Internal audit en robotic process automation

Vroeger vond robotisering grotendeels plaats bij logistieke en productiebedrijven, maar inmiddels is dat bij alle typen organisaties en afdelingen. Wat betekent dit voor internal audit? **Pag. 36**

## De ‘why’ van internal audit

Hoe vanzelfsprekend is het bestaan van internal audit? En wat is ook alweer de toegevoegde waarde? Terug naar de essentie van het vakgebied. **Pag. 60**

# Rubrieken

Thema Complexe technologie
Tekst Drs. N.E. Engel-de Groot RA
Drs. Huub van Hout RA CIA
Beeld NFP Photography
Adobe Stock

# *Remaining* relevant in a fast moving *organisation*

Remaining relevant as an audit function in a fast moving technology organisation is a challenge. Anthony Latella, head of Internal Audit Function (IAF) at Adyen, tells *Audit Magazine* about his experiences at Adyen.

## Adyen at a glance

Adyen was founded in 2006 by a group of entrepreneurs. The payments technology at that time consisted of a patchwork of systems built on an outdated infrastructure. With the aim of helping businesses to grow, the founders set out to build a platform capable of meeting the rapidly evolving payment needs of today's fast-growing global businesses. Adyen's founding team called the business Adyen - Surinamese for 'start over again' - and focused on building a modern infrastructure directly connected to card networks and local payment methods across the world, allowing for unified commerce and providing data insights to merchants. The Adyen platform enables merchants to accept payments in a single system, enabling revenue growth online, on mobile devices and at the point of sale.
Adyen today is a company with over 650 employees working out of 15 offices across the world and over 100 billion euro in payment volume processed in 2017.

**What does Adyen do?**
"Adyen is a technology company with a banking license who is redefining payments for merchants globally. It has built an efficient single platform that enables the acceptance and processing of cards and local payments globally across its merchants' online, mobile and point of sale ('POS') channels. Adyen aims to change the payments industry, which traditionally comprised a patchwork of providers and legacy systems resulting in fragmented merchant services. Adyen has in response built a bottom-up, single, global platform capable of meeting the rapidly evolving needs of fast-growing global merchants. This single platform enables Adyen's data capabilities, which includes services that utilize sophisticated algorithms across machine learning, data mining and artificial intelligence. These capabilities allow us to increase authorization rates for merchants while reducing the risk of fraudulent transactions.
Adyen targets large, global companies but increasingly also domestic/mid-market merchants. In 2017, Adyen processed transactions for several thousand merchants across the globe and across a wide number of industries, including retail, travel, digital services, hospitality and marketplaces. Adyen's merchant portfolio includes merchants like Uber, Facebook, Spotify and booking.com. Payments is a fee business and the businessmodel is based on fees on payments processed."

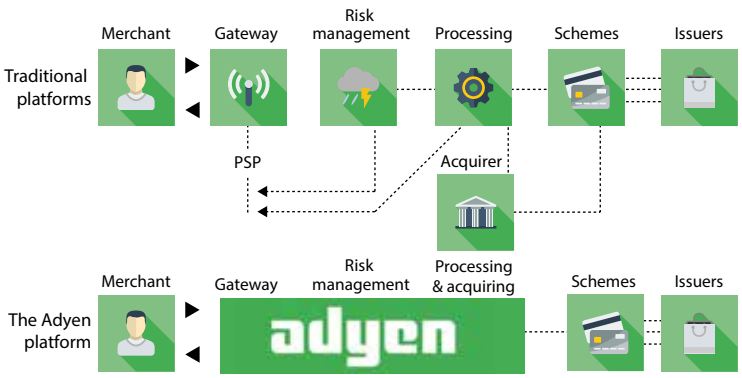
**How has complex technology changed the payment industry?**
"Adyen believes that simplicity, transparency, and innovation are the key to future success. Adyen's global platform has simplified and integrated the payments value chain, enabling it to partner with large merchants to rapidly scale their businesses both locally and globally, overcoming inherent inefficiencies in traditional payment platforms.
Since its founding in 2006, Adyen has built a completely new infrastructure that encompasses the entire payment value chain, from (online) checkout by the customer to settlement of funds to the merchant.
Adyen's technology removes friction for both shoppers and merchants and allows for an improved shopper experience while simplifying the global management of payments across sales channels and geographies for merchants."

**What are Adyen's major risks?**
"The main risks Adyen is facing are definitively in the technology domain and relate to downtime and availability of its website and systems, system failure, and any real or perceived data breaches. Aside from IT and cyber risks, Adyen faces risks in the areas of competition and innovation, and also compliance and the changing regulatory framework are significant risks for Adyen. Finally maintaining key staff and safeguarding our corporate culture and values are also important factors to consider."

**How does Adyen manage these risks?**
"The most effective risk mitigating approach for Adyen is to maintain a strong risk culture across the organization and to ensure the company culture and corporate values are embraced by everyone and retained globally, despite the very high pace at which the organization is changing and growing. We have defined the Adyen Formula, which summarizes the values the organization has embraced. The formula is not only used to attract talents that share our same values, but it is also used as a framework for risk management and decision making.
By living the values of the formula and acting accordingly, we have developed a strong risk awareness and risk culture. The Adyen Formula and the company culture allows us to do things differently. Adyen empowers its people to try and to make errors as long as you learn. Furthermore we developed our platform in-house. This means that we have complete ownership and control over our platform. We consider this to be a great advantage as we can minimize supply chain risks."

**How many people work at the IAF and what is their background?**
"The IAF at Adyen is currently a team of two employees. A third auditor has already been recruited and will join the team in the coming weeks. I started at Adyen with the task to set up an IAF as Adyen applied for a banking license."

**What are the main tasks and challenges of the IAF?**
"The aim of the IAF at Adyen is to become a trusted advisor, a true business partner, and to support the organization in building an ethical and sustain exible enough and is slowing us down and hinders us to be on top of new developments and add value when needed. The main challenge we face is to align ourselves to a fast-moving organisation while at the same time comply with ECB and IIA standards. Our Audit Committee expects us to work and report in line with methodologies and procedures which are fully in line with ECB/IIA standards. On the other hand, there is a business which requires us to be agile and fast. Moreover, the ever-changing regulatory landscape and increased scrutiny also poses




**Figuur 1.** The power of one platform

1. We build to **benefit all merchants** (not just one)
2. We make **good choices** to build an ethical business and drive sustainable growth for our merchants
3. We **launch fast** and iterate
4. **Winning is more important than ego**; we work as a team - across cultures and time zones
5. **We don't hide behind email**, instead we pick up the phone
6. We **talk straight** without being rude
7. We include **different people** to sharpen our ideas
8. We **create our own path** and won't be slowed down by 'stewards'

**Figuur 2.** The Adyen formula

a continued challenge for both Compliance and the IAF. Simply think about the impact and reach of new regulations such as General Data Protection Regulation (GDPR) and the second Payment Services Directive (PSD2)."

### What is ahead of us in terms of complex technology in the field of payments?

"The global payments and commerce landscape is changing fast: the globalization of commerce, the changing shopper behaviour and the rise of mobile are driving innovation and the adoption of new technologies. Mobile wallets, crypto-currencies, voice-based payments and internet of things payments in general are examples of complex technologies entering the payments landscape. The philosophy of Adyen is to support merchants in growing their business while reducing payment complexity. If merchants want to embrace a new payment technology Adyen will support these while aiming to keep it simple for the merchants."

### What is the effect of complex technology for Internal Audit (in terms of competences, scope, tools)?

"Complex technologies will inevitably affect IAF's. The main challenge I see would be to timely identify and comprehensively assess risks introduced by complex technologies. I doubt every Internal Auditor understands what an algorithmic bias is – for instance – and what its impact would be. In addition, the approach and tools required to provide assurance around these new technologies and related risks will also have to change. As an example, auditing machine learning, artificial intelligence or robotic process automation will require a completely different approach and a different set of competencies compared to traditional operational audits. Adyen is expected to grow fast and therefore the IAF has to embrace more technology in their audit approach

and processes to remain relevant. This is not only the case for the IAF but also for other support functions. There is no need to significantly increase the size of the team in case better use is made of automation. In this way staff can focus on relevant and important things."

**Should Audit in general, in your view, prepare better for complex technology?**

"In my view, the future of IAF will largely depend on their ability to prepare for upcoming complex technologies - such as AI, bots, wallets, blockchain, quantum computing - and all of its associated risks.IAF's need to develop continuous learning to make sure it understands the risks and the impacts of the new complex technologies and also to determine what would be the best approach to mitigate these risks and provide assurance around these technologies.
I truly believe that for IAF's to survive they need to stay relevant. And to stay relevant, IAF's have to evolve and become capable of fully understanding complex upcoming technologies and its associated risks. But not only does it require that auditors understand new technologies but also it requires them to make a mind shift.
As an example, if an IAF says that they have a risk-based approach in a fast-moving environment then it is impossible to continue with a multi-year planning horizon. Working with a risk-based audit backlog seems a more logical way forward.
In my view the auditor of the future needs to be a lifelong learner, technology savvy, work agile, think risk-based and have convincing presentation skills as less focus will be put on written reports." <<

*"To stay relevant, IAF's have to evolve and become capable of fully understanding complex upcoming technologies and its associated risks"*

# Van het bestuur

IIA NL streeft ernaar de dienstverlening aan de decentrale overheid en zelfstandige bestuursorganen (zbo's) uit te breiden en te verbeteren, zo was te lezen in de vacature voor een nieuw bestuurslid. Veel enthousiaste kandidaten meldden zich. Tijdens de daaropvolgende gesprekken werd het mij duidelijk dat niet iedereen zich herkent in de begrippen die we als IIA meestal gebruiken in onze uitingen. Niet elke organisatie kent immers een CEO en onder een 'auditcommissie' wordt niet overal hetzelfde verstaan. Wel is het zo dat ook 'het bevoegd gezag' in overheidsland zeker behoefte kan hebben aan een goede auditfunctie.
Uit de potentiële bestuurskandidaten hebben we als bestuur een voorkeurskandidaat gekozen die we onlangs tijdens de ALV in december aan jullie hebben voorgesteld. De nieuwe bestuurder gaat vol enthousiasme aan de slag met een team om onze huidige producten meer herkenbaar te maken en via bijvoorbeeld een kennisgroep het IIA nog aantrekkelijker te maken voor potentiële leden vanuit decentrale overheden en zbo's.

Wat betreft innovatie staan we als bestuur ook niet stil. Tijdens onze laatste heidag spraken we met name over innovaties en de wijze waarop ons vak gaat wijzigen. Natuurlijk ook wat we daar als auditfunctie en beroepsvereniging mee kunnen en vooral moeten. Een taskforce Innovatie, onder leiding van onze nieuwe manager Vaktechniek, spreekt de komende tijd met zowel leden als niet-leden (outside-inperspectief) over verschillende toekomstscenario's voor het auditvak.

Als vereniging zijn we behoorlijk actief, het najaar barst traditioneel van de evenementen. Zo vond afgelopen september het jaarlijkse Presidentsdinner plaats waar we John Bendermacher verrasten met de mededeling dat het bestuur en vele anderen hem graag als erelid van onze vereniging zien. Verder bezocht ik het Comissarissensymposium met als thema 'Morele moed bij auditors en commissarissen' en werd ik een dag geinspireerd bij de summer course over digitalisering.

Begin oktober van dit jaar presenteerde de taskforce IAAM namens IIA Nederland en NBA-LIO de nieuwe versie van het internal audit ambition model (IAAM) op de European conference for super internal auditors in Madrid. De taskforceleden boden tijdens de European association of institutes of internal auditing (ECIIA) conferentie het nieuwe model aan Naohiro Mouri, chairman of the board of IIA Global, aan. Tijdens het overleg dat ik met hem had in Madrid, zegde hij mij toe het model in te vullen bij AIG waar hij chief audit executive is en toonde hij zich net zo enthousiast over het vak als tijdens zijn 2018-19 Chairman's video: 'Emphasize the basics. Elevate the standards' (zie https://www.youtube.com/watch?v=-H1gvNRANrM). Zijn enthousiasme hield de Europese IIA-voorzitters uit 33 landen, inclusief mijzelf, een lange warme zaterdag in Madrid geboeid in een ondergronds zaaltje. Tijdens het European leadership forum bespraken we het global strategic plan voor 2019-2023, inclusief de nieuwe doelstelling, visie en doelen voor het IIA als organisatie en het vakgebied internal auditing.

Net terug uit Madrid, mocht ik aanwezig zijn bij het 'digitalisation event'; vanuit Heineken Internal Audit werd bevlogen verteld over de robots die internal audit gebruikt en de inzet van data mining in veel van hun audits. Als een auditor daar geen gebruik van maakt bij de voorbereiding van het werkprogramma, daagt de manager hem uit dat wel te doen. We zagen een robot die e-mails en een administratie doorploegde en een auditdossier vulde, zodanig dat de auditor slechts de werkzaamheden hoefde te reviewen. De aanwezigen werden vervolgens uitgedaagd hun auditfuncties te plotten op een 'digitalisation maturityschaal'. Toen Heineken Internal Audit zichzelf plotte op de schaal ergens tussen 'digital beginner' en 'digital follower', realiseerde ik mij dat onze auditfunctie wellicht dan uitkomt bij de enige minder 'mature' stap op de schaal: 'digital sceptic'.

Werk aan de winkel dus!

IIA Nederland
Jantien Heimel is voorzitter van het IIA.

Thema Complexe technologie
Tekst Ir. Simon Lelieveldt
Beeld 123RF®

# Blockchain: **waar staan we na tien jaar?**

Dit artikel schetst in hoofdlijnen welke ‘reis’ we de afgelopen tien jaar op de technologieladder hebben gemaakt en hoe een libertair experiment op een hoekje van internet uiteindelijk toch de grondvesten doet schudden van klassieke kantoorautomatisering.

*Er ontstond een oerwoud aan bitcoinklonen, met als doel mee te liften op de hype en om als uitgever van zo'n coin eigen voordeel te behalen*

Dit jaar is het tien jaar geleden dat het bitcoin whitepaper werd gepubliceerd waarin een vorm van elektronisch geld werd geschetst.[1] Rondom de achterliggende technologie: de blockchain, ontstond een hausse aan initiatieven. Wie al die nieuwe ideeën probeert te doorgronden ontdekt dat er in feite drie industrieën te herkennen zijn:

- de bitcoinindustrie,
- de blockchainindustrie,
- de 'distributed-ledger'-industrie.

**De bitcoin: de munt die geen munt is**

Wie het whitepaper over de bitcoin leest, doet er goed aan stil te staan bij de volgende kerndefinitie: 'We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.'
Het is een definitie die onvolledig is. In feite wordt vooral een digitaal handtekeningensysteem geschetst waarmee een zekere waarde kan worden overgedragen. Die waarde wordt bitcoin genoemd en wordt gepositioneerd als 'electronic cash', te gebruiken voor veiliger e-commercebetalingen op het web. Er is echter geen interne technische voorziening die reflecteert wat de waarde inhoudt. De waarde wordt niet in de techniek maar door de gebruikers bepaald.

***Externe marktwaarde***

De praktijk leert dat de 'munt' van zo'n systeem per definitie een externe marktwaarde zal krijgen. Dat gebeurde immers ook met de door David Chaim ontwikkelde voorloper: e-cash. Toen die digitale munt gratis in de markt werd neergezet ontstond een secundaire markt die er waarde aan toekende. Hetzelfde gebeurde met de bitcoin, waarbij tegelijkertijd libertaire idealisten en venture capitalisten de bitcoin omarmden. Het perspectief op een staatsonafhankelijk betaalmiddel stond en staat daarbij centraal.
Er ontstond al snel een oerwoud aan klonen, alt-coins, vaak met als doel om mee te liften op de hype van bitcoin en vooral ook om als uitgever van zo'n coin je eigen voordeel te behalen. Tegelijk concentreerde de rekenkracht die benodigd was om bitcoins te maken zich bij een aantal grote spelers in plaats van bij het grote publiek, zoals aanvankelijk de bedoeling was. Zo ontwikkelde zich een heel ecosysteem rond de bitcoin met bitcoinwisselaars, bitcoin miners, bitcoin-walletaanbieders, developers en nieuwssites.
Als breed betaalmiddel voor het publiek is de bitcoin sindsdien nog steeds niet omarmd en ook als generiek betaalmiddel op internet heeft het niet gebracht wat aanvankelijk werd verwacht. Wel is evident dat het een prima redmiddel is voor al degenen die in een 'failed-state' leven. Voor hen vormt de bitcoin nog steeds de ideale methode om, buiten hun overheid om, waarde over te dragen en veilig te stellen naar familie of vrienden in andere landen. Evenzo kwam het gebruik voor illegale doeleinden ruimschoots in de publiciteit. Daarnaast werd de bitcoin geleidelijk de 'instapvaluta', een rekeneenheid en ruilmiddel voor iedereen die een stap in de wereld van crypto-valuta ging nemen.

***Stammenstrijd***

Het is goed om vast te stellen dat in technische zin de bitcoin al tien jaar zijn kracht bewijst. Hoewel er zeker compromitterende inbreuken op techniek en protocol denkbaar zijn, toont het hart van de techniek zich robuust. Tegelijk is er een stammenstrijd gaande binnen deze industrie, waardoor inmiddels ook een variant van de bitcoin in de markt staat: bitcoin cash.[2] Er wordt doorontwikkeld richting verbeteringen van het protocol en er wordt actief gewerkt aan een aantal alternatieve coins met verhoogde privacy of veiligheidskenmerken. Er is dus nog steeds een levendige bitcoinindustrie die het netwerk en de basistechnologie verder verfijnt en aanpast, zodat het wereldwijd voor transacties gebruikt kan worden.

***Beleidsreacties***

Naarmate de bitcoin meer bekendheid kreeg en zich als aparte asset class een plaats veroverde in de samenleving, formuleerden overheden hun beleidsreacties op de munt. Failed states herkenden het gevaar en verboden de bitcoin. In de overige naties werd hetzij gekozen voor behandeling als ware het een regulier betaalsysteem (zoals in de VS) of behandeling als een virtuele munt die geen echt geld is (zoals in Europa). De meest recente ontwikkeling op dit vlak bestaat eruit dat wereldwijd een beweging in gang wordt gezet om spelers in het ecosysteem rond de bitcoin of andere cryptovaluta te onderwerpen aan standaard bancaire regelgeving rond 'anti-money laundering' en anti-terrorismemaatregelen.

**Blockchain als crowd-based transactietechniek**

Na de eerste vijf jaar verschoof de aandacht van de munttoepassing bitcoin naar de techniek erachter: blockchain. De term blockchain verwijst naar de keten van blokken met transacties die aan elkaar worden geknoopt tot een grote gemeenschappelijke, niet wijzigbare basisregistratie. Er verschenen variaties op de bitcoin-blokchain met allerlei andere kenmerken. Te denken valt aan systemen als Ripple, Bitshares, Steemit en EOS.

***Ethereum***

Het meest in het oog springend was het alternatieve blockchainsysteem Ethereum dat in 2015 ontstond. Dit gebruikt

niet slechts één adres voor waardeoverdracht (in dit geval ethers in plaats van bitcoins), maar maakte het ook mogelijk programma's toegankelijk te maken op een blockchainadres. Die programma's zijn openbaar toegankelijk en iedereen kan ze aanroepen en laten uitvoeren. De applicaties werken als 'smart contracts' waarbij de enige spelregels die van toepassing zijn, de spelregels zijn zoals in het programma opgenomen. De slogan die daarbij hoorde was: 'Code is law'.
Nog geen jaar later bleek een cryptobeleggingsfonds op Ethereum zo slecht geprogrammeerd te zijn dat een van de gebruikers er met alle ethers vandoor kon gaan. De eigenaren besloten om niet hun eigen dispuutresolutiemechanisme in te zetten, maar het recht in eigen hand te nemen door zelf de blockchain terug te zetten naar het moment van voor de 'diefstal'. Het voorval toont duidelijk hoe deze nieuwe wereld nog aan het begin van de leercurve staat, zowel in termen van governance als in termen van ontwikkeling van valide smart contracts.
Wat Ethereum ook onderscheidde van de bitcoin-blockchain is dat de valuta die bij blockchain hoort, in één keer werd gemined en daarna gedistribueerd en verkocht aan toekomstige gebruikers c.q. investeerders. De term hiervoor was: initial coin offering (ICO). Er kwam een protocol beschikbaar dat het mogelijk en makkelijk maakt om zélf je eigen ecosysteem te maken met specifieke coins voor gedecentraliseerde applicaties (DAPPS, decentralized apps). Zo ontwikkelde zich een volledige industrie rond het opzetten van nieuwe blockchainsystemen, businessapplicaties in een open blockchainwereld. Het wemelde van de snelgeschreven whitepapers en ICO's waar het merendeel na verloop van tijd een stille dood stierf.

***Open architecturen***
Kenmerkend voor deze blockchainwereld is het gebruik van open architecturen, de zogeheten 'permissionless' omgevingen. Iedereen kan deelnemen aan blockchain en te zien is dat er met veel energie en enthousiasme met name ook door start-ups wordt onderzocht welke maatschappelijke vraagstukken met behulp van deze open blockchains kunnen worden geoptimaliseerd. Denk aan het gebruiken/verbruiken van pgb-budgetten, het stimuleren van eigen stroomopwekking, het traceren van herkomst in voedselketens, het distribueren van muziek door de originele artiesten zelf, het samen delen en investeren in onroerend goed en dergelijke.[3]

***'Tokens'***
De aandacht van de regelgever gaat bij deze industrie met name uit naar de vraagstukken rond 'tokenisation'. Als iemand een token maakt dat een deel van het eigenaarschap van een huis of een bedrijf vertegenwoordigt: hoe kwalificeer je dan dat token? Wordt het token een financieel instrument

onder de regelgeving? Of moeten tokens gezien worden als een alternatieve vorm van crowdfunding?
Een eerste antwoord van de Zwitserse regelgever maakte onderscheid tussen payment tokens, utility tokens, asset tokens en hybride tokens, maar ook alternatieve indelingen zijn denkbaar. In de kern van de zaak komt het erop neer dat hetzij het investeringskarakter of de beoogde verhandelbaarheid van een blockchain-token tot gevolg heeft dat sprake is van een financieel instrument of security. Marktpartijen zetten inmiddels steeds vaker in op uitgifte van security tokens (security token offering) onder een bepaald raamwerk. Aan overheidszijde is te zien dat Zwitserland, Malta en Gibraltar erg hun best doen om met transparante richtlijnen deze industrie naar zich toe te halen.

**Distributed ledgers: automatisering over ondernemingsgrenzen heen**

Voor bestaande ondernemingen ontstond rond 2015 het moment om met variaties op blockchain te gaan experimenteren. Geleidelijk aan werd duidelijk dat in vertrouwde waardeketens, niet per se een energieslurpende blockchain nodig was: de crux van de techniek was vooral om te ontdekken hoe een gedistribueerde, gezamenlijke administratie de bedrijfsprocessen over ondernemingsgrenzen heen kon optimaliseren. Denk bijvoorbeeld aan de documentenstromen en overdrachtsmomenten rond handelsfinanciering en letters of credit.[4]
Tegelijk met de meer publiek georiënteerde blockchainindustrie, ontwikkelde zich de toepassing van blockchains in beperkte omgeving; de permissioned blockchains. Deze evolueerden tot variaties van distributed ledger technologie (DLT), die je ook wel 'blockchain-zonder-blockchain' zou kunnen noemen. Aangezien de crux hierbij is om over bedrijfsgrenzen heen te ontwikkelen, zien we hier op bedrijfstakniveau allerlei consortia ontstaan.
Een vroeg privaat initiatief was het Amerikaanse R3i, dat het Corda-framework neerzette voor gebruik door financiële instellingen. In het verzekeringswezen werd vanuit de sector zelf het initiatief B3i neergezet. Op vergelijkbare wijze ontstonden zo in allerlei maatschappelijke sectoren samenwerkingsverbanden op sectoraal niveau. Het doel hiervan is om vroegtijdig de toepassing van distributed ledgers te begrijpen en zo mogelijk ook de standaarden te zetten (om tot een early-mover voordeel te halen).

***Platformen en de rol van de regelgever***

Op technisch niveau zien we een vergelijkbare ontwikkeling waarbij technische platformen als Corda, Ethereum, Quorum en Hyperledger de mogelijkheid bieden om blockchain of DLT te implementeren. Evenzo is een rijke adviesindustrie ontstaan waarbij alle grote accountantskantoren hun eigen blockchainteams en expertise neerzetten en uitventen. Want hoewel op tal van vlakken nog te ontdekken is welke toepassingsmogelijkheden het best uitpakken, is het onvermijdelijk dat blockchain en DLT aan de achterkant de basis zullen vormen van toekomstige applicaties.
De rol van de regelgever springt bij deze laatste ontwikkeling het minst in het oog. In feite is sprake van een volgende fase bedrijfsautomatisering en er doen zich niet per se nieuwe juridische vraagstukken voor. Wel is er een serie meer fundamentele vraagstukken aan de orde die gerelateerd zijn aan de brede overgang naar een peer-to-peersamenleving met nieuwe digitale technieken en sensoren. Het

is zaak dat in die nieuwe wereld goed recht gedaan wordt aan de borging van privacy, autonomie en veiligheid.[5]

**De auditor op blockchain?**

Het spreekt voor zich dat de blockchainontwikkelingen ook de auditors raken. Wellicht krijgen auditors daarin hun eigen view op een blockchain. Zelf zie ik echter veel meer brood in een proactieve rol voor de auditor in de ontwerpfase, zodat we uitkomen op 'audit-by-design'. <<

**Noten**

1. Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system*. Te vinden op: https://bitcoin.org/bitcoin.pdf
2. Er zijn nog veel meer afsplitsingen ontwikkeld, maar de strijd tussen bitcoin en bitcoin cash is het meest in het oog springend.
3. Zie ook dit artikel van Matteo Gianpietro Zago: *50+ Examples of How Blockchains are Taking Over the World*. https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b
4. Zie ook de beslisboom als opgenomen in: *Blockchain Beyond The Hype*, *WEF*, april 2018. http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf
5. Zie ook de diverse rapporten en aanbevelingen van het Rathenau Instituut: *Doelgericht Digitaliseren*, 2018, en *Opwaarderen – het borgen van publieke waarden in de digitale samenleving*, 2017.

Simon Lelieveldt is zelfstandig gevestigd als regulatory consultant op het gebied van betalingsverkeer en blockchain. De laatste twee decennia vervulde hij verscheidene toezichthoudende en adviserende rollen binnen de Nederlandse financiële sector.

Thema Complexe technologie
Tekst Drs. Paul van der Zwan EMIA RO
Beeld Adobe Stock

# “Het is **nog niet** te laat”

Marc van Heese, partner bij ARC People, vertelt over de innovatie van de internal auditfunctie en hoe we deze toekomstbestendig kunnen houden.

**Wie is Marc van Heese? En via welke wegen loopt zijn carrière tot dusver?**
“Ik begon na het afronden van mijn studie Bedrijfskunde in Rotterdam bij KPMG Management Services. Dat onderdeel was met name actief in AO/IC en daar kwam ik voor het eerst in aanraking met internal audit. Via Mees Pierson kwam ik terecht bij Achmea Internal Audit, waar ik mijn RO-opleiding heb behaald. Daarna ben ik in 2005 samen met een collega een bedrijfje begonnen in Internal Audit en heb ik een zzp-platform ontwikkeld. Omdat de meeste processen die je tegenkomt ondersteund worden door IT dan wel volledig op IT gebaseerd zijn, ben ik ook de RE-opleiding gaan volgen. In 2013 startte ik samen met Sander van Oosten AuditPeople. Vorig jaar hebben we er RiskPeople en CompliancePeople aan toegevoegd, met als overkoepelend label ARC People. Samenvattend kun je stellen dat ik mijn hele werkende leven actief ben in internal audit en aanpalende vakgebieden, in diverse rollen, variërend van riskmanager tot hoofd Internal Audit. Die laatste rol vervul ik nog steeds op ad-interimbasis bij een kleinere verzekeraar.”

