AUDIT MAGAZINE

VAKBLAD VOOR DE INTERNAL AUDITOR
NUMMER 3 2019 JAARGANG 18

THEMA
Audit 2025

"If you cannot *change*
they will *change* you"

De **lerende** zorgorganisatie

Het *droombeeld*
van internal audit

RISK ADVISORY

Internal Audit Quality Assessment

veel ervaring

veel toegevoegde waarde

The Advantage of Risk

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
Bas de Jong MSc RA
Jip Olieroock MSc RO CIA
Raymond Wondergem MSc RO
Drs. Paul van der Zwan EMIA RO

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

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

Cover foto
Edi Libedinsky on Unsplash

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

Audit 2025

We hebben een jarige! De Stichting Verenigde Register Operational Auditors (SVRO) bestaat 25 jaar en dat is iets om trots op te zijn! Om dit te vieren brengt het IIA tegelijk met dit nummer van *Audit Magazine*, eenmalig het SVRO-magazine uit.

Het thema van *Audit Magazine* is dit keer 'Audit 2025'. We laten diverse stakeholders van onze beroepsgroep aan het woord om hun visie te geven over de ontwikkeling van het auditvak, waaronder Naohiro Mouri, voorzitter IIA Global. We zijn trots dat we hem konden interviewen over dit thema.

Een belangrijke vraag: in welke richting ontwikkelt het auditvak zich, en met welk tempo? Niemand ontkent dat digitalisering en geautomatiseerde gegevensverwerking een belangrijke rol gaan spelen. De mate waarin hangt overigens sterk af van het type organisatie en de wensen van de stakeholders. Belangrijke stakeholders als het bestuur en de auditcommissie bepalen in bijzondere mate of een internal auditaffunctie (IAF) nog relevant is. De komende jaren is het cruciaal om met hen in gesprek te blijven over de toegevoegde waarde van de IAF. De steeds veranderende omgeving is van invloed op de strategie van de organisatie en dus ook op de IAF.

De zoektocht om van toegevoegde waarde te blijven, is een interessante uitdaging voor de auditor. In die zoektocht is het van belang te zoeken naar in hoeverre we de rol van 'trusted advisor' nog beter tot zijn recht kunnen laten komen. Dat vraagt om flexibiliteit, creativiteit, de kunst van goed luisteren en meebewegen met de strategie van de organisatie.

Om alle ontwikkelingen het hoofd te kunnen bieden helpt een intern en extern netwerk. Het interne netwerk bestaat uit de collega's uit de eerste en tweede lijn die zich bezighouden met innovaties. Als auditor kun je gebruikmaken van de kennis van je collega's. Deze kennis kun je ook inzetten bij het uitvoeren van audits. Daarnaast is het uitwisselen van kennis tussen auditors van verschillende organisaties een absolute must om aangehaakt te kunnen blijven bij alle ontwikkelingen.

Het spookbeeld dat de internal auditor over tien jaar overbodig is, lijkt te pessimistisch. Dat het auditvak gaat veranderen is evident, maar de relevantie van het auditvak blijft. Het is dan ook aan ons auditors om zelf de aspecten te vinden om relevant te blijven!

Wij wensen u veel leesplezier!

De redactie van *Audit Magazine*

THEMA: Audit 2025

"If you cannot change, they will change you"

Dat zegt Naohiro Mouri, voorzitter van IIA Global. *Audit Magazine* sprak met hem over zijn visie op het internal auditberoep, het belang van de Standards, en over "going back to the very basics". **Pag. 6**

Performance en strategie-uitvoering

"Veel auditors leven een beetje in een bubbel, net zoals medewerkers in iedere andere beroepsgroep overigens." Aldus prof.dr. Edo Roos Lindgren, hoogleraar aan de UvA. Over de toekomst van de IAF en de rol van data science daarin. **Pag. 20**

Het droombeeld van internal audit

Wat is de toekomst van internal audit bij de overheid? Topbestuurder bij het Rijk Hans van der Vlist, deelt zijn ervaringen en toekomstbeeld. **Pag. 12**

Het gaat om de allerbeste zorg: nu en in de toekomst

Mirjam Velthuizen-Lomans (RvB UMC Utrecht) heeft als aandachtsgebied bedrijfsvoering. Ze vertelt over haar eerste ervaringen met de IAF, dat het UMC sinds 2017 heeft. **Pag. 24**

De lerende zorgorganisatie

's Heeren Loo is Nederlands grootste aanbieder van zorg voor mensen met een verstandelijke beperking. Sinds 2014 heeft het bedrijf een internal auditfunctie. Een gesprek met Jan Fidder (RvB) en Louis Beenen (hoofd IA). **Pag. 16**

Internal audit bij pensioenfondsen: 2020-2025 en daarna

Sinds januari 2019 moeten pensioenfondsen een internal auditfunctie hebben ingericht. Maar bij veel pensioenfondsen staat deze functie nog in de kinderschoenen. Wat is de komende jaren belangrijk? **Pag. 28**

Gamification voor de internal auditor

Gamification rukt op in onze samenleving. Kijk naar de vele klant- en bonuskaarten met te verdienen punten en cadeaus om ons koopgedrag te beïnvloeden. Maar wat kun je er als internal auditor nu precies mee? **Pag. 32**

Waarom BCM en crisismanagement belangrijk is

Business continuity management (BCM) en crisismanagement: de eigen organisatie hierop actief toetsen levert een belangrijke bijdrage aan het verminderen van kwetsbaarheden en aan het vergroten van de veerkracht van de organisatie. **Pag. 39**

Financial chaos engineering

Twee medewerkers van Pathé maakten 19 miljoen euro over naar aanleiding van nepmails. Weg geld. Hoeveel nepfacturen betaalt uw organisatie eigenlijk? Maar nog belangrijker: hoe voorkom je dat? Kun je dat überhaupt voorkomen? **Pag. 44**

Focus op essentiële zaken in IT-audits

Waar let je op als je de kwaliteit van informatiebeveiliging wilt verbeteren of op het reeds hoge niveau wilt houden? **Pag. 50**

Cybergeddon: een reëel gevaar?

“Voor software heb je updates, maar ons brein is al eeuwenlang niet geüpdatet. Daar maken cybercriminelen gebruik van.” Cybersecurity-expert Peter Zinn over de kansen voor de auditor om ‘het lek in de dijk’ te dichten. **Pag. 54**

Terugblik IIA Congres 2019: Intelligence & Impact

Het congres was ook dit jaar weer een groot succes. Een terugblik. **Pag. 58**

Kennisdelen: wat werkt?

Een inventariserend waarderend onderzoek geeft inzicht in de factoren die mensen helpen om kennis te delen. Hoe stimuleer je dat als auditor? **Pag. 62**

Rubrieken

- Audit 2025
- IIA Global
- IPPF

Thema

Tekst Bas de Jong MSc RA
Drs. Paul van der Zwan EMIA RO
Beeld NFP Photography

"If you cannot *change*, they will *change* you"

Audit Magazine spoke with Naohiro Mouri, Chairman of IIA Global about his vision on the internal audit profession. His theme is: 'Emphasize the Basics. Elevate the Standards.' In a quote he said: "Because I truly love the profession, I wanted to stress the importance of going back to the very basics. That means understanding how important the Standards are to become the trusted advisors we aspire to be."

What 'Emphasize the Basics. Elevate the Standards' means to you and is the key take away for being a trusted advisor?
"I would like to start with trusted Advisor (TA), because that's easier to explain. Being a TA means that an internal auditor really helps senior management and the line management to do what they are supposed to do, in a better, faster and cheaper way. The way we do this is by giving assurance to the business. My belief is that if you do not give assurance, you do not really understand the business well enough. So as the TA you must really understand the business and the agenda of senior management. In addition the knowledge of control is essential, which brings me to the basics: the standards, as a guidance for the internal auditor. It's like a visit to the doctor. For a reliable judgment, the doctor must examine your body first to give the right diagnosis, or advice. Having a set of standards is important for professionals in order for people to understand what, how and why they do things."

Changes in today's and tomorrow's business environment, the associated risks are accelerating. How does that affect 'the basics and standards' and is internal audit still needed?
"So that's a really good question on 'how we do things'. Why we do thing, or what we do probably does not change. Going back to the year 1941 when internal auditing started, internal auditors used pen and paper. The way we do things now have changed with computer, but the purpose of why back then and now are much the same. The demand for assurance on the effectiveness of controls, or advice and insight on senior management to perform their controls better, cheaper etc. has not changed. And I don't think that the purpose of internal audit is going to change for another 50-100 years as long as organizations exists. How we do things is going to change, due to Artificial Intelligence, using robots and blockchain. When the businesses changes and become digitalized, the way we audit changes. I think that how we will do things will possibly radically change over the next 50 years."

And will internal audit still be needed in the future?
"Yes internal audit will still be needed. However, the way we add value will change. Everything that is quantifiable or tangible can be used to test controls. I think that in 10-20 years machines can help us make decisions based on results of machine-testing activities. Maybe in the future internal audit will be responsible for the maintenance of the machines that test. For other things that are not tangible or quantifiable such as culture, behavior and conduct, only humans can audit. Humans would still be needed to connect the dots and to analyze the results of machine tested decisons. The skillset of the auditor is also going to change. Testing skills would be less important. The use of cognitive power would increase, the power to think, power to construct and to create things are becoming more important. My view is that this is what the future internal auditors will be doing. Analyzing, reporting, communicating and facilitating. As testing time becomes smaller, the cognitive activities can be expanded, where our value creation comes in and that is where our future is. For me it is an exciting new world. But I can image for some auditors, it is threatening because testing activities will become insignificant for human auditors and will probably be taken over by bots."

Which key characteristics would best describe the optimal Internal Auditor, and what developments do you see?
"I see some critical characteristics, like analytical ability, communication and also facilitation of the conversation with the business. Things we really need to put effort into enhancing our skills. Combined with machine learning and use of robotics, I expect the third line will become closer to the second line of defense, because there is instant insight with real time full population testing with the business, and the auditor's time could be spent on the cognitive power. Once you harness real time full population testing, the next step is to predict behavior and minimalize the audit risk if we have enough data. At the end of the day it comes with the acceptance of the board to be open in discovering what data means and invest in further developments. Internal audit must put this topic as their priority. Internal audit must step up and come forward to push this agenda."

Given today's changing business environment, requirements of regulators and – customers' demands: Do you see internal audit adding value primarily as an assurance provider or as a trusted advisor?
"I am not sure why we make the distinction between two as I see both of them inter-related. As I said, my view of internal audit is primarily as the assurance provider. As we provide assurance (including automated testing) to the business, that would lead to insight and advise, which leads to being their trusted advisor. If the CEO, or audit committee trust me, they will ask for my opinion. Key is stating my opinion with honesty and integrity, and building and earning trust is the key. It's important to provide information to stakeholder about what is aligned with their needs and worries, not what you want to tell them. And having the courage to say things they don't want to hear and bring the truth in front of them. I call that occupational hazard."

The new IPPF show resemblance and overlap with other professional standards, such as the external auditor's professional standards. Has IIA sought alignment with other professional standards? And to what extend are the standards differ?
"I do not think we have deliberately sought alignment with other professional standards. As this is the 52nd revision of the Standards, we have a deep understanding and

About…

Naohiro Mouri is chairman of The Institute of Internal Auditors Global (IIA) and executive Vice president and chief internal auditor of American International Group (AIG).

knowledge of what Internal Audit is. The last update was in 2017, so we continue to update the standards. Is there a similar way of thinking between us and accountants? Maybe. Many internal auditors have an accounting back ground including myself. Even though accounting, external auditing and internal auditing are completely different professions, I can see there are many similarities. This also makes sense when considering that internal audit started by looking at operations and finance. Internal audit from the finance perspective is very similar to external auditing."

Years from now: how do you want your Global Chairmanship to be remembered, what legacy will you have left behind?
"I love Internal Audit. It is my passion, my commitment, my life. I have been in this profession for 26 years and will probably continue to engage myself in this profession until the day I stop working, which will probably be the day that I die. It is my passion, because internal auditing gives me the opportunity to learn things. By having a conversation with you, I am also learning, by speaking at conferences, I learn, and by being involves in audit engagements I learn quite a bit. Every audit engagement is different, which is really fascinating to me. I am passionate about learning and then sharing that knowledge with others to help the organization deal with problems."

The various countries around the world may perceive internal audit differently. To what extent are differences allowed or would IIA global always aim for harmonization?
"Let's look at the accounting profession. Even though basics of accounting is same in every country, each country regulates with different accounting standards. As a result, even though we have a single international financial reporting framework, it is applied differently from country to country. That creates issues with multinational companies when you operate worldwide and adjustments are required for local reporting. Unlike accounting profession, the internal audit profession currently is not regulated. The IIA holds a single set of global Standards. I know some countries in Africa that regulate the internal audit profession, but they always refer to the IPPF as the Standards. We are happy to work with local legislators to adapt the standards, but do not want them to create local sets of standards and create differences with the global IPPF. Most regulators are happy to refer to the IPPF as the professional standard."

"My belief is that if you do not give assurance, you do not really understand the business well enough"

The final question: what does The IIA do well and what could The IIA do better?

"I am happy to report that we have just passed the 200,000 members mark, which is a significant effort in all parts of the IIA global organization including the IIA Nederland. The IIA is a membership service organization. We help our members to do their job right every day. So, do I think we have done all we can to help our members? Perhaps yes, perhaps no. We have very good Standards and very good certification programs. Perhaps the Standards can continue to improve. In my opinion, not every member understands, respects and then conforms to the standards. If you look at the Common Body of Knowledge study that is done every 5 years the complete conformance is still less than 60%, partial conformance is another 30%, which makes up about 90% in total. I fully understand there are some difficulties to conform for the smaller audit shops, so IIA is now contemplating how to deal with that issue. But, we really have to come to a consensus as to what it is that we expect the conformance level to be. So that is something we are working on.

How we service our members is also something that we are discussing. Currently each institute has its members, and each institute is a member of the global IIA. The question is whether this is the right model to service our members with the best possible way? While each institute understands the needs of the local members, some of the members work at global companies, which may trigger different, global needs. These needs could be served better by the IIA headquarters or other institutes, where their company headquarter is situated. We are currently contemplating how to best service our members. For instance, what is the content they need, what are the seminars that they need, what topics do they need researched. I think we have some work to do on this. From the member service, we need to strive for our service to be the best in class. We need to elevate that. But I am happy to say we are doing everything we can and with the growing number of members world-wide, we will be better able to improve. IIA Global is currently undergoing a large technological change with the membership database and the examination systems as well as its internet portal. We are really re-bumping the technology platform. Stay tuned for some better service coming through."

That was the final question. Is there anything you would like to add?

"One thing I would like to say is that our future is bright as long as you are willing to change. Because change is the only constant thing in this world. If you cannot change, they will change you. If we can successfully transform ourselves to leverage technology to help us help our stakeholders then we are in a great place. I am actually very excited about the future." <<

Column
Tekst Jantien Heimel

Van het bestuur

Drieduizend leden. Een vloggende voorzitter. Een app waarmee alle leden via hun telefoon toegang hebben tot best practices en elkaar eenvoudig kunnen bereiken voor allerlei kennisuitwisselingen, presentaties en cursussen online kunnen volgen en opnieuw bekijken. Zou onze vereniging dat allemaal te bieden hebben in 2025? De tijd zal het leren.

Het is in dit kader interessant de voorspellingen en ambities uit het verleden over het heden nog eens terug te lezen. De ambities van IIA Nederland uit 2014 voor de strategie 2016-2020:

- Sterkere profilering – IIA Nederland heeft het profiel verhoogd van de vraag naar professionele internal auditing als zijnde onmisbaar in governance.
- Sterke waardepropositie van IIA Nederland – IIA Nederland levert een sterke waardepropositie voor bestaande, toekomstige en voormalige internal auditors, zodanig dat zij hun lidmaatschap als noodzakelijk zien.
- Verbeterde professionaliteit – IIA Nederland is de leidende autoriteit in de ontwikkeling van internal auditfuncties (en professionals).
- Blijvende verbinding met IIA Europa en Global – Doel: IIA Nederland draagt bij aan de internationale beroepsontwikkeling en profilering en maakt gebruik van de internationale ontwikkelingen van IIA.

We hebben de afgelopen jaren als vereniging stappen gezet in deze richting, maar we zijn er nog niet. Voor het opstellen van de strategie van IIA Nederland 2020-2025 zijn de hierna volgende vragen relevant.

Hoeveel internal auditors werken er over vijf jaar in Nederland? In sommige bedrijfstakken, zoals die van pensioenfondsen, is de functie recentelijk verplicht geworden. We zien dan ook een toenemende vraag naar auditors met kennis van de branche. Ook in de zorg en binnen woningbouwcorporaties en de decentrale overheid zien we een toenemende vraag. Daarnaast worden steeds vaker zelfstandige auditors ingehuurd om specifieke kennis binnen de interne auditfuncties aan te vullen. Zo is er bijvoorbeeld steeds meer vraag naar experts op het gebied van algoritmen. Per saldo ga ik voor de strategie uit van een lichte groei van het aantal auditors in Nederland en daarmee samenhangend van het aantal leden.

Hoe ziet het landschap van internal auditgerelateerde beroepsverenigingen eruit in 2025? De structuurwijziging binnen de NBA maakt dat de ledengroep Interne en overheidsaccountants (LIO) waarschijnlijk in de huidige vorm verdwijnt. Daarvoor in de plaats komt dan een zogenaamde community Internal audit. We zijn met NBA/LIO en de NOREA in overleg over hoe we kunnen samenwerken binnen deze community. De verenigingen hebben nu weliswaar elk hun eigen profiel, maar het is soms lastig uit te leggen aan de buitenwereld dat meerdere beroepsverenigingen naast elkaar bestaan.

Is de inhoud van het auditvak in 2025 wezenlijk anders? Eerder dacht ik dat de business – die via continuous monitoring realtime inzicht heeft in hoe het bedrijfsonderdeel ervoor staat ten opzichte van de doelen – minder behoefte aan internal auditors zou hebben. Maar tot op heden lijkt bij de organisatie waar ik werk het tegendeel waar te zijn. Meer dan ooit is er behoefte aan zekerheid omtrent de juistheid en volledigheid van de cijfers en de efficiency van de totstandkoming van die cijfers. De aandachtsgebieden wijzigen wellicht, maar het vak blijft relevant.

Rapporteert de auditor in 2025 nog op dezelfde wijze als in 2019? In rap tempo wordt de geschreven boodschap vervangen door vlotte fimpjes. Dit gaan we ook terugzien op het werk, waar de auditor de kernbevindingen in een korte videoboodschap toelicht. Ik sprak laatst een jonge executive en merkte al snel dat hij het conceptrapport niet had gelezen en ook geenszins van plan was het te gaan lezen. In dit kader grijp ik graag terug op het beeld van brilsmurf. Hij kan best gelijk hebben, maar krijgt het niet omdat hij niet effectief communiceert. Als (bebrilde) auditor wil ik voorkomen dat ik word gezien als brilsmurf. Dus als ik zie dat mijn boodschap niet aankomt, dan zal ik mijn manier van communiceren moeten aanpassen. Immers, stilstand is achteruitgang!

IIA Nederland
Jantien Heimel is voorzitter van het IIA.

Thema

Tekst Petra Hamm-van Bodegraven MSc CPsA
Raymond Wondergem MSc RO

Het *droombeeld* van internal audit

Hans van der Vlist, topbestuurder bij het Rijk, commissaris en auditcommitteelid, vertelt over zijn ervaringen bij en zijn toekomstbeeld van de Rijksoverheid, en de verwachte rol voor internal audit daarbij.

Kunt u iets meer over uzelf vertellen?
"Ik heb jaren als topambtenaar bij de Rijksoverheid gewerkt, onder meer als secretaris-generaal van het ministerie van Onderwijs, Cultuur en Wetenschap. Momenteel ben ik directeur bij ABDTOPConsult. Dat is een adviesgroep van ervaren topambtenaren binnen de rijksoverheid die snel inzetbaar is bij complexe vraagstukken en/of interim-opdrachten. Deze opdrachten richten zich vooral op bestuurs- en governancevraagstukken. Wij komen vaak in beeld als er 'iets' aan de hand is. Zo heb ik onder andere adviezen gegeven over de marktwerking op het spoor, de informatisering van de strafrechtketen en de verantwoordelijkheidsverdeling van voedselveiligheid."

Dat klinkt als een overvolle agenda
"Ik heb altijd ruimte in mijn agenda. Vanuit mijn rol als directeur ABTOPConsult houd ik me ook bezig met een groepscoachingprogramma voor directeuren bij de rijksoverheid. Mijn visie op leiderschap aan de top is: minder doen en meer zijn. Dat kan ik uitleggen. Ik heb namelijk naast mijn werkzaamheden bij het Rijk ook een aantal nevenfuncties.

Over...

Mr. Hans van der Vlist is directeur bij ABDTOPConsult. Daarnaast is hij voorzitter van de raad van commissarissen bij Woonbron en lid van de raad van commissarissen bij Parnassia Groep. Verder is hij voorzitter van de auditcommissie van de Nationale Politie.

Dat klinkt als een volle agenda, maar ik heb, zoals gezegd, altijd voldoende ruimte in mijn agenda. Die ruimte gebruik ik om er te zijn als mensen mij nodig hebben. Dat doe ik door minder focus te leggen op de zaken en afdelingen die goed lopen binnen een organisatie. Dat kan met goede bemensing en vertrouwen. Ik vind het de kunst om medewerkers op de juiste plek en vooral in hun kracht te zetten. En het is belangrijk om tijd te nemen voor kennis van de praktijk. Dat doe ik nu ook in mijn rol als voorzitter van het audit committee van de Nationale Politie. Daarnaast is het belangrijk om er te staan als er incidenten zijn. Hiervoor heb je tijd en ruimte nodig in je agenda om aan het incident voldoende aandacht te kunnen besteden. Dit soort situaties vraagt om het krachtenveld te kennen en een positie in te nemen. In het groepscoachingsprogramma probeer ik de directeuren in te laten zien dat ze hun agenda zo in kunnen richten dat ze tijd kunnen besteden aan de juiste dingen."

Hoe hebt u kennis gemaakt met internal audit?
"In mijn eerste leidinggevende functie als hoofd Uitvoering Huursubsidie was er een interne controleafdeling. Deze afdeling onderzocht de kwaliteit van processen en voerde steekproeven uit. De onderzoeken waren gericht op het doen van uitspraken over tolerantiegrenzen en op het geven van advies. In het vervolg van mijn carrière heb ik in verschillende vormen te maken gehad met internal audit. Het ging dan over werkprocessen en geld. Een voorbeeld hiervan is de bruteringsoperatie (privatiseringsactie van de Nederlandse woningcorporaties uit 1995 – red.). Tijdens deze operatie ging het om groot geld. De interne accountantsdienst was toen nauw betrokken bij de controles. Toen ik commissaris was bij de Rabobank speelde internal audit een grote rol. Ik

vond dat de intensiteit van interne controle en internal audit daar was doorgeschoten. In mijn andere commissariaten maak ik gebruik van de uitkomsten van de internal audits. Dus mijn hele leidinggevende periode en als commissaris heb ik met internal audit te maken gehad."

Hoe kijkt u daarop terug?
"Ik zie dat de internal auditor zich heeft ontwikkeld van controleur naar adviseur. Bovendien zie ik een verschuiving van hard controls naar soft controls, naar hoe mensen werken en samenwerken. De internal auditor is meer de sparringpartner van de bestuurder dan een controleorgaan. Verder heeft de internal auditor oog voor de dingen die ik als bestuurder of commissaris niet zie."

Wat is uw droom voor de rijksoverheid?
"Mijn ideaal is dat de overheid meer als eenheid gaat functioneren vanuit het burgerperspectief. Dat de verschillende lagen van de overheid intensief met elkaar samenwerken. Je ziet dat de digitalisering zich steeds verder ontwikkelt. Dat is goed voor de meeste burgers. Maar voor een grote groep wordt dit steeds ingewikkelder en soms te complex. Het liefst zie ik één dienstverlenend loket op gemeenteniveau waar meerdere overheidsdiensten in geïntegreerd zijn. Dit is een verregaande ontkokering met als uitgangspunt: de burgers. Hier worden burgers geholpen door deskundige medewerkers. De beste mensen aan de front office die de complexe back offices snappen. Ik besef dat dit een ingewikkelde opgave is, maar we kunnen stappen in die richting zetten. Een belangrijk onderdeel van deze opgave is het zetten van een stip op de horizon. Waar wil je als overheden naartoe en wat heb je hiervoor nodig. Een stip op de horizon, een visie, is nodig om stappen te zetten om je doelen te kunnen bereiken."