**U hebt een blog geschreven over het innovatieve karakter van internal audit of eigenlijk, in uw ogen, het gebrek daaraan. Kunt u de blog samenvatten en uw zorgen toelichten?**
“In mijn blog (https://www.auditpeople.nl/nieuws/houden-we-internal-audit-nog-voldoende-future-proof/ – red.) zeg ik dat we dagelijks horen dat de wereld in een heel hoog tempo verandert. Naast geopolitieke ontwikkelingen zijn die veranderingen vooral ingegeven door technologische ontwikkelingen. Denk aan het incorporeren van blokchain in bestaande businessmodellen, ‘quantum computing’, ‘quantum internet’, ‘artificial intelligence’, en zo verder. Allerlei nieuwe technieken tuimelen over elkaar heen, wat maakt dat bestaande businessmodellen razendsnel achterhaald lijken te raken. Dat deze ontwikkelingen bepalend zijn voor bedrijfsmodellen, en daarmee ook voor internal audit, is evident. Maar wat is nu het juiste antwoord van internal audit op al deze ontwikkelingen? Hoe kunnen wij hierin meegaan en relevant blijven? We roepen vaak dat we meer dan een ‘assurance provider’ willen zijn, een ‘insight provider’, of – nog beter – een ‘trusted advisor’. Ik vraag me sterk af of wij dat als beroepsgroep nu goed doen en of we daar wel goed voor worden opgeleid.

## Over...

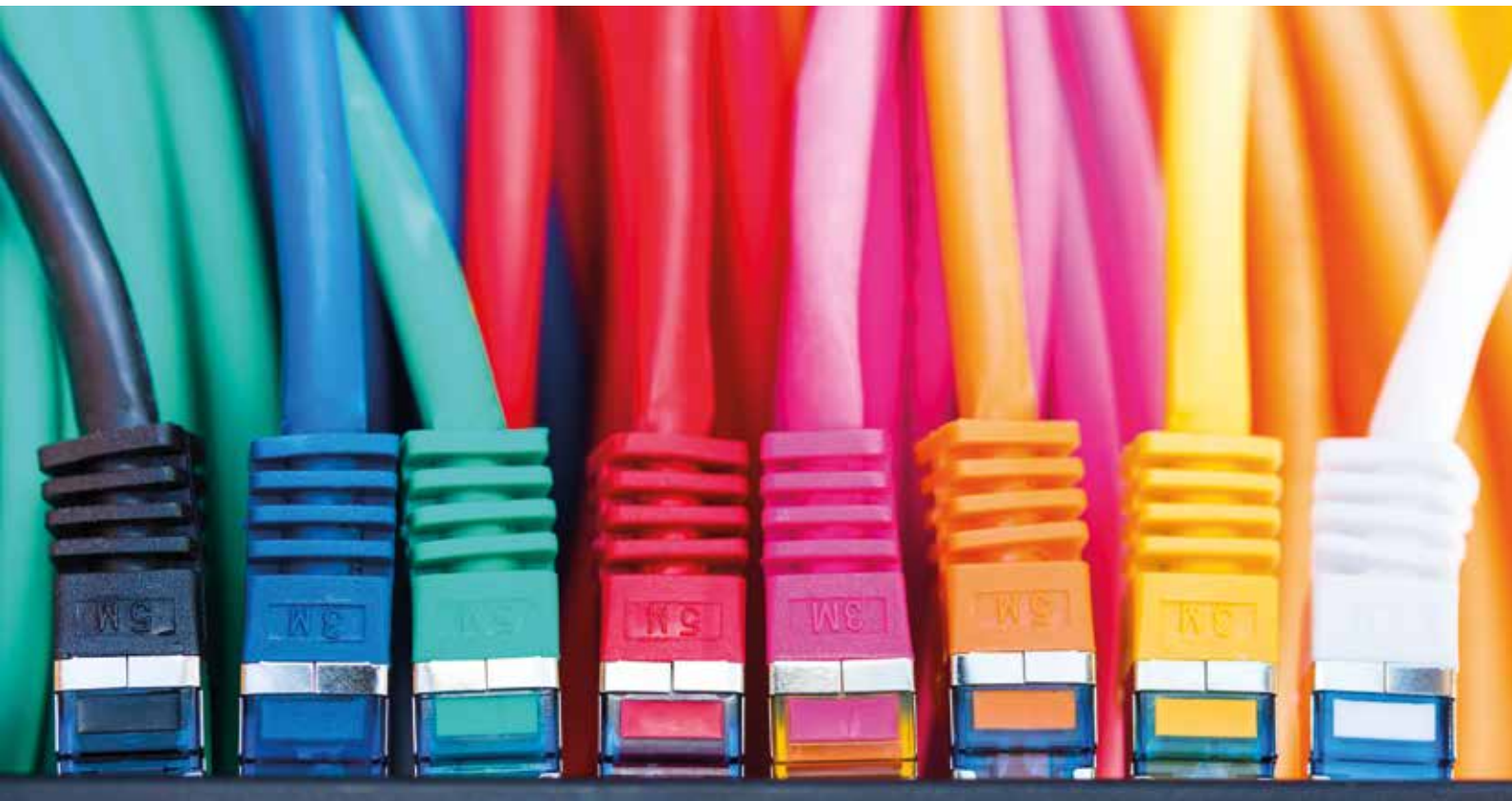
Drs. Marc van Heese RO RE CIA is partner bij ARC People. ARC People voorziet organisaties van capaciteit en deskundigheid op de gebieden audit, risk en compliance.

*"Ik vraag me echt af waarom RE en RO twee gescheiden opleidingen zijn nu bijna alles om IT draait"*

We hebben nu wettelijke verankering in de Corporate Governance Code en ook Europese wetgeving zoals IORP II en PSD2 verplichten een internal auditfunctie. Dat is natuurlijk heel goed, maar nu moeten we het als beroepsgroep ook waarmaken. Begrijp me goed, ik ben uiteraard voorstander van internal audit en zie ook de grote toegevoegde waarde ervan, maar dan moeten we alle ontwikkelingen wel kunnen bijbenen. Ik wil geen functie worden die er puur is vanwege externe dwang, maar door intrinsieke motivatie van de organisatie zelf. Ik wil niet dat we een functie zijn die door het eventueel wegvallen van wetgeving direct wordt opgeheven. Kijk voor de grap even naar internal-auditvacatures bij de bekendere 'disruptive organisations'. Bij deze openstaande auditvacatures kom je nogal vaak de term SOx tegen, deze bedrijven zijn genoteerd aan de NASDAQ en moeten daarom voldoen aan SOx. Dat lijkt dan toch te duiden op internal audit als een verplicht nummer, of in ieder geval voor een groot deel. Terwijl we zoveel meer waarde zouden kunnen toevoegen dan sec het testen van financial controls.
En ik denk werkelijk dat we ons vergissen in de snelheid van ontwikkelingen. Ik lees al dat blokchain volgens sommigen alweer verouderd is en dat de 'flash-channel'-techniek beter is. Ook twijfel ik of de focus op data-analyse, waar iedereen mee bezig is, nog vernieuwend genoeg is. Is er straks geen artificial intelligence tool waar je je data instopt, de tool vervolgens zelf externe databases betrekt zoals het weer, verkeer, et cetera, en met conclusies komt die we als auditor niet hadden kunnen bedenken? Wat is de rol van internal audit dan nog bij data-analyse? Google weet nu al eerder dan de huisartsen wanneer er een griepgolf is. Als we op de huidige manier blijven acteren, houden we het best nog even vol, maar actie is geboden. Ik gebruik graag als voorbeeld het sprookje over de waterlelie die elke dag in omvang verdubbelt en dus in toom moet worden gehouden. Als de vijver halfvol is, zeggen we 'dat pakken we morgen als eerste op'. Dan zijn we dus te laat. Kijk ik naar het onderzoek van PWC *State of the audit profession* van 2017 dan onderbouwt deze mijn zorgen: het aantal stakeholders dat vindt dat internal audit significante waarde toevoegt, daalde van 54% naar 44%."

**Kunt u een voorbeeld geven waaruit blijkt dat we achterblijven bij de ontwikkelingen?**

"Vooropgesteld, ik zeg niet dat alle internal auditfuncties achterblijven en ik wil ook niet beweren dat ik in de toekomst kan kijken. Ik denk dat de internal auditfunctie prima is geëquipeerd voor het uitvoeren van gedegen en onafhankelijk onderzoek waar een organisatie wat mee kan, maar we moeten wel naar de goede onderwerpen kijken. Onderwerpen die aansluiten bij de strategie en ontwikkeling van de organisatie en haar omgeving.
Ik zie nog veel afdelingen vooral bezig met het auditen van business as usual: alle processen in drie jaar raken en daarnaast nog even een audit op een belangrijk project. Ik vind dat we veel meer naar changeprocessen moeten kijken en ook veel meer naar buiten moeten kijken. Natuurlijk moeten we zorgen dat er geen klanten en geld door de achterdeur



naar buiten gaan, maar nu er zoveel 'disruptive' veranderingen zijn, zou de focus veel meer buiten de organisatie moeten liggen en hoe de organisatie deze veranderingen ten eerste signaleert en vervolgens daarop acteert. We moeten geen strategie bepalen, maar wel inzicht geven in wat er speelt en welke consequenties dat heeft voor de strategie en de interne organisatie.
Ik hoor nog steeds van auditafdelingen die bij voorkeur alleen maar RA's willen, omdat die goed weten hoe je een gedegen dossier moet opleveren. Dan maak ik me zorgen over de toegevoegde waarde van die afdeling.
Ik vraag me af hoeveel afdelingen geabonneerd zijn op de nieuwsbrief van (bijvoorbeeld) security.nl waarin alle securitylekken, virussen, et cetera, worden genoemd en die dan kijken wat de gevolgen daarvan zijn voor hun eigen organisatie. Op het IIA Congres van afgelopen juni werd verteld dat de verwachting is dat al het dataverkeer van de afgelopen jaren door de Chinezen en Amerikanen is opgeslagen en dat met quantum computing de encryptie te kraken is en alles dus te lezen is. Hoeveel auditors zijn dit na het congres intern gaan bespreken met het management en hebben in kaart gebracht welke risico's dit met zich mee brengt? Ik denk dat het aantal tegenvalt."

internal auditor en auditafdeling heeft hierin uiteraard zijn eigen verantwoordelijkheid, maar ik denk dat het opstarten van initiatieven vanuit het IIA een aantal grote voordelen biedt. Het biedt structuur, een groot netwerk, brede communicatie en wellicht ook de nodige funding. Inmiddels heeft het eerste brainstormgesprek plaatsgevonden met twee leden van het IIA-bestuur en ik hoop en verwacht dat dit een positief vervolg gaat krijgen."

**Hebt u ook concrete oplossingen voor de geschetste problematiek?**
"Als een echte auditor zou ik willen zeggen dat we daar eerst goed onderzoek naar moeten doen. Maar ik kan wel wat suggesties doen. Zoals in de blog aangegeven ben ik voorstander van een soort 'deltawerkenplan' binnen het IIA op dit onderwerp. Laten we starten met een commissie die binnen een korte periode met een gedegen plan komt hoe het vakgebied

*"Ik hoor nog steeds van auditafdelingen die bij voorkeur alleen maar RA's willen. Dan maak ik me zorgen over de toegevoegde waarde van die afdeling"*

**Jullie zijn actief als wervings-, selectie- en interimbureau. Welke ontwikkelingen ziet u in de markt? Vragen bedrijven al om andere profielen?**
"Bijna elke nieuw gezochte auditor moet IT-affiniteit hebben. Er is ook zeker meer vraag naar IT-auditors. Enkele bedrijven vragen ook om echte 'hardcore' IT'ers, maar dat aantal valt vooralsnog mee. We zien ook meer vraag naar trainees. Dat zijn net afgestudeerden, vanuit diverse studierichtingen, breder dan economie en bedrijfskunde, die na een gedegen opleiding starten bij de klant en daar training on the job krijgen. De frisse blik van deze jonge starters (de generatie Y) valt goed bij klanten. Op het laatste congres is het ook herhaaldelijk gezegd: haal jonge mensen in je team voor meer innovatie. Deze generatie heeft toch een hele andere kijk op zaken dan oudere generaties.
Op interimgebied zie je dat er steeds vaker specifieke skills worden gevraagd: niet meer gewoon een internal auditor of een IT-auditor maar een internal auditor die alles weet van AVG of een IT-auditor die alles weet van SAP of logische toegangsbeveiliging. Dat lijkt te duiden op meer specialisatie. Als auditor kun je gewoonweg niet alles meer weten: er zijn te veel ontwikkelingen op het gebied van IT en wetgeving."

**U hebt het gehad over wat afdelingen anders moeten doen. Maar wat is volgens u de rol van het IIA hierin?**
"Voor het plaatsen van de blog heb ik deze ook naar voorzitter Jantien Heimel gestuurd om haar hierover te informeren omdat ik het a) netjes vond als partner van het IIA en b) wilde aanbieden om samen met het IIA op te trekken in het toekomstvast houden van het internal auditvak. Elke

voor de toekomst relevant te houden. Ik denk dat daarin een aantal onderwerpen aan de orde moeten komen. We moeten allereerst kritisch kijken naar de opleidingen. Ik vraag me echt af waarom RE en RO twee gescheiden opleidingen zijn nu bijna alles om IT draait. Ik zou ook willen pleiten voor een vorm van samenwerking met de IT-auditberoepsvereniging NOREA.
Auditafdelingen zelf zouden alvast kritisch kunnen kijken naar hun planning: doen we wel de goede dingen? Niet te veel business as usual en te weinig change. Ik denk ook dat het in vervolg daarop goed is om te kijken naar de samenstelling van het team. Hebben we de juiste expertise in huis, hebben we nog een frisse blik? En ik denk dat kleinere teams met een grotere flexibele schil beter zijn, zodat de benodigde specifieke kennis kan worden ingehuurd op het moment dat het nodig is."

**Ziet u het nog zitten met het vak?**
"Zeker. Het is een schitterend vak: ik ben hierin niet voor niets al zo lang actief. Zoals eerder gezegd, ik ben ervan overtuigd dat een internal auditafdeling veel kan betekenen voor het succes van een organisatie. Dat moet zo blijven, maar dan moeten we wel tijdig veranderen. Het is nog niet te laat, de vijver is nog niet halfvol. Ongetwijfeld zijn er afdelingen die hierin al heel ver zijn. Ik nodig ze bij deze uit om hun kennis te delen en het vak vooruit te helpen." <<

# De internal auditor wordt in de toekomst IT-auditor

## Bert van den Bosch RO
**Internal auditor De Nederlandsche Bank**

☐ Eens ☑ Oneens

Een denkfout die volgens mij in de stelling ligt opgesloten, is dat als we de risico's van de automatisering beheersen, we ook de beheersing van de processen op orde hebben. Natuurlijk is het nodig dat wij wanneer internal auditors verstand hebben van IT en oog hebben voor de risico's die dat met zich meebrengt. Het is een noodzakelijke vereiste, maar geen voldoende vereiste. De stelling gaat eraan voorbij dat het mensen zijn die keuzen maken wat geautomatiseerd wordt, dat het mensen zijn die de systemen ontwikkelen en dat het mensen zijn die de systemen gebruiken. Als zich problemen voordoen bij op zich goede systemen ligt de oorzaak veelal in menselijk gedrag (al dan niet opzettelijk). Ik durf de stelling aan dat het mensen zijn die – net zo als nu – in de toekomst zullen zorgen voor de grootste risico's in al dan niet geautomatiseerde processen. Volgens mij hebben we internal auditors nodig die oog hebben voor en kennis hebben van menselijk gedrag en menselijk falen. Auditors die in ieder geval belangstelling hebben voor het gedachtegoed van winnaars van de Nobelprijs voor de economie als Herbert Simon, Daniel Kahneman en Richard Thaler. Het is volgens mij geen toeval dat twee van de drie geen economen zijn, maar socioloog of psycholoog. Volgens mij heeft het internal auditvak van de toekomst vooral meer psychologen en sociologen nodig.

## Gerard de Heide
**Concerncontroller woningcorporatie SOR**

☐ Eens ☑ Oneens

Ik ben het oneens met de stelling. De werkgebieden van de internal auditor en de IT-auditor verschillen naar mijn mening te veel van elkaar. Waar de internal auditor zijn focus legt op het goed en betrouwbaar functioneren van de interne organisatie, beoordeelt de IT-auditor het goed en betrouwbaar functioneren van de IT-organisatie. De internal auditor is over het algemeen een generalist, de IT-auditor heeft zich gespecialiseerd. Daarom verwacht ik eerder een goede samenwerking tussen beide auditors dan dat de internal auditor de toekomstige IT-auditor zal worden.

## Drs.ing. Gert-Jan van der Donk RO
**Interim professional**

☐ Eens ☑ Oneens

Op grond van mijn werkervaring en de ontwikkelingen wat betreft de werkgelegenheid zou ik de stelling willen wijzigen naar: De internal auditor dient zijn instrumentarium uit te breiden met IT. We zien dat steeds meer werk wordt geautomatiseerd en dat de mens in productieprocessen wordt vervangen door robots. Ook worden er meer apparaten op internet aangesloten. Om vast te stellen dat het productieproces of het apparaat voldoet, zal de internal auditor ook meer verstand van IT moeten hebben. Als interimmer krijg ik ook steeds meer de vraag van klanten om interfaces tussen systemen te auditen die normaliter door de EDP-auditor worden uitgevoerd. Daarnaast verwacht ik dat de vraag om audits waarbij IT niet wordt getoetst blijvend is. Denk bijvoorbeeld aan een audit waarbij de soft controls van een organisatie worden getoetst.

## Patrick Beekhuizen RO RE
**Auditmanager GAD, gemeente Den Haag**

☐ Eens ☑ Oneens

Ik ben het niet eens met de stelling, de vraag is waar je je als auditor op richt. Het aandachtsgebied van de internal auditor is de interne beheersing van systemen, processen en projecten binnen organisaties. IT is het woonhuis geworden van de interne beheersing, dus is IT-kennis onmisbaar. Zonder basis IT-kennis heb je een achterstand. Maar dat zal ons geen IT-auditors maken. Bij de GAD vliegen wij de audits zoveel als mogelijk geïntegreerd aan. Financiën, maar ook IT, cultuur, leiderschap en zelfs fiscale aspecten zijn in hetzelfde onderzoek in scope. We onderzoeken de gehele interne-beheersingscyclus integraal. Per audit bepalen we op basis van de informatiebehoefte welke specialistische kennis noodzakelijk is. Dat kan IT-kennis zijn maar ook andere kennis. IT is het woonhuis van de interne beheersing, maar interne beheersing is veel meer dan IT.

De reacties op de stellingen zijn gegeven op persoonlijke titel.

Thema Complexe technologie
Tekst Owen Strijland
Beeld Adobe Stock

# Het belang van risicomanagement voor de Nederlandse FinTech

Een succesvolle FinTech is slechts enkelen gegund, vele interne en externe factoren zijn van invloed op falen en/of slagen. Risk management is een belangrijke factor om te slagen. Dit artikel belicht een select aantal belangrijke risk-managementprocessen die van belang zijn.

De Nederlandse FinTechmarkt heeft een significante groei laten zien in de afgelopen jaren.[1] Al in de zomer van 2016 analyseerde De Nederlandsche Bank (DNB) de snelle intrede van innovatieve technologieën in de financiële markten. In dit onderzoek onderkent en beschrijft DNB drie belangrijke scenario's voor groei van FinTech waarvan we weten dat alle drie zich nu in hoog tempo voordoen:[2]

- De adoptie van technologische innovatie door gevestigde spelers. Een goed voorbeeld hiervan is Tikkie van ABN AMRO: in nog geen twee jaar gaat Tikkie van 'minimum viable product', bedacht door een aantal medewerkers, naar een door ABN AMRO geadopteerde en ondersteunde dienst.[3]
- De fragmentatie van financiële diensten als gevolg van de adoptie van technologie. Hier hint DNB naar FinTech als start-up die heel effectief een enkele dienst verkoopt. Ook dit scenario zien we terug in de markt in de vorm van bijvoorbeeld Bunq met zijn razendsnelle klantacceptatie en online omgeving of bij AfterPay dat een mogelijkheid biedt om bij webbestellingen alleen te betalen als je het product houdt.
- De absorptie door bigtech. Ook al zijn de meest bekende, ApplePay en GooglePay, in Nederland (nog) niet mogelijk, als men even over de grens gaat blijkt dit heel anders te zijn. Reis je af naar China, dan blijkt dat meer dan 80% van de online betalingen door consumenten niet meer via reguliere banken wordt gedaan.

**Snelle ontwikkeling**

De Nederlandse FinTechmarkt ontwikkelt zich snel. Er zijn vooral veel nieuwe toetreders op het gebied van betalen, alternatieve manieren van financieren en toeleveranciers aan financiële dienstverleners, zoals BusinessForensics en Five°degrees. Waarom nu juist deze markten groeien is niet vreemd; online betalen en alternatieven als AfterPay volgen simpelweg de groei van online winkelen. Alternatieve financieringen volgen de roep om krediet van zowel particulieren als bedrijven, het liefst zonder de inmenging van banken.
En er is nog een belangrijke factor waarom de FinTechsector zo hard kan groeien. Er ontstaat namelijk een ecosysteem waarin slimme apparaten met name de steeds meer geavanceerde smartphones een belangrijke centrale rol hebben. IOS van Apple en Android van Google hebben samen zo goed als de hele markt van operating systems van smartphones in handen. Het beschikbaar stellen van een app als Tikkie via deze platforms garandeert daarmee het bereik van een groot publiek.
Naast het beschikbaar zijn van technologie en het tot stand komen van standaarden waarmee nieuwe technologie mogelijk wordt gemaakt, is er nog een belangrijke Europese factor. Dat is de meer en meer geharmoniseerde Europese regelgeving. Neem als voorbeeld de payment service directive 2 (PSD2). Simpel gezegd regelt deze wetgeving, zij het met zeer strenge eisen aan de onderneming, dat banken hun systemen beschikbaar (via API) moeten stellen voor PSD2-vergunninghouders, en dat deze vergunninghouders toegang krijgen tot betaalgegevens van haar klanten die hiervoor toestemming hebben gegeven.[4] Bij het hebben van de zwaarste vergunningsvorm kunnen deze PSD2-vergunninghouders zelfs betalingen initiëren in het systeem van de bank.

**Is FinTech dan altijd succesvol?**

Garandeert deze groei van de Nederlandse FinTechmarkt en het gemak waarmee FinTech bij een grote hoeveelheid klan-

# *Online betalen en alternatieven als AfterPay volgen simpelweg de groei van online winkelen*

ten onder de aandacht komt, ook het succes? Een FinTech is nu eenmaal altijd nog een onderneming of initiatief, geleid door mensen en bestuurd met processen. Hoe agile er ook gewerkt wordt of hoe veel dagstarts er ook aan voorafgaan, er is een doel dat de betreffende FinTech nastreeft.[5] Ieder doel is onderhevig aan risico's die ervoor zorgen dat doelen niet of maar gedeeltelijk gehaald worden.
Een voorbeeld. In 2016 startten drie grootbanken in Nederland met een initiatief voor een platform om groepsbetalingen aan een ontvangende partij te vereenvoudigen. Hiervoor werden, zoals vaker gehanteerd in de FinTechindustrie, pakkende namen verzonnen zoals GRPPY en TWYP. MyOrder, een dochter van Rabobank ontwikkelde GRPPY (Groepie) als betaalapp waarmee vrienden gedeelde betalingen konden verrichten. ING ontwikkelde TWYP (The Way You Pay) ook als betaalapp voor groepen en gaf daarnaast een mogelijkheid om te chatten met leden van de groep. Deze twee apps leken zeer succesvol te worden, totdat een paar handige medewerkers van ABN AMRO kwamen met Tikkie. De ontwikkelaars van de eerste Tikkie-app maakten de keuze – die later een cruciale bleek te zijn – om groepsbetalingen aan te bieden in hun app door gebruik te maken van iDEAL in combinatie met het zeer succesvolle WhatsApp. Het gevolg is bekend.
Wat waren nou de key differentiators die Tikkie de voorsprong hebben gegeven?

- bruikbaar voor iedereen, ook zonder ABN AMRO-rekening;
- gebruik van al bekende en breed ondersteunde technologie (iDEAL);
- communicatie via de in Nederland meest gebruikte chatapp WhatsApp.

Waar de concurrentie koos voor eigen klanten en een eigen platform, waren de producteigenaren van ABN AMRO bereid meer risico te nemen en een meer 'open' omgeving aan te bieden. Dit resulteerde in circa 90% marktaandeel, ruim 2 miljoen unieke gebruikers en bijna 100.000 tikkies per dag. Niet zo gek dat Tikkie Business ontstaat en expansie naar Duitsland wordt gezocht.

**Relatie met risicomanagement en governance**
Waarom is die ene FinTech een succes en de andere niet? Een belangrijke vraag die meerdere antwoorden kent. Interessant is de vraag of risk management en governance een rol spelen in het succes van FinTech en of te achterhalen is of er een positieve of negatieve invloed wordt ervaren.
Dit is onderzocht bij twaalf FinTechondernemingen en gelieerde personen, waarbij is gekeken naar de rol en functie van de geïnterviewden binnen de FinTech, hun kennis van risk en governance, welke factoren in hun ogen een positieve of negatieve bijdrage hebben geleverd aan het succes van de FinTech en in welk stadium van de FinTech dit effect zich heeft voorgedaan. De uitkomsten zijn vervolgens gegroepeerd in thema's:

- Thema's die door de FinTech als duidelijk *negatief* werden ervaren. Door deze thema's trad vertraging op of werden initiatieven niet doorgezet.
- Thema's die duidelijk een *positieve* invloed hadden op de FinTech door bijvoorbeeld de ontwikkeling te versnellen of klanten eerder te binden.
- Thema's die zelf niet direct positief of negatief waren, maar indirect wel een grote *invloed* hadden op de negatieve en positieve thema's.

Twee van de gevonden positieve thema's zijn risk identification en risk response. Een van de beïnvloedende thema's is de klant/auditor.

**Risk identification**
Bijna alle FinTechs gaven aan dat het goed kunnen identificeren van risico's vroeg in het ontstaan van de FinTech een positieve bijdrage heeft geleverd aan het succes van de organisatie. Het in beeld krijgen van de juiste risico's voor een FinTech vereist echter wel dat de persoon die de risico's identificeert of helpt bij het identificeren van de risico's, bepaalde expertkennis moet hebben. Er wordt hierbij een flexibele houding tegenover de risico's verwacht, waarbij rekening wordt gehouden met het 'nieuwe' dat de FinTech nastreeft. Dit nieuwe kan het proces zijn waarmee de FinTech de markt benadert of zichzelf organiseert, de nieuwe technologie die wordt ingezet of zelfs de nieuwe markt die ontstaat door de FinTech.
Naast deze kennis moet tijdens de identificatie ook rekening worden gehouden met de constante veranderingen binnen de FinTech. Bijvoorbeeld door impactvolle wijzingen, door veranderende doelen, of belangrijke klanten en investeerders die veranderingen in de organisatie of het product kunnen afdwingen. Het effect dat deze veranderingen hebben op eventuele vergunningen is een bijkomende complexiteit voor

het management van de risico's. Als de risico-identificatie aansluit bij de behoefte en business van de FinTech is het management veel beter in staat om op kansen en bedreigingen te reageren.