Wat kan de rol van internal audit zijn bij dit droombeeld?
"De internal auditor kan helpen bij inrichtingsvraagstukken. De internal auditor moet zich niet alleen concentreren op de status quo, maar ook een bijdrage leveren aan de toekomstige ontwikkelingen. In vergelijking met vroeger is er veel meer dynamiek. De enige constante is eigenlijk dat alles verandert. Dan is het makkelijk om vanuit de status quo kritiek te leveren. Het is veel moeilijker en een grotere uitdaging om een bijdrage te leveren aan de gewenste dynamiek. De internal auditor stelt dan de belangrijke en prikkelende vragen, zoals: is de stip op de horizon van een organisatie helder, is er überhaupt een stip op de horizon? Zo ja, wordt deze stip gemeenschappelijk gedeeld in de organisatie? De internal auditor is in de toekomst een belangrijke adviseur, omdat hij het overzicht over het geheel heeft.
Naast het beoordelen of alles goed loopt moet hij ook zicht hebben op de relevante ontwikkelingen. Op een gegeven moment haak je als organisatie af als je niet mee kunt gaan met deze ontwikkelingen. Het is de uitdaging voor internal auditors om zicht te hebben op de ontwikkelingen in relatie tot de omgeving. Voor medewerkers (dus ook internal auditors) wens ik dat ze vanuit hun kracht werken (inside out) en voor organisaties wens ik juist een focus op de ontwikkelingen en innovaties (outside in). Het beleid bij de overheid moet gericht zijn op het helpen van de burgers, de buitenwereld. Dus internal auditors moeten zich niet alleen richten op interne processen, maar ook op de processen naar buiten. Staar je niet blind op de binnenkant!"

U hebt ervaring bij organisaties in verschillende sectoren. Wat valt u op aan de rol van internal audit?
"Toen ik bij Woonbron kwam was 'het schip' verkocht (de ss Rotterdam – red.). Enkele bestuurders gingen weg en er moest een grote reorganisatie komen. Je maakt het verschil als bestuurder of als commissaris om er op dat moment te zijn en de juiste beslissingen te nemen. Een ander voorbeeld zijn de ggz-instellingen. Daar speelt de impact van de decentralisatie een grote rol. Het gevolg van deze decentralisatie is dat ook de administratieve processen zijn gedecentraliseerd. Met de gevolgen daarvan voor zorgverleners is door de rijksoverheid onvoldoende rekening gehouden. Elke gemeente heeft zijn eigen administratieve processen na de decentralisatie. Zorgverleners worden er stapelgek van. Het zou beter zijn geweest als de inhoud wel gedecentraliseerd was, maar de administratieve processen centraal waren georganiseerd. Het zou dan helpen als internal auditors dit vroegtijdig signaleren en aangeven bij de beleidsmakers. Bij al deze functies moet er een brede auditblik zijn, van buiten naar binnen, om zo inzicht te krijgen en te adviseren aan bestuurders." <<

De ontwikkelkalender 2025 voor de internal audit professional

Verplichte kost moet ook lekker smaken!

Elk jaar staan veel opleidingsinstellingen weer voor de uitdaging om een inspirerende en relevante ontwikkelkalender te creëren die niet alleen voldoet aan de vraag, maar ook deelnemers verrast, inspireert en motiveert met inzichten die de deelnemer versnellen in zijn of haar impact in de praktijk.

Carole Beelen

Arthur Izeboud

In dit artikel komen Arthur Izeboud en Carole Beelen aan het woord over hun zienswijzen op de behoeften en kansen om trainingen te laten renderen als input voor de ontwikkel-kalender 2019-2020 van Vanberkel Academy, onderdeel van Vanberkel Professionals

Arhur Izeboud RA, programma manager Vanberkel Academy en Carole Beelen, change & learning architect en onder andere facilitator bij Vanberkel Professionals, werken nauw samen bij het ontwerp, ontwikkeling en ook het faciliteren van de diverse trainingen van Vanberkel Academy.

Beelen: 'Veel mensen percipiëren verplichte Permanente Educatie als iets negatiefs, het uitzitten van een 'training' om PE-punten te sprokkelen. Het is mijn missie om het zogenaamde "PE-zaaltjes leed" te elimineren.' Hierbij maakt Beelen gebruik van diverse actieve methoden en technieken die vanuit een enorme creativiteit en positiviteit deelnemers laten ervaren en hen onbewust laten leren.

Carole maakt gebruik van Moreno-technieken. De kern van de Moreno-methode ligt in het uitbeelden en uitspelen van gebeurtenissen, situaties, toekomstvragen, dilemma's en conflicten in plaats van erover te praten. Het doorleven en beleven zorgt voor diepere en rijkere inzichten dan praten alleen.

Dit komt ook terug in de NBA-verplichte fraude training die Vanberkel Academy heeft ontwikkeld en verzorgd.
Eerst gaan de deelnemers aan de slag met een E-learning om vervolgens met elkaar aan de slag te gaan in een classroomsessie.

Izeboud: 'De doelstelling was om, ondanks dat het een verplichte training betreft, er een onvergetelijke leerervaring van te maken waar deelnemers het praktisch nut voelen en ermee aan de slag willen. Nu is het leuk dat wij dat zo voor ons zien, maar je weet het pas echt wanneer de eerste evaluaties binnenkomen. Die bleken 'uitmuntend' te zijn, waarbij juist de elementen van de Moreno-methode expliciet als positief worden genoemd.'

De top 5 ontwikkelagenda voor de internal audit professional voor het komende jaar, ziet er volgens Beelen en Izeboud als volgt uit:

1. ***Persoonlijke impact:*** *bewust zijn van je persoonlijke impact en de kansen tot impactvergroting*
2. ***Spelen met rapporteren:*** *het verhogen van de impact van audit rapportages op stakeholders door creatief en inno-vatief te schrijven en presenteren.*
3. ***Waarderend en waardevol auditen:*** *bijdragen aan de positief emotionele staat van de auditee*
4. ***Rendement op Data:*** *van data naar inzicht naar besluit-vorming en uitvoering en de rol van internal audit daarin*
5. ***De Customer Journey van de auditee:*** *het bewust managen van de maximale klant/stakeholder beleving met verworvenheden uit de marketing en communicatie*

Izeboud: 'Wat we ook zien is dat de wat grotere internal audit teams steeds meer maatwerk kiezen bij hun interne opleidingsbehoeften. Wij helpen ze dan bij het samenstellen van de juiste mix van onderwerpen en methoden gericht op hun specifieke behoeften.'

In 2025 is internal audit 'echt' the trusted advisor

Ing. Erwin de Koster CIA CISA RO
Internal auditor KPN

☐ Eens ☑ Oneens

"Deze stelling roept bij mij een aantal vragen op. Bestaat internal audit in 2025 in de huidige vorm nog wel? Voorspellingen zeggen dat de kans bijna 100% is dat de taken van auditors worden vervangen door robots. Wanneer ben je een trusted advisor? En voor wie dan? Volgens de Rijksuniversiteit Groningen noemen opdrachtgevers zelden kennis en kunde als doorslaggevende factor. Het gaat meer om het woord vertrouwen, en dat baseren opdrachtgevers voornamelijk op emotie. Het woord 'echt' impliceert dat internal audit nu nog niet wordt gezien als trusted advisor? Als dit nu al niet het geval is, waarom zou dat in 2025 dan wel zo zijn? Wat, of nog beter, wie moet er dan veranderen?"

Drs. Hans Jaap Abma EMIA RO
Manager Internal Audit Ipse de Brugge

☐ Eens ☑ Oneens

"Ik heb een beetje moeite met de stelling. De stelling lijkt te impliceren dat de internal auditor op dit moment 'nog niet echt' the trusted advisor is. Ik mag hopen dat de internal auditor nu ook al als zodanig wordt gezien. Over zes jaar moet het bestuur de auditor nog steeds als zijn gewaardeerde adviseur zien. Mogelijk vindt er een verschuiving plaats over de onderwerpen waar de auditor aanvullende zekerheid over geeft, maar dat hij 'trusted' is en blijft, staat buiten kijf."

Cora Timmers RO
Quality Assurance Officer IFRS 17, Aegon

☑ Eens ☐ Oneens

"Dat zou mooi zijn. Ik ben optimistisch en ik denk dat we er als beroepsgroep steeds meer naar toe groeien. Maar we zijn er nog niet. Belangrijk bij het worden van trusted advisor is dat we 'echt' goed snappen wat ontwikkelingen zijn binnen het bedrijf en in de wereld daarbuiten en dat we goed snappen wat de zorgen zijn van het management. Als we daarbij op een goede en aansprekende manier adviseren, worden we als trusted advisor gezien door het management."

Drs. Korstiaan Kegel RA CIA CRMA
Hoofd Internal Audit Allianz Nederland

☐ Eens ☑ Oneens

"'Echt' is te sterk verwoord. Onze beroepsgroep groeit hier steeds meer naartoe door verdere professionalisering (IAF en AC), datagebruik en specialisatie. En door onze kennis van het bedrijf, inclusief cultuur en politiek, spelen wij deze rol al deels, zeker inzake de interne beheersingsomgeving. Echter, er zijn voor veel onderwerpen betere gespecialiseerde adviseurs, die naast meer relevante ervaring ook gerichte tooling en externe vergelijkingsdata gebruiken. Wel ervaar ik dat internal auditors in veel landen steeds minder als politieagent en meer als sparringpartner worden gezien."

De reacties op de stellingen zijn gegeven op persoonlijke titel.

- Audit 2025
- Zorg
- Lerende (zorg)organisatie

Thema
Tekst Drs. Nicole Engel-de Groot RA
Beeld NFP Photography

De LERENDE zorgorganisatie

's Heeren Loo, Nederlands grootste aanbieder van zorg voor mensen met een verstandelijke beperking, zette in 2014 een internal auditfunctie op. Jan Fidder (voorzitter RvB) en Louis Beenen (hoofd IA) over hoe de internal auditfunctie nu en in de toekomst waarde toevoegt.

Over…

Jan Fidder is sinds 2016 CEO van 's Heeren Loo. Daarvoor was hij CEO van Gelre Ziekenhuizen, Ipse de Bruggen en commercieel directeur bij de ArboUnie. Daarnaast vervulde hij vele bestuurs-en toezichthoudende functies. Fidder begon zijn loopbaan als arts en fysiotherapeut.

Louis Beenen is sinds 2014 hoofd Internal Audit bij 's Heeren Loo. Daarvoor werkte hij bij het ministerie van Defensie in functies op het gebied van auditing, finance, IT en bedrijfsvoering.

Wat doet 's Heeren Loo?

Fidder: "'s Heeren Loo is een stichting die zorg biedt aan ruim 10.000 cliënten met een verstandelijke beperking. De zorg varieert van lichte ondersteuning aan huis tot intensieve 24-uurs opvang op woonlocaties. De zorg vindt plaats in 15 regio's in heel Nederland. Regiodirecteuren zijn integraal verantwoordelijk voor hun zorgregio. 's Heeren Loo heeft 14.000 werknemers in dienst. Daarbovenop zijn er 4600 vrijwilligers. De raad van bestuur (RvB), bestaande uit 3 personen, is verantwoordelijk voor het strategisch beleid en geeft leiding aan 15 regiodirecteuren en 7 concerndirecteuren. Een raad van toezicht ziet toe op het functioneren van de RvB. De internal auditfunctie (IAF) is rechtstreeks onder de voorzitter van de RvB gepositioneerd."

Waarom heeft 's Heeren Loo een IAF?

Beenen: "In 2014 is besloten om een IAF op te richten conform het three-lines-of-defensemodel. Doel van de IAF was om te zorgen voor een continue verbetering van de organisatie. Vanuit het uitgangspunt dat het management verantwoordelijk is, dienen de werkzaamheden van de IAF eraan bij te dragen dat de organisatie continu leert en verbetert. De IAF geeft onafhankelijke oordelen op vraagstukken die er leven binnen 's Heeren Loo. De IAF werkt vraaggestuurd. De vragen kunnen komen van de RvB, maar ook van de directeuren. In de loop der jaren is de IAF verder ontwikkeld. Dit heeft erin geresulteerd dat we sinds kort ook het IIA-certificaat hebben. We zijn met 5 mensen en ambiëren geen groei in mensen. We zorgen ervoor dat we een groot (intern) netwerk hebben, dat mensen binnen 's Heeren Loo ons weten te vinden. We werken met een flexibele pool bestaande uit 25 mensen uit de regio's met een heel diverse achtergrond, maar met één belangrijk gemeenschappelijk element: zij vinden kwaliteit belangrijk. Dit werkt heel goed. Als we een auditopdracht uitvoeren putten we uit de flexibele pool waarbij iemand van de IAF de regie houdt. We merken dat een IAF niet alleen binnen de RvB wordt gewaardeerd, maar ook daar waar de zorg verleend wordt. We staan middenin de organisatie en praten met medewerkers, cliënten en hun

"Alles wat we doen is vraaggestuurd en onze focus ligt altijd op een toetsende rol en het geven van inzicht"

naasten. We ervaren dat mensen zich veilig voelen om te praten over kwaliteit en hoe dingen mogelijk beter kunnen. Doorgaans zijn mensen blij dat ze aandacht krijgen en hun verhaal kwijt kunnen."

Omschrijf de IAF eens

Fidder: "Continu verbeteren, leren en ontwikkelen vanuit een onafhankelijke positie. We zitten met 1000 teams in 1000 gebouwen in 210 gemeenten in Nederland. Tegelijkertijd willen we met één beeld naar buiten treden. Onze IAF raakt alle regio's en alle activiteiten. Het is ontzettend behulpzaam om ons beleid te toetsen aan de realiteit. De IAF is altijd onafhankelijk, heeft geen eigen- of afdelingsbelang. Ze staan middenin de organisatie met kennis en kunde en zicht op de processen, de context en de branche. Ze kijken naar het primaire proces en geven terug wat wel werkt en wat niet."

Omschrijf de bestuurder als opdrachtgever eens

Beenen: "Het samen doen, een gezamenlijk doel en nabijheid. Met dat laatste bedoel ik dat we elkaar makkelijk vinden. Na elk onderzoek volgt uiteraard een formeel rapport, maar evengoed lopen we bij elkaar naar binnen om open te praten over bevindingen. We trekken samen op met ieder een eigen rol. Als IAF zijn we de neutrale aanbrenger van feiten en bevindingen. We zijn hierin belangeloos en onafhankelijk. De RvB staat meer in de wind. Zij zijn aanjager van de discussie over wat te doen met de bevindingen. Die rolverdeling is cruciaal."

Wat zijn de taken van de IAF?

Beenen: "Alles wat de organisatie raakt, raakt de IAF. Onze taken zijn het uitvoeren van onderzoeken en het adviseren over risicomanagement. Alles wat we doen is vraaggestuurd en onze focus ligt altijd op een toetsende rol en het geven van inzicht. We doen wel financiële onderzoeken maar geen werkzaamheden voor de externe accountant. Ook doen we geen onderzoeken volgend uit een wettelijke taak. We adviseren vooraf over risico's. Deze adviesfunctie komt ook tot uiting in de bilaterale overleggen tussen RvB en IAF waar we ook spreken over wat er op 's Heeren Loo afkomt. Verder doen we ook quick scans om zo in een kort tijdsbestek inzicht te geven. We maken jaarlijks in november een jaarplan met input uit een 'rondje langs de velden'. Dit jaarplan wordt vastgesteld door de RvB. We bouwen voldoende flexibiliteit in het jaarplan om gedurende het jaar door middel van bijvoorbeeld quick scans in te spelen op actuele vragen. We doen ongeveer 35 onderzoeken in het jaar."

Aan wie rapporteert de IAF?

Fidder: "In de eerste plaats ontvangt de opdrachtgever een rapport. In het rapport zijn bevindingen en praktische aanbevelingen voor verbetering opgenomen. Daarnaast worden alle rapporten van internal audit (IA) besproken in de RvB en daarna ook in de vergadering van de RvB met de directeuren. Dit doen we omdat we het belangrijk vinden om best practices te delen binnen de organisatie. Dat maakt het ook best spannend voor directeuren, want de rest ziet aan de hand van de IA-rapportage hoe het ervoor staat in die betreffende regio of bij die concerndienst. Door de RvB wordt een actieverantwoordelijke voor het uitvoeren van de aanbevelingen uit het rapport benoemd. Alle besluiten en acties vanuit de RvB komen op een zogenaamde actiekaart.

De actiekaart bevat, onder andere, alle aanbevelingen van IA. De voortgang wordt door de RvB periodiek besproken met het lijnmanagement. Op verzoek toetst de IAF de juiste follow-up van acties. Daarnaast maakt IA ieder kwartaal een voortgangsrapportage met hierin de realisatie van het jaarplan, een samenvatting van de uitgebrachte rapportages inclusief follow-up, en ontwikkelingen op het gebied van risicomanagement, interne beheersing en governance."

Wat zijn de uitdagingen voor 2020 voor de IAF?
Fidder: "Het nog beter verspreiden van kennis over uitgevoerd onderzoek, zodat leren van elkaar nog meer gestalte krijgt. En een uitdaging is om niet verzeild te raken in eerste- en tweedelijns werkzaamheden maar om juist de eerste en de tweede lijn binnen de organisatie sterker te maken, zodat doelstellingen effectiever en efficiënter behaald worden. De IAF moet zo klein mogelijk blijven. Je wilt dat mensen in de organisatie zelf gaan nadenken over of ze compliant zijn en waarom er afgeweken wordt. De bijdrage van de IAF is om mensen te laten nadenken wat nu de meest effectieve checks in een proces zijn. Als je mensen in de lijn die dicht op het proces zitten zelf aan het stuur zet om na te gaan wat kwaliteit is en hoe ze het beste kwaliteit kunnen monitoren, dan heb je de grootste kans om als organisatie je doelstellingen te behalen. We willen mensen bewust(er) maken."

In hoeverre voert het hoofd IA de door hem gewenste werkzaamheden uit?
Beenen: "Vraaggestuurd werken helpt om de goede dingen te doen. We doen datgene waar echt een behoefte aan is. We geven additionele zekerheid, wat waarde toevoegt gezien de omvang van een organisatie als 's Heeren Loo."

Krijgt de bestuurder de door hem gewenste additionele zekerheid?
Fidder: "Absoluut. Om een grote organisatie te besturen anno 2019 is de IAF een onmisbare schakel. Dit kan alleen als het eigenaarschap op de goede plek belegd is. Als rollen helder en duidelijk zijn en de IAF vanuit een absoluut onafhankelijke positie feiten toetst, dan geeft dit veel toegevoegde waarde. In de zorg moeten we constant alert zijn. Er verandert veel, vanuit de overheid, de zorgvrager of de branche. Je kunt hier alleen goed mee omgaan als je flexibel bent. De quick scans die de IAF uitvoert zijn belangrijk om te kijken wat werkt en wat niet. Ons doel is om goede zorg te bieden. Dat is zorg van goede kwaliteit, die veilig, betaalbaar en toegankelijk is. Uiteindelijk is dat afhankelijk van mens-tot-menscontact. Om dit te borgen in een organisatie met zoveel mensen op zoveel locaties, hebben wij veel baat bij een kleine effectieve IAF met een groot netwerk. <<

"De IAF kijkt naar het primaire proces en geeft terug wat wel werkt en wat niet"

■ Audit 2025
■ Internal auditfunctie
■ Data science

Thema
Tekst Drs. Margot Hovestad RO
Naeem Arif EMIA RO
Beeld Adobe Stock

Performance en strategie-uitvoering

Hoe ziet de toekomst van de interne auditfunctie eruit? Wat is de rol van data science binnen audit? In gesprek met prof.dr. Edo Roos Lindgreen RE, hoogleraar Data science in auditing aan de Universiteit van Amsterdam.

Over...

Edo Roos Lindgreen studeerde informatica aan de UvA, promoveerde aan de TU Delft en is hoogleraar Data science in auditing aan de Universiteit van Amsterdam. Daarvoor was hij partner bij KPMG waar hij diverse functies vervulde.

Voor onze lezers die u niet kennen: wie is Edo Roos Lindgreen?

"Ik heb informatica gestudeerd aan de Universiteit van Amsterdam (UvA). Daarnaast heb ik gewerkt als developer. Na korte tijd gewerkt te hebben bij een startup heb ik promotieonderzoek met betrekking tot informatiebeveiliging gedaan aan de Technische Universiteit Delft. Vervolgens ben ik bij KMPG gaan werken in diverse functies, waaronder in IT-audit en advisory. Bovendien ben ik een aantal jaren verantwoordelijk geweest voor het uitvoeren en opzetten van het innovatieprogramma binnen KPMG.
In 1998 werd ik docent aan de UvA en in 2002 ben ik benoemd als deeltijd hoogleraar IT en Auditing. Sinds twee jaar ben ik fulltime hoogleraar Data science in auditing. In die hoedanigheid verzorg ik onderwijs en voer ik onderzoek uit op het snijvlak van auditing en data science. Tevens ben ik programmadirecteur van de opleidingen Executive MSc of Internal Auditing (EMIA) en Executive Programme of Digital Auditing (EPDA), en eindverantwoordelijk voor het Institute of Executive Programs van UvA."

Hoe definieert u het vak data science?

"Data science is de wetenschap en praktijk die zich bezighoudt met het verzamelen, bewerken, verwerken en interpreten van data om inzicht te krijgen en conclusies te kunnen trekken. Hierbij wordt gebruikgemaakt van zowel gestructureerde als ongestructureerde data, vanuit zowel interne als externe bronnen. Het gaat om het verkrijgen en geven van inzicht en hierbij is statistiek ontzettend belangrijk. De auditor hoeft geen data-expert te zijn maar de basiskennis is wel noodzakelijk.
Zonder voldoende kennis is het risico van verkeerde conclusies levensgroot. De auditor moet weten wanneer welke methoden en technieken toegepast dienen te worden. Er zijn een paar simpele dingen die de auditor in ieder geval moet weten. Een voorbeeld daarvan is dat een hoge mate waarin twee variabelen met elkaar samenhangen (correlatie) niet per definitie betekent dat er een causaal verband is

tussen deze variabelen. Correlatie en causaliteit zijn twee verschillende dingen. Hier zie je ook een verschil tussen een 'gewone' wetenschapper en een data scientist."

Wat is dat verschil dan?

"Een wetenschapper zoekt doorgaans oorzakelijke verbanden en stelt op basis daarvan een model op en verkrijgt daarmee inzicht. Een data scientist gaat op zoek naar patronen en verbanden en stelt op basis daarvan een model op waarmee inzicht wordt verkregen. Daarnaast moet je als auditor oppassen voor 'spurious correlations': een toevallig verband tussen twee variabelen die niets met elkaar te maken hebben. Zo blijkt er een sterk verband te zijn tussen de gemiddelde temperatuur in een bepaald jaar en het aantal films met Nicolas Cage in de hoofdrol.
Een laatste gevaar is dat mensen – en dus ook auditors – de neiging hebben overal patronen in te zien, ook als die er niet zijn. Veel processen die wij observeren zijn willekeurig, dat is nu eenmaal zo."

Hoe kijkt u naar de relevantie van de beroepsgroep van interne auditors?

"De relevantie van de beroepsgroep wordt steeds groter. Wat is de 'why' van een interne auditfunctie? Dat is naar mijn mening het geven van aanvullende zekerheid aan het bestuur, de auditcommissie, de aandeelhouders en vele andere stakeholders. Stakeholders verkrijgen primair zekerheid door eigen observaties en rapportages uit de eerste lijn. Maar soms is er dan sprake van schijnzekerheid, omdat zaken mooier worden voorgesteld dan ze zijn. In die gevallen is het de derde lijn die zekerheid geeft.
In de herziene Corporate Governance Code wordt een prominentere rol ingeruimd voor een interne auditfunctie. De functie is een steeds belangrijker voelspriet voor de auditcommissie om te meten of alle risico's adequaat worden beheerst en of de strategie van de organisatie goed wordt uitgevoerd. We zien een verschuiving in de eisen die worden gesteld aan de interne auditfunctie; steeds minder compliance en steeds meer performance. De werkzaamheden worden meer proactief en zijn gericht op het auditen van een

"Elvis Presley zong het al: 'Before you abuse, criticize and accuse, walk a mile in my shoes'"

consistente uitvoering van de strategie en op de sturing en beheersing van de organisatie."

Welk profiel heeft de interne auditor nodig in de toekomst?
"Vroeger had je de interne accountant die de interne cijfers controleerde, en bij een aantal organisaties is dat nog steeds zo. In de tweede helft van de jaren negentig kwam de nadruk te liggen op operational audits. Vervolgens werd compliance steeds belangrijker, mede door de schandalen aan het begin van deze eeuw. En op dit moment zien we weer een beweging naar operational audit en strategie-uitvoering.
Dit is een natuurlijke ontwikkeling die de interne auditor doormaakt en die gestuurd wordt door de behoeften van de stakeholders. De interne auditor past zich hierop aan, dat gaat heel organisch. Een deel van de populatie interne auditors past zich iedere keer aan de ontwikkelingen aan. Daarnaast komen er specialisten op nieuwe gebieden, zoals data science of gedrag en cultuur. En er blijven natuurlijk ook financiële experts. Het belangrijkste is dat een interne auditfunctie diversiteit heeft in het team. Hiermee moet rekening worden gehouden bij het aannamebeleid."

Hoe ziet u de interne auditfunctie in 2025?
"Compliance blijft een belangrijk werkgebied van de functie, zeker in de financiële sector. Ik denk dat de functie belangrijker wordt in impact en omvang. De belangrijkste uitdagingen zijn het aantrekken van goede mensen, het behouden van goede mensen en het krijgen van waardering vanuit de business. Met dat laatste bedoel ik dat interne auditors zich moeten afvragen: hoe voeg ik waarde toe? Geef ik inzichten die de organisatie niet had?
Een andere trend is dat er meer aandacht uitgaat naar performance en strategie-uitvoering, dus meer proactief. Internal auditing wordt zeker meer data driven. Het besef groeit steeds meer dat een interne auditfunctie deze expertise op peil moet brengen en houden. Er moet geïnvesteerd worden in tools, technieken, kennis, middelen en mensen."