**Risk response**
Net zo belangrijk als de identificatie van risico's zijn de maatregelen die genomen worden als reactie op de geïdentificeerde risico's. Alleen als de identificatie van de risico's op een passende wijze verloopt, heeft het herkennen, benoemen en nemen van maatregelen een positief effect. Deze maatregelen kunnen FinTechspecifiek zijn of komen uit een good practice, zoals COSO of COBIT.[6,7] Als de maatregel is geëffectueerd, is het belangrijk dat deze geëvalueerd wordt op de toepasbaarheid terwijl de FinTech zich beweegt in de markt, producten ontwikkelt en nieuwe partnerships aangaat.
Voor internal auditors zijn de voorgaande twee thema's natuurlijk niets nieuws. Voor FinTechs vaak wel. Een FinTech heeft een sterke product- en marktfocus met een team dat verantwoordelijk is voor het ontwikkelen van een bepaald product of dienst en een team dat zich bezighoudt met het plaatsen van het product in de markt. Zeker in het ontstaan van een FinTech is men niet snel geneigd aandacht te hebben voor risico's en maatregelen. Bij het aantrekken van investeringen, het acquireren van een eerste grote klant en het eventueel verkopen van de organisatie krijgen deze twee thema's wel aandacht. En helemaal bij het overtuigen van een toezichthoudende instantie, zoals de AFM of DNB. Tijdens het beschrijven van de drie fasen (investeringen, acquireren en verkoop) is door de onderzochte FinTech's een belangrijke beïnvloeder genoemd, namelijk de auditor. De auditor is veelal een eerste persoon die de FinTech wijst op risico's die worden gelopen. De auditor heeft wel expertise op het gebied van de beheersing van risico's, maar is zich minder bewust van de snelheid, flexibiliteit en de (soms) tijdelijkheid van producten. Dit wordt door de FinTech's soms als stroef en remmend ervaren. Hier is voor auditors dus nog terrein te winnen.

**Conclusies**
Risk management en governance kunnen zeker een positieve invloed hebben op het succes van FinTechs. Belangrijke reden is dat een FinTech juist in de huidige zeer competitieve markt goed op de hoogte moet zijn van bedreigingen en kansen, iets waar een goede risk professional/auditor bij kan ondersteunen, maar alleen als deze zich kan aanpassen aan het tempo en flexibiliteit van de FinTech.
Een FinTech komt daarnaast veel groeifase-issues tegen die verband houden met risk en control, zoals een eerste klant, een samenwerkingspartner, een toezichthouder of een belangrijke investeerder die veeleisende standaarden oplegt aan de organisatie en het product. FinTechs die in een vroeg stadium weten welke standaarden zij tegenkomen, hebben aanzienlijk voordeel bij het aangaan van een verhouding met deze partijen. Een vroege voorbereiding op het adopteren van een standaard, ondersteund door een eventueel tijdelijke professional kan een groot verschil maken op het moment dat er vragen worden gesteld.
Risk professionals/auditors kunnen bij het voorgaande alleen een belangrijke rol vervullen als zij gevoel hebben voor de wezenlijke kenmerken van een FinTech en over voldoende inhoudelijke kennis van de markt beschikken. Voorts moeten ze goed om kunnen gaan met de wensen van deze organisaties om niet alleen te helpen inventariseren, maar ook juist te helpen implementeren. Dit betekent dat de professional om moet kunnen gaan met een bottom-up en top-down risk managementbenadering die aansluit bij de FinTech. Dit vraagt om professionals met kennis van nieuwe technologie, markten en mogelijke klanten van de FinTech. <<

*Zeker in het ontstaan van een FinTech is men niet snel geneigd aandacht te hebben voor risico's en maatregelen*

**Noten**
1. In mijn onderzoek heb ik aan FinTech een brede definitie gegeven: nieuwe initiatieven ondersteund door technologie die ingezet wordt door financiële instellingen.
2. *Technologische innovatie in de Nederlandse Financiële sector*, DNB, 2016.
3. Minimum viable product; het eerste werkende product met minimale bruikbaarheid.
4. API, application programming interface.
5. Agileteams beginnen de dag met een dagstart waarin de details van de dag worden doorgenomen
6. The Committee of Sponsoring Organizations of the Treadway Commission.
7. Control objectives for information and related technologies.

Owen Strijland werkt sinds 2012 bij Protiviti, maakt onderdeel uit van het MT en is sinds 2018 verantwoordelijk voor de diensten aan FinTech. Hij behaalde in 2018 zijn MBA aan de Nyenrode Business Universiteit met een onderzoek naar FinTech en risk management.

Thema Complexe technologie
Tekst Jelte Coenraads MSc EMA RA
Beeld 123RF®

# Staat **blockchain** al in het auditplan 2019?

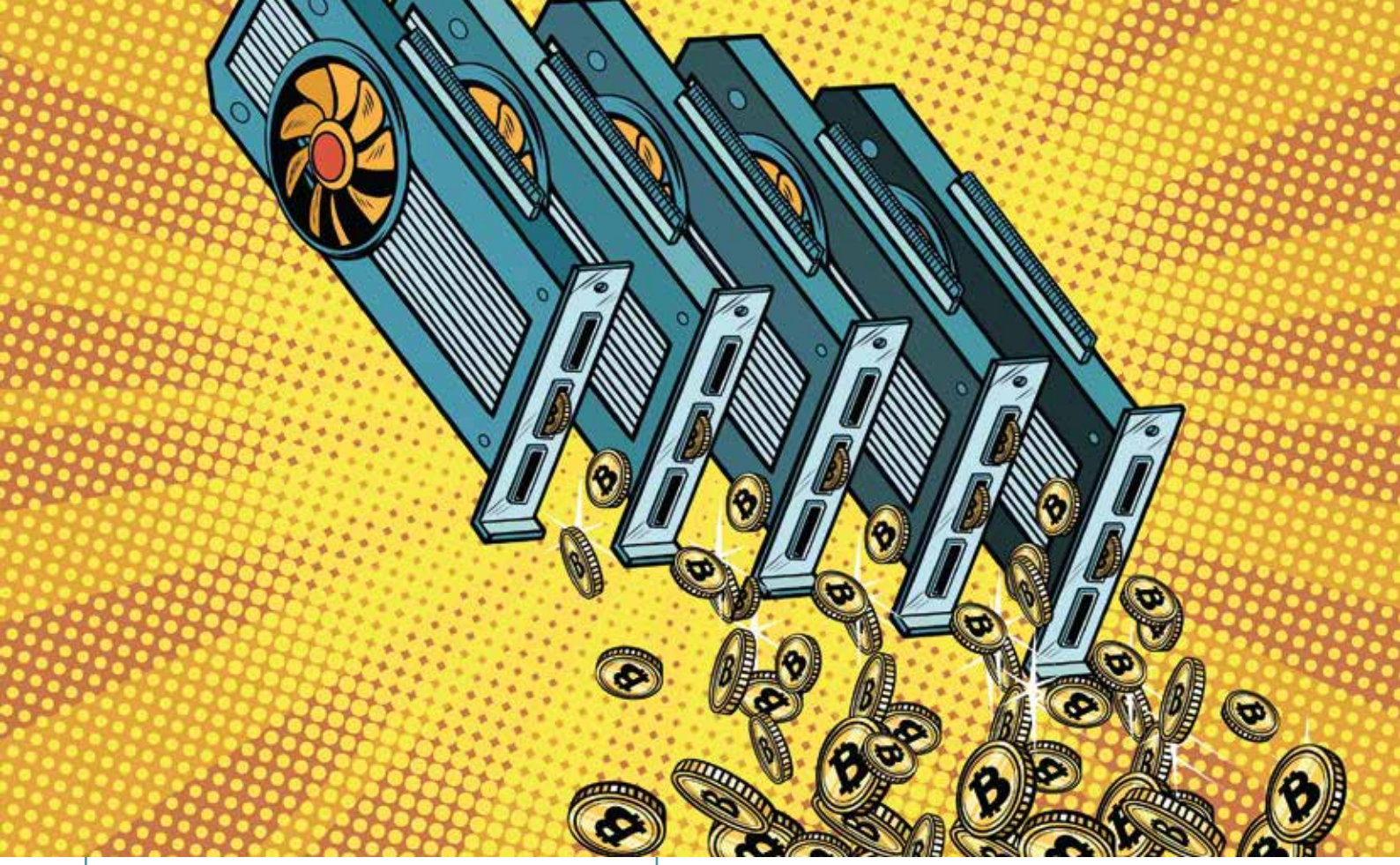
Ondanks de hype lijkt het erop dat blockchain bedrijfsprocessen en businessmodellen gaat veranderen. Kan de auditor zich permitteren om een van de belangrijkste technologische ontwikkelingen van deze tijd nog langer te negeren?
Blockchain verdient een plek in het auditplan 2019.

Bitcoin en blockchain, het is bijna onmogelijk dat je er nog niet van gehoord hebt. Een paar jaar geleden leek bitcoin een soort hype die wel weer zou overwaaien, alsof het over flippo's ging. Inmiddels is er veel veranderd. Naarmate er meer over de onderliggende technologie, blockchain, bekend wordt, groeit de overtuiging dat dit een grote impact kan hebben op bedrijfsprocessen en businessmodellen. Zeker in de financiële wereld. Hoewel, ook nu nog word je niet altijd serieus genomen als je over blockchain of cryptovaluta spreekt. Men ziet het nog steeds als een hype en bovendien worden cryptovaluta vaak geassocieerd met criminele activiteiten, zoals het witwassen van geld.
Het doel van dit artikel is niet om uit te leggen hoe deze technologie werkt. Wel wordt ingegaan op hoe te anticiperen op mogelijke consequenties voor organisaties en de auditafdeling en hoe dit te vertalen naar het auditplan.

**Van bitcoin naar blockchain**
Afgelopen jaren gingen de ontwikkelingen razend snel. Niet de met criminelen geassocieerde bitcoin, maar blockchain werd het nieuwe toverwoord. Het bedrijfsleven begon de mogelijkheden van de onderliggende technologie in te zien. De beurswaarde van techondernemingen die iets met blockchain deden gingen door het dak. Ook ABN AMRO experimenteert met blockchaintechnologie en heeft zich aangesloten bij diverse blockchain consortia en samenwerkingsverbanden, waaronder Hyperledger, R3 en de Dutch Blockchain Coalition (zie *kader*). Die eerste twee consortia zijn inmiddels uitgegroeid tot twee van de grootste internationale samenwerkingsverbanden, op het gebied van 'distributed ledger technologie'.[1]

De opkomst van blockchaintechnologie is mogelijk een bedreiging voor de toekomst van een bank en wellicht ook voor andere organisaties. Daar moeten wij als internal auditors dus alert op zijn, zeker als het impact heeft op de toekomstbestendigheid van traditionele verdienmodellen.

**Toepassingen**
Veelbelovende toepassingen van blockchain zijn onder andere het efficiënter en goedkoper maken van administratieve processen, internationale betalingen, maar bijvoorbeeld ook het op een betrouwbare en veilige manier opslaan en vaststellen van de (digitale) identiteit van personen en objecten, zoals machines of vastgoed.
Een responsieve organisatie dient tijdig in te spelen op ontwikkelingen om te voorkomen dat het businessmodel achterhaald wordt of dat er nieuwe kansen gemist worden. Het begint uiteraard met het opbouwen van kennis en opzoeken van samenwerkingsverbanden. Dit geldt niet alleen voor de organisatie zelf, maar ook voor ons als internal auditors. Als een auditor niet precies weet wat blockchain is of wat je ermee kunt, dan kan een auditor ook niet goed inschatten wat de risico's en impact voor de organisatie zijn. Het opbouwen van kennis is dus een eerste stap voor de auditor. Begin 2017 organiseerde Group Audit in samenwerking met het Innovation Centre van ABN AMRO voor alle collega-auditors een kennissessie over blockchain. De opkomst was hoog en er werd aandachtig geluisterd, maar auditors blijven kritisch en velen geloven dat het niet zo'n vaart zal lopen, omdat er nog veel obstakels overwonnen moeten worden.



**Hyperledger** is een cross-industrie open source blockchainconsortium dat oorspronkelijk is opgericht door IBM in samenwerking met de Linux foundation en enkele andere oprichters. Inmiddels telt het consortium meer dan tweehonderd leden, bestaande uit multinationals en start-ups uit diverse landen en sectoren. Kijk voor meer informatie op http://hyperledger.org/_

**R3** is een internationaal consortium, oorspronkelijk opgericht door financiële instellingen. Dit samenwerkingsverband telt inmiddels meer dan tweehonderd leden uit diverse sectoren en richt zich voornamelijk op de financiële wereld met Corda, het op blockchain geïnspireerde platform. Meer informatie is te vinden op https://www.r3.com/

**Dutch Blockchain Coalition** is een samenwerkingsverband tussen de Nederlandse overheid, het bedrijfsleven en kennisinstituten met als doel de grootschalige uitrol van blockchaintechnologie in Nederland te bevorderen. De leden bestaan onder andere uit ABN AMRO, ING, Rabobank, diverse ministeries, maar ook partijen als Havenbedrijf Rotterdam, Enexis en Alliander. Kijk voor meer informatie op https://www.dutchdigitaldelta.nl/blockchain

**Obstakels**

Zo zouden blockchains niet schaalbaar zijn. Een veelgehoord argument om de impact van blockchain te bagatelliseren. Soms lijkt een nieuwe technologie geen bedreiging voor bestaande producten of verdienmodellen, maar dat kan snel veranderen. Het is nog niet zo lang geleden dat het een half uur duurde om met een 56k modem via de kabel een paar mb muziek te downloaden. Het leek geen bedreiging voor de verkoop van cd's of dvd-spelers. Tegenwoordig is het mogelijk om overal draadloos te streamen via Netflix of Spotify en zijn cd's verleden tijd.

Wereldwijd worden miljarden geïnvesteerd in blockchain en er zijn tal van partijen die werken aan nieuwe innovatieve oplossingen om blockchaintechnologie te verbeteren. Het is waarschijnlijk een kwestie van tijd voordat gebrek aan schaalbaarheid en andere technologische beperkingen zijn verholpen.

Een ander obstakel is het ontbreken van een internationaal juridisch kader rondom blockchain en cryptovaluta. In maart 2018 schreef Christine Lagarde van het Internationaal Monetair Fonds nog dat een mondiale aanpak noodzakelijk is. Blockchains en cryptovaluta kennen immers geen geografische grenzen. Bedrijven, innovatie en de economische voordelen zullen zich simpelweg verplaatsen naar landen met de meest vriendelijke regulering. Dit gebeurt al in Malta en Zwitserland, wat op dit moment populaire landen zijn voor het starten van aan blockchain of cryptovaluta gerelateerde bedrijven. Op het niveau van de G20 en de EU krijgt dit inmiddels ook de aandacht, maar een internationaal juridisch kader en een duidelijke norm voor de auditor laat voorlopig nog op zich wachten.

**Blockchain en digitale tokens**

Een belangrijk punt dat mensen vaak niet begrijpen, is dat blockchains en cryptovaluta nauw met elkaar verbonden zijn. Het afgelopen jaar zei Mohanty, de chief fintech officer van de Monetary Authority of Singapore, nog het volgende: "I want to quash this false narrative that's been going around for the past two years that you can separate blockchain from crypto. You can't."

Cryptovaluta zijn niets anders dan digitale tokens. Het is te vergelijken met een stuk papier. Zo'n token kan een bioscoop- of treinkaartje vertegenwoordigen, maar ook een aandeel in een bedrijf of hypotheekakte. Het is bijvoorbeeld mogelijk om aandelen te verhandelen en automatisch dividend uit te betalen via tokens op een blockchain zonder

RSG CORPORATE GOVERNANCE
HUMAN KEY SOLUTIONS

## GEZOCHT: TALENTVOLLE PROFESSIONALS

RSG Governance, Risk&Compliance is gespecialiseerd in de bemiddeling van professionals op het gebied van Internal Audit, Risk Management en Compliance. Dit doen wij voor zowel vaste (Executive Search) als tijdelijke functies (interim management).

Voor meerdere organisaties zijn wij op zoek naar talentvolle professionals voor de volgende functies:

Risk Manager
Internal Audit Manager
Compliance Manager/Officer

Functievereisten:

- Een postdoctorale opleiding (RA/RO/RE) en/of CIA
- Minimaal 5 jaar werkervaring in een soortgelijke functie
- Competenties als zelfvertrouwen, doortastend en pro-actief
- Goede communicatievaardigheden en eigenaarschap nemen

Ben je geïnteresseerd en wil je meer weten neem dan contact op met Michael McGourty via michael.mcgourty@rsg.nl of bel naar 06-51833360 of 085-2736170.

## RSG FINANCE HUMAN KEY SOLUTIONS

## ACCOUNTANT? EN NU?

Je vindt de accountancy een geweldig vak en een prachtige leerschool. Maar toch jeukt het en zoek je een verbreding van je werkveld. Je wilt nieuwe mogelijkheden aanboren. Herkenbaar? RSG is de kickstarter die professionals uit de accountancy de kans biedt zich te ontwikkelen tot (Business) Controller.

RSG biedt daartoe onder meer het model van de Flexibele Vennoot: Het bureau gaat dan een arbeidsovereenkomst voor onbepaalde tijd met je aan met een bovengemiddeld basissalaris en een bonus die afhankelijk is van je projectresultaat. Minstens even belangrijk: men investeert veelvuldig in je hard en soft skills en laten je kennismaken met projecten in verschillende Business Lines, zodat je jezelf flink ontwikkelt.

Ben je geïnteresseerd en wil je meer weten neem dan contact op met RSG Finance via info@rsg.nl of bel naar 085-2736170.

RSG FINANCE
HUMAN KEY SOLUTIONS

Vestdijk 57a
5611 CA Eindhoven
The Netherlands

+31 (0)85- 273 61 70
info@rsg.nl
www.rsg.nl

| Blockchain readiness assessment | Zwak | | <--> | | Sterk |
|---|---|---|---|---|---|
| Is het management van de organisatie bekend met de mogelijkheden en beperkingen van blockchaintechnologie? | 1 | 2 | 3 | 4 | 5 |
| Is er binnen de organisatie voldoende kennis en expertise op het gebied van blockchain en cryptovaluta? Daarbij gaat het niet alleen om IT'ers maar ook businessmanagers en collega's van compliance, risk, legal en audit moeten kunnen meepraten over de technologie | 1 | 2 | 3 | 4 | 5 |
| Heeft het management onderzocht welke invloed blockchain kan hebben op bestaande processen, systemen, verdienmodellen en de strategie van de organisatie? | 1 | 2 | 3 | 4 | 5 |
| Is disruptie door blockchaintechnologie als risico onderkend in strategische risico-assessments? | 1 | 2 | 3 | 4 | 5 |
| Maakt blockchain deel uit van innovatieplannen? | 1 | 2 | 3 | 4 | 5 |
| Worden relevante (externe) ontwikkelingen op het gebied van blockchain actief gevolgd? Bijvoorbeeld door het deelnemen aan congressen en kennissessies | 1 | 2 | 3 | 4 | 5 |
| Is de organisatie aangesloten bij relevante blockchainconsortia en neemt de organisatie deel aan experimenten? | 1 | 2 | 3 | 4 | 5 |
| Zijn blockchaininnovaties en -initiatieven van concurrenten belicht in een concurrentieanalyse en heeft het management een goed beeld van nieuwkomers en start-ups in de markt? | 1 | 2 | 3 | 4 | 5 |
| Is disruptie door blockchain een inherent risico dat je als auditor onderkent tijdens risicoanalyses? | 1 | 2 | 3 | 4 | 5 |
| Beschikt de interne auditafdeling over de juiste tools en technieken om smart contracts en transacties op een blockchain te analyseren en beoordelen? | 1 | 2 | 3 | 4 | 5 |

**Score 35 – 50**
De organisatie en auditafdeling zijn goed voorbereid op de komst van blockchain. Er is al behoorlijk wat kennis en expertise opgebouwd en er wordt actief gewerkt aan innovaties op basis van blockchaintechnologie. Als auditafdeling is het belangrijk om de interne- en externe ontwikkelingen continu te blijven volgen. Blockchain krijgt een duidelijk e plaats in het auditplan (denk aan project audits).

**Score < 35**
De organisatie en auditafdeling zijn nog niet voldoende voorbereid op de komst van blockchaintechnologie. Er is een verhoogd risico dat de organisatie niet tijdig kan inspelen op de veranderingen en wordt ingehaald door concurrenten of start-ups. Blockchain dient te worden opgenomen in het auditplan om vast te stellen dat blockchain voldoende aandacht krijgt in de organisatie, waar de grootste risico's zitten en welke acties noodzakelijk zijn om dit risico te mitigeren.

**Tabel 1.** Blockchain readiness assessment

tussenkomst van een bank. Ook kan een blockchain goed worden ingezet als een kadaster van onroerend goed.
Digitale tokens zijn dus een essentieel onderdeel van een blockchain en deze mogelijkheden maken dat steeds meer partijen geïnteresseerd zijn. In april 2018 publiceerde Reuters de resultaten van een survey onder vierhonderd financiële instellingen. 20% van deze instellingen overweegt om binnen een jaar te gaan handelen in cryptovaluta. Het blijft niet alleen bij overwegingen, want Intercontinental Exchange, het moederbedrijf van de New York Stock Exchange, kondigde in augustus 2018 aan dat het een wereldwijd platform ontwikkelt waar consumenten en bedrijven bitcoins en later ook andere tokens, kunnen kopen, verkopen, bewaren en spenderen.
Het gebruik en de populariteit van blockchain en digitale tokens als cryptovaluta lijkt een niet te stuiten fenomeen. Dit wordt bevestigd door Valdis Dombrovskis, vice president van de Europese Commissie: "We see that crypto-assets are here to stay. Despite the recent turbulence, this market continues to grow. One challenge with crypto-assets is how to categorise and classify them, and whether and how to apply existing EU financial rules to these assets or if we need new EU rules."
De hoge volatiliteit en de enorme koersdaling van begin 2018 hebben het geloof in blockchain en cryptovaluta dus niet ondermijnd.

### Wat kan de auditor doen?

Er zijn weinig organisaties die nu al op grote schaal gebruikmaken van blockchain of cryptovaluta, en het is nog onzeker hoe de technologie zich verder ontwikkelt. Daarnaast ontbreekt een duidelijk normenkader of wet- en regelgeving. Dat maakt het lastig om nu al een oordeel over blockchain te vormen. Maar alles negeren totdat dit er wel is, is ook geen optie. Als de auditor alleen naar de processen en risico's van vandaag blijft kijken, dan mist hij grote bedreigingen die de continuïteit van de organisatie over een paar jaar mogelijk in gevaar brengen. Ook wanneer de organisatie nog niet gebruikmaakt van blockchaintechnologie kan de auditor wel degelijk iets doen. Zijn de organisatie en de auditafdeling goed voorbereid op de komst van deze nieuwe technologie? Het assessment als in *tabel 1* kan als hulpmiddel dienen om te bepalen wat de aandacht vergt in het auditplan 2019.
Óf en wanneer blockchain een impact heeft op de eigen organisatie is lastig te voorspellen. Hype of niet, blockchain is in ieder geval iets om serieus te nemen. Het zou vreemd zijn als er komend jaar in de auditplanning geen aandacht wordt besteed aan blockchain. <<

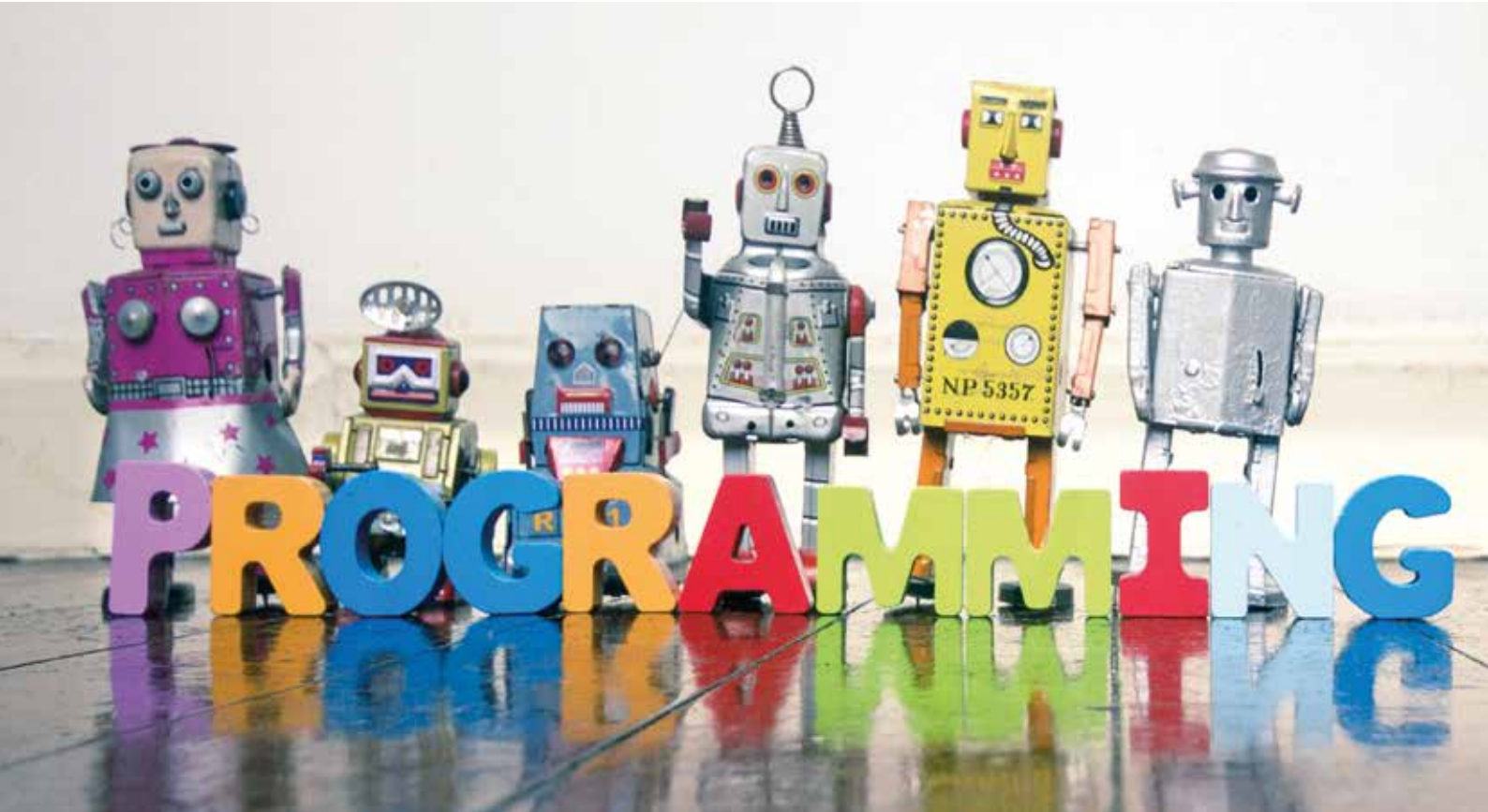
**Noot**
1. Een verzamelnaam voor technologie waar blockchain een variant van is.

Jelte Coenraads is senior auditor bij Group Audit ABN AMRO.

Thema Complexe technologie
Tekst Steven Boekhoudt MSc
Beeld Adobe Stock

De opkomende technologie robotics process automation (RPA) doet in steeds meer organisaties haar intrede. Dit artikel gaat in op de nieuwe uitdagingen en RPA-specifieke risico's en relateert deze aan de COBIT IT-controleprocessen die als handvatten dienen voor internal auditors om de interne beheersing rondom RPA te beoordelen.

# Wat vinden **robots** van COBIT?



RPA is een technologie die hoogvolume gestandaardiseerde, repetitieve, veelal voor de mens onaantrekkelijke taken vervangt door softwarerobots. De voordelen hiervan zijn dat deze robots zonder onderbreking kunnen doorwerken en taken consistent uitvoeren op basis van vooraf geprogrammeerde regels. De RPA-technologie is zo ontworpen dat het geen hoge investeringskosten kent en dat deze moeiteloos integreert met applicaties in het huidige IT-landschap, waardoor de robots snel werken en winst kunnen opleveren.

**Zelf software bouwen**

De belangrijkste en meest vernieuwende eigenschap van RPA is dat het de business zelf in staat stelt om software (robots) te bouwen. Waar voorheen het ontwikkelen van software het exclusieve domein van de IT-functie was, is het voor gebruikers met een minder technische achtergrond aanzienlijk toegankelijker geworden om softwarecode te schrijven. Onder andere zogenaamde 'drag & drop'-functionaliteiten, het opnemen ('screenrecording') van processen en een gebruiksvriendelijke 'user interface' (UI) maken het bouwen van een robot een stuk eenvoudiger. In de praktijk is dan ook zichtbaar dat de meeste RPA-initiatieven vanuit de business beginnen.

Deze verschuiving in kunde resulteert in nieuwe en specifieke RPA-risico's voor organisaties die (veelal meerdere) robots willen implementeren. Werknemers zonder IT-achtergrond zijn nu in staat robots te programmeren. Daar komt bovenop dat uit verschillende, door de big four uitgevoerde, enquêtes (gehouden bij meer dan 150 organisaties) blijkt dat een van de belangrijkste pijnpunten bij de implementatie van RPA is dat de IT- afdeling en de business onvoldoende geïntegreerd zijn. Dit leidt tot grote risico's met potentieel verstrekkende gevolgen als er geen adequate interne beheersing rondom RPA wordt ingericht.

**COBIT: handvatten voor samenwerking**

Het algemeen aanvaarde IT-governanceraamwerk COBIT is erop gericht om 'good-practice'-handvatten te bieden om de samenwerking tussen IT en business effectief in te richten aan de hand van 34 IT-controleprocessen.[1] De vraag is alleen of het implementeren van COBIT nog steeds een voldoende mate van interne beheersing geeft in de context van RPA. Om dit vast te stellen voerde PwC een onderzoek uit (op 08/2018), gericht op het identificeren van RPA-specifieke risico's. Deze risico's zijn vervolgens gerelateerd aan de IT-controleprocessen van COBIT. Hierna worden eerst de risico's kort behandeld en daarna worden deze gerelateerd aan de IT-controleprocessen van COBIT.

***R1 Change management***

Robots maken gebruik van zogenaamde 'selectors' waarin informatie is opgeslagen over een bepaald zichtbaar onderdeel op de UI. De werking is vergelijkbaar met een HTML-code van een website waarin de opbouw en de tekst staat beschreven. Aan de hand van deze selectors kan de robot dus een deel van het scherm identificeren en er een actie op uitvoeren. Dit kan op verschillende applicaties, systemen, internetwebsites, Microsoft Office en alles wat een gebruiker ziet op de UI. Deel van deze identificatie kan de kleur van een button zijn of de geschreven tekst die erop staat. Op het moment dat een of meerdere identificatiekenmerken wijzigen, komt de selector niet meer overeen met de UI en kan de robot de geprogrammeerde acties niet meer uitvoeren.

*De belangrijkste en meest vernieuwende eigenschap van RPA is dat het de business zelf in staat stelt om software (robots) te bouwen*

Een goed werkend change-managementproces is dan ook essentieel, maar tegelijkertijd ook een ware uitdaging bij het opschalen naar meer robots.

***R2 Afhankelijkheid van werknemers***

Een robot bouwen is bij uitstek een combinatie van IT en de business. Waarbij de business vooral de kennis over de te robotiseren processen zal aanleveren en IT zich meer richt op vraagstukken als toegang en het onderhoud van de robots. Robots worden veelal gebruikt om manuele processen te vervangen. Tijdens het opschalen van het aantal robots zal er dus een verschuiving plaatsvinden in verantwoordelijkheid, indien mensen ook daadwerkelijk worden vervangen door robots. Het onderhoud van de robots komt in handen van maar een paar werknemers. Businesscontinuïteit komt dus in het gedrang.

***R3 Systematische fouten***

Waar voorheen een organisatie zich moest bekommeren om menselijke fouten is dit verleden tijd in de wereld van robots. Echter, als robots een fout maken is dit meteen systematisch en kan deze fout zich snel verspreiden door de hele organisatie, aangezien de robots vaak toegang hebben tot (in verbinding staan met) meerdere systemen. De fout is systematisch omdat het in essentie een falende business rule is, die constant wordt herhaald. Ondanks dat COBIT voorschrijft dat organisaties in staat moeten zijn te kunnen reageren op eventuele onverwachte fouten, wordt dit een andere zaak in het geval van RPA. Is een organisatie bijvoorbeeld in staat

om transacties terug te draaien als het om grote volumes gaat? Kan een organisatie traceren welke robot welke fout heeft gemaakt en deze meteen uitzetten?

***R4 Toegang***

In de meeste gevallen zullen robots toegang hebben tot meerdere systemen en werken met verhoogde rechten. Robots maken gebruik van inloggegevens. Met als gevolg dat iedereen die toegang heeft tot de robots ook toegang heeft tot alle systemen in kwestie. Hier komt nog bovenop dat, gezien de selectors zo gevoelig zijn voor de zichtbare elementen op een UI, de robots in de productieomgeving vaak nog aangepast moeten worden. Dat zou betekenen dat iedereen die toegang tot de robots heeft ook inloggegevens heeft tot systemen in de productieomgeving. COBIT adresseert dit punt, maar de implicaties voor RPA zijn verstrekkender omdat de inloggegevens nu ook in handen kunnen komen van iedereen die toegang heeft tot de robots.

***R5 Monitoring***

Omdat robots relatief makkelijk gebouwd kunnen worden en in de organisatie verschillende plekken zijn waar ze van pas kunnen komen, zoals operationele, financiële of andere processen, is het niet ondenkbaar dat ze verspreid door de organisatie beheerd worden. Hoe blijft een organisatie in dit geval in staat om de operationele effectiviteit van de robots te monitoren?

***R6 Kwaliteit van de code***

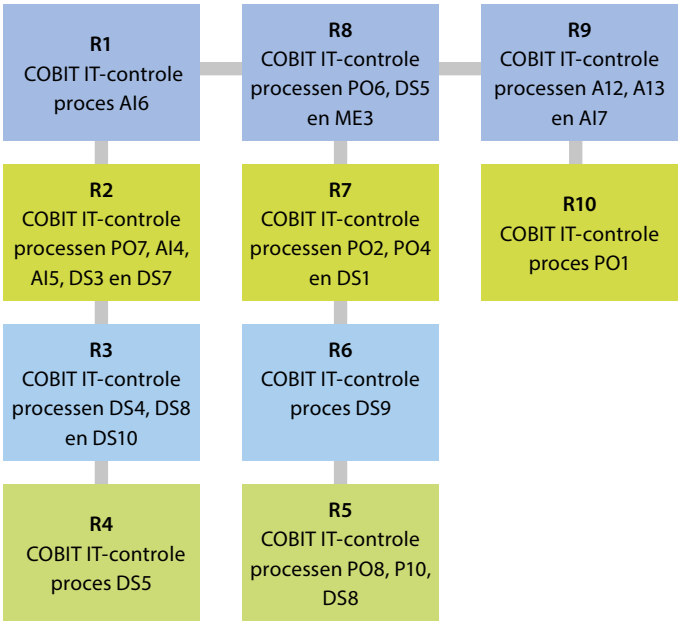
De ene robot is de andere niet. Er is veel keuzevrijheid in het bouwen van robots. Zo kunnen twee robots dezelfde resultaten genereren maar geheel anders zijn gebouwd. Een voorbeeld is dat in de ene robot alle activiteiten betekenisvolle namen hebben gekregen maar in de ander niet. Het ontbreken van naamconventies kan leiden tot moeilijk onderhoudbare robots, aangezien er geen herleidbare structuur is waardoor veranderingen makkelijk doorgevoerd kunnen worden. Kortom, het is essentieel dat ook voor het bouwen van de robots een kwaliteitsstandaard wordt opgelegd die vooral rondom begrippen als flexibiliteit, leesbaarheid, onderhoudbaarheid en betrouwbaarheid duidelijkheid verschaffen.

***R7 Compliance***

De robots kunnen ook te maken hebben met (privacy)-gevoelige informatie. Ondanks dat het robots zijn, betekent dit nog niet dat zij zich niet moeten houden aan bepaalde wet- of regelgeving. Achter de identiteit van een robot gaan personen schuil die verantwoordelijk gesteld moeten kunnen worden. COBIT adresseert dit, maar als er decentraal door de organisatie vele robots actief zijn, hoe weet men dan zeker dat aan alle wet- een regelgeving wordt voldaan?

***R8 Selecteren en prioriteren van robots***

Het selecteren en prioriteren van de juiste robottoepassingen is een kunst op zich. Enerzijds moet door de business rekening gehouden worden met de kwaliteit en continuïteit van het proces door bijvoorbeeld zeker te weten dat het te robotiseren proces gestandaardiseerd is en niet snel gaat


**Figuur 1.** RPA-risico's en COBIT

veranderen. Anderzijds moet er rekening gehouden worden met technische beheersing (bijvoorbeeld onderhoud, updates en authenticatie). Het zo vroeg mogelijk starten van het gesprek tussen IT en de business is essentieel en kan vooral in een later stadium een hoop kosten besparen.

***R9 In productie brengen van robots***

Bijzonder aan de RPA-technologie is dat robots ook gebouwd kunnen worden door niet-programmeurs. Echter, als diezelfde mensen ook de robots in productie brengen of geen adequate testomgeving tot hun beschikking hebben, kan dit verstrekkende gevolgen hebben. Dit wordt geadresseerd in COBIT maar het is een uitdaging voor IT om een testomgeving te bouwen die een exacte replica is van de productieomgeving, aangezien de robots gebruikmaken van de UI en dus ook de verbanden tussen de systemen weten na te bootsen.

***R10 Onduidelijke rollen en verantwoordelijkheden***

Onduidelijkheid rondom de rollen en verantwoordelijkheid aangaande een RPA-programma is iets wat veel voorkomt. Taken die traditioneel bij IT zijn belegd verschuiven naar de business, omdat daar vaak de initiatieven worden ontplooid. Typische rollen rondom het in kaart brengen van de te robotiseren processen zijn bouwen, onderhouden, continuïteit waarborgen en monitoren.

**Risicoanalyse op implementatie**

Als laatste is het belangrijk te onderstrepen dat als onderdeel van COBIT (IT-controle proces PO9) een volledige risicoanalyse moet worden uitgevoerd op, in dit geval, het implementeren van een RPA-programma. Deze analyse zou de RPA-specifieke risico's boven tafel moeten krijgen, zodat de overwegingen en impact op de interne beheersing worden doorgevoerd binnen de verschillende IT-controleprocessen. Echter, uit de ervaring opgedaan door PwC tijdens het auditen van robots (binnen een COBIT context) blijkt dat, omdat RPA nog redelijk onbekend terrein is, de RPA-specifieke risico's onvoldoende geïdentificeerd worden en COBIT dus niet in staat is IT en business dichter bij elkaar te brengen. In *figuur 1* is weergegeven welke RPA-risico's, worden gemitigeerd door de COBIT IT-controleprocessen. De kleuren van de blokken geven aan in welke mate COBIT het betreffende risico mitigeert (groen: volledig, blauw: met kanttekeningen). De verschillende COBIT IT-controleprocessen hebben allemaal een uitgebreide beschrijving omtrent de activiteiten die uitgevoerd dienen te worden en de bijbehorende monitoringactiviteiten. Dit geeft internal auditors de juiste richtlijnen en handvatten om een RPA-audit uit te kunnen voeren met in het achterhoofd de hiervoor genoemde risico's.

Samenvattend is er dus een belangrijke taak toevertrouwd, nu en in de toekomst, aan internal auditors. Waarin de interne beheersing rondom robots essentieel is en de samenwerking tussen IT en de business nog nooit zo belangrijk was. COBIT geeft goede handvatten om dit te bewerkstelligen, maar dient zorgvuldig in het licht van deze nieuwe technologie te worden bestudeerd en aangevuld waar nodig. <<

**Noot**

1. In dit artikel wordt gerefereerd aan COBIT 4.1, aangezien COBIT 5.0 nog niet eenzelfde wijdverspreide dekking heeft in de praktijk.

Steven Boekhoudt MSc werkt als data-analist en auditor bij PwC Assurance. Hij is gespecialiseerd als RPA developer.
steven.boekhoudt@pwc.com

Thema Complexe technologie
Tekst Drs. Nicole Engel-de Groot RA
Jip Olieroock MSc RO CIA
Beeld ESA - S. Corvaja

# Beheersing van de technologie voor een **rondje** om de **aarde**

Bij ESA en ESTEC worden ultiem complexe technologische projecten gerealiseerd in de ruimtevaart. Reden voor *Audit Magazine* om te spreken met Franco Ongaro, directeur Technology, Engineering and Quality en hoofd van ESTEC, over hoe een – in allerlei opzichten – complex project te beheersen.

**Over...**

Franco Ongaro is de director Technology, Engineering and Quality (D/TEC) en hoofd van ESTEC in Noordwijk. Hij verkreeg de titel doctor in de luchtvaarttechnologie in Milaan. Ongaro stond op de shortlist als kandidaat voor de Europese astronautenselectie in 1991.

**Wat doet ESA?**

"ESA staat voor European Space Agency, het Europees ruimtevaart agentschap. ESA is in 1975 ontstaan uit een fusie van het ELDO (European Launcher Development Organisation) en het ESRO (European Space Research Organization). ESA draagt de verantwoordelijkheid voor de ontwikkeling van nieuwe technologieën in de ruimtevaart en bedenkt manieren om deze toe te passen op aarde. Het agentschap werkt voor de overheden van de 22 aangesloten landen. Door de middelen van 22 lidstaten in Europa gezamenlijk in te zetten, kan ESA programma's en activiteiten uitvoeren die geen enkele lidstaat in zijn eentje zou kunnen dragen. Zo lanceert Europa, door middel van ESA, satellieten voor aardobservatie, navigatie, telecommunicatie en astronomie, stuurt sondes naar de verste uithoeken van het zonnestelsel en werkt samen met andere landen om bemande missies mogelijk te maken. We maken geen onderdeel uit van de EU, maar zijn een aparte internationale organisatie. Overigens hebben we wel opdrachten voor de EU gedaan, zoals het bouwen van Galileo (een programma voor satellieten ten behoeve van een navigatiesysteem) en Copernicus (een programma voor aardobservatiesatellieten). ESA is geen bedrijf en heeft dus geen winstoogmerk."

**Welke rol speelt ESTEC hierin?**

"Het European Space Research and Technolgy Centre (ESTEC) voert alle technische projecten van ESA uit. ESTEC levert alle beheersings- en technische competenties om de ontwikkeling van ruimtevaartsystemen mogelijk te maken. We hebben hier in Noordwijk een testcentrum en gespecialiseerde laboratoria om technologie, systemen en componenten voor de ruimtevaart te testen."

**Hoe komen projecten tot stand?**

"ESA conceptualiseert nieuwe ruimtemissies samen met de communities die deze nieuwe missies nodig hebben. Vervolgens presenteert ESA de diverse nieuwe projecten aan de deelnemende landen en kijkt of deze de projecten willen financieren. ESA zorgt vervolgens voor het uitzetten van opdrachten via een aanbesteding aan bedrijven van de financierende lidstaten, waarbij de omvang van de uitgezette opdrachten in verhouding staat tot de financiering die vanuit een bepaald land wordt ontvangen. De lidstaten

bepalen zelf of ze in een missie willen participeren of niet. ESA heeft twee typen programma's, namelijk verplichte en optionele programma's. De afzonderlijke lidstaten dragen financieel bij aan de verplichte programma's naar rato van hun bruto nationaal product. De verplichte programma's omvatten het basis technologische programma en het wetenschappelijke programma. Daarnaast zijn er optionele programma's waarbij lidstaten zelf kunnen bepalen of ze hierin willen investeren. Zo zijn bepaalde landen bijvoorbeeld erg geïnteresseerd in de ontwikkeling van lanceerinstallaties waar andere daarin minder geïnteresseerd zijn. Ontwikkelingen in de ruimtevaart worden nog sterk door de overheden geïnitieerd. Zelfs in Europa, waar toch sprake is van sterk ontwikkelde industrieën, wordt nog circa 60% van de ruimte-innovaties betaald door de overheden. ESTEC heeft tot doel het concentreren en behouden van erg specifieke en dure faciliteiten en kennis en kunde. Alle lidstaten kunnen hiervan gebruikmaken, zodat de betreffende kosten slechts eenmaal gemaakt hoeven te worden. Dit is in het voordeel van de belastingbetalers van de aangesloten overheden."

### Is er een rol voor het bedrijfsleven?

"De voorzieningen die bij ESTEC beschikbaar zijn, zijn vaak zo specifiek dat er in onvoldoende mate een markt voor is. Het gevolg is dat het bedrijfsleven er niet in zal investeren. Denk bijvoorbeeld aan de situatie dat je iets op Mars wil laten rijden. Dan heb je met allemaal uitdagingen en beperkingen te maken die je niet in het dagelijks leven tegenkomt. Dankzij ESA hoeven bedrijven dan niet 'from scratch' te beginnen, maar kunnen ze steunen op ESA. We werken nauw samen met de private sector. De private bedrijven in een land krijgen, in lijn met het aandeel dat door hun lidstaat wordt gefinancierd, projecten toegewezen. De keuze welke partij welke activiteit uitvoert, gebeurt door open aanbesteding. Vervolgens test ESTEC de door de private industrie opgeleverde producten.
ESA is ten opzichte van andere ruimtevaart organisaties uniek op twee gebieden. Ten eerste doet ESA alles ten aanzien van ruimteprogramma's. Andere organisaties, zoals bijvoorbeeld NASA, werken niet aan zaken als navigatie, meteorologie en telecommunicatie. Ten tweede moet ESA verantwoording afleggen aan 22 overheden. Dit leidt ertoe dat besluitvorming soms veel tijd vergt. Dit heeft als voordeel dat wanneer de besluitvorming wordt voorbereid, het werk erg grondig is gedaan."

### Hoe is ESA georganiseerd?

"Zoals gesteld, telt ESA 22 lidstaten. Die zijn allemaal vertegenwoordigd binnen de raad, het hoogste orgaan. De raad geeft opdracht aan de directeur-generaal. Vaak is er echter sprake van een wisselwerking: zo neemt de directeur-generaal niet alleen opdrachten aan, maar benadert hij de raad zelf ook met voorstellen voor nieuwe initiatieven. Ook komt de directeur-generaal met ramingen voor benodigd budget. Voor elk verschillend programma wordt een toezichthoudend orgaan ingesteld, de zogenaamde program board. De verantwoordelijke directoraten voor de programma's leggen verantwoording af aan de program boards via kwartaalrapportages (financiële en operationele voortgang). ESA werkt in de vorm van een matrixorganisatie waarbij zes programma's de verticale as bezetten, en de horizontale as uit vier directies bestaat. De zes program directories zijn Science, Observation, Telecom, Navigation, Launchers en Human Spaceflight and Exploration. De horizontale as bestaat uit Technology, Engineering and Quality (waar ESTEC onder valt), Operations & Quality (waar ESTAC onder valt), Operations, Internal support en External support. Internal support betreft human resource, finance, IT en sites. External support betreft procurement, legal en industry policies."

### Hoe is risicomanagement georganiseerd?

"Risicomanagement is in verschillende lagen georganiseerd. Voor elke nieuwe missie vindt een risicoafweging plaats ter onderbouwing van een akkoord op het niveau van program board. Risico's kunnen van programmatische of technische aard zijn. Op programmaniveau zijn kosten en tijd belangrijke factoren omdat dit de kaders zijn waarbinnen eindproducten moeten worden opgeleverd. Technische risico's zijn vanzelfsprekend cruciaal, die moeten te allen tijde beheerst worden. Als zich technische problemen voordoen kunnen deze direct de realisatie, tijd en kosten beïnvloeden. Daarnaast geldt dat identieke risico's een verschillende impact kunnen hebben op elk projectniveau (wat geen issue is voor het ene project kan een groot probleem zijn voor het andere project) en dat de diverse projecten vaak van elkaar afhankelijk zijn.


ESA–Manuel Pedoussaut, 2017

*"Een belangrijke uitdaging voor mijn directoraat is de competenties van mijn medewerkers te behouden en uit te breiden"*

Op de verschillende niveaus binnen de organisatie worden managers gevraagd de geldende risico's in kaart te brengen. Er ligt altijd een focus op de 'Top-10 risico's'. Het is niet een administratieve exercitie maar een cyclisch proces ter ondersteuning van de besluitvorming."

**Hoe vindt de rapportage plaats?**

"Rapportage over risico's vindt periodiek plaats (afhankelijk van de activiteit) op het niveau van project, directoraat en op het totaalniveau van het agentschap. In de rapportage wordt de conclusie per risico vaak gepresenteerd in de vorm van dashboards met stoplichten.

Projectcontrollers en businessmanagers in de lijn zijn verantwoordelijk voor het risicomanagementproces. Uiteraard ben ik ben zelf verantwoordelijk voor de verschillende risico's van ESTEC en mijn directoraat. Ik bespreek de risico's periodiek in het managementteam. In deze bespreking is ook een verantwoordelijke voor internal audit aanwezig als secretaris. Op corporate niveau (ESA) hebben we een internal audit department (IAD). Daar ligt de verantwoordelijkheid voor de diverse certificeringen van ESA en voor het verrichten van jaarlijkse audits. Audits kunnen betrekking hebben op zowel projecten als afdelingen. Fraude geldt daarbij als specifiek aandachtspunt. De IAD stelt periodiek een auditplan op dat een horizon beslaat van twee á drie jaar. Dit plan wordt goedgekeurd door de board of directors. De financiële verantwoording wordt gecontroleerd door een externe accountant.

Risicomanagement is ingebed in ons programmamanagement. Risicoregisters worden gebruikt om risico's te registreren, ten behoeve van de monitoren en ten behoeve van de follow-up van afgesproken mitigerende maatregelen. Daarbij heeft EY een handboek opgesteld over hoe het risicomanagementproces binnen de organisatie dient te verlopen."

**Hoe worden risico's geïnventariseerd?**

"Risico-inventarisatie vindt meestal bottom-up plaats. Elk directoraat heeft een risicocoördinator aangewezen met twee functies. Allereerst het faciliteren en verzamelen van informatie (risico's) binnen het directoraat, het bundelen van de risico's en het zorgen dat er monitoring plaatsvindt. Ten tweede vormen de risicocoördinatoren samen een netwerk. Zij komen op reguliere basis bijeen, samen met het corporate risk management. Het doel van deze bijeenkomsten is om de risico's van de verschillende directoraten en de impact daarvan op andere directoraten en het agentschap te beoordelen."

**Wat zijn de belangrijkste risico's?**

"Een belangrijke uitdaging voor mijn directoraat is de competenties van mijn medewerkers te behouden en uit te breiden. De komende jaren gaan veel medewerkers met pensioen en we nemen veel nieuwe jonge mensen aan. Hoe zorgen we er nu voor dat het benodigde niveau wordt behouden? Maar ook de installaties binnen de laboratoria zijn een uitdaging. Deze moeten altijd up-to-date en technisch van voldoende niveau zijn om de diverse projecten te kunnen uitvoeren. Een andere uitdaging is funding, bijvoorbeeld voor het pand waarin we zitten. Dit is circa zestig jaar oud en op een gegeven moment zullen de kosten de pan uit gaan rijzen. Daarnaast zijn we een bedrijf met 2800 medewerkers in Nederland dat dus ook de gebruikelijke/meer gangbare bedrijfsrisico's kent. ESTEC is gecertificeerd voor diverse ISO-normen. Het is onze doelstelling  om gecertificeerd te blijven.

Op een hoger niveau is een belangrijke uitdaging het uitzetten van de diverse opdrachten die uit een missie voortkomen. Zoals ik eerder aangaf, krijgen bedrijven binnen landen die missies financieren naar rato opdrachten voor die missie. Dit is een uitdaging op zich, zeker in combinatie met aanbesteding en omdat elk bedrijf wel de capaciteiten voor de opdrachten moet hebben. Een ander voorbeeld is het risico dat deelnemende landen een cashflowprobleem krijgen. Hierdoor kunnen programma's in gevaar komen. Je kunt immers binnen een programma, vanwege afhankelijkheden, niet zomaar bepaalde activiteiten even stilleggen totdat het beter gaat."

**Welk risico is moeilijk of nauwelijks te beheersen?**

"Een heel grote missie van ESA is een robot op Mars te zetten. Het is een project met een groot budget dat we met NASA hebben opgezet. Toen de regering van de Verenigde Staten veranderde, werd vrij plotseling besloten dat de NASA hieruit zou stappen. Echter, we wilden niet stoppen met onze missie. We hebben toen besloten om ermee door te gaan en op zoek te gaan naar een nieuwe partner. Die hebben we gevonden in Rusland. Een dergelijk risico is heel moeilijk om vooraf te beheersen. Het is iets wat je als organisatie overkomt en je dient er op dat moment zo goed mogelijk naar te handelen." <<

Rubriek **Column**
Tekst **Prof.dr. Mark van Twist**

# Technologische vernieuwing: zegeningen tellen maar ook zekerheid bieden

Publieke verantwoording is aan verandering onderhevig door digitalisering en dataficering. Nieuwe vormen van rekenschap dienen zich aan. Denk aan inwoners die vergaderingen van de gemeenteraad live via Twitter van kritisch commentaar voorzien, ondernemers die op Facebook verantwoording vragen over een nieuw kabinetsplan of accountants die via LinkedIn discussiëren met Haagse beleidsmakers over de precieze formuleringen van een voorgenomen wetswijziging.
Met onze laptops, tablets en smartphones kunnen we niet alleen via allerlei websites de kwaliteit van bestuur en dienstverlening recenseren, maar ook zelf met allerlei datasets aan de gang gaan om na te gaan hoe een overheidsinstelling of ondernemingsbestuur opereert – en daar desgewenst ook (publiek) rekenschap over vragen.

Natuurlijk moet je weten waar je zoekt, maar de mogelijkheden zijn er. En het wordt ook steeds gemakkelijker om zelf grote gegevensbestanden te combineren ten behoeve van de publieke verantwoording. Geen wonder dat digitalisering en dataficering vaak worden opgevat als beloftevolle technologische vernieuwingen die gaan zorgen voor toegenomen transparantie. Zozeer zelfs dat de vraag is gesteld of toetsend onderzoek door de auditor langzaamaan niet overbodig aan het worden is. Wat dan evenwel over het hoofd wordt gezien, is dat er ook aan deze technologische ontwikkelingen een keerzijde zit. Het mooist opgetekend is dat nog wel in het boek *Weapons of Math Destruction* van Cathy O'Neil, een dataspecialist verbonden aan Harvard die drie belangrijke kwesties aanvoert met betrekking tot onze nieuwe datagedreven wereld.

Ten eerste: de schijn van objectiviteit. Als we spreken over data hebben we het niet over ondubbelzinnige gegevens, maar over registraties die diep met onze vooronderstellingen en voorkeuren verweven zijn. Om een voorbeeld te noemen, het kan zijn dat de politie meer dieven oppakt op bepaalde plekken in de stad dan op andere, omdat hier toch al vaker wordt gepatrouilleerd door agenten. De 'objectieve' data die dan vervolgens door algoritmes worden opgehoest, bevestigen alleen wat van tevoren al vanuit het eigen politieoptreden te voorspellen viel.

Ten tweede: de schijn van effectiviteit. Wanneer data worden gebruikt als basis voor handelen, kan dat leiden tot zichzelf verwerkelijkende voorspellingen die daarna voor waar worden aangezien. Denk aan de Belastingdienst die op basis van algoritmes besluit om bepaalde groepen intensiever te controleren en hier dan inderdaad meer overtredingen constateert dan bij andere groepen. Is dat nu een bewijs van effectief handelen en een handige omgang met schaarse capaciteit, of juist van een vooraf ingebouwde 'bias' in de data die door eigen optreden wordt waargemaakt?

Ten derde: de schijn van kwaliteit. Mensen weten of leren op den duur altijd hoe ze data kunnen manipuleren en hoe voordeel te behalen valt uit een algoritme dat het verschil tussen succes en falen bepaalt. In mijn academische omgeving geldt de publicatienorm als een bekend voorbeeld, omdat het aantal publicaties eenvoudig is op te voeren door artikelen die eerst in het Nederlands zijn verschenen vervolgens ook nog in het Engels (en Russisch of Chinees) te publiceren en daarna in een boek te verwerken. Een keer hard werken, maar meermaals resultaat. En zo zijn er natuurlijk vele voorbeelden te noemen van 'gaming the system'.

Juist door kwesties als deze zijn en blijven auditors ook in de toekomst hard nodig. Toegenomen transparantie door dataficering en digitalisering kan een zegen zijn, maar ook nieuwe zorgen oproepen. Auditors zijn nodig om op dit punt toetsend onderzoek uit te voeren en waar mogelijk enige aanvullende zekerheid te verschaffen.