Nog meer trends?
"Gedrag en cultuur krijgen een steeds prominentere plaats. Gedrag en cultuur worden vaak aangeduid als zachte factoren, onterecht wat mij betreft. Deze factoren zijn keihard en bepalend voor wat er in een organisatie echt gebeurt. Gedrag valt niet te ontkennen. Over gedrag kun je niet liegen: het vindt plaats en heeft een grote impact. Cijfers zijn eigenlijk veel zachter. Cijfers representeren een bepaalde interpretatie van de werkelijkheid. Er kunnen legio aannamen in zitten. Dat maakt manipulatie veel makkelijker. Veel auditcommissies vinden de betrouwbaarheid van de financiële rapportage helemaal niet zo interessant meer, ze zien het meer als een hygiënefactor. Zij zijn meer geïnteresseerd in strategie en risicobeheersing. Dat gaat ook – juist – over gedrag en cultuur. Immers, het zijn de medewerkers die de strategie moeten uitvoeren."

Hebt u wijzigingen aangebracht in het curriculum van de auditopleidingen richting 2025?
"Voor het succes van een interne auditfunctie is omvang een belangrijke factor. Hoe groter de omvang, hoe meer diversiteit kan worden aangebracht. Voor het inrichten van het curriculum is het belangrijk dat je weet wie je doelgroep is. Leid

ik een specialistische interne auditor op voor een grote bank met een superervaren team? Of leid ik een jonge auditor op die werkt bij een woningcorporatie met een klein en relatief onervaren team? Wij willen de internal auditopleiding van keuze zijn voor alle interne auditors in Nederland, of je nu bij een grote of een kleinere organisatie werkt. Er wordt een breed spectrum aan auditors opgeleid.
Wat de student in ieder geval moet leren zijn de basisbeginselen van auditing. Bij de basis hoort ook de inrichting van de administratieve organisatie en processen (accounting information systems, voorheen BIV/AO). Een belangrijk vak in het eerste jaar, een soort combinatie van een marathon en een ontgroening. Daarna komt de specialisatie met vakken als management accounting, ethiek en integriteit, quality assurance review, managing the internal audit function, personal development, internal governance en internal audit excellence. In dit laatste vak is veel aandacht voor gedrag en cultuur.
En natuurlijk het vak data science for auditors, een gecomprimeerde versie van een groter programma dat we hebben ontwikkeld voor de accountantsopleiding. In dit vak leren de studenten de eerste beginselen van data science, zoals: 'hoe stel ik een data driven auditplan op?', wat is regressie?', 'wat is machine learning'?' We zouden graag meer tijd aan dit onderwerp willen besteden, maar dan moet er ook een vak verdwijnen anders wordt de opleiding te zwaar, dat is een lastige keuze. Gelukkig komt data science steeds meer voor in de reguliere masteropleidingen. Dus uiteindelijk hoeven wij dat niet meer te doen. Het toepassen in de dagelijkse praktijk blijft wel een aandachtspunt voor ons. Hetzelfde geldt voor gedrag en cultuur, ook hier zouden we meer tijd aan willen besteden."

In uw oratie stelt u dat er een paradigmaverschuiving nodig is. Kunt dit toelichten?
"Onze huidige omgang met data en computers is ontstaan in de jaren zeventig van de vorige eeuw, toen de computer voor het eerst werd geïntroduceerd in bedrijven. Destijds hebben auditors bepaald hoe daar mee om te gaan en deze manier van werken hebben ze de afgelopen drie á vier decennia meegenomen. De interne auditor kijkt naar de interne beheersing in de systemen. En zo wordt er nog steeds gewerkt. Maar nu is er een nieuwe wereld. Er is een oceaan aan data die voor iedereen toegankelijk is, met fantastische tools die de interne auditor kan gebruiken om in die data te gaan zoeken en deze te analyseren. Maar daar moeten ze wel even aan wennen. Het gewenste paradigma is de focus hebben op data en niet op systeemcontroles. En de data zijn niet alleen data van de organisatie zelf, maar ook van externe bronnen en zowel gestructureerd als ongestructureerd. Deze paradigmaverschuiving zal zonder twijfel plaatsvinden, dat is een kwestie van tijd."

Welke blinde vlekken heeft de beroepsgroep?
"De beroepsgroep heeft soms een blinde vlek voor de waardering van hun werk door de auditees en stakeholders. Hoe kijken deze partijen tegen de interne auditfunctie aan? De beroepsgroep heeft soms een te rooskleurig zelfbeeld, schat de appreciatie van de business te hoog in. Veel auditors leven een beetje in een bubbel, net zoals medewerkers in iedere andere beroepsgroep overigens. Interne auditors denken soms dat ze toegang hebben tot alle informatie en deze ook krijgen. Maar dat is niet altijd zo. We moeten de bubbel zien te doorbreken door in de spiegel te blijven kijken, ook proberen te voelen wat het effect is van ons werk op de ander. Een uiterst kritische blik en een onderzoekende geest combineren met enig empathisch vermogen. Een rotatieprogramma kan hierbij enorm helpen. Laat de business een tijdje bij de interne auditfunctie komen werken en laat interne auditors in de business werken. Elvis Presley zong het al: 'Before you abuse, criticize and accuse, walk a mile in my shoes.'" <<

"Interne auditors denken soms dat ze toegang hebben tot alle informatie en deze ook krijgen. Maar dat is niet altijd zo"

■ Audit 2025
■ UMC Utrecht
■ Semipubliek

Thema
Tekst Naeem Arif EMIA RO
Jip Olieroock MSc RO CIA
Beeld UMC Utrecht

"Het gaat om de allerbeste zorg: *nu en in* de toekomst"

UMC Utrecht heeft sinds 2017 een interne auditfunctie (IAF). Mirjam Velthuizen-Lomans is lid van de raad van bestuur met als aandachtsgebied bedrijfsvoering. Ze vertelt over haar eerste ervaringen met de IAF.

Over...

Mirjam Velthuizen-Lomans studeerde beleid en management gezondheidszorg in Rotterdam. Sinds 2000 werkt zij voor UMC in verschillende rollen en sinds 2013 neemt zij plaats in RvB van UMC. Daarnaast vervult zij vanaf maart 2019 tijdelijk de rol van vicevoorzitter.

Kunt u iets over uzelf vertellen?

"Sinds vijf jaar ben ik lid van de raad van bestuur van het UMC Utrecht. Ik beheer daarbinnen de portefeuille bedrijfsvoering. Voor het UMC Utrecht betreft dit de onderwerpen: financiën, informatietechnologie, vastgoed & huisvesting en duurzaamheid. Wanneer ik invulling geef aan mijn werkzaamheden staat de vraag centraal hoe ik het best toegevoegde waarde kan leveren aan de medewerkers en patiënten. Zo begin ik elke week met mijzelf de vraag te stellen wat ik de komende week ga toevoegen voor de mensen die ons nodig hebben. Het gaat om de allerbeste zorg: nu en in de toekomst. Dus om continu vernieuwen.
Ik ben van mening dat de bedrijfsvoering minstens net zo innovatief moet zijn als de medische zorg. Denk bijvoorbeeld aan het steeds meer thuis organiseren van de zorg met behulp van ICT, zodat een ziekenhuisbezoek niet meer of minder nodig is. Dit vergt vergaande vernieuwingen op ICT-gebied. En als je dat organiseert, moet je ook weer kijken naar de gevolgen hiervan voor je gebouw: de patiënten die nog komen, vragen ook dan een specifiek type zorg. Zo hebben we bijvoorbeeld een pilot, genaamd 'save@home', bij kritische zwangerschappen.
Met behulp van e-health en thuismonitoring hoeven patiënten veel minder vaak naar het ziekenhuis. Zij voelen zich beter begeleid, minder belast en we denken dat het op termijn goedkoper is. Bedrijfsvoering raakt in die zin het hart van het primaire proces, namelijk de zorg, het onderzoek en het onderwijs. Ik vind dan ook dat bij elk type bedrijfsvoering de medewerkers zich af moeten vragen wat zij toe kunnen voegen aan betere zorg. Dat geldt ook voor de interne auditor."

Wat waren de motieven om een IAF in te richten bij UMC Utrecht?

"Aan het inrichten van een eigen IAF lagen zowel externe als interne motieven ten grondslag. De interne motieven hebben alles te maken met zelf vast willen stellen in hoeverre wij

in control zijn. Wij als UMC hebben te maken met veelheid aan extern toezicht. Vaak met een wettelijke basis. Diverse externe toezichthouders beoordelen de kwaliteit van onze zorg en de bedrijfsvoering. Het gevolg is legio inspecties en certificeringen, denk bij de bedrijfsvoering bijvoorbeeld aan brandveiligheid en voedselveiligheid. Als raad van bestuur vonden we het daarbij belangrijk dat we niet alleen door externe onderzoeken een beeld krijgen van de kwaliteit, maar dat wij als bestuur zelf ook een feedbackmechanisme hebben. Daarbij willen wij internal audit inzetten als verbeterinstrument. Het beter worden staat centraal: het gaat niet zozeer om een bepaalde hoeveelheid rapporten op te leveren (lees: productie draaien) maar juist om wat het in en rondom de zorg kan worden verbeterd. De IAF moet echt iets bijdragen."

Wat zijn de interne motieven?

"We kunnen nooit 100% in control zijn. Dit is ook geen doel op zich, het is juist om je steeds af te vragen wat je nog beter kunt doen om beter in control te geraken. Die vraag stelden we ons als bestuur ook. Daarbij hebben we gekeken wat we van het bedrijfsleven konden leren en zo kwam het oprichten van een IAF in beeld.
Daarbij sluiten de motieven om een IAF in te richten ook aan op het genoemde principe dat iedereen in de organisatie blijvend moet nadenken hoe ze hun toegevoegde waarde kunnen vergroten. Ik vind het belangrijk dat we ons continu afvragen hoe we kunnen verbeteren op de gebieden zorg, onderzoek en onderwijs. Voor vandaag en voor de toekomst. Dit was misschien wel de belangrijkste reden om een IAF op te richten. Interne audit moet je helpen om de blinde vlekken binnen de organisatie aan te stippen en je zo er op te wijzen waar je kunt verbeteren. Eigenlijk vind ik audit een instrument om je als organisatie continu te verbeteren."

Wat zijn de externe motieven?

"De externe motieven om een IAF in te richten hebben te maken met de ontwikkeling dat de maatschappij geen fouten meer accepteert en altijd een schuldige aan wil wijzen. Het is dan belangrijk om je te realiseren dat als er iets fout gaat, je bestuurlijk verantwoordelijk bent, maar dat je tegelijkertijd niet alles kunt weten. Waar mensen werken worden fouten gemaakt en van die fouten moet je kunnen leren. Als je wilt dat je organisatie leert, dan moet je beginnen met te accepteren dat fouten gemaakt worden. Alleen dan kun je bevorderen dat er van fouten wordt geleerd. Als je fouten afstraft, gaan mensen fouten verdoezelen en wordt leren onmogelijk."

Hoe is de IAF organisatorisch gepositioneerd?

"De IAF valt direct onder de raad van bestuur en heeft een lijn naar het audit comittee. Het hoofd Audit neemt deel aan vergaderingen van het audit committee en heeft ook altijd toegang daartoe indien nodig. Binnen het bestuur ben ik het eerste aanspreekpunt voor de IAF. Zo wordt bijvoorbeeld het auditjaarplan eerst met mij afgestemd. We zetten audit breed in op de gebieden zorg, onderzoek, onderwijs en bedrijfsvoering. De uitkomsten van de audits worden altijd afgestemd met de betreffende portefeuillehouder binnen de raad van bestuur.
Met de invoering van de IAF zijn we ook gestart met het three-lines-of-defensemodel. De IAF vormt de derde lijn. De tweede lijn is verantwoordelijk voor het maken van het overkoepelende beleid en het monitoren en ondersteunen van de eerste lijn. De tweede lijn bestaat uit afdelingen zoals recruitment, planning & control, finance, ICT, en het

onderzoeksbureau. Bij de tweede lijn staat de kwaliteit en veiligheid centraal. We hebben in de tweede lijn geen afzonderlijke afdeling Risicomanagement.
Om de IAF op te zetten hebben we een kwartiermaker gezocht die enerzijds wist wat interne audit inhoudt, en anderzijds ook in staat was de verbinding te maken met de lijnafdelingen om zo specifiek op zoek te gaan naar de toegevoegde waarde die interne audit ons zou kunnen bieden."