Mark van Twist is onder andere hoogleraar bestuurs- en beleidsadvisering op het grensvlak van publiek en privaat aan de Erasmus Universiteit Rotterdam en wetenschappelijk directeur van de IAA-opleiding van de Erasmus School of Accounting & Assurance.

Thema Complexe technologie
Tekst Drs. Huck Chuah RA RO
Matthijs Pouwer MSc
Beeld 123RF®

Het toepassen van nieuwe technologieën zoals robotisering, neemt in hoog tempo toe. Een aantal jaren terug vond dit grotendeels plaats bij logistieke en productiebedrijven, maar tegenwoordig bij alle typen organisaties en afdelingen. Wat zijn de gevolgen van robotisering en wat betekent dit voor internal audit?

# Internal audit en **robotic process automation** (RPA)

# *Wie is verantwoordelijk wanneer er iets fout gaat met de robot?*

Vandaag de dag komen investeringen in geavanceerde technologieën zoals robotic process automation (RPA), artificial intelligence (AI), natural language processing en machine learning steeds vaker voor binnen organisaties. Technologische ontwikkelingen zijn natuurlijk niet nieuw. Er zijn een paar verschillen. Zo kent de introductie van de RPA-technologieën een aantal specifieke voordelen:

1. De leerkosten nemen gestaag af waardoor de kosten significant lager worden en daarmee wordt de businesscase van het investeren in RPA steeds aantrekkelijker. Wanneer je de kosten van een gemiddelde werknemer afzet tegen die van een robot, dan is de investering op dit moment binnen een jaar terugverdiend.
2. De implementatietijd om RPA-technologie te implementeren neemt degressief af: op dit moment kan het robotiseren van een bedrijfsproces al in enkele weken worden volbracht.
3. Het volume van de output is significant hoger: de output (gemeten in hoeveelheden) van een robot is vele malen groter dan wat een gemiddelde medewerker of een afdeling kan produceren.

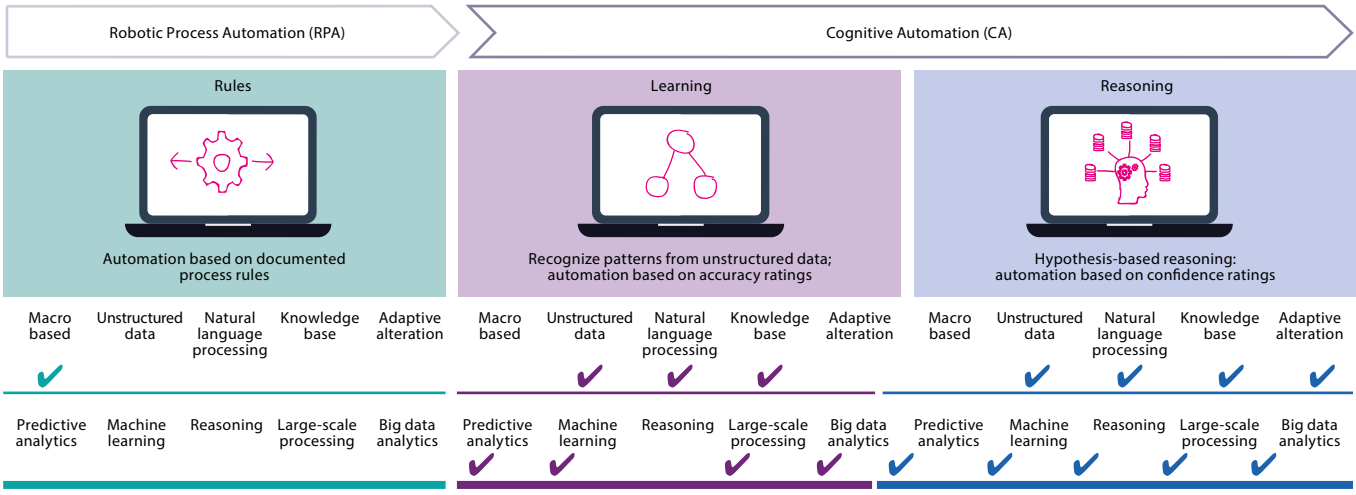
**Hogere controlekwaliteit**

Het uit handen nemen van repeterende werkzaamheden van medewerkers heeft naast kostenvoordelen ook andere voordelen. Het robotiseren van bedrijfsprocessen leidt bijvoorbeeld tot hogere controlekwaliteit, aangezien de robot werkzaamheden altijd in een keer juist verwerkt en geen last heeft van menselijke fouten. Ook op het gebied van compliance en control levert een robot voordelen op. De keuzen die een robot maakt, worden immers altijd gelogd en hiermee kun je de audit trail van begin tot eind goed in kaart brengen. Controles worden geautomatiseerd en de robot voert te allen tijde deze checks uit. Concrete voorbeelden van gerobotiseerde processen op financiële afdelingen zijn: verwerken van facturen in het ERP-systeem, invoeren van journaalboekingen en opstellen van financiële rapportages. Naast RPA zetten veel organisaties de volgende stap in robotisering. Deze volgende stap betreft een vorm van robotisering die meer cognitief van aard is en die in staat is om te werken met ongestructureerde data. Daarnaast komt het lerend vermogen op basis van handelingen uit het verleden om de hoek kijken (zie *figuur 1*). De grote organisaties zijn druk bezig om dit soort capaciteiten toe te voegen aan hun bestaande RPA-oplossingen en de volgende stap te maken in robotisering.

**Impact op internal audit**

Nu duidelijk is wat RPA en robotisering omvatten, komt logischerwijs de vraag naar voren hoe een internal auditfunctie (IAF) dient om te gaan met deze ontwikkelingen. Op basis van onze huidige ervaringen bij diverse organisaties kunnen de volgende vier relevante thema's voor internal audit worden geïdentificeerd:

1. inspelen op risico's ontstaan door de opkomst van RPA;
2. beheersing van risico's rondom robots;
3. auditen van software robots;
4. toepassen van RPA-elementen binnen de internal auditfunctie.




**Figuur 1.** Volwassenheidsfasen van robotisering

***1. Inspelen op risico's ontstaan door de opkomst van RPA***

Wanneer organisaties starten met het implementeren van RPA, krijgen zij al snel te maken met nieuwe risico's. Een van de meest interessante risicovraagstukken op het gebied van robotisering raakt aan de governance en het eigenaarschap van robots.

Vanuit een businessperspectief zal het management de softwarerobot zien als (mogelijke) vervanging of ondersteuning van een normale medewerker. Processen die door robots worden uitgevoerd, zoals het invoeren van journaalboekingen, bevatten vaak processtappen die deels door de robot worden uitgevoerd en deels door de medewerker. Robots worden dusdanig geprogrammeerd dat er sprake is van een interactie tussen de werkzaamheden van de 'objectieve' robot en de meer 'subjectieve' processtappen waarbij een medewerker bijvoorbeeld nog goedkeuring geeft.

Vanuit een governanceperspectief is de business verantwoordelijk voor de primaire processen en voert het continue interactie met de robot. Echter, het robotiseren van bedrijfsprocessen gebeurt door middel van een applicatie. Vanaf het eerste moment dat organisaties aan de slag gaan met robotisering wordt samen gewerkt met de IT-afdeling om deze

zodat functiescheiding in stand blijft? Of is functiescheiding niet meer nodig? Wat betekent robotisering voor interne controles in het proces? Dit is een dilemma waar organisaties, riskfuncties en IAF's mee te maken hebben bij het beheersen van RPA-risico's.

Andere nieuwe risico's hebben betrekking op het ontwikkelen, beheer en onderhoud van de robot en op toegangsbeveiliging. Wanneer de business er voor kiest om nieuwe beheersmaatregelen in te richten voor de robot, ontbreekt vaak kennis van welke (IT-)risico's er spelen. Zowel riskfuncties als IAF's kunnen hier een proactieve rol spelen door vroeg in het implementatietraject mee te kijken naar de

## *Wanneer organisaties starten met nieuwe RPA-technologieën krijgen zij al snel te maken met nieuwe risico's*

nieuwe applicatie te installeren, robot user accounts aan te vragen voor bestaande applicaties en een infrastructuur neer te zetten waarop de robots veilig processen kunnen uitvoeren. Maar dan rijst de vraag wie van deze twee partijen verantwoordelijk is wanneer er iets fout gaat met de robot? Het risico van onduidelijkheid over rollen en verantwoordelijkheden op het gebied van robotisering is een concreet voorbeeld uit de praktijk. Wanneer een robot een verkeerde transactie uitvoert in het ERP-systeem, wie is dan verantwoordelijk voor 'het gedrag' van deze robot en wie kan dit preventief controleren? Wie is eigenaar van de robot? De IAF kan hier proactief een rol spelen in het identificeren en het auditen van risico's.

***2. Beheersing van risico's rondom robots***

Naast de voordelen van onder andere kostenreductie en procesverbetering, brengt het introduceren van RPA uitdagingen met zich mee. Het gebruikmaken van robots roept interessante vragen op het gebied van interne beheersing op, bijvoorbeeld met betrekking tot functiescheiding. In een traditionele financeafdeling stelt een medewerker een factuur op en accordeert een tweede medewerker deze in het systeem. Hierdoor kan functiescheiding en juiste autorisatie worden vastgesteld. Wat is het gevolg als dit proces door een robot wordt uitgevoerd? Dienen er dan twee aparte robots te worden gecreëerd (bijvoorbeeld Robot_01 en Robot_02)

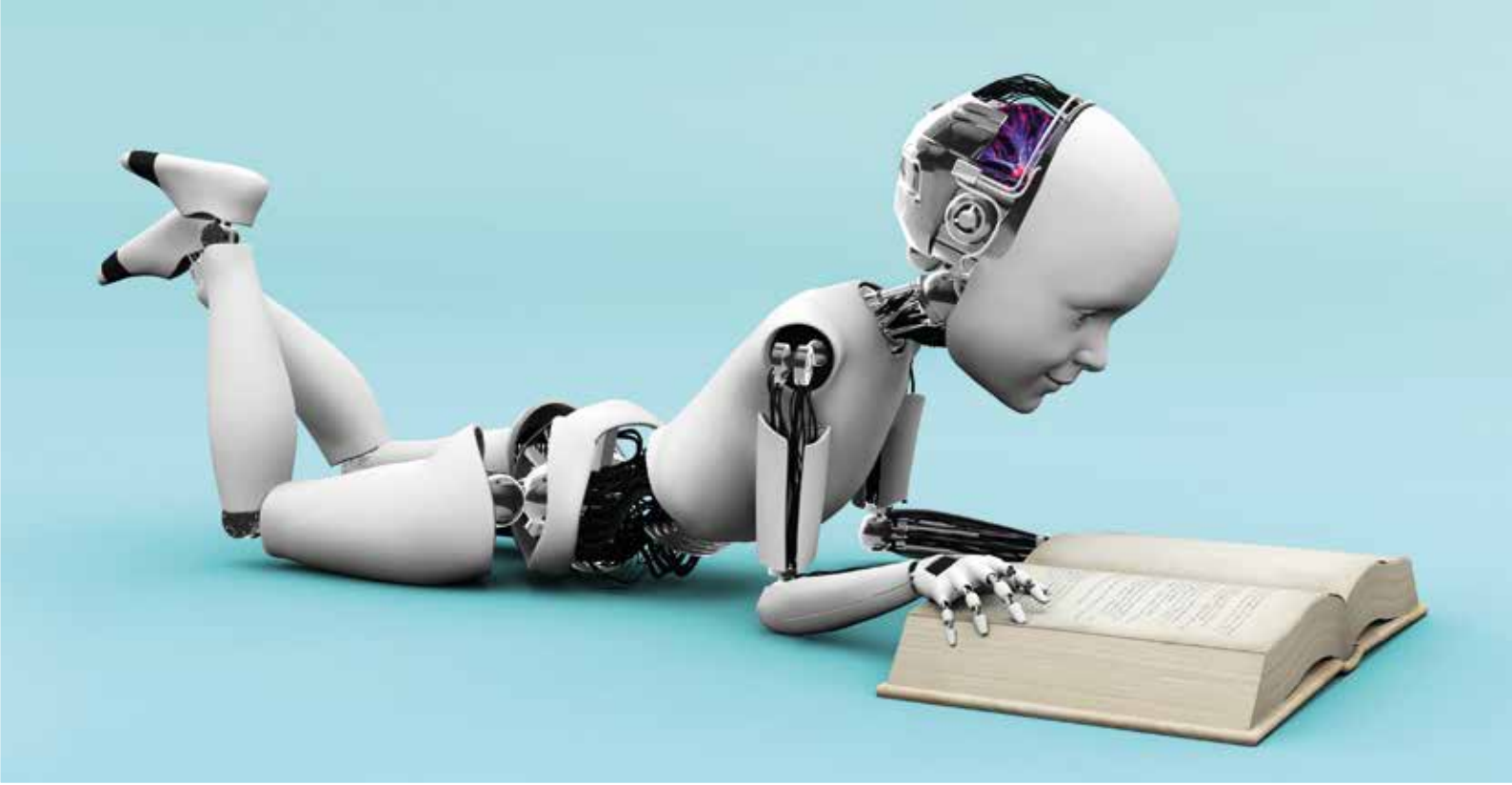
risico-inschatting en de opzet en implementatie van controls voor RPA.

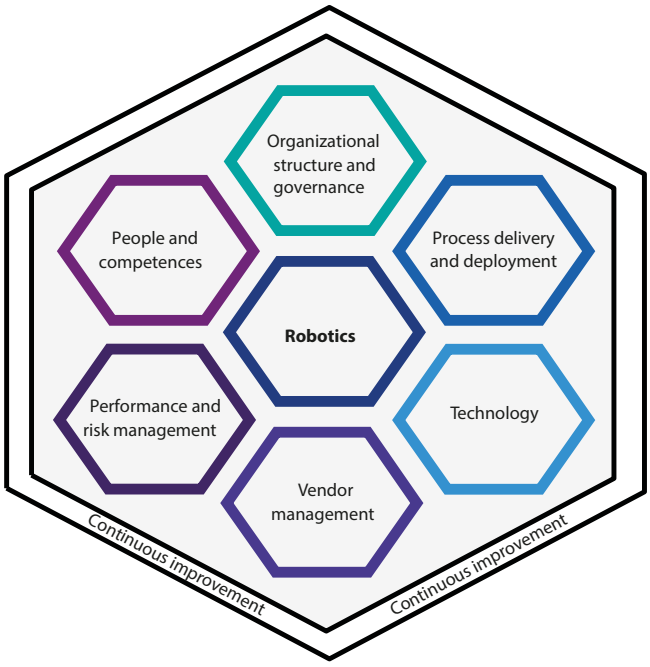
***3. Auditen van software robots***

Nadat veel organisaties zijn gestart met een 'proof of concept' waarin de werking van RPA-technologie wordt aangetoond, komen robots in het vizier van internal auditors zodra deze in een productieomgeving actief worden. Zeker wanneer kritische processen worden uitgevoerd door robots en medewerkers die voorheen het proces uitvoerden niet meer werkzaam zijn bij de organisatie, wordt de vraag of de robot betrouwbaar werkt levert steeds relevanter. Het daadwerkelijk auditen van robots vergt een aanpak die nieuw kan zijn voor IAF's. Specifieke kennis over de roboticsoplossing en van de achterliggende geprogrammeerde code is vereist, alsmede kennis van het gerobotiseerde proces.

***4. Toepassen van RPA-elementen binnen de IAF***

Tot slot kan het toepassen van robotics ook resulteren in kostenreductie, procesefficiëntie en verhoogde kwaliteit binnen de IAF zelf. Uiteraard hangt de toepasbaarheid sterk af van de mate van standaardisatie, beschikbaarheid van IA-tooling en data. Echter, in alle fasen van het internal auditproces bestaan diverse mogelijkheden voor robotisering (bijvoorbeeld risk assessment, planning, testen, rapportages, opvolging & monitoring, dossiervorming, auditmanage-






**Figuur 2.** Het KPMG 6x6 robotics implementatiemodel

ment en administratie). Een logisch voorbeeld hierbij is het toepassen van RPA voor bepaalde testwerkzaamheden met een repetitief karakter.
Met de toegevoegde waarde die RPA levert, kunnen IAF's ook andere voordelen realiseren:

1. verbeteren van de kwaliteit en consistentie van het internal auditproces;
2. verbeteren van de efficiëntie in het plannen, testen en rapporteren waardoor IAF's meer tijd kunnen besteden aan bijvoorbeeld interviews, observaties en analyses;
3. vergroten van de omvang en frequentie van testwerkzaamheden die worden uitgevoerd;
4. vergroten van de audit scope voor individuele audits;
5. inspelen op de capaciteitsvraagstukken en geografische beperkingen binnen IAF's.

Voor het implementeren van robotics bij organisaties gebruikt KPMG het 6x6-model. Het 6x6-model bestaat uit 6 hoofdstukken met ieder 6 paragrafen die relevant zijn bij het succesvol inrichten van robotics. Deze 6 hoofdstukken zijn: Organisatiestructuur & governance, Pijplijn en implementatie, Technologie, Leverancier management, Performance & risicomanagement, Medewerkers en competenties (zie *figuur 2*). Tevens wordt dit framework gebruikt door de IAF voor het inschatten van RPA-specifieke risico's, het inrichten van gerelateerde beheersmaatregelen en het auditen van robots. Het model leent zich ook uitstekend als referentiemodel voor een internal audit.

## Conclusie

Met de komst van nieuwe RPA-technologieën kunnen menselijke vaardigheden steeds vaker worden overgenomen. Het is een kans voor IAF's om in dit stadium een bijdrage te leveren aan het inzichtelijk krijgen wat de specifieke risico's zijn en welke controls en beheersing noodzakelijk zijn. Een volgende stap voor IAF's is om de robots en de gerobotiseerde processen te auditen en om tegelijkertijd na te denken over waar RPA-elementen binnen de IAF zelf kunnen worden toegepast. <<

Huck Chuah is director bij KPMG Internal Audit Services, IIA-bestuurslid en associate program director executive MSc of Internal Auditing aan de UvA.
Matthijs Pouwer is senior consultant bij KPMG op het gebied van robotics & operational excellence.

Rubriek PAS op de plaats
Tekst Raymond Wondergem MSc RO
Beeld 123RF®

# Patricia Michel:

# *"Binnen een kleine IAF heb je echt impact"*

PAS op de plaats is een rubriek waarin auditors van kleine auditdiensten aan het woord komen. Dit keer Patricia Michel, manager Audit bij De Goudse Verzekeringen.

| **Algemene informatie** | |
|---|---|
| Aantal fte organisatie | circa 500 |
| Aantal fte IAD | 4 |
| Rapporteert aan | de voorzitter van het bestuur |

**Kunt u iets vertellen over de Internal Auditfunctie (IAF) van de Goudse?**
"De Goudse Verzekeringen is een familiebedrijf en richt zich met name op mkb-verzekeringen. De Goudse Verzekeringen verkoopt haar verzekeringen via onafhankelijke adviseurs. De IAF bestaat uit vier fte (inclusief mijzelf). Momenteel hebben we een vacature en maken we gebruik van externe inhuur. In mijn team heb ik een onderverdeling in verschillende disciplines (RO/RA/RE). Dit heeft als doel om zoveel mogelijk verschillende audit expertise in mijn team te hebben.
Wij voeren operational, IT-, compliance audits, en incidenteel financial audits uit. Wij doen geen werkzaamheden specifiek voor de jaarrekening. Deze keuze hebben wij expliciet voorgelegd aan het bestuur in een workshop, waarbij we de visie van de IAF hebben bepaald. Natuurlijk werken we wel samen met de externe accountant, waarbij de accountant waar mogelijk gebruikmaakt van onze werkzaamheden. Maar het uitgangspunt is dat we zoveel mogelijk complementair zijn en dat de overlap van werkzaamheden beperkt is. Ten slotte voert de IAF ook incidenteel onderzoeken uit op verzoek van de toezichthouders, zoals de AFM."

**Voeren jullie tweedelijnstaken uit?**
"Natuurlijk vindt er overleg plaats met collega's van de tweede lijn en de samenwerking is goed. We zitten ook op dezelfde afdeling. Verder is er periodiek overleg tussen de sleutelfunctionarissen (tweede en derde lijn) van de verschillende afdelingen om elkaar bij te praten over de verschillende ontwikkelingen. In de basis voert de IAF formeel geen tweedelijnstaken uit, maar soms voeren we wel onderzoeken uit samen met de tweede lijn."

**Met welke uitdagingen krijg je als kleine IAF te maken?**
"Zodra een collega ziek is of uit dienst gaat, merken we dat direct in de planning. Ik heb in de auditplanning wel wat ruimte voor uitval, maar vaak niet genoeg. Ik ga in overleg met het bestuur op welke wijze we het auditplan moeten aanpassen mocht de uitval een grote impact hebben."

**Wat haalt u uit de PAS-commissie?**
"Dit is voor mij op dit moment beperkt, dat komt ook doordat ik lid ben geweest van de PAS-commissie en de Commissie Professional Practices van het IIA. De PAS-bijeenkomsten zijn meestal vrij hoog over en meer gericht op het vergroten van je netwerk. Mijn behoefte ligt op dit moment meer in management-, vaktechnische en sectorspecifieke trainingen."

**Maakt u gebruik van co-sourcing?**
"Soms. Wij huren expertise in op het gebied van technical IT Audit (bijvoorbeeld social engeneering) en actuariële expertise."

**Hoe zorgt u ervoor dat u op de hoogte blijft?**
"Ik haal mijn informatie uit nieuwsbrieven van het IIA, het Verbond van Verzekeraars, DNB, NBA en NOREA. Verder volg ik specialistische en algemene cursussen, zoals bijvoorbeeld de summer course van PwC. Ook ga ik periodiek naar IIA round tables en het Chief Executive Forum. Daarnaast lees ik artikelen over relevante ontwikkelingen."

**Op welke manier vindt kwaliteitsborging plaats?**
"Dit jaar hebben we voor de tweede keer het IIA Certificaat Kwaliteitstoetsing behaald. Vijf jaar geleden waren wij de eerste kleine zelfstandige IAF die dit lukte. Door mijn kennis vanuit de Commissie Professional Practices was ik goed op de hoogte aan welke eisen een IAF moet voldoen vanuit de IPPF-standaarden. Ik ben van mening dat het voor een IAF met een omvang van drie fte goed te doen is om aan de IPPF-standaarden te voldoen. Voor een nog kleinere IAF met een of twee fte is deze uitdaging groter, omdat binnen een IAF verschillende verantwoordelijkheden belegd moeten zijn. Dat is lastiger als de omvang van de IAF beperkt is.

Om de kwaliteit te borgen werken we onder andere met checklists, een kwaliteitsbeleid en voeren we onderling peer reviews uit. Daarnaast zijn er bij de Goudse meerdere RA's werkzaam die, indien noodzakelijk, ook een OKB kunnen uitvoeren."

**Wat maakt het werken in een kleine IAF leuk?**
"Voor mij betekent dit dat ik zowel uitvoerende en aansturende werkzaamheden heb. Die combinatie maakt het voor mij leuk. Daarnaast ben je binnen een kleine IAF breed inzetbaar en richt je je niet op één expertisegebied. Je bent geen klein radartje in een groot geheel, maar hebt echt impact."

**Wat is de ambitie van de IAF op de langere termijn?**
"Voor de langere termijn wil ik het gebruik van tooling en data-analyse vergroten. Verder wil ik de kwaliteit van de oorzaakanalyse verder verbeteren."

**Welke adviezen hebt u voor andere IAF's?**
"Zorg voor een onafhankelijke positionering, dat de basishygiëne op orde is (auditjaarplan, auditcharter, et cetera) en dat medewerkers breed inzetbaar zijn."

## Over...

Drs. Patricia Michel RE is manager Internal Audit bij De Goudse Verzekeringen.

Artikel Vaktechniek
Tekst Sander Diks CIA
Beeld 123RF®

# “Ik zie de auditor in de **toekomst** meer in netwerken **functioneren**”

Sinds 1 juni is Peter Hartog de manager Vaktechniek binnen IIA Nederland. Een nieuwe functie, een nieuw geluid? *Audit Magazine* vroeg het hem.

**Over…**

Peter Hartog is sinds juni 2018 de vaktechnisch manager van IIA Nederland. Daarvoor was hij werkzaam als auditmanager en concern riskmanager binnen de Sociale Verzekeringsbank (SVB) en als consultant voor ACS en KPMG. Hij doceert aan de ESAA.

**Wat houdt deze functie in?**

“Het fijne is dat de functie geen vastomlijnde kaders heeft en dat ik de ruimte heb om te ontdekken hoe we het best invulling aan de functie kunnen geven. Daar ben ik momenteel druk mee bezig. We zijn een vereniging en we stimuleren kennisontwikkeling en kennisdeling van en voor de leden. Veel van wat we doen als IIA en met de diverse commissies heeft een vaktechnisch aspect. De commissie Professional Practices (CPP) richt zich primair op de vaktechniek, daar werk ik dus nauw mee samen. Ik zie mezelf ook als iemand die onderzoeken, visies en ontwikkelingen binnen ons vakgebied beschouwt en deze duidt. Met andere woorden, inzicht geven in de betekenis van ontwikkelingen binnen ons vakgebied, inclusief handvatten en voor- en nadelen voor het vak van internal auditor. Zo was ik laatst bij het seminar van de Young Professionals over het auditen van cultuur en gedrag met bijdragen van experts van KPMG, ACS en DNB. De inzichten die hieruit volgden heb ik vervolgens gekoppeld aan hetgeen corporate antropologe Danielle Braun hierover zei in haar masterclass en aan de inzichten uit de round table van CAE’s over cultuur en gedrag. Mijn toegevoegde waarde zit in het duiden van de overeenkomsten en verschillen van deze verschillende aanvliegroutes om cultuur en gedrag te benaderen.
Het bestuur geeft mij de vrijheid om zelf invulling te geven aan mijn rol. Tegelijkertijd geeft het bestuur al een bepaalde inhoudelijke richting aan mijn functie, omdat zij de strategie van de vereniging en daarnaast de onderwerpen bepalen om het IIA op de kaart te zetten en te houden. Het is een fulltime functie waarbij ik samenwerk met de CPP en met allerlei mensen binnen het IIA. Ik ben de postbus binnen het IIA voor vaktechnische vragen over bijvoorbeeld de standaarden en implementatierichtlijnen en daarnaast houd ik mij bezig met nieuwe ontwikkelingen binnen het vakgebied door ze zelf in gang te zetten, te doen of te begeleiden. Ik zit in het CPP en samen bepalen we welke onderzoeken opgepakt gaan worden. We werken daarin samen met onze partners, universiteiten, studenten en bedrijven.”

*"Je kunt je afvragen of we als auditors nog steeds op de goede manier naar de goede dingen kijken"*

**Wat gaan de IIA-leden merken van de komst van een vaktechnisch manager?**

"Er komen meer berichten aan de leden. Dit zijn berichten met als doel duiding te geven aan rapporten van beroepsverenigingen, toezichthouders en bedrijven, die ons vakgebied raken. Ik doe dit allemaal niet alleen. Veel van de berichten stel ik op samen met de collega's van het IIA-bureau. Verder volgen meer onderzoeken die handvatten zullen bieden voor onze leden. Er speelt momenteel ontzettend veel. *Risk in focus* is een belangrijk rapport dat net is uitgekomen en onze leden handvatten biedt voor de auditjaarplanning. Ook is inmiddels een update verschenen van het Internal Audit Ambition Model.
Een van mijn allereerste wapenfeiten als manager vaktechniek was het updaten van een richtsnoer van het TKT (het toezichtsorgaan kwaliteitstoetsingen). Deze is ontwikkeld om meer richting te geven aan het komen tot een oordeel in de externe kwaliteitstoetsing van de auditfuncties. De input van toetsende organisaties is daarin meegenomen. Dit document is samen met Linda Poort en Hans Nieuwlands van het IIA-bureau tot stand gekomen."

**Welke onderzoeken kunnen we verwachten?**

"Het IIA zegt dat de internal auditfunctie assurance, insight en advies geeft. Assurance en advies zijn vrij helder voor iedereen, hieraan is ook nader invulling gegeven in de Standards. Wat insight betekent is nergens gedefinieerd. Ik wil verder duiden wat we bedoelen met insight. En met name hoe we waarde kunnen toevoegen door het geven van insight. Een ander onderzoek wat ik wil oppakken heeft betrekking op innovatie, een belangrijke topic voor het bestuur. Eerst door te inventariseren wat we moeten verstaan onder innovatie en hoe dat vorm kan worden gegeven. De inventarisatie zal leiden tot een aantal onderwerpen die ik verder ga uitwerken."

*"Innovaties gaan steeds sneller en dat heeft impact op de beheersing van organisaties en dus ook op de manier van auditen"*

**Werk je ook samen met andere beroepsgroepen?**
"Met NBA/LIO werken we actief samen. Met hen stellen we bijvoorbeeld een 90-minutenpitch op om aan studenten binnen die tijd te vertellen wat het vak inhoudt. Verder heb ik gesprekken gehad met NOREA maar doen we met hen concreet nog te weinig. Dit is wellicht opvallend want het belang van IT wordt steeds belangrijker. De intentie is er zeker om samen te werken. Wel werken we al samen met het ISACA. We hebben hen meegeholpen om hun congres te organiseren. En we werken Europees samen in de European Institute Research Group. Dit is een groep van IIA's uit zeven landen (waaronder IIA Nederland) die samen onderzoek doen. We wisselen uit waar we mee bezig zijn en hebben net gezamenlijk het rapport *Risk in focus* uitgebracht."

**Is de auditor voldoende voorbereid op complexe technologie?**
"Ik vraag het mij af. Dat zal zeker niet zo zijn voor de gehele beroepsgroep. Innovaties gaan steeds sneller en dat heeft impact op de beheersing van organisaties en dus ook op de manier van auditen. Je kunt je afvragen of we als auditors nog steeds op de goede manier naar de goede dingen kijken. Zijn de traditionele opvattingen van goede governance, risk en control processen nog wel passend? Met andere woorden, kijken we nog wel met een goed normenkader? Agile werken gaat bijvoorbeeld vaak samen met besluitvorming op een lager niveau in de organisatie. Dit heeft impact op risicobeheersing en governance. En het heeft ook consequenties voor de auditor op het gebied van zowel kennis als vaardigheden. Minder dingen staan op papier, auditbewijs zal vaker op basis van interviews en observaties verzameld dienen te worden. En het is belangrijk om op zijn minst basiskennis te hebben van IT. Je hoeft niet allemaal IT-auditor te worden, je kunt IT-processen ook vanuit een operational audit benaderen. Maar als het gaat om specifieke technische kennis en bijvoorbeeld kennis op het gebied van hacking, dan schiet je kennis als auditor al snel te kort. De technologie ontwikkelt zich razendsnel, dus de vraag is of je deze kennis zelf moet hebben of dat het efficiënter is om gebruik te maken van kennis van derden. Ik zie de auditor in de toekomst meer in netwerken functioneren omdat het belangrijker wordt om te beschikken over kennis die steeds specialistischer is. Daarnaast is er meer behoefte aan assurance over de keten of het netwerk, waardoor het nodig is samen te werken met partners buiten de eigen organisatie."

**Hoe ziet het vakgebied er over tien jaar uit?**
"Het leuke én vervelende is dat dé auditfunctie niet bestaat. Je kunt de auditor zien als iemand die assurance geeft door het geven van een oordeel, maar je kunt de auditor ook zien als iemand die verbeteringen initieert. Er zijn binnen Nederland auditfuncties die relatief sterk 'georiënteerd zijn' op de RvC en daarmee relatief sterk een toezichthoudende rol hebben, en auditfuncties die vooral een ondersteunende rol hebben voor de RvB en het management. Het is mogelijk dat enkele IAF's, mede door de diverse schandalen, opschuiven naar een versterkte rapportagelijn aan de RvC. Tegelijkertijd zie ik in het vakgebied, sterk gestimuleerd vanuit IIA Global, veel aandacht voor het vergroten van onze toegevoegde waarde, ook in relatie tot de strategische risico's van de organisatie.
Ik zou het mooi vinden als de auditfunctie tegen die tijd een meer geaccepteerde, 'natuurlijke' functie is dan het nu is. Ondanks dat we nu genoemd worden in de Corporate Governance Code zijn we er nog lang niet. Ik sprak een advocaat die zei dat je er pas toe doet als er in het geval van een schandaal met de vinger naar je wordt gewezen. Nu wordt in de publiciteit de vinger vaak direct gewezen naar de extern accountant, maar niemand lijkt zich af te vragen waar internal audit was. We zijn nu zover dat het nut en de noodzaak breed worden erkend, maar daarmee zijn we nog geen vanzelfsprekendheid." <<

# Rondom het kampvuur

Heel wat jaren geleden stond ik met mijn gezin op een camping in Zuidelijk Afrika. Op een dag zagen wij een lange rij auto's met grote caravans het terrein oprijden. Tot onze verbazing werden deze caravans en 'bakkies' in een cirkel neergezet en werd in het midden een lange paal geplaatst. Bovenaan die paal prijkte de oude Zuid-Afrikaanse vlag. Ik moest toen denken aan de verhalen uit het wilde westen, waarin de kolonisten uit veiligheid zich ook in cirkels opstelden. Het verraste ons dat de Afrikaanders zich op deze manier nog steeds veilig voelen. Overigens is die veiligheid wel eenzijdig. Wij konden geen contact met ze krijgen, immers wij bevonden ons niet in hun cirkel…

Het boek *Circulair leiderschap* refereert aan de veiligheid van een cirkelopstelling en gebruikt onder andere het beeld van het kampvuur. Het kampvuur waar iedereen omheen zit en waar het prettig toeven is als er een goed gesprek gevoerd gaat worden. Het centrale vuur is immers een mooie plek om naar te kijken en niemand vindt het gek dat je de anderen niet aankijkt, maar 'naar het vuur' praat.

De 'cirkel way', zoals de methode in Amerika heet, is een vaste methodiek waarin alle stoelen in de ruimte in een cirkel worden gezet. In het midden wordt een centraal element geplaatst wat representatief is voor de groep deelnemers. Dat mag van alles zijn. Een zak met geld (bijvoorbeeld voor accountmanagers), een brandende kaars, wat dan ook. Er zijn drie vaste rollen die iedere deelnemer in principe kan innemen. De gastheer, de procesbewaker en de schrijver. De personen die deze rollen vervullen zitten ieder op een derde van de cirkel (respectievelijk op vier, acht en twaalf uur). Op deze manier is contact goed mogelijk en is er balans.
De gastheer leidt het gesprek door vragen te stellen, de groep te helpen zich aan de afspraken te houden en de intentie in het oog te houden. De procesbewaker mag de bel luiden. Die metafoor is belangrijk. De bel wordt geluid als het gesprek uit focus dreigt te gaan. De eerste keer om stilte te vragen en de tweede keer, zo'n tien tot twintig seconden later, om weer verder te kunnen gaan. Iedereen mag vragen om de bel te luiden. De stilte is belangrijk en na de tweede bel volgt altijd een uitleg waarom de pauze is gevraagd. De schrijver heeft als rol de gemaakte afspraken, uitkomsten, conclusies op te schrijven, om zo als geheugen van de groep te dienen.

Hoewel deze beschrijving absoluut onvoldoende is om de grote hoeveelheid voorbeelden en uitvoeringen die het boek biedt weer te geven, is dit wel de essentie van de circle way: een gelijkwaardig, rustig en gefocust gesprek aangaan, waarbij niet via de voorzitter wordt gewerkt maar via de kern. Meer persoonlijk, veelal veiliger en vaak met meer diepgang dan een gewone vergadering. Het is daarom voorstelbaar dat een organisatie die deze werkvorm toepast zich ook aanpast, meer de menselijke maat gaat hanteren en meer gelijkwaardig wordt (er is immers niet echt een voorzitter aan het hoofd van de tafel). In dat proces helpen de drie geformuleerde principes ook: leiderschap roteert, verantwoordelijkheid wordt gedeeld en het groepsbelang staat centraal.

In de metafoor 'rondom het kampvuur' om groepsgesprekken met meer gelijkwaardigheid, diepgang en veiligheid te laten verlopen zit wel wat. Of je het echt kunt leren door dit boek te lezen, vraag ik me af. Daarvoor ervaar ik het boek te veel als verslagen van in het verleden behaalde successen. Iets te veel geschreven door een fan en met iets te veel 'amerikanismen' in de vertaling.


**Circulair Leiderschap**
Ann Linnea en Christina Baldwin
Innervida
ISBN 9789090294964
€ 24,95

Renze Klamer is agile-coach en Semco-consultant bij Bijenco en werkt als zelfstandig agile-coach voor verschillende organisaties. Klamer is daarnaast kerndocent bij de agile-coachopleiding van Bijenco.

Artikel Cyberrisico's
Tekst Mr.drs. Pieter Steenwijk
Beeld 123RF®

De cyberrevolutie is onverbiddelijk en voltrekt zich in hoog tempo. Dit artikel zet de relevantie van cyberrisico's en een handzame aanpak voor de beheersing ervan uiteen.

# Stairway to digital heaven

De digitale revolutie voltrekt zich in hoog tempo. Naar verwachting zullen er in 2020 meer dan 20 miljard laptops, mobiele telefoons en tablets met elkaar verbonden zijn tot een gigantisch wereldwijd netwerk. Spoedig zullen we voortdurend en overal verbonden zijn met internet. De virtuele ruimte die ontstaat uit de complexe interactie van mensen, technologie, software, en dienstverlening over het internet wordt steeds vaker cyberspace genoemd.[1]

**Onbeperkte kansen**

Nederland is een koploper in het gebruik van mobiele apparaten, internetaankopen en het benutten van online-diensten.[2] De cybersamenleving biedt onbeperkte kansen, nieuwe manieren van communiceren, leren, werken, gamen en carrièremogelijkheden. Bedrijven kunnen hun productiviteit, concurrentievermogen en zichtbaarheid vergroten door op een verstandige manier gebruik te maken van cyberkansen. Daar tegenover staan grote risico's zoals cyberpesten, grooming (online sexueel misbruik van minderjarigen), online diefstal en bedrog, het doorspelen van vertrouwelijke informatie door corrupte agenten en het faciliteren van van terrorisme en witwassen.

Vrijwel alle grote bedrijven hebben de afgelopen jaren te maken gehad met online aanvallen, virussen, datalekken en digitale afpersing. De kosten van deze inbreuken op de digitale integriteit namen de afgelopen jaren fors toe en bedragen in Nederland jaarlijks ongeveer 10 miljard euro.[3] Dit verklaart ook waarom cyber risk het grootste auditrisico voor internal auditors is geworden.[4]

**Effectief beheersen is strategische noodzaak**

De cyberrevolutie valt niet te stoppen. Organisaties zullen steeds meer afhankelijk worden van online dienstverlening en hun netwerken zullen steeds verder integreren. Het effectief beheersen van de digitale kansen en risico's is daarmee een strategische noodzaak geworden. Stakeholders verwachten dat bedrijven passende maatregelen nemen om hun online activiteiten te beschermen en digitale bedreigingen serieus nemen. Er staat ook veel op het spel bij digitaal mismanagement: reputatieverlies, het missen van kansen in de markt, complianceproblemen met overheden en toezichthouders, verlies van data en intellectueel eigendom en tenslotte verslechtering van de relaties met stakeholders.

Het Institute of Risk Management (IRM) definieert cyber risk als: 'Any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems'.[5] Het IRM onderscheidt vijf verschillende dreigingsactoren die de motor vormen achter cyberrisico's:

1. *activisten* (ook wel hacktivisten genoemd) die vooral ideologisch of politiek zijn gemotiveerd;
2. *cybercriminelen* die organisaties en bedrijven aanvallen om er financieel beter van te worden;
3. *vijandige spionnen* ('hostile spies') die worden aangestuurd door buitenlandse regeringen;
4. *insiders,* eigen medewerkers die bewust of onbewust om verschillende redenen fouten maken of bewust schade aanrichten;
5. *slechte IT-systemen* die door ontwerpfouten, verouderde software, onvoldoende support etc. de organisatie kwetsbaar maken voor dreigingsactoren.[6]

In de traditionele benadering werd het beheersen van cyberrisico's beschouwd als een technisch vraagstuk dat thuishoort bij de IT-afdeling. Deze benadering is inmiddels achterhaald. Volgens de gangbare opvatting kunnen cyberrisico's het best worden beheerst binnen het raamwerk van de organisatiebrede enterprise risk (ERM) raamwerk.[7]

**Onzekerheid voor organisaties**

Zo op het oog heeft cyber risk management (CRM) ook veel gemeen met andere vormen van riskmanagement op het gebied van IT, data security en privacy. Maar CRM onderscheidt zich van andere risicodisciplines door een aantal specifieke kenmerken. In de eerste plaats verandert de technologie voortdurend en in hoog tempo. Dit heeft grote impact op de strategie en de doelstellingen van organisaties. De dynamiek van de technologische ontwikkelingen creëert veel onzekerheid voor organisaties. Wanneer is het verstandig om een nieuwe technologie over te nemen, welke kansen biedt het en welke risico's zijn eraan verbonden? Daarnaast zijn er risico's met zeer grote impact op de organisatie, waarvan het zo goed als onmogelijk is om ze tijdig te voorzien dan wel een zinvolle inschatting van de kans van optreden te kunnen maken.[8] Deze 'black-swan'risico's kunnen gemakkelijk over het hoofd worden gezien of worden gebagatelliseerd als gevolg van misplaatst vertrouwen in de eigen beheersingsmaatregelen.
Ten slotte heeft de digitale revolutie ervoor gezorgd dat de grens tussen privé en werk allengs aan het vervagen is. Medewerkers werken steeds meer met hun eigen tablets en mobiele telefoons, of gebruiken de zakelijke IT-voorzieningen ook voor persoonlijke doeleinden (filmpje downloaden, chatten, et cetera). Het voordeel voor de organisatie is dat medewerkers flexibeler kunnen worden ingezet, buiten werktijd bereikbaar zijn en op een natuurlijke wijze vertrouwd raken met nieuwe technologie. De keerzijde is dat al dat gechat en het gebruik van eigen apparatuur ook veiligheidsrisico's met zich mee kan brengen.

**Hoog op de corporate agenda**

Door de combinatie van snelle technologische, stijgende kosten van cybercrime en de bescherming tegen langetermijnreputatieschade staat cyberrisicomanagement hoog op de corporate agenda. Na compliance is kwetsbaarheid voor cyberaanvallen het belangrijkste zorgpunt voor raden van bestuur in de financiële sector.[9] Veel organisaties, overheden en toezichthouders worstelen echter met de vraag op welke manier de risico's en de kansen op een evenwichtige wijze kunnen worden

**NIST CYBER SECURITY FRAMEWORK**

| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Asset management | Access control | Anomalies & events | Response planning | Recovery planning |
| Business environment | Awareness & training | Security continuous monitoring | Communications | Improvements |
| Governance | Data security | Detection processes | Analysis | Communications |
| Risk management | Info protection process & procedures | | Mitigation | |
| Risk management strategy | Maintenance | | Improvement | |
| | Protective technology | | | |

**Figuur 1.** NIST cyber security framework

afgewogen. In Nederland ontbreekt het bij de meerderheid van de bedrijven aan een solide, overkoepelende cyberrisicostrategie en is de board onzeker over de effectiviteit van de investeringen in technologische beheersmaatregelen. Ook in de publicatie *Cybersecuritybeeld Nederland* wordt met zorg geconstateerd dat het gat tussen cyberdreiging en weerbaarheid is gegroeid en de digitale kwetsbaarheid ondanks alle inspanningen over de gehele linie is toegenomen.

**Top-7 verstandige algemene randvoorwaarden**

Bedrijven bevinden zich tussen de Scylla en Charibdes van de online revolutie. Wie niet bereid is om alle technologie overboord te gooien, moet op zoek naar een passende vorm van cyberrisicomanagement. Naast de standaardsystemen zijn er talrijke tools, checklisten, stappenplannen, technische systemen, handige vragenlijsten, quick reference cards en specifieke diensten van advieskantoren beschikbaar. Uit dit aanbod kan een Top-7 van verstandige algemene randvoorwaarden voor effectief cyberrisicomanagement worden afgeleid.

1. Bepaal de cyber risk en opportunity appetite van de organisatie en communiceer het daaruit voortvloeiende risicoprofiel op maat met in- en externe stakeholders.
2. Maak een lijst met de bedrijfsmiddelen die de grootste toegevoegde waarde voor online activiteiten hebben en hun kwetsbaarheid voor cyberdreigingen.
3. Identificeer en implementeer basale beheersmaatregelen. Dit voorkomt tot 85% van alle cyberaanvallen.
4. Investeer zowel in preventieve beheersing maar ook in robuuste incident response procedures (IRP) om reputatieschade te voorkomen.
5. Ken de oorzaken en kwetsbaarheden van cyberrisico's en identificeer de kosten-opbrengsteneffecten van beheersingsmaatregelen.
6. Besteed voldoende aandacht aan de menselijke aspecten, zoals de risicopercepties van in- en externe stakeholders. De effectiviteit van technische controls (firewalls, encryptie, et cetera) wordt medebepaald door acceptatie en het bewustzijn van gebruikers.
7. Beheers cyberrisico's vanuit het overkoepelende risk management en niet stand-alone.

**ERM of stand-alone?**

Schade door cyberrisico kan gemakkelijk uitwaaieren buiten de directe operationele en financiële impact. Een geslaagde hackoperatie kan uiteindelijk de reputatie van een bedrijf voor jaren aantasten, klanten wegjagen en een wezenlijk gevaar voor de continuiteit teweegbrengen. Juist omdat cyberrisico's gemakkelijk kunnen cascaderen naar andere enterprise-riskcategorieën is het effectiever en goedkoper om ze te beheersen als onderdeel van het brede enterprise riskmanagement. De belangrijkste risicostandaarden hebben cyber in hun algemene riskfocus opgenomen. Zowel COSO, COBIT als IRM hebben leidraden en algemene adviezen gepubliceerd die

organisaties kunnen helpen om het management van cyberrisico's op een lijn te brengen met de eigen standaard. ISO Standaard 27032-IEC-2012 bevat een aantal uitgangspunten en richtlijnen voor het beheersen van cyberrisico's. In tegenstelling tot ISO 27001-IEC voor information security management (ISMS) leidt invoering van de cyber securitystandaard niet tot certificering. ISO 27001 (met een uitgebreide catalogus van controlmaatregelen) en ISO-IEC 27032 (met een specifieke lijst van bedrijfsmiddelen met focus op cyber risk en incident response) in combinatie met de algemene van 27005 is een bewerkelijke, maar interessante optie.

**NIST cybersecurity framework**

Voor wie liever een op cyber risk toegesneden raamwerk prefereert, is er het NIST cybersecurity framework (NIST CF) dat in 2014 ontwikkeld is om de vitale infrastructuur van de Verenigde Staten te beschermen tegen cyberdreigingen (zie *figuur 1*).

NIST bestaat uit drie onderdelen, te weten 1) de kern, 2) de implementatieniveaus, 3) profiel.

1. Kern: de kern bestaat uit de vijf functies (identificeren-beschermen-detecteren-respond-recover) waarmee de cyberrisico's worden beheerst. De functies zijn onderverdeeld in 22 activiteiten (assetmanagement, data security, response planning, et cetera) die de ruggengraat van een solide cyber riskmanagementsysteem vormen. De activiteiten kunnen worden opgedeeld in subactiviteiten. De subactiviteiten zijn weer opgedeeld in best practices, standaarden en richtlijnen gebaseerd op COBIT, ISO 2700, ISA 62443, et cetera.
2. Implementatie: implemenatie gebeurt in een iteratief proces waarin de 'isst en soll' centraal staan. Het model onderscheidt vier fasen (partieel, risk informed, repetetief en adaptief) voor het markeren van de huidige situatie en het formuleren van het ambitieniveau.
3. Profiel: waarin cyberstrategie, risk appetite en governance samenvallen en fungeert als monitorings, plannings, en communicatie-instrument.

NIST is een overzichtelijk, holistisch, technologisch onafhankelijke aanpak op basis van best practices en andere standaarden. Het volgt de ERM-benadering en is bruikbaar voor elke organisatie, ongeacht sector of omvang. Het is een flexibele, kosteneffectieve benadering die naast – en dus niet in plaats van – de bestaande risicobenadering wordt ingezet. Op de website worden best practices, casestudies, en algemene adviezen gedeeld. In de Verenigde Staten is NIST aan een indrukwekkende opmars bezig. Naar verwachting zal de helft van alle bedrijven in de Verenigde Staten op termijn de aanpak toepassen.

**Conclusie**

De toekomst is digitaal. De komende jaren zullen het internet of things, het gebruik van social media en de uitbreiding van oplossingen in de cloud de bestaande businessmodellen en risicopercepties ingrijpend op de proef stellen. De enige manier om digitale risico's volledig te neutraliseren is door alle online activiteiten stop te zetten. Zoals Bill Gates al een decennium geleden in Davos opmerkte; "In de 21e eeuw zullen er slechts twee typen bedrijven zijn, bedrijven die op internet zitten en bedrijven die het loodje zullen leggen". Voor riskmanagers en auditors ligt er de nobele taak om te kijken op welke wijze cyberrisicomanagement effectief kan worden ondergebracht binnen de overkoepelende benadering van de organisatie. <<

*De enige manier om digitale risico's volledig te neutraliseren is door alle online activiteiten stop te zetten*

**Noten**

1. https://www.iso.org/standard/44375.html
2. https://tweakers.net/nieuws/97212/google-nederland-heeft-hoogste-tablet-en-laptopgebruik.html
3. Deloitte, *Cyber Value at risk in the Netherlands 2017,* 2017.
4. KPMG, Top 10 Internal Audit Considerations, 2017. https://home.kpmg.com/nl/nl/home/insights/2017/01/top-10-internal-audit-considerations.html
5. Institute of Risk Management, Cyber Risk, 2014. www./.theirm.org/media88344/final_IRM_Cyber_Risk-Executive Summary_A5_low-res.pdf
6. Zie onder meer: https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf.
7. Zie onder meer: Philpott, D. en S. Ganz, *FISMA and the Risk Management Framework: The new practice of federal cyber security,* Syngress Media, 2012.
8. Zie: Taleb N.N., *The black swan: The impact of the highly improbable.* Random House, 2007.
9. Deloitte, *2016 Financial Servics Survey*, 2016.

Pieter Steenwijk is jurist en bedrijfskundige en is docent risicomanagement. Hij doet onderzoek naar witwassen en terrorismefinanciering aan de The Hague School of Applied Sciences en is promovendus aan de Universiteit van Maastricht.

# Intelligentie:

## sociaal, emotioneel, kunstmatig?

De meesten van ons vinden zichzelf intelligent, waarschijnlijk terecht. We hebben overigens de neiging onze eigen intelligentie iets hoger in te schatten dan die van de ander – het zij zo. Maar wat is intelligentie eigenlijk? En wat houdt sociale, emotionele en kunstmatige intelligentie in?

Intelligentie bestaat eigenlijk niet. Het is, wat psychologen noemen, een *construct*, een samenstelling van diverse factoren, die uiteindelijk uitmonden in het intelligentiequotiënt. Het IQ is betrouwbaar en valide te meten. Een operationele definitie van intelligentie is dan ook dat intelligentie datgene is wat de intelligentietest meet. Het IQ volgt overigens een standaardnormale verdeling, we herinneren ons nog: de Gauss Kromme. Intelligentie is sterk genetisch bepaald en is relatief stabiel in de tijd.

In de tweede helft van de vorige eeuw realiseerde men zich – met name in managementkringen – dat intelligentie weliswaar een noodzakelijke, maar geen voldoende voorwaarde is voor professioneel functioneren op een hoger niveau. Op dat niveau is intelligentie dan ook nauwelijks meer onderscheidend. Met intelligentie alleen redt men het niet, meer en meer worden dan intermenselijke, sociale managementcompetenties gevraagd.

Eind jaren negentig kwam de wetenschapsjournalist Goleman dan ook op het slimme idee om een bijzonder succesvol boek in de markt te zetten, met de titel *Emotional intelligence*, waarop hij een paar jaar later nog de publicatie *Social intelligence* liet volgen. Een gat in de markt. Eindelijk aandacht voor medemenselijkheid! Origineel kan men de auteur echter niet bepaald noemen. Reeds eind jaren twintig werd het begrip social intelligence geïntroduceerd en omschreven als het vermogen om met mensen om te gaan.

Een duidelijk onderscheid tussen de termen emotionele en sociale intelligentie is er overigens niet echt. Volgens Goleman focust het een meer op het individu en het ander op interpersoonlijke betrekkingen. Inhoudelijk zijn het beide echte kapstokbegrippen, en dan gaat het om een reusachtige kapstok. Wat valt er *niet* onder? Wij vinden daar alles wat sociaal wenselijk is op de werkvloer. Ik noem een aantal factoren en ik beperk me extreem: luistervaardigheid, nieuwsgierigheid, verbaal vermogen, empathie, authenticiteit, introspectie, goed met kritiek kunnen omgaan, et cetera. Hiervoor zijn uiteraard ook diverse tests ontwikkeld, sommige ervan van het 'test-uzelfprincipe'. De wetenschap laat weinig heel van het succes van Goleman. Zoals gezegd wordt er bij hem vooral verwezen naar morele kwaliteiten en niet naar skills. Er worden geen competenties gemeten, maar vooral conformiteit en sociale wenselijkheid. De bijbehorende tests hebben nauwelijks of geen predictieve waarde.

Zijn zaken als authenticiteit, introspectie en empathie dan niet meer actueel? Integendeel. Ze zijn actueler dan ooit. Maar we hebben er Goleman niet voor nodig. Er bestaan betrouwbare en valide meetinstrumenten voor, ook binnen het Nederlands taalgebied.

Naast, of tegenover, de intelligente mens staat de intelligente machine (artificial intelligence, AI) gevoed door eindeloze stromen big data waardoor zij ook zelf kan leren. Met haar schat aan cognitieve functies formuleert zij algoritmes en speelt zij in ons dagelijks leven reeds een onmisbare rol bij techindustrieën als automotive, in de gezondheidszorg, maar ook bij schaken en vertalen. AI komt voort uit continue, creatieve vormen van samenwerking tussen information engineers, mathematici, psychologen, neurowetenschappers en zo meer.

AI triggert nogal wat emoties. Doemdenkers vrezen massale werkeloosheid en het einde van de democratie. Optimisten – of realisten? – zien onbegrensde mogelijkheden op gebieden als onder andere klimaatbeheersing, gezondheidszorg, voeding en robotica. Zal AI de menselijke intelligentie op termijn vervangen? Op beperkte schaal is dit al het geval. Authenticiteit, introspectie en empathie echter zijn bij dit proces menselijke kwaliteiten die meer dan ooit relevant zijn.

Michael M.Tophoff is klinisch psycholoog en doceert Personal Skills aan de Business School van de UvA (EMIA).

Artikel Interview
Tekst Sander Diks CIA
Raymond Wondergem MSc RO

# "Mijn **missie** is om van elk **event** een **succes** te maken"

Een kijkje achter de schermen bij Annemiek van Raalten, eventmanager bij IIA Nederland. Wat doet een eventmanager bij IIA Nederland precies en welke ontwikkeling maakte de functie de afgelopen jaren door?

**Over...**

Annemiek van Raalten is sinds 2014 eventmanager bij het IIA. Daarvoor werkte ze als opleidingsmanager bij Hogeschool van Amsterdam, HES Amsterdam, Markus Verbeek Praehep en bij verschillende Rabobanken en Deloitte.