Hoe komt het auditjaarplan (van de IAF) tot stand?
"Aan de basis van het auditjaarplan ligt het audit universe. Het audit universe bestaat bij ons uit een matrix waarin alle processen van de organisatie zijn genoemd. We verrichten ten aanzien van deze processen een risicoanalyse, via gesprekken met de directies en het divisiemanagement. Daarbij staan de volgende vragen centraal: waar heb je al goed zicht op en waar heb je nu buikpijn van? Uit die gesprekken kwam een lijst met onderwerpen die we konden opnemen in het auditjaarplan. Deze is vervolgens voorgelegd aan de raad van bestuur en het audit comittee. Bij de start is besloten om de scope niet te groot te maken, om het instrument internal audit te kunnen leren gebruiken binnen de organisatie. Dat is enigszins strijdig met de wens van de auditor, die graag gelijk volledig wil zijn."

Welke typen audits staan op de planning?
"Het type audits dat wordt verricht is sterk wisselend en afhankelijk van de uitkomsten van de risicoanalyse. We hebben daarbij de audits niet ingedeeld naar de meer traditionele bloedgroepen: financial, IT en operational. We verrichten audits naar medicatieveiligheid, informatiebeveiliging, trials bij onderzoek (onderzoek samen met de industrie), energie en water en tijdschrijven. Zeer uiteenlopende onderwerpen. Dit maakt het noodzakelijk dat onze auditors ook breed inzetbaar zijn. Daar zitten natuurlijk ook grenzen aan. Per audit wordt dan ook gekeken of we expertise moeten aantrekken, uit de tweede lijn of via externe inhuur. Wat wel als belangrijke basis voor onze auditors geldt is kennis van auditmethodologie en kennis van de organisatie. Je moet de belangen van het bedrijf goed kennen en het auditobject goed snappen. Het UMC is een brede en complexe organisatie, dit is dan ook een blijvende uitdaging."

Hoe zijn de eerste auditrapporten ontvangen?
"Hoewel het even wennen was voor de organisatie zijn de eerste auditrapporten goed ontvangen. Het 'wennen' zit enerzijds erin dat het nieuw is voor de medewerkers dat ze nu beoordeeld worden door collega's, en anderzijds dat de rollen (en bijkomende taken en verantwoordelijkheden) niet altijd even duidelijk zijn. De organisatie is ook nieuwsgierig naar deze nieuwe functie, dus dat is positief. Ik denk dat we het instrument interne audit puur als faciliterend voor organizational learning hebben ingezet, daaraan heeft bijgedragen. In de gevallen dat er wel sprake was van frictie, had dit te maken met onbekendheid van de auditors met de processen binnen de organisatie. De auditee is dan van mening dat de auditor te weinig kennis heeft van het auditobject. Kritiek die we op dit punt hebben gehad was bij de opstart ook niet altijd onterecht.

"De volgende vragen staan centraal: waar heb je al goed zicht op en waar heb je nu buikpijn van?"

Wat ik ook belangrijk vind bij het opstellen van auditrapporten is de 'tone of voice'. Ik vind het relevant dat de auditor zich altijd goed uitspreekt zonder het spreekwoordelijke opgeheven vingertje. Voorheen kenden wij geen interne audit en elkaar aanspreken is dan in het begin nog best moeilijk. We zijn allemaal professionals en weten wat goed gaat en wat voor verbetering vatbaar is. Je ziet in de eerste rapporten dat daar nog naar gezocht wordt (niet te scherp), maar ik ben wel tevreden. Het gaat eigenlijk best wel goed. Rapporten worden altijd aangeboden aan de betreffende portefeuillehouder binnen de raad van bestuur. Deze geeft het rapport vervolgens aan de tweede lijn om een managementreactie op te stellen. Daarna gaan het rapport en de managementreactie samen naar de raad van bestuur en het audit comittee. Daarbij hebben wij ervoor gekozen de managementreactie niet op te nemen in het rapport. Hiermee willen wij voorkomen dat de conclusies uit een audit 'een compromis' worden. Wij willen, zeker in deze beginfase, dat eventuele tegenstellingen tussen wat de auditor vindt en wat de verantwoordelijke lijnmanager vindt, duidelijk naar voren komen. De auditor moet ook kunnen zeggen wat hij ziet. Iedereen moet echt zijn eigen rol kunnen vervullen."

Zijn de verwachtingen ten aanzien van de IAF uitgekomen?
"Jazeker! Ik denk dat een IAF het UMC echt helpt en dat het ook zo binnen de organisatie beleefd wordt. Daarbij heeft het invoeren van het three-lines-of-defensemodel ook bijgedragen aan het verder verduidelijken van rollen en verantwoordelijkheden binnen de organisatie. Een van de grote reserves bij de invoering van de IAF was dat we een extra administratieve last zouden creëren. Binnen de zorg is de administratieve last al enorm. Als de IAF als extra administratieve last wordt beleefd doen we het niet goed, het moet een instrument zijn om de professional te helpen. Overigens moeten we er scherp op blijven dat externe instanties producten van de IAF niet op een verkeerde manier gaan gebruiken. Omdat we interne audit als lerend instrument inzetten en niet als verantwoordingsinstrument, hoeven niet standaard alle aanbevelingen te worden opgevolgd door de auditee. De auditee kan, gezien zijn verantwoordelijkheden en professionaliteit, zelf ook goed een afweging maken welke aanbevelingen wel en welke (nog) niet worden overgenomen. Als een externe toezichthouder vervolgens de aanbevelingen als een set 'must-do' behandelt, dan werkt dit contraproductief. Het moet een leerinstrument zijn waarbij het niet direct noodzakelijk is dat alle aanbevelingen gelijk worden opgepakt. Dan kan het namelijk een zwakte worden."

Wat is de stip op de horizon voor de IAF van het UMC in 2025?
"De grootste uitdaging voor interne audit is telkens de juiste keuzen maken. Zowel qua te verrichten audits als ten aanzien van de omvang en aard van de aanbevelingen die je doet. Het is daarbij belangrijk dat de kern eruit wordt gelicht. Dit geldt ook voor de uitvoering en opvolging. Een ander belangrijk punt is het vertrouwen, enerzijds specifiek ten aanzien van de IAF en anderzijds breed binnen de hele organisatie. Vertrouwen is cruciaal in het werk dat we met zijn allen doen. Iedereen komt elke dag naar het UMC om zijn werk goed te doen. Dat is de grondhouding, maar waar mensen werken worden fouten gemaakt. Hoe houd je dan dat vertrouwen vast? De IAF moet bijdragen aan dat vertrouwen, anders heeft een IAF geen toegevoegde waarde voor organisatie. Alles driedubbel checken kan simpelweg niet en je moet erop kunnen vertrouwen dat medewerkers hun verantwoordelijkheid nemen. Dat kun je niet met afvinklijstjes bewerkstellingen."

Waar moet interne audit aan bijdragen volgens u?
"Ik denk dat het heel belangrijk is dat interne audit bijdraagt aan de groei van het vertrouwen dat medewerkers in elkaar hebben. Dit kan door op relevante processen 'in te prikken', het gesprek aan te gaan en inzicht te bieden in blinde vlekken die in loop der tijd ontstaan. Dat helpt het vertrouwen te laten groeien. Waar wij aan bouwen is een cultuur waar mensen vertrouwen krijgen en het normaal vinden dat ze verantwoordelijkheid nemen. Het nemen van verantwoordelijkheid hangt sterk samen met vertrouwen: je krijgt vertrouwen op het moment dat je verantwoordelijkheid neemt. We werken aan een cultuur waarin het vanzelfsprekend is dat je vertelt wat je doet, en waarom je het doet. En dat het niet als controle wordt gezien wanneer iemand vraagt hoe je het werk doet, maar juist als iets dat bijdraagt aan het verbeteren van het werk en aan veilig samenwerken. Daar moeten we naartoe en onze IAF draagt daar aan bij!" <<

Thema
Tekst Bas de Jong MSc RA
Beeld Adobe Stock

Sinds januari 2019 is het voor pensioenfondsen vanuit IORP II verplicht een internal auditfunctie te hebben ingericht.[1] De internal auditfunctie beoordeelt in hoeverre het systeem van interne beheersing adequaat en doeltreffend is. Bij veel pensioenfondsen staat deze functie op dit moment nog in de kinderschoenen. Wat is de komende jaren belangrijk voor een startende internal auditfunctie bij pensioenfondsen?

Internal audit bij pensioenfondsen: **2020-2025 en daarna**

Je hebt iemand in het kraaiennest nodig die tijdig waarschuwt waar de zandbank ligt: de auditor

Allereerst zijn de inrichting van de functie en de verschillende rollen daarbij van belang. IORP II maakt onderscheid tussen het sleutelfunctiehouderschap en de vervullersrol. Het sleutelhouderschap zie ik veelal (maar niet uitsluitend) bij een bestuurslid liggen. De vervullersrol kan op verschillende manieren worden ingevuld. Dat kan via de internal auditafdeling van een bestuursbureau, door gebruik te maken van de internal auditfunctie van uitvoerders of door een ingehuurde internal auditor.
De uitdaging is om voor voldoende deskundigheid en countervailing power te zorgen tussen de sleutelhouder en de vervuller van de internal auditfunctie en tussen de auditor en de auditee. Het is daarom logisch dat De Nederlandsche Bank (DNB) geschiktheidscriteria heeft opgesteld voor het effectief kunnen dragen van het sleutelhouderschap. Daarnaast is het belangrijk dat in het systeem van kwaliteitsbeheersing aandacht wordt besteed aan het zekerstellen van de benodigde ervaring en vaardigheden binnen de internal auditfunctie ten aanzien van de onderzoeksobjecten.

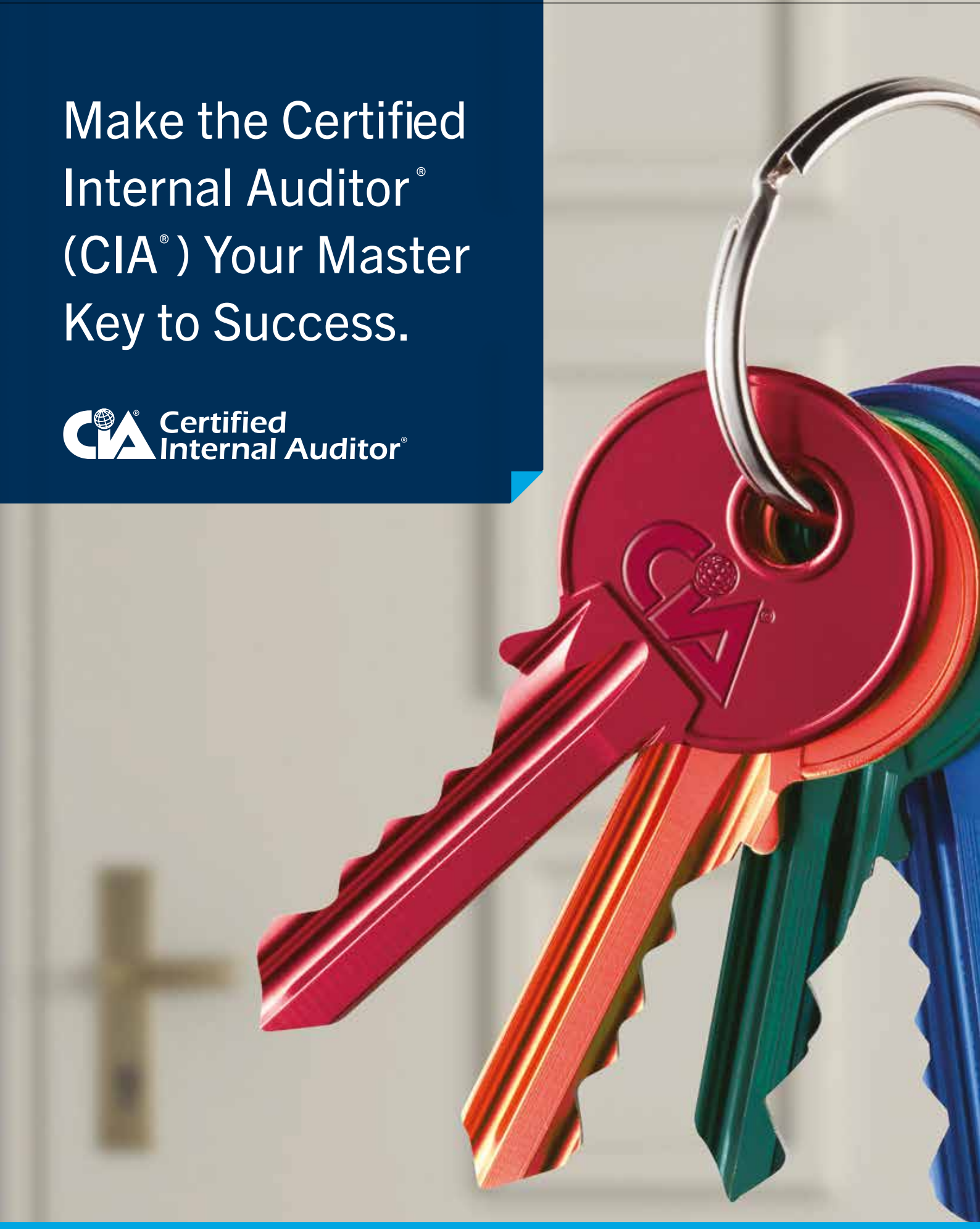
Proportionaliteit
Vervolgens rijst de vraag hoe omvangrijk en diepgaand de internal auditfunctie moet worden ingevuld. IORP II stelt dat de internal auditfunctie proportioneel mag worden ingevuld. Proportionaliteit draait om het afstemmen van de intensiteit van de internal auditfunctie op de aard en complexiteit van de organisatie. Maar dat is niet concreet. DNB heeft haar visie gegeven hoe zij de internal auditfunctie per categorie pensioenfonds normaliter ingevuld zou willen zien.[2] Deze visie heeft hoofdzakelijk betrekking op de inbedding van de internal auditfunctie in de organisatie, maar gaat niet in op de vraag hoe proportionaliteit uitwerkt op de diepte en reikwijdte van de werkzaamheden van de internal auditfunctie. Het goed toepassen van het proportionaliteitsbeginsel begint bij een goede risicoanalyse door het bestuur van het pensioenfonds. De uitkomst daarvan moet richtinggevend zijn voor interne beheersing van de organisatie en daarmee ook een belangrijke rol spelen in het auditplan van de internal auditfunctie.
De pensioensector kent een hoge mate van uitbesteding. Het is van belang te beseffen dat men risico's niet kan uitbesteden. Men besteedt de uitvoering van het proces dat gericht is op de beheersing van risico's uit. Dit betekent dat de beheersing van uitbestedingsrelaties een kernpunt is in de beheersingsraamwerken van veel pensioenfondsen.
Ik merk dat de pensioensector zich steeds meer bewust wordt van de inherente risico's die zij lopen. Daarbij zie ik een transitie waarbij sprake is van verdieping in het risicomanagement, dat wil zeggen dat de nadruk in toenemende mate op de inhoud van de risico's komt te liggen in plaats van op risicomanagement als proces. De vervolgvraag: hoe zorg ik ervoor dat ik aantoonbaar in control ben?, krijgt een steeds centralere rol in de organisatie. Pensioenfondsen professionaliseren hierdoor als organisatie en dwingen dergelijke volwassenheid af in de hele keten van dienstverleners.