**Hoe ben je bij het IIA terechtgekomen?**

"Ik was freelancer en niet op zoek naar een baan. Ik kreeg de tip dat bij het Instituut van Internal Auditors de vacature van eventmanager openstond. Ik heb contact opgenomen met Michel Vlak en daarna ging het snel. Ik heb gesprekken gehad met Michel Vlak, Huck Chuah en Hans Nieuwlands. Twee weken later was ik aangenomen en in april 2014 ben ik begonnen. Ik had direct mijn vuurdoop toen ik op de ALV bij de ING werd voorgesteld aan de ongeveer tachtig leden die daar waren. Ik was destijds, naast Hans Nieuwlands, de eerste werknemer van IIA Nederland. Ik zat bij Hans op de kamer en hierdoor kon hij zijn kennis en netwerk dagelijks met mij delen."

**Wat zijn je belangrijkste taken als eventmanager?**

"IIA Nederland heeft voor 2018 zo'n negentig events op de planning staan. Het plannen en organiseren van al die events neemt dus ook het merendeel van mijn tijd in beslag. Momenteel ben ik druk met het commissarissensymposium dat afgelopen 1 oktober is gehouden en met het samenstellen van het programma van de RO-masterclass. Sinds een aantal jaren maak ik een eventkalender die we naar onze leden sturen. De lezers van *Audit Magazine* kregen hem ook dit jaar weer samen met het magazine in de bus.
Het opleidingsprogramma stel ik samen met onze trainers, partners en verschillende IIA-commissies op. Bovendien gebruik ik het IIA Congres om nieuwe trainers te vinden. Als een spreker bij ons congres positief geëvalueerd wordt, dan bekijk ik of het interessant is om de spreker ook een training bij het IIA te laten verzorgen. Jitske Kramer met haar aansprekende boodschap over corporate tribes is hier een goed voorbeeld van. Ook met Peter Hartog, onze nieuwe vaktechnisch manager, spar ik over het opleidingsprogramma. Verder is het regelen van event- en congreslocaties een belangrijk onderdeel van mijn werk. Mijn missie is om van elk event een succes te maken."

**Wat zijn de voorwaarden voor een succesvol event?**

"Alle events laat ik evalueren door de deelnemers. Deze evaluaties gebruik ik om events als trainingen nog verder te verbeteren. Een voorbeeld hiervan was de feedback op de PwC Summer Course die ik vorig jaar kreeg. Een aantal

*"Een auditor mag wat creatiever en innovatiever zijn"*

deelnemers gaf aan dat, in vergelijking met de voorgaande jaren, de groep te groot was geworden. Dit jaar hebben we daarom het maximaal aantal deelnemers teruggebracht naar twintig. Het IIA organiseert veel en het gaat goed. Ik krijg ook regelmatig complimenten van andere organisaties, dat wij in staat zijn om ver van te voren een planning voor zoveel trainingen en events op te stellen.
Daarnaast word ik zelf ook geaudit! Om de opleidingen en trainingen te kunnen geven is het namelijk noodzakelijk om een erkend opleider te zijn (CEDEO en CRKBO). Dit is van belang voor het kunnen toekennen van PE-punten. Toen ik net in dienst kwam zijn er een aantal kritische aandachtspunten naar voren gekomen bij een externe toets. Ik heb vervolgens een aantal verbeteringen doorgevoerd en vorig jaar zijn we summa cum laude voor de toets geslaagd."

**IIA Nederland is de afgelopen jaren gegroeid. Wat merk jij daarvan?**
"Het IIA is de afgelopen jaren tot bloei gekomen. Ik zie veel tevreden mensen die steeds terugkomen naar de events. De groei van IIA Nederland en de tevredenheid van de leden met de events blijkt bijvoorbeeld uit de groei van het IIA Congres. In 2014 hadden we 250 deelnemers en dat is gegroeid tot 700 in 2018. Hiervoor hebben we veel te danken aan Hans Nieuwlands. Door zijn fantastische netwerk en ervaring met (internationale) congressen regelt hij veel goede sprekers. Ook is het fijn dat we ons eigen bureau hebben dat specifiek voor onze beroepsorganisatie werkt."

**Waar ben je trots op?**
"Natuurlijk ben ik trots op de mooie events die we organiseren en de waardering die we daarvoor terugkrijgen, zoals onder andere voor het congres, de RO Masterclass, PwC Summercourse en het Commissarissen Symposium. Daarnaast ben ik trots op CAE Services, het CAE Forum geeft veel energie en we hebben voor de nieuwe hoofden internal audit een starterskit samengesteld met best practices en templates en een CAE starterstraining ontwikkeld."

**Wat zou je nog willen realiseren?**
"Ik vind het jammer dat het aantal vrouwelijke internal auditors achterblijft. IIA Nederland is toch een beetje een mannenclub (75% van de leden is man). Vorig jaar hebben we een foto in het kader van 20 jaar IIA laten maken met alle voorzitters van IIA Nederland. Op die foto staan alleen maar mannen! Een belangrijke eerste stap is in 2018 al gezet door een vrouwelijke voorzitter te benoemen. Ook hebben we dit jaar voor het eerst een internationale vrouwendagbijeenkomst georganiseerd. Ik zou dit best wat groter willen aanpakken in 2019. Vooraf hebben we getwijfeld of we als beroepsorganisatie hier speciaal aandacht aan moesten schenken, maar het is een groot succes geworden. De bijeenkomst was binnen een paar dagen al volgeboekt."

**Wat zijn de belangrijkste competenties van een eventmanager?**
"Het beroep eventmanager staat al jaren in de Top-5 van meest stressvolle beroepen in de wereld, maar het is ook het leukste beroep dat ik me kan voorstellen. Je moet dus stressbestendig zijn. Verder is het belangrijk voor een eventmanager om creatief te zijn en buiten de gebaande paden te durven gaan. Je moet branden kunnen blussen. Een voorbeeld hiervan is dat een belangrijke spreker op het IIA Congres zijn vliegtuig miste en dat ik op het allerlaatste moment een andere spreker heb geregeld. Of sprekers die tien minuten voor hun optreden voor zevenhonderd man pas arriveren. Dat zijn wel stressvolle momenten."

**Wat kan een auditor leren van een eventmanager?**
"Een auditor mag wat creatiever en innovatiever zijn. Kom met nieuwe ideeën en toon moed! Als ik zie welke innovatieve ideeën worden aangeboden voor de IIA Innovatie Award dan valt dat toch een beetje tegen. Auditors kunnen meer initiatief nemen om zichzelf en het vakgebied verder te ontwikkelen. Bovendien ben ik van mening dat auditors veel meer gebruik kunnen maken van social media. Dare to share."

**Waar doe je auditors het grootste plezier mee?**
"Het is een uitdaging om auditors tevreden te stellen. Het is de meest kritische beroepsgroep die ik ken. Ze zijn getraind op een professioneel kritische houding, hoogopgeleid en een hoge standaard gewend. Het zijn ook betrokken mensen en ik vind het fijn als ze zich thuis voelen tijdens de events."

**Kun je al een tip van de sluier oplichten voor de volgende IIA-conferentie?**
"Kijk op www.iia.nl/congres2019!" <<

Artikel Innovatie
Tekst drs. Huub van Hout RA CIA
Raymond Wondergem MSc RO

Het aantal innovaties neemt toe en de levensduur van producten en processen wordt steeds korter. Aldus Gijs van Wulfen, schrijver, autoriteit op het gebied van innovatie en keynote speaker – in Pacmankostuum – op het laatste IIA Congres. Reden om opnieuw in gesprek te gaan en stil te staan bij de gevolgen voor de internal auditor.

# “Er is een groot verschil tussen **uitvinden** en **innoveren**”

### Wat is innoveren?

"Innoveren is risico's nemen. Alleen wanneer neem je risico? Een organisatie innoveert alleen als niets doen een groter risico is. Toch is de neiging groot als organisatie om niets te doen, omdat bedreigingen worden onderschat of organisaties hopen dat het zo'n vaart niet zal lopen. Zeker als een verdienmodel steeds positieve resultaten oplevert. Een mens verandert ook niet graag, omdat verandering moeite kost en routines vaak moeilijk te doorbreken zijn. Hoe vaak verander je van bank of van verzekeringsmaatschappij of dichter bij huis: van kapper? Meestal innoveer je pas als iets irriteert of pijn doet. Innoveren is risicovol, omdat slechts een op drie innovaties de markt haalt en daarvan wordt slechts de helft een succes. Het is voor organisaties daarom een moeilijke afweging om geld te investeren als de kans op succes klein is. Bovendien is innoveren een chaotisch proces. Door deze chaos te organiseren en te vertalen naar eenvoudige stappen wordt de kans op succes groter. In mijn methode heb ik tien stappen benoemd hoe te innoveren. Het gaat niet zozeer om kennis vergaren, want kennis is overal en toegankelijk. Het gaat niet meer om het 'wat', het gaat om het 'hoe'. Dus niet wat is innoveren, maar hoe moet ik innoveren!
Ook in het huidige onderwijssysteem ligt nog steeds te veel nadruk op het vergaren van kennis, terwijl het belangrijker is om de kunde van het toepassen van deze kennis te ontwikkelen. De ontwikkeling van 'applied sciences' is hiervan een goed voorbeeld."

### Waar komt innovatie vandaan?

"Regelmatig start innovatie met een creatief idee. Organisaties zijn vaak niet goed in creativiteit omdat men juist veel heeft vastgelegd in procedures en beleid. Er wordt vervolgens een brainstormsessie georganiseerd wat vaak leidt tot goede ideeën, maar bij zo'n sessie zijn de procedures en het beleid weer van toepassing. Vandaar ook dat kleine start-ups veel beter zijn in het genereren van ideeën. Een idee is echter nog geen innovatie.
Soms komt de innovatie voort uit een klantprobleem en biedt de innovatie een oplossing. Hier is de driver dat een organisatie ook wil veranderen. Dat is heel anders dan wanneer je moet veranderen. Innovatie komt dan voort uit noodzaak. Dit is een zeer krachtige route omdat het moet, men heeft geen keuze. Denk aan de invoering van wetten als MiFID, GDPR en Wmo. De vraag is wel of dit echt innovaties zijn of dat het aanpassingen zijn van bestaande processen of producten.
De laatste tijd wordt technologie aangehaald als 'rootcause' voor innovatie. Denk aan blockchain of zonne-energie. De innovatie wordt dan als het ware bij de technologie gezocht. Een mooi voorbeeld is de bankensector. De bankensector is allang over de product life cycle heen. Zij proberen door het oprichten van start-ups de levenscyclus te verlengen. Alleen voorspel ik dat deze sector over twintig á dertig jaar niet meer bestaat.
De mate van innoveren is generatiegebonden. Mijn generatie zal altijd naar een traditionele bank gaan, maar dat geldt niet voor de komende generaties. Dit geldt overigens niet alleen voor de bankensector. De gemiddelde levenscyclus van producten en diensten is verkort met een factor vier."

### Welke soort innovatie komt het meest voor?

"De noodzaakroute komt het meeste voor. Je moet 'uitverbeterd' zijn, voordat je gaat innoveren. Als het mogelijk is om met kleine stappen te overleven, dan kiest een organisatie doorgaans deze optie. Er is echter een groot verschil tussen innoveren en verbeteren. Innoveren is 'anders' en verbeteren is 'beter'. Dus als het gaat over operational excellence dan ben je bezig met vandaag. Het accent ligt op verbeteren. Innovatie gaat over 'morgen' en wijkt echt af van hoe zaken vandaag lopen.
Een land als Japan is goed in het optimaliseren van processen met daarbij hoge kwaliteitsstandaarden (denk aan de Toyotamethode, JIT, Kaizen). De nadruk ligt op verbeteren. Verbeteren is het maken van kleine stapjes. Innoveren is springen. Cultuur speelt hierbij een grote rol. Landen als Nederland zijn goed in het bedenken van concepten maar veel minder goed in het omzetten van concepten naar de praktijk. Daar zijn we te vrijgevochten voor, het vergt discipline. Het zou mooi zijn om een Nederlands concept op een Japanse manier door te voeren. Om innovatie makkelijker te maken probeer ik innovatie te vertalen in kleine stapjes die samen een grote sprong vormen. Dat is de kern van mijn methode."

### Aan welke eisen moet een innovatie voldoen?

"Een goede innovatie voldoet voor mij aan drie eisen:
1. het is een simpele oplossing;
2. het is voor een relevant klantprobleem;
3. het maakt gebruik van een nieuwe methode, verdienmodel of technologie.

De klant moet als het ware zitten te wachten op deze nieuwe oplossing. Daarnaast is complexiteit van de innovatie een belangrijk aandachtspunt. Voor mij staat dit voor onbruikbaar en als iets onbruikbaar is, dan is het niet relevant. Het mag best een complex product zijn maar de klant moet het ervaren als eenvoudig, probeer iets complex om te zetten in iets makkelijks. Een auto is complex maar de bediening is relatief eenvoudig. Hiermee is het voor de klant makkelijk

## Over...

Gijs van Wulfen is key note speaker en schrijver van *Het innovatiedoolhof*, managementboek van het jaar 2017.

gemaakt. Bovendien is een klant ook niet geïnteresseerd in de onderliggende technologie. Innovatie is ook makkelijk te volgen aan de hand van apps. Als een app op een telefoon geen probleem oplost en moeizaam is in de bediening, dan is het geen innovatie."

**Uitvinden is innoveren?**

"Er is voor mij een groot verschil tussen uitvinden en innoveren. Uitvinden kun je in je eentje. Je kunt iets bedenken, een Eurekamoment hebben, maar het omzetten van een idee naar de praktijk, daar moet je een soort Willie Wortel voor zijn. En ook Willie Wortel was niet erg succesvol overigens. Als je een idee hebt dan heb je anderen nodig om je idee om te zetten, en kost het veel energie om anderen van je idee te overtuigen. Bij een groot bedrijf zijn meerdere afdelingen betrokken en moet een veelvoud aan mensen overtuigd worden. Vaak aan de hand van een businesscase. Dat is heel complex en vraagt veel doorzettingsvermogen. Iets wat een stuk makkelijker gaat bij een Fintech dan bij een bank. Je ziet dan ook dat mensen die echt geloven in een idee, een organisatie verlaten en een start-up beginnen. Dit neemt niet weg dat het omzetten van een idee in een business voor een start-up ook niet eenvoudig is. Het bepalen van het moment om een innovatie te lanceren is mogelijk nog lastiger."

**Bestaat er zoiets als de mooiste innovatie?**

"Dat is een moeilijke vraag en ook heel persoonlijk. Mijn voorkeur gaat uit naar sociale innovatie, dan denk ik aan een 'liter of light'. Dit is een goedkope en eenvoudige manier om licht te brengen in donkere hutten zonder elektriciteit, waarvoor enkel een fles, water en een beetje bleekmiddel nodig is. Het voldoet ook aan mijn criteria. Het is eenvoudig, het lost een klantprobleem op en maakt gebruik van een nieuwe techniek. En wat nog mooier is, is dat het bijna gratis is, minder dan een euro per fles."

**Kunt u iets vertellen over uw aanpak?**

"Ik heb geen tool ontwikkeld, maar een methodiek, de Voortmethodiek. Deze is verdeeld over vijftien workshops, stappen zo je wilt. Zoals gezegd gaat het mij dus niet om het 'wat' maar om het 'hoe'. Hoe maak je mensen innovatief en in het verlengde daarvan, hoe maak je organisaties innovatief. Veel mensen zeggen dat ik een innovatieconsultancy had kunnen starten, maar dat past niet bij mijn filosofie. Met consultants zou je innovatie juist uitbesteden en leert een organisatie het niet zelf. Ik zie mijzelf dan ook meer als een innovatiemissionaris. Het gaat dus niet zozeer om het overdragen van kennis – het wat – maar het aanleren van kunde – het hoe."

**Hoe raakt innovatie de internal auditor?**

"Als ik naar internal auditors kijk, dan denk ik aan het langzaamste dier van de kudde. Het is ook een rol die van hen wordt verwacht, ze moeten assurance geven en doorgaans heeft die assurance betrekking op het verleden en op de huidige processen. Internal auditors zijn vooral bezig met gisteren en vandaag en nog te weinig gericht op morgen. Gisteren is voor een bedrijf minder relevant. Vandaag, denk aan procesverbetering is al relevanter en door de focus te verleggen naar morgen zal de toegevoegde waarde van een internal auditor belangrijk kunnen toenemen.

*"Als ik naar internal auditors kijk, dan denk ik aan het langzaamste dier van de kudde"*

Het langzaamste dier van de kudde loopt, net als in de natuur, risico. Door ervoor te zorgen dat je je als internal auditor meer op morgen richt, kom je vanzelf meer vooruit in de kudde en loop je minder risico. Én kun je je toegevoegde waarde opkrikken. Daarnaast signaleren internal auditors doorgaans problemen/issues. De internal auditor kan met deze signalen ook een aanjager van innovatie zijn. Organisaties moeten innoveren om te kunnen overleven. Het is voor de internal auditor de uitdaging om bij audits vast te stellen of er voldoende aandacht is voor innovatie, heeft men de blik voldoende op morgen. Internal auditors zijn deskundigen in het heden, maar zeker ook in het signaleren van het gat tussen het heden en de toekomst. Het begint bij jezelf innoveren. Daarbij is de belangrijkste vraag, willen jullie internal auditors, jezelf wel innoveren?" <<

Artikel De overstap
Tekst Drs. Paul van der Zwan RO EMIA
Beeld Gemeente Waddinxveen

# Gezina Atzema:

# *"Van de derde lijn bij de Rijksoverheid naar de frontlinie van de gemeente"*

In de rubriek De overstap dit keer Gezina Atzema, inmiddels ex-redactielid van *Audit Magazine* en tot voor kort werkzaam bij de Auditdienst Rijk (ADR). Zij maakte de overstap naar een bestuurlijke functie als wethouder in Waddinxveen.

**Over de gemeente Waddinxveen**
De gemeente Waddinxveen heeft 28.000 inwoners. Het college van B&W bestaat naast de burgemeester uit vier wethouders. Bij de gemeente werken ongeveer 220 mensen.

**Waarom ben je overgestapt van het auditvak naar de gemeentelijke politiek?**
"De mogelijkheid om een rol te vervullen als wethouder in je eigen gemeente doet zich niet vaak voor. En toen ik die kans kreeg, heb ik hem gegrepen. Als college van burgemeester en wethouders (B&W) vorm je het bestuur van de gemeente en kun je echt dingen voor elkaar krijgen. Dingen die jij belangrijk vindt en die tastbaar zijn voor de bevolking."

**Wat waren je eerste indrukken van je nieuwe werkkring?**
"De eerste weken kwam er veel op mij af. Van de ene op de andere dag ben je wethouder en volledig verantwoordelijk voor de zaken binnen je portefeuille. Om snel ingewerkt te raken, was er een programma met verschillende kennismakingsgesprekken met ambtelijke medewerkers en belangrijke stakeholders, met de bedoeling zo snel mogelijk de dossiers te kunnen doorgronden. Daarnaast was het natuurlijk ook belangrijk om als nieuw college van B&W, met vier nieuwe wethouders, elkaar te leren kennen en een team te vormen. Daar hebben we echt in geïnvesteerd. Samen vorm je de komende jaren immers het bestuur van de gemeente. Kortom, de eerste honderd dagen waren heel intens."

**Wat zijn de opmerkelijkste verschillen?**
"Bij de ADR werkte ik voor de Rijksoverheid en nu voor een gemeente. Bij de gemeente gaat het om zaken die dicht bij de burgers staan, dingen die spelen in je directe woon- en leefomgeving. Ik ben bijvoorbeeld betrokken bij ruimtelijke en economische ontwikkelingen en bij het opstellen en uitvoeren van een regionale energiestrategie. Sinds ik wethouder ben fiets ik heel anders door Waddinxveen. Ik weet veel meer wat er speelt en waar ik voorheen soms geen idee van had. Dat directe en concrete is een groot verschil."

**Hoe ziet de interne auditafdeling van de gemeente eruit?**
"Onze gemeente heeft geen interne auditfunctie. Wel kent de gemeente een verbijzonderde interne controle, waarbij processen worden gecontroleerd op basis van een risicobenadering. Hierbij wordt aansluiting gezocht bij de interimcontrole als onderdeel van de controle van de jaarrekening door de externe accountant. De gemeentesecretaris is

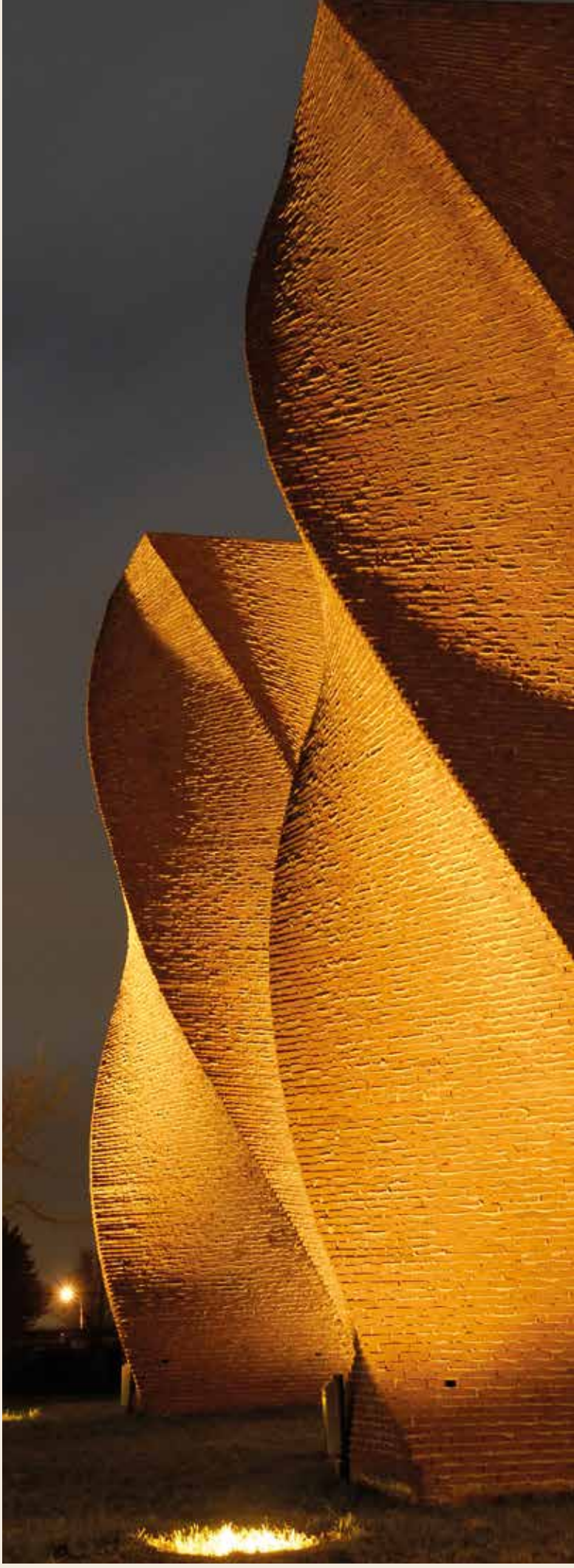
eindverantwoordelijk voor de bedrijfsvoering, waaronder de verbijzonderde interne controle. De burgemeester is politiek verantwoordelijk voor de bedrijfsvoering."

**Keer je ooit nog terug naar het auditvak?**
"Op dit moment heb ik voor een periode van maximaal vier jaar politiek verlof. Dit betekent dat ik na afloop van mijn periode als wethouder terug kan naar de ADR. Maar eerlijk gezegd ben ik daar op dit moment helemaal niet mee bezig. Ik richt me nu echt op de komende vier jaren. Wel vind ik het mooi dat de Rijksoverheid de mogelijkheid tot het opnemen van politiek verlof biedt aan haar medewerkers. Dat zouden veel meer organisaties moeten bieden."

**Wat wil je mensen meegeven die een overstap overwegen?**
"Dat het je ontzettend veel energie kan geven! Een verandering van werkomgeving geeft nieuwe impulsen. Veel vanzelfsprekendheden en routines vallen in een keer weg. Ik heb in ieder geval het idee dat ik in een hele steile leercurve zit waar ik heel veel voldoening uit haal. Ik werk keihard, maak veel uren, ook in de avond en in het weekend, maar dat is het (voor mij) meer dan waard. En met een overstap in een latere fase van je loopbaan kun je je ervaring en kennis soms op een verrassende wijze en in een geheel nieuwe omgeving inzetten. Zonder mijn bagage van bijna dertig jaar werkervaring bij de Rijksoverheid was het voor mij erg lastig geweest deze overstap te maken. Het gaat dan niet zozeer om vakinhoudelijke kennis, maar vooral om kennis en inzicht in interacties tussen mensen en hoe belangenafwegingen worden gemaakt. Kortom, krijg je de kans een overstap te maken, grijp die kans!"

## Over...

Gezina Atzema is wethouder in de gemeente Waddinxveen met in haar portefeuille ruimtelijke ontwikkeling, economie en duurzaamheid. Daarvoor werkte ze als auditmanager bij de Auditdienst Rijk en was ze lid van de redactie van *Audit Magazine*.



Artikel Onderzoek
Tekst Inge van Dijk LLM
Beeld 123RF®

# De 'why' van internal audit

Hoe vanzelfsprekend is het bestaan van internal audit? Wat is ook alweer de toegevoegde waarde van internal audit? Even terug naar de essentie van ons vakgebied.

Tijdens de opleiding executive MSc of internal auditing (EMIA) heb ik gemerkt dat wij als internal auditors niet goed zijn in het promoten van de eigen toegevoegde waarde. Internal auditors zijn immers geen verkopers! Door het geven van inzicht in onze toegevoegde waarde, hoop ik dat dit ons als internal auditors de handvatten biedt om duidelijk te kunnen maken waarom wij doen wat we doen. Door inzicht te hebben in de toegevoegde waarde van de internal auditfunctie, kunnen internal auditors met hun dienstverlening aansluiten bij de wensen van de (key) interne stakeholders. Tevens kunnen we hiermee onszelf en ons vakgebied beter 'aanprijzen'. Daarom heb ik onderzoek gedaan naar de 'why' van internal audit: over de (gepercipieerde) toegevoegde waarde van de internal auditfunctie binnen Nederlandse beursgenoteerde bedrijven, waar het hebben van een internal auditfunctie strikt genomen geen wettelijke verplichting is.[1] Hiermee ben ik gestart met een zoektocht naar de kern van onze toegevoegde waarde. Met dit onderzoek hoop ik bij te dragen aan het verstevigen van het bestaansrecht van de internal auditor.

**Aanleiding onderzoek**

De aanleiding van het onderzoek is de introductie van de herziene Nederlandse Corporate Governance Code (hierna: code) in december 2016 waarin meer expliciet aandacht wordt gegeven aan het belang van een internal auditfunctie.[2] De herziene code is wettelijk verankerd per 1 januari 2018. Onder de code zijn Nederlandse beursgenoteerde bedrijven verplicht om een internal auditfunctie te hebben, dan wel om uit te leggen waarom er geen internal auditfunctie is ingesteld. De vraag kan worden gesteld of de herziene code, en de aandacht en het belang dat deze code hecht aan het hebben van een internal auditfunctie, een reden is van de stijging in het aantal Nederlandse beursgenoteerde bedrijven met een interne auditfunctie.[3] Zou het echter niet zo moeten zijn dat als de toegevoegde waarde van de internal auditfunctie een vanzelfsprekendheid is, deze niet hoeft te worden 'afgedwongen' door middel van een code? Om deze reden is het een geschikt moment om de toegevoegde waarde van internal auditfunctie te onderzoeken.

**Het onderzoek zelf**

Er is literatuuronderzoek verricht, gericht op het identificeren van kwalitatieve variabelen die als mogelijke toegevoegde waarde(n) van de internal auditfunctie kunnen worden gezien:[4]

1. Informatie-asymmetrie: het verminderen van de informatie-asymmetrie tussen opdrachtgever en opdrachtnemer.
2. Externe druk: het wegnemen van de ervaren (formele dan wel informele) externe druk tot het inrichten van een internal auditfunctie.
3. Kostenbesparing: de werkzaamheden van de internal auditfunctie zijn kostenbesparend ten opzichte van de kosten voor de external auditor en voorzien managers van andersoortige informatie voor kostenbesparingen dan alleen de financiële verantwoordingsinformatie geleverd door externe audits.
4. Specifieke kennis van de (interne) organisatie: de specifieke combinatie van onafhankelijkheid en objectiviteit bij het uitvoeren van haar onderzoeken in combinatie met haar kennis van de business, de cultuur en de verhoudingen binnen de organisatie.

Het onderzoek is opgesplitst in twee delen, namelijk:

- Het beoordelen van jaarverslagen van lokale Nederlandse beursgenoteerde bedrijven.[5] Hierbij is onderzocht welke overwegingen er tot het al dan niet inrichten van een internal auditfunctie zijn geweest (desk research).

- Het afnemen van interviews (6) met de hoofden van internal audit van Nederlandse beursgenoteerde bedrijven. Het doel was te achterhalen welke ervaren toegevoegde waarde de internal auditfunctie heeft voor Nederlandse beursgenoteerde bedrijven (kwalitatief onderzoek).

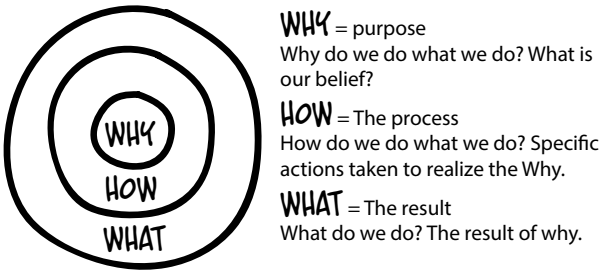
Qua periode is onderscheid gemaakt tussen Nederlandse beursgenoteerde bedrijven die in 2017 een internal auditfunctie hebben ingericht en Nederlandse beursgenoteerde bedrijven die voor 2017 reeds een internal auditfunctie hebben ingericht. Het onderscheid is gekozen vanwege de introductie van de herziene Nederlandse Corporate Governance Code eind 2016 en de verhoogde aandacht die deze code heeft voor het belang van de internal auditfunctie.
De gouden cirkel van Simon Sinek is als rode draad gebruikt in het onderzoek.[6] Sinek heeft het met zijn gouden cirkel namelijk ooit pakkend verwoord: mensen overtuigen doe je niet door te vertellen wát je doet, maar door ze te vertellen waaróm je doet wat je doet.

De gouden cirkel van Sinek is geen gevalideerd onderzoeksmodel. Het is daarom ook alleen gebruikt als denkmodel om gezamenlijk met de geïnterviewden te komen tot de vraag wat de (belangrijkste) toegevoegde waarde van de internal auditfunctie is. De achterliggende gedachte hierbij is dat de geïnterviewden vrij zijn om na te denken over de eigen toegevoegde waarde respectievelijk die van de auditfunctie binnen de eigen organisatie, en niet al meteen in het kader van de geïdentificeerde kwalitatieve variabelen te denken. Vervolgens is aan de geïnterviewden uitleg gegeven over de kwalitatieve variabelen, en gevraagd deze te rangschikken van 'meest waarschijnlijk' tot 'minst waarschijnlijk' als toegevoegde waarde van de internal auditfunctie binnen de eigen organisatie.

**Belangrijkste uitkomsten**

***Jaarverslag***

Uit het onderzoek naar de jaarverslagen van lokale Nederlandse beursgenoteerde bedrijven (niet AEX, AMX en AScX) blijkt dat de toegevoegde waarde van de internal auditfunctie nog niet wordt gezien door het merendeel van de lokale beursfondsen. Als er geen verplichting is voor het inrichten van een auditfunctie is er geen auditfunctie aanwezig. Tevens wordt dit veelal onvoldoende verklaard in hun jaarverslag. Als er een internal auditfunctie is ingesteld, is dit een verplichting vanwege de beurs waarop zij hun aandelen verhandelen of wordt het als een verplichting gezien. Geconcludeerd wordt dat de aanwezige internal auditfuncties zijn geïnitieerd vanwege externe druk (beursverplichting).




**Figuur 1.** De gouden cirkel van Simon Sinek

| Omschrijvingen van de belangrijkste toegevoegde waarde(n) van de internal auditfunctie | Aantal keren genoemd |
|---|---|
| Bijdragen aan een lerende organisatie | 5 |
| Bijdragen aan procesoptimalisatie | 5 |
| Het voorhouden van een kritische spiegel | 5 |
| Het zijn van de 'ogen en oren' van de (key) interne stakeholders | 4 |

**Tabel 1.** Toegevoegde waarde van de internal auditfunctie

***Eerste deel interviews***

Uit het eerste deel van de interviews blijkt dat de toegevoegde waarde van de internal auditfunctie wel wordt ervaren. De belangrijkste elementen van toegevoegde waarde zijn:

- het voorhouden van een kritische spiegel;
- het zijn van de ogen en oren van de (key) interne stakeholders;
- het bijdragen aan een lerende organisatie en streven naar procesoptimalisatie.

***Tweede deel interviews***

Als gemene deler uit het tweede deel van de interviews blijkt dat variabel 4 'specifieke kennis van de (interne) organisatie' het hoogste scoort als (ervaren) toegevoegde waarde van de internal auditfunctie. Aangegeven is dat toegevoegde waarde van de internal auditfunctie niet variabele 2 'externe

# *Als er geen verplichting is voor het inrichten van een auditfunctie is er geen auditfunctie aanwezig*

druk' is. Het wegnemen van de ervaren (formele dan wel informele) externe druk is een aanleiding geweest tot het instellen van de internal auditfunctie bij Nederlandse beursgenoteerde bedrijven die recentelijk een internal auditfunctie hebben ingesteld, maar waarbij wordt aangegeven dat dit niet dé reden is geweest tot het instellen van de internal auditfunctie.

Vanuit de interviews met bedrijven die al langer een internal auditfunctie hebben, waren de redenen tot het aanstellen van een internal auditfunctie divers, van incidenten met grote verliezen tot aan publieke schandalen. Alle hadden echter te maken met leden van de raad van bestuur die hierdoor 'verrast' werden. Dit kan een verklaring geven voor het feit dat in deze groep de variabele 1 'informatie-asymmetrie' beter scoort dan in de groep met recent aangestelde internal auditors.



Uit de interviews blijkt een link met de volgende kwantitatieve variabelen:

- variabele 1 'informatie-asymmetrie', waarbij een link wordt gelegd met het zijn van de ogen en oren van een raad van bestuur en/of een audit committee;
- variabele 4 'specifieke kennis van de (interne) organisatie', waarbij een link wordt gelegd met het bijdragen aan de lerende organisatie en procesoptimalisatie.

**Aanbevelingen**

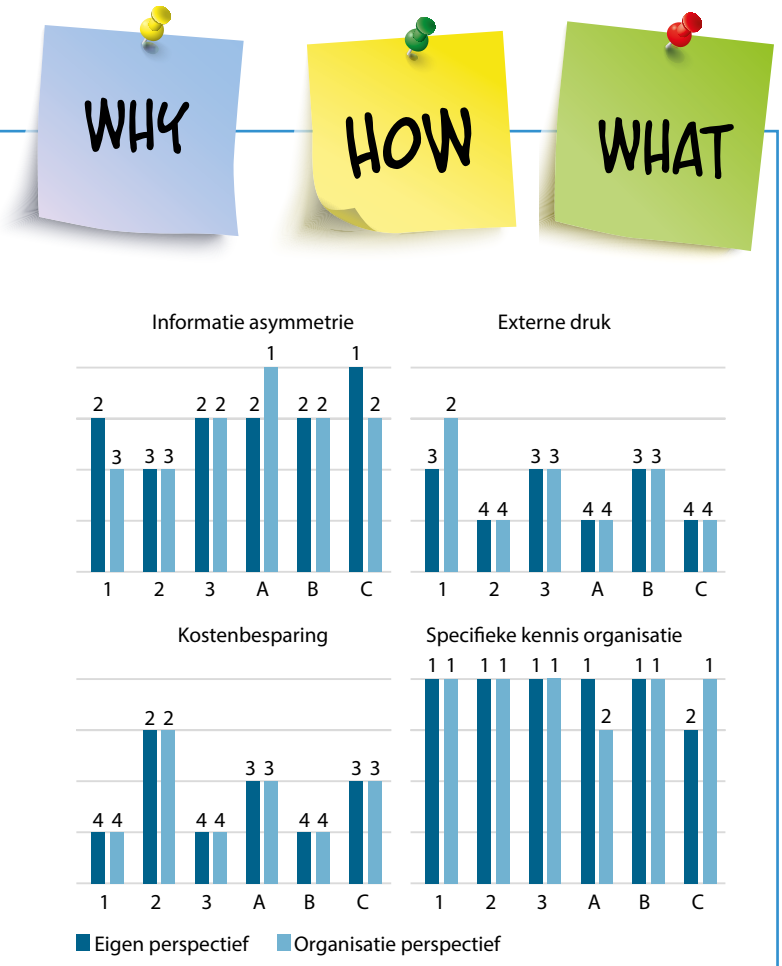
Het onderzoek biedt inzicht in de (gepercipieerde) toegevoegde waarde van de internal auditfunctie. De diverse inzichten geven voer voor, en mogelijk andere gedachten over, de toegevoegde waarde van de internal auditor binnen de organisatie en kan een inspiratie zijn voor nieuwe onderzoeken of helpen bij het vinden van een antwoord op de eigen 'why'-vraag. Aanbevelingen zijn:

- Afstemming tussen de internal auditor en de interne (key) stakeholders is van belang om de toegevoegde waarde van de internal auditfunctie aan te laten sluiten bij de wensen vanuit de organisatie.
- Het is van belang als internal auditor te achterhalen wat de specifieke behoefte van de key stakeholders is en waar de specifieke toegevoegde waarde van de internal auditfunctie zit binnen die specifieke organisatie. Uit de interviews blijkt de behoefte per organisatie namelijk verschillend te zijn. Bij de ene organisatie is er meer behoefte aan financieel gedreven audits, bij de andere organisatie meer aan procesmatige audits of audits op behaviour controls.
- De geïnterviewden geven aan dat het delen van best practices, het verbinden van mensen en/of afdelingen, alsook het delen van signalen respectievelijk onderbuikgevoelens, belangrijke aspecten zijn van de internal auditfunctie om de toegevoegde waarde van de auditor te vergroten.
- Het is voor een internal auditor van belang de eigen onafhankelijkheid en objectiviteit te waarborgen. Door de geïnterviewden wordt benadrukt dat het zijn van onafhankelijk en objectief, belangrijke randvoorwaarden zijn van de internal auditfunctie om van toegevoegde waarde te kunnen zijn. Hiermee onderschrijven zij de standaarden vanuit het IIA.
- Antwoord op de vraag naar de grootste toegevoegde waarde van de internal auditfunctie binnen de eigen organisatie kan veranderen, omdat ook de organisatie continu verandert en in ontwikkeling blijft. Het is belangrijk je hier als internal auditor bewust van te zijn en op te anticiperen. Kortom, blijven reflecteren!

**Beperkingen**

Bij de onderzoeksresultaten worden de volgende kanttekening geplaatst:

- Het onderzoek beschouwt internal auditfuncties als vergelijkbaar. In de praktijk verrichten interne auditafdelingen verschillende soorten activiteiten.




**Figuur 2.** Uitkomsten kwalitatief onderzoek (interviews)

Toelichting: per variabele staan horizontaal aangegeven de geïnterviewden (1 t/m 3 na 2017 aangestelde internal auditors en A t/m C voor 2017). In de eerste donkerblauwe balk is de score gegeven vanuit eigen perspectief, in de tweede blauwgrijze balk de score vanuit het organisatieperspectief, waarbij score 1 'meest waarschijnlijk' en score 4 'minst waarschijnlijk' is.[7]

- Het onderzoek omvat slechts één boekjaar. Een onderzoek dat een langere tijdspanne omvat biedt robuustere resultaten.
- Het interview is afgenomen met hoofden internal audit of internal auditmanagers, niet met leden van de raad van bestuur of de raad van commissarissen.[8]
- In totaal zijn zes interviews afgenomen. Een uitbreiding van de groep in de toekomst zou een verdere onderbouwing van de uitkomsten valideren.
- De populatie is beperkt gebleven tot Nederlandse beursgenoteerde bedrijven met een keuzevrijheid tot het instellen van een internal auditfunctie. Daarbij is geen onderscheid gemaakt naar de sector waarin het bedrijf opereert. <<

Inge van Dijk is internal auditor bij Vesting Finance. Daarnaast is zij commissielid van IIA Young Professionals.

**Noten**

1. Van Dijk, 2018.
2. MCCG, 2016, p. 14.
3. Volgens Paape is er een link tussen de steeds groter wordende roep om meer zekerheid en de – corporate governance – codes die meer terrein winnen (Paape, 2007, p. 8-9). Zie ook de uitkomsten van de *Internal Audit Monitor 2017*, waaruit blijkt dat er sprake is van een stijging in het aantal Nederlands beursgenoteerde bedrijven met een internal auditfunctie sinds de laatste meting in 2014 (Bogtstra & Renes, 2017).
4. Deze kwalitatieve variabelen zijn ontleend uit de economische theorieën van de principaal-agenttheorie, transactiekostentheorie en institutionele theorie. Deze theorieën zijn gekozen vanwege eerder verrichte onderzoeken naar verklaringen voor het bestaan van de internal auditfunctie met gebruik van deze theorieën. Zie Swinkels, 2012, p. 133. Zie Mihret, 2014, en Mihret & Grant, 2017, voor alternatieve theorieën die het bestaan van de internal auditfunctie kunnen verklaren.
5. Deze resultaten zijn ook input geweest voor het onderzoek van de *Internal Audit Monitor 2017* (over de mate en verschijningsvormen waarin de internal auditfunctie voorkomt binnen Nederlandse beursgenoteerde bedrijven), uitgevoerd door Robert Bogtstra en Remko Renes.
6. Sinek, 2011.
7. Met eigen perspectief wordt bedoeld: de toegevoegde waarde van de internal auditfunctie voor zijn organisatie bezien vanuit zijn eigen optiek. Met het perspectief van de organisatie wordt bedoeld: het perspectief bezien vanuit de key stakeholder binnen de eigen organisatie.
8. Hier is in het onderzoek wel rekening mee gehouden. Daarom is in het eerste deel van het interview gevraagd naar de key stakeholder(s) binnen de organisatie. Bij de vraag naar wat vanuit het organisatieperspectief de belangrijkste toegevoegde waarde is, is gevraagd wat deze key stakeholder zou antwoorden als hem of haar deze vraag zou worden gesteld. De uitkomsten vanuit organisatieperspectief is gevraagd vanuit de mening van de geïnterviewde, en daarmee subjectief. Vanuit de interviews blijkt echter dat de geïnterviewden veelvuldig contact hebben met hun (key) interne stakeholders en feedback krijgen over hun functioneren, waardoor zij een gedegen inschatting kunnen geven over de ervaren toegevoegde waarde van hun functie vanuit het perspectief van deze stakeholders.

**Literatuur**


- Bogtstra, R. en R. Renes, *Internal Audit Monitor 2017. Een goede bestuurder en toezichthouder verdient een goede Internal Audit Functie,* IIA Nederland: Stichting Vaktechnisch Onderzoek, 2017.
- Mihret, D.G., 'How can we explain internal auditing? The inadequacy of agency theory and a labor process alternative', *Critical Perspectives on Accounting,* vol. 25, nr. 8, p. 771-782, 2014.
- Mihret, D.G. en B. Grant, 'The role of internal auditing in corporate governance: a Foucaldian analysis', *Accounting, Auditing & Accountability Journal,* vol. 30, nr. 3, p. 699-719, 2017.
- Monitoring Commissie Corporate Governance Van Manen, *De Nederlandse Corporate Governance Code. Voorstel voor herziening. Een uitnodiging voor commentaar*, 2016. Geraadpleegd 14 oktober 2017, https://www.mccg.nl/?page=5405
- Paape, L., *Corporate Governance: The Impact on the Role, Position, and Scope of Services of the Internal Audit Function.* Rotterdam, Erasmus Research Institute of Management, 2007.
- Sinek, S., *Start with Why: How Great Leaders Inspire Everyone to Take Action,* Londen, Penguin Books, 2011.
- Swinkels, W.H.A., *Exploration of a Theory of Internal Audit: a study on theoretical foundations of internal audit in relation to the nature and the control systems of Dutch public listed firms.* Delft: Eburon, 2012.
- Van Dijk, I., *De 'why' van internal audit. Over de toegevoegde waarde van de internal auditfunctie,* 2018. Te raadplegen via de digitale bibliotheek van de Universiteit van Amsterdam.

## Uitgegeven certificaten Kwaliteitstoetsing

De internal auditafdelingen van de volgende organisaties ontvingen sinds de publicatie van het vorige *Audit Magazine* een Certificaat Kwaliteitstoetsing: De Volksbank, Intertrust, Robeco, Vion. Zie ook https://www.iia.nl/kwaliteit/kwaliteitstoetsingen.

## Save the dates 2019

Zet de grote evenementen voor volgend jaar vast in uw agenda.

**IIA Congres**
13 en 14 juni 2019

**PwC Summercourse**
23 en 24 september 2019

**Commissarissen Symposium**
30 september 2019

**PAS Conferentie**
7 november 2019

**RO Masterclass**
21 en 22 november 2019

## *Audit Magazine* en *Internal Auditor* blijven lezen?

Via uw persoonlijke profielpagina op de website van het IIA dient u vanaf dit jaar zelf aan te geven of u *Audit Magazine* (gedrukt) wilt ontvangen en of u toegang wilt tot *Internal Auditor* (online). In het streven papier en geld te besparen, hebben we voor alle leden beide mogelijkheden automatisch op opt-out gezet. Ga naar 'Ledenprofiel' op de pagina 'Ledenservice' en klik op de knop 'Privégegevens bewerken'.

Lees hier meer: http://bit.ly/2DMBPlm.


## IIA feliciteert de geslaagden

**Nieuwe RO's**: Marvin Berendse, Marianne Boerman, Monica Boom, Rishi Djairam, Stephan van Hofwegen, Pauline Kamps, Tim Oostvriesland, Wim Ottema, Leo Verbaan

**Nieuwe CIA's**: Maya Avital, Jeroen Bellinga, Fanneke Bertens, Jeroen de Beurs, Martin Biemond, Rachel Blok, Remko Boer, Jacobus Boortman, Yvo Bos, Esther Bosch, Adriaan Bouw, Wim van de Bovenkamp, Daniel Bruggeman, Chiel van Burken, Pooja Chitoe-Sham, Ronald Cornelisse, Yuri Davidsson, Frank van Dissel, Tamara van Doesburg-Bongers, Sonja Drewes-van den Belt, Arshia Faramarzi, Shane Fryer, Diederik Geerits, Menno van Gessel, Stephan Geuzebroek, Sinem Guven Isiklar, Sander Hendriks, Roy Hof, Rob van Hofwegen, Vincent van Hooijdonk, Bart Huisman, Sjors Jansen, Harald Janssen, Robert Janssen, Bobbie Jeurissen, Patricia Jones-Hoendervangers, Erik Jörning, Kasper Karelse, Teunis Kok, Maarten Kranenburg, Mark Leermakers, Gerry Liauw Kie Fa, Nadine van Loenen, Bart van Loon, Annet Man, Lawrence Man A Hing, Theodorus Molenbrugge, Maya Mungra, Erik Nieuwlaats, Carina van Oers, Willem Ottema, Arjen Overduin, Nick van der Plas, Edwin Poels, Jacobus Ponjée, Joanna van Rijs-Zarzycka, Innes Rinkes, Jolanda van Rooij-Jeuken, Hans Salfischerger, Arie Schep, Hugo van Schie, Bert Schijf, Cosmo Schuurmans, Walter Slee, Dennis Smit, Eugene Solognier, Katarzyna Supranionek, Marvin van Tilburg, Renate Timmer-Hassink, Danny Tingelaar, Shanley Tjong Akiet, Herman Tukker, Coenraad Valk, Marc Verberne, Richard Verduin, Rens Vermeer, Klaes Visser, Lizzy Vissia, Henk van Vliet, Fieke van der Vlist, Bart Vorstermans, Caroline de Vries, Gerwin de Vries, Dennis Wenders, René van Wijk, Peter Willemsen, Muhammed Yaseen

**Nieuwe CRMA**: Shane Fryer
**Nieuwe QIAL**: Peter Kruysifix
**Nieuwe CGAP**: Marianna Karras

## De Harvard case-methode

Voor het vierde jaar op rij geven we in onze post-masteropleiding Internal Auditing & Advisory een college volgens de Harvard case-methode. De Harvard case-methode is een lesmethode die ontwikkeld is door de Harvard University. De studenten krijgen vooraf een casus die zij doornemen. Tijdens het college gaan ze onder begeleiding van de docent met elkaar in discussie over de keuzen die ze zouden maken in de betreffende case. De student verplaatst zich in de schoenen van de manager, de auditor en de raad van commissarissen. Deze lesmethode heeft als doel om de analytische vaardigheden en het probleemoplossend vermogen van de deelnemers te verbeteren.

**17 mei casus 'Corruption at Siemens'**
Op vrijdagmiddag 17 mei 2019 is het mogelijk om aan te sluiten bij dit college. Centraal staat dan de casus 'Corruption at Siemens'. Vragen die onder andere aan de orde komen zijn hoe een multinational als Siemens in deze situatie terechtkwam, wat de rol was van internal audit en hoe ze hadden moeten handelen.
Het college wordt gegeven door prof. dr. Fred van Eenennaam. Hij volgde zelf ook diverse courses en gaf cases aan de Harvard Business School.
Voorafgaand aan het college krijgen de deelnemers de casus en een uitgebreide toelichting van Harvard op deze lesmethode toegestuurd.
Het afgelopen jaar is zowel het college als de docent beoordeeld met een 8,6. Een deelnemer geeft aan: 'Deze leermethode is waardevol en inspirerend! Onder leiding van de docent hebben we een levendige dialoog gevoerd en argumenten uitgewisseld over de verschillende mogelijke managementacties.'

**Beperkt aantal plaatsen**
Dit college is onderdeel van de module Capita Selecta en staat open voor een beperkt aantal alumni en belangstellenden. Per college worden 3 PE-uren toegekend. Vooraanmelding kan via esaa-auditing@ese.eur.nl.


Fred van Eenennaam

## Actualiteiten
Het Academisch collegejaar is begonnen. Dit jaar zijn 29 ambitieuze studenten gestart met de opleidingen EMIA en EPDA. Op 31 augustus 2018 was de kick-off van deze opleidingen met als thema informatiebeveiliging. Keynote speaker was dr. Martijn Dekker, corporate information security officer bij ABN AMRO Bank. Dekker studeerde wiskunde aan de Universiteit Utrecht en promoveerde aan de Universiteit van Amsterdam. Hij is tevens lid van de raad van commissarissen van Stater nv en lid van de security board of advisors van IBM.

Op een zeer inspirerende manier vertelde hij de studenten wat de meest actuele ontwikkelingen zijn op het gebied van IT, Informatiebeveiliging en cyber binnen de bankensector.

Universiteit van Amsterdam

**Amsterdam Business School**

## Algemene informatie
Het executive MSc of internal auditing (EMIA), 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.

## Interesse
Wilt u een boost geven aan uw internal auditcarrière? Bezoek onze website www.abs.uva.nl en start de uitdagende opleiding op 1 september 2018 of 1 februari 2019. U kunt ook contact opnemen per e-mail: eiap@uva.nl of per telefoon: 020-5254020.

# Waarom **complexe** technologie niet **complex** is

Complexe technologie is van alle tijden. Hierbij geldt ook dat huidige complexe technologie in de toekomst mogelijk een simpele, routinematige technologie is. Hoogstwaarschijnlijk alweer vervangen door nieuwe technologie, die op dat moment als complex wordt ervaren.

Complexe technologie heeft veel vooruitgang gebracht en nuttige toepassingen. Zo heeft General Electric de laatste 120 jaar voor veel vernieuwing gezorgd door middel van complexe technologie, die inmiddels als gangbaar wordt beschouwd – zoals de elektrische lamp. Het heeft verandering in de welvaart gebracht. Daarnaast heeft complexe technologie het ondernemerslandschap ook volledig veranderd. General Electric was lange tijd de onderneming met de hoogste marktwaarde ter wereld. Anno 2018 is dit niet meer het geval, het bedrijf is ingehaald door ondernemingen die meer technologisch innovatief zijn.

Complexe technologie zou ook onderdeel moeten zijn van de vernieuwing binnen het internal auditvakgebied. Recent las ik een artikel van Alessandro Baricco rond de verandering van de huidige samenleving. Hij gaf aan dat we niet bang moeten zijn voor nieuwe, complexe technologie maar juist de stap moeten maken naar vernieuwing. Mede omdat het ook in het verleden zorgde voor een stap naar een nieuwe vorm van beschaving.

De uitdaging voor internal auditfuncties is om complexe technologie te adopteren als noodzaak voor vooruitgang. Vanuit de 'oude' cybernetische literatuur bestaat allang het inzicht dat het in-controlvraagstuk uit drie niveaus bestaat. Allereerst het niveau van reguliere routinematige processen en activiteiten. Ten tweede de adaptieve processen en activiteiten naar aanleiding van veranderingen in de omgeving. Tot slot de herinrichting van processen en activiteiten in het kader van rigoureuze innovatie.

Hoe is de balans van internal auditfuncties tussen going concern, de adaptie en het herinrichten van de eigen processen en activiteiten? Het voelt vertrouwd om te blijven focussen op het 'bekende', met kleine adapties hier en daar. Is het gebruik van data-analyse, machine learning en artificial intelligence al echt in het vizier? Uit de scripties van de internal auditopleiding aan de UvA lijkt het dat de angst voor verandering het wint van de vernieuwing. Ik hoor nog te vaak het belang van de traditionele, bureaucratische three-lines-of-defensemodel. Dat is geen vernieuwing die ik bedoel.
Een meer datagedreven, complexe technologieaanpak kan een revolutie betekenen in het kader van inzicht en voorspellende uitkomsten. Controles en audits kunnen meer worden geautomatiseerd en een heroriëntatie van benodigde competenties en teaming is noodzakelijk. En letterlijk en figuurlijk herprogrammeren met behulp van complexe technologie. We moeten er niet bang voor zijn. Ik zal zelf starten het gesprek aan te gaan met de internal auditfunctie binnen mijn eigen onderneming. Over tien jaar vragen we ons af waarom het zolang heeft geduurd. In de tussentijd hoor ik het graag als de eerste Popperiaanse 'zwarte' zwaan is geïdentificeerd.

Walter Swinkels is group director Governance Risk Compliance bij Royal BAM. Hij is tevens verbonden aan het Executive Internal Audit Program van de Universiteit van Amsterdam.

# Is voldoen aan de verwachtingen van vandaag, morgen nog genoeg?

Wij ondersteunen u graag op gebieden als GRC-technologie, cyber security en data & analytics. Zo leveren we een bijdrage aan de cruciale rol van internal audit binnen uw organisatie. Meer informatie? Daniël Smidts (daniel.smidts@nl.ey.com, +31 6 29 08 40 22) of Birgit Stein (birgit.stein@nl.ey.com, +31 6 29 08 40 01).

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

# Hoe om te gaan met ethische principes bij de toetsing van algoritmes?

Als auditor zullen we steeds meer moeten kijken naar algoritmes die besluitvorming bepalen. Horizontaal ingebedde algoritmes kunnen we nog wel begrijpen, maar ook verticale (quantum) algoritmes zullen straks op ons pad komen en zijn een stuk lastiger om te doorgronden. Op het moment dat we algoritme audits uitvoeren, moeten we ook steeds de vraag stellen: voldoet het algoritme wel aan de ethische principes zoals transparantie, beheersbaarheid en rechtvaardigheid?

Om algoritmes integraal, dus ook op ethische principes te kunnen toetsen zijn heldere normenkaders nodig. Wij helpen u met het bepalen en opstellen van deze kaders en het uitvoeren van algoritme audits. Zodat u als auditor heldere toetsnormen heeft en de organisatie in staat stelt complexe technologieën op de juiste wijze in te zetten.

**Nieuwsgierig?**

Bart van Loon
+31 20 656 7796
vanloon.bart@kpmg.nl

Huck Chuah
+31 20 656 4501
chuah.huck@kpmg.nl

www.kpmg.com/nl