Stakeholders en belangen
Risicomanagement en de bijbehorende interne beheersing is de voorbije jaren fors verbeterd en volwassen geworden. De groeikansen liggen er om risicomanagement beter aan te laten sluiten op de strategische doelstellingen en daarmee op de belangen van alle stakeholders. Ik zie vaak dat de invulling nog te veel 'toezichthoudergericht' is.
Er is een reëel gevaar dat pensioenfondsen auditmoe worden doordat verschillende partijen (toezichthouders, internal auditors, financial auditors) soortgelijke onderzoeken instellen die gericht zijn op het testen van de interne beheersing. Ik pleit daarom voor het opzetten, testen en verbeteren van een geïntegreerd risicobeheersingsraamwerk waarmee het waarborgen van de belangen van verschillende stakeholders aantoonbaar kan worden gemaakt.
Verder voorzie ik de behoefte dat men op efficiëntere wijze aantoonbaar in control wil zijn. Het interne beheersingsraamwerk moet voorzien in de belangen van alle stakeholders, wat doublures in audits vanuit toezichthouders, internal audit en financial audits moet minimaliseren. Eenmaal in control moet gewaarborgd worden dat de organisatie in control blijft. Daar heb je iemand in het kraaiennest voor nodig, de auditor, die tijdig waarschuwt waar de zandbank ligt. Door bij te sturen voordat het moet, ben je in staat om op efficiënte wijze aantoonbaar in control te blijven. Internal audit heeft daarin absoluut een sleutelrol.

Trends en thema's
Ik zie een duidelijke samenhang tussen de thema-audits van toezichthouders, trends binnen internal audit en de focus van pensioenfondsen. Enerzijds ligt de oorzaak hiervan in het eerder genoemde 'toezichthoudergericht' risicomanagement. Anderzijds zijn veranderingen in de sector, zoals technologische veranderingen, aanleiding voor nieuwe risicobeheersingsvraagstukken. Denk bijvoorbeeld aan cybersecurity, data-integriteit en privacy; onderwerpen die door nieuwe manieren waarop met deelnemers wordt gecommuniceerd bij ieder fonds veel aandacht krijgen.
In recent onderzoek (2018) concludeert DNB dat informatiebeveiliging bij instellingen in de financiële sector nog

Make the Certified Internal Auditor® (CIA®) Your Master Key to Success.

Certified Internal Auditor®



www.theiia.org/goto/CIAGlobal

The Institute of Internal Auditors | Global

niet op het vereiste volwassenheidsniveau is. Een van haar waarnemingen betreft het feit dat aandacht voor cybersecuritydreigingen en -maatregelen niet expliciet wordt gemaakt. Om het bewustzijn van cybersecurity bij instellingen te verhogen, heeft DNB haar toetsingskader Informatiebeveiliging geactualiseerd. Dit onderwerp, voor zover al niet op de agenda van pensioenfondsen, zal in de komende jaren prominenter verschijnen op de risicoagenda van pensioenfondsen en daarmee ook in de uitbestedingsketen.
Tussen 2020 en 2025 zie ik de volgende relevante thema's:

- de beheersing van datakwaliteit in de digitale wereld en de hierop gebaseerde rapportages, zowel financiële informatie als niet-financiële informatie;
- de verdere professionalisering en groei naar volwassenheid op het gebied van IT-risicobeheer;
- het effectief toepassen van het proportionaliteitsbeginsel bij pensioenfondsen;
- individualisering van informatiebehoefte bij pensioendeelnemers;
- het beheersen van de uitbestedingsketen (en mede daaraan gerelateerd);
- het behouden/verbeteren van voldoende deskundigheid en countervailing power op bestuursniveau.

De toekomst van de toekomst

De uitdaging daarna is misschien nog veel interessanter. Mijn verwachting is dat beheersingsmodellen van organisaties in den brede gaan veranderen en daarmee ook de rol van internal audit. Ik verwacht dat de eerste en tweede lijn, mede door verdergaand gebruik van data en automatisering steeds dichterbij elkaar komen te liggen. Robotics en algoritmische data-analyse kunnen waarschijnlijk beter en sneller afwijkingen detecteren dan mensen. De vraag is wie de robots programmeert, de algoritmen schrijft en de software onderhoudt. Het lijkt mij logisch dat de derde lijn in toenemende mate een IT-expertise ontwikkelt, zodat het gespecialiseerde IT-beheer effectief kan worden getoetst. Tegelijkertijd verwacht ik dat nadruk komt te liggen op gedrag en cultuur. De vraag hoe beslissingen en beleid tot stand komen en of dit kwalitatief in het belang van álle stakeholders is, laat zich misschien moeilijk in algoritmen vatten. Op papier kan een beslissing in een evenwichtig samengestelde groep tot stand zijn gekomen, terwijl besluitvorming in de praktijk helemaal niet in balans is. Bijvoorbeeld doordat bepaalde karaktereigenschappen in groepsdynamiek ertoe leiden dat een of meerdere personen 'de facto control' hebben en een overheersende stem laten horen. De vraag is of de internal auditor voldoende is opgeleid en in staat is dergelijke situaties te herkennen en op te volgen.

Sommige pensioenfondsen zijn organisaties die vanwege de omvang van het beheerd vermogen significante impact op de maatschappij als geheel kunnen hebben. Dat betekent dat de maatschappij een stakeholder van het fonds is. De vraag wat het rendement van die pensioenfondsen is, reikt verder dan het antwoord op de vraag of het fonds de pensioenen kan indexeren. Om het maatschappelijk rendement te berekenen moet je ook de niet-financiële impact meten.

De toekomst? Robotics en algoritmen. De vraag is wie de robots programmeert en de software onderhoudt

Het maatschappelijk rendement omvat bijvoorbeeld ook de impact van investeringsbeslissingen op de duurzaamheid van de samenleving, zoals uitgedrukt in CO_2-uitstoot, het financieren van projecten met een sociaal karakter, maar ook in de creatie van werkgelegenheid.
De vraag is hoe je de belangen van de stakeholders afweegt wanneer deze conflicterend lijken te zijn. Zijn deelnemers aan pensioenfondsen bijvoorbeeld bereid een lagere uitkering, hogere premie of latere pensioendatum te accepteren als dat een positief effect heeft op het behalen van ESG-doelstellingen? Hoe meet je dat, hoe weeg je belangen af en hoe adviseer je daarover als trusted advisor en assurance verstrekker?

Binnen of buiten de lijntjes kleuren

Samengevat verwacht ik dat het belang van een onafhankelijke functie die vaststelt of binnen de lijntjes wordt gekleurd, in de toekomst afneemt. Aan die behoefte kan waarschijnlijk grotendeels geautomatiseerd worden voldaan. De toegevoegde waarde van de internal auditor ligt wat mij betreft bij het toetsen van de kwaliteit van het waardemanagementproces. Waar niet zozeer de vraag centraal staat of de significante risico's adequaat worden beheerst, maar of het maatschappelijk rendement op een toereikende manier wordt gegenereerd. En dat roept weer allerlei andere vragen op, zoals hoe je maatschappelijk rendement meet en wat het normenkader is (wanneer is het toereikend?).

Hoe we daar komen? Met een stap tegelijk. Eerst 2020 dan maar. <<

Noten

1. https://www.toezicht.dnb.nl/2/6/50-237243.jsp
2. https://www.toezicht.dnb.nl/3/50-237612.jsp

Bas de Jong is registeraccountant bij Solutional, waar hij zich bezighoudt met interne beheersingsvraagstukken in de vermogenssector. Daarnaast is hij redactielid van *Audit Magazine*.

■ Gamification
■ Behavioral control

Artikel
Tekst Drs. René Taphoorn MPM
Beeld Adobe Stock
Agniseszka Boeske

Gamification voor de internal auditor

Gamification rukt op in onze samenleving. Kijk bijvoorbeeld naar de vele klant- en bonuskaarten met te verdienen punten en cadeaus om ons koopgedrag te beïnvloeden. Wat kun je als internal auditor nu precies met gamification?

Er zijn de afgelopen jaren veel publicaties verschenen over gamification. Het verschijnsel is niet nieuw, maar de term gamification is wel van relatief recente datum. De Engelse programmeur en uitvinder Nick Pelling gebruikte in 2002 gamification als eerste. Gamification trad op de voorgrond door de snelle technologische ontwikkelingen, waaronder ICT. Het komt voort uit de ontwikkeling van video- en computergames en de aandacht voor het game-ontwerp.

Doel en inhoud

Bij gamification gaat het niet om een volledige game, maar ligt de nadruk op spelelementen als bijvoorbeeld badges, scoreboards, feedback, levels en punten. Bij gamification worden spelelementen in een andere context gebruikt dan in een spelsituatie, bijvoorbeeld in een beleidsveld, een proces of product. Entertainment staat niet voorop, beleving is wel belangrijk. Spelelementen worden ingezet om mensen te betrekken bij een onderwerp (bewustwording) of hen te motiveren om bepaald gewenst gedrag te vertonen.
Hoe iemand een toepassing beleeft, is van grote invloed op zijn motivatie om wel of niet deel te nemen, verder te spelen, en zijn gedrag aan te passen. Gamification maakt daarbij vaak gebruik van ICT. Het uiteindelijk doel van gamification is het behalen van doelstellingen en/of het beheersen van risico's.
Gamification via motivatie en gedragsaanpassing is in feite een behavioural control. Het is een andere, meer speelse benadering dan de reguliere interventies van bijvoorbeeld aanspreken, verbieden, regels maken of sanctioneren. De reguliere interventies werken niet altijd even goed; gamification kan daarop een aanvulling zijn en kan wellicht een sterker effect hebben dan de reguliere interventies.

Gamification bij DJI

In mijn onderzoek ter afronding van de RO-opleiding heb ik een aanzet gegeven voor het ontwikkelen van gamification-toepassingen op hoofdlijnen voor een primair proces van een organisatie.[1] Om het concreet te maken heb ik het reïntegratieproces van jongeren in een justitiële jeugdinrichting bij DJI als uitgangspunt gekozen.
Een belangrijke taak van justitiële jeugdinrichtingen is het opvoeden, opleiden en behandelen van in de inrichting verblijvende jongeren, zodat zij zo goed mogelijk terug kunnen keren in de maatschappij (reïntegratie). De jongeren krijgen daartoe in verschillende fasen een programma met onderwijs/arbeid, trainingen van vaardigheden en behandelingen aangeboden. De motivatie om hier aan mee te werken is bij de jongeren vaak ver te zoeken. Gesprekken met de mentor en begeleiders en een uitnodigend klimaat in de leefgroepen zijn erop gericht om de jongeren te stimuleren aan de verschillende onderdelen mee te doen. De inzet van gamification kan hier een positieve bijdrage aan leveren en het sluit aan bij de belevingswereld van de jongere.
Het doel van de inzet van gamification is daarbij het volgende: gamification kan de bestaande interne beheersmaatregelen ondersteunen en daarmee een bijdrage leveren aan het voorkomen van risico's, zoals bijvoorbeeld het niet deelnemen of voortijdige uitval van jongeren aan trainingen

Onderdeel: **Confidence**	**Motivatiestrategie** (Keller) Het vertrouwen van de deelnemer kan worden vergroot door het volgende:	**Spelelementen** (o.a. Nuijten en Van Twist)
• Learning requirements	• Geef duidelijk het doel van de (leer)stof aan (om te slagen) en welke vereisten/stappen nodig zijn	• Story-walking
• Success opportunities	• Maak het mogelijk dat de deelnemers in het (leer)proces met stapjes groeien • Geef de deelnemers feedback over de verbeteringen en tekortkomingen gedurende de stappen, zodat zij hun prestaties kunnen verbeteren	• Levels/status, beloning via punten/scores, story-walking, simulatie • Feedback, punten/scores, scoreboard, competitie, leaderboards, challenges
• Personal control	• Geef de deelnemer (een gevoel van) controle over het eigen leerproces	• Keuzemenu's, simulatie

Tabel 1. Motivatie en spelelementen

en opleidingen. Gamification kan ook tot doel hebben om de kans op een geslaagde terugkeer van de jongere in de maatschappij te vergroten.

Ontwikkelen

Voor de ontwikkeling van gamificationtoepassingen is in het onderzoek een schema op basis van wetenschappelijke literatuur van Keller over motivatie en Nuijten en Van Twist over spelelementen samengesteld.[2,3] De motivatietheorie van Keller heeft betrekking op leren, waarbij motivatie onderverdeeld is naar de elementen ARCS, te weten Attention (aandacht trekken), Relevance (relevantie laten inzien), Confidence (vertrouwen laten groeien in eigen kunnen) en Satisfaction (voldoening hebben over de eigen prestatie). Aan de motivatie-elementen zijn strategieën verbonden om de motivatie te bevorderen. Daaraan zijn spelelementen gekoppeld. Het ziet er voor het motivatie-element Confidence uit zoals in *tabel 1*.

Toepassingen

Samen met acht gamificationdeskundigen, die tevens kennis hebben van justitiële jeugdinrichtingen, is vervolgens gebrainstormd over mogelijke gamificationtoepassingen die goed zouden passen bij een activiteit uit het primaire proces van reïntegratie. Daarbij zijn schema's van alle motivatie-elementen en activiteiten op elkaar gelegd ('mapping'). Per activiteit is met elkaar gekozen voor een of meer ARCS-elementen met bijbehorende spelelementen. De vraag daarbij was steeds: door welke motivatie-elementen worden de jongeren bij deze activiteit 'getriggerd'? Vervolgens is, uitgaande van de gekozen motivatie- en spelelementen, de gamificationtoepassing op hoofdlijnen omschreven en is een vorm voor de toepassing gekozen.

Deze mapping is op alle activiteiten van het primaire proces reïntegratie van jongeren in justitiële jeugdinrichtingen toegepast en resulteerde in 21 mogelijke gamificationtoepassingen op hoofdlijnen. De toepassingen hebben onder meer betrekking op het interactief geven van voorlichting (over verslaving, middelengebruik, beroepsmogelijkheden), het oefenen van vaardigheden (solliciteren, budgetteren) en het voorbereiden op de terugkeer naar de maatschappij (verlof, scholings- en trainingsprogramma buiten de inrichting).

Van de 21 mogelijke gamificationtoepassingen worden in dit artikel twee toepassingen nader toegelicht. Het betreft de toepassingen visualisatie perspectiefplan en planmatig verlof. Deze twee toepassingen zijn door de geïnterviewde deskundigen zonder meer als waardevol voor DJI bestempeld.

Visualisatie perspectiefplan
Een van de ontwikkelde gamificationtoepassingen betreft het opstellen van een perspectiefplan voor een jongere, inclusief de voortgang op het plan. In de huidige praktijk wordt door behandelaars in de intakefase (maximaal tien dagen) van het verblijf in de justitiële jeugdinrichting een eerste schriftelijk perspectiefplan voor de jongere opgesteld met een analyse van het probleemgedrag/psychische problematiek inclusief eerste leerdoelen. Het eerste plan wordt besproken met de jongere, die moet wennen aan de nieuwe omgeving van een gesloten inrichting en vaak nog weinig gemotiveerd is. Het uiteindelijk doel van het plan is bij te dragen aan de reïntegratie van de jongere.

Bij het ontwikkelen van een toepassing is het belangrijk dat de jongere geprikkeld wordt mee te gaan doen, dat de jongere de relevantie inziet van het traject en dat hij bij vallen en opstaan gesteund wordt om door te gaan. In feite gaat het om het gebruikmaken van alle ARCS-elementen, inclusief spelelementen, in de toepassing. Op basis van de mapping is als volgt inhoud gegeven aan de toepassing. Laat de jongere het perspectiefplan omzetten in eigen beelden. Geen dertig pagina's tekst, maar beelden (tekening, foto, animatie) vormen het plan, aan de hand waarvan de jongere een reis gaat ondernemen (storytelling) met te overwinnen hobbels ('welke draak moet ik verslaan') en een einddoel ('de schat'). Hiermee wordt het perspectiefplan voor de jongere doorleefbaar. De jongere wordt zodoende eigenaar van zijn eigen levensverhaal en is daarbij zelf aan zet. Door een koppeling van het plan aan een dashboard kan de jongere zijn eigen voortgang zien en bij zijn prestaties opbouwende feedback van zijn mentor krijgen.

Planmatig verlof
Een andere toepassing betreft het voorbereiden van een jongere op planmatig verlof. Planmatig verlof bestaat uit opeenvolgend: begeleid verlof, eendaags onbegeleid verlof en meerdaags onbegeleid verlof. Het is vooral gericht op het oefenen met vrijheden ter voorbereiding op terugkeer in de maatschappij. Het verlof is ook doelgericht: het bestaat uit bezoek aan familie of instanties buiten DJI. In de huidige praktijk bestaat het voorbereiden vooral uit het oefenen van sociale vaardigheden door bijvoorbeeld rollenspellen in de leefgroep en gesprekken met de mentor. Het doel van de voorbereiding is het beheersen van het risico van recidive en/of onttrekking tijdens verlof.

Bij het ontwikkelen van een toepassing is het van belang dat de jongere binnen de gesloten inrichting kan oefenen met kritische situaties. Oefenen van de stappen in het proces planmatig verlof in een virtuele werkelijkheid met een 360°-film, maakt het meer realistisch en benadert de echte werkelijkheid. Als vorm kan gekozen worden voor een applicatie met een VR-set, inclusief mogelijkheden van een begeleider om live verschillende virtuele personages ten tonele te voeren en via stemvervorming aanwijzingen te geven. De jongere krijgt informatie, gaat virtueel op verlof en krijgt te maken met uitdagingen (keuzen maken, verleidingen). Bij een keuze krijgt hij direct feedback van de begeleider met directe aanwijzingen. Ook kunnen punten worden verdiend bij gewenst gedrag. Bij voldoende punten krijgt de jongere de mogelijkheid de volgende stap in het verlof te maken (levels).

Belemmeringen
Het ontwikkelen en implementeren van gamificationtoepassingen komt bij organisaties, waaronder DJI, niet zo maar van de grond. Er zijn 'beren op de weg'. Uit de literatuur in het algemeen en voor DJI in het bijzonder komen een aantal belemmerende factoren naar voren. Belemmeringen kunnen met maatregelen worden tegengegaan. Belangrijke factoren zijn:

Beperkte houdbaarheid van gamificationtoepassingen – Het positieve effect op motivatie en gedrag lijkt na verloop van tijd weg te vloeien. Gewenning treedt op. Door het aanbrengen van variatie in de toepassing en het up-to-date houden ervan kan de houdbaarheid langer in stand blijven.

Effecten van gamification op houding en gedrag zijn niet duidelijk – Onderzoeken laten zowel geen effect als positieve effecten van toepassingen zien. Door het bewust creëren van meetpunten in de vorm van prestatie-indicatoren bij de ontwikkeling van de toepassing, kan regelmatig het effect worden gemeten.

Onvoldoende draagvlak voor innovatie – De sprong van innovatie (door een team) naar implementatie (in de organisatie) is vaak nog te groot. De infrastructuur voor vernieuwing is onvoldoende ontwikkeld: hoe introduceer je een vernieuwing, hoe evalueer je een pilot, hoe betrek je relevante doelgroepen?

Onvoldoende inzicht in de (leefwereld van de) doelgroep – Het is van belang na te gaan hoe de groep van jongeren is opgebouwd en wat de jongeren motiveert. Dat betekent dat het verder ontwikkelen van een toepassing op hoofdlijnen niet voor, maar samen met de jongeren moet gebeuren.

Knellende randvoorwaarden (wet- en regelgeving, budgetten) – Er is binnen inrichtingen geen toegang tot externe netwerken (internet) en social media en het is dus niet

mogelijk om apps te downloaden. Om een toepassing binnen de inrichtingen te kunnen gebruiken is beperkte toegang tot internet voor jongeren noodzakelijk, waarbij het gebruik van jongeren wordt gemonitord. Pilots worden hiervoor bij DJI uitgevoerd.

Conclusie

Uit mijn onderzoek blijkt dat gamification veel mogelijkheden biedt om in organisaties te worden toegepast. Gamification is net iets anders dan de reguliere beheersmaatregelen en kan hierop aanvullend zijn. Te denken valt aan de inzet van gamification als beheersmaatregel om het gedrag van medewerkers in een organisatie in lijn te brengen met de organisatiedoelstellingen. Bij DJI kan het daarbij ook gaan om het gedrag van justitiabelen.
Mijn onderzoek laat zien dat gamification via mapping in een primair proces concreet kan worden toegepast en hoe daarbij te werk kan worden gegaan. Dat levert voor een primair proces mogelijke gamificationtoepassingen op. Als voorbeeld voor DJI kan gewezen worden op de toepassing visualisatie perspectiefplan. De toepassing is aanvullend op de reguliere beheersmaatregelen en levert een bijdrage om het gedrag van jongeren meer te richten op reïntegratie.
Bij integriteitsrisico's van medewerkers kan gamification ook als beheersmaatregel worden ingezet. Ook hier is sprake van een iets andere benadering. Bij DJI is daarvoor een interactieve speltafel ontwikkeld om in een groep op een aantrekkelijke manier (met film, stellingen en het verdienen van punten) integriteitsdilemma's te bespreken. Bij veiligheidsrisico's van jongeren bij DJI kan gewezen worden op de beschreven toepassing planmatig verlof. De twee genoemde gamificationtoepassingen leveren een bijdrage aan het beheersen van de risico's.

Nut voor internal auditors

Gamification is ook voor internal auditors een interessante ontwikkeling. Kennis van en inzicht hebben in gamification is voor de internal auditor nuttig. Met kennis van gamification is de auditor beter in staat over het onderwerp te adviseren. Gamification is immers een andere, meer speelse benadering dan de reguliere beheersmaatregelen. De auditor kan ook brainstormbijeenkomsten inhoudelijk faciliteren, waarin voor een organisatie via een quick scan mogelijkheden van gamificationtoepassingen in kaart worden gebracht om de organisatie verder te helpen.
Belemmeringen lijken momenteel nog te veel een sta-in-de-weg te zijn om toepassingen binnen organisaties daadwerkelijk te ontwikkelen en te gebruiken. Ik vermoed dat op de langere termijn deze belemmeringen – door onder meer bewustwording – grotendeels kunnen worden 'opgelost'. Ik verwacht dat de ontwikkelingen van gamification en ICT in organisaties ertoe kunnen leiden dat gamification een steeds belangrijkere rol gaat innemen ten opzichte van de reguliere interventies. In de toekomst is gamification dan wellicht niet meer weg te denken als een van de mogelijke interventies voor het realiseren van gedragsverandering en als instrument voor sturing en beheersing van de organisatie. <<

Noten

1. Taphoorn, R., *Een verkenning van toepassingsmogelijkheden en belemmeringen van gamification, aan de hand van de casus reïntegratieproces van jongeren in justitiële jeugdinrichtingen*. Referaat in kader van de postmaster-opleiding Internal Auditing & Advisory, Erasmus Universiteit Rotterdam, 2018.
2. Keller, J., *Handbook of human performance technology*, Jossey-Bass, 1999.
3. Nuijten, A. en M. van Twist, *Bewust omgaan met het onbewuste. Over de relevantie van gamification voor internal audit,* Instituut van Internal Auditors Nederland, 2017.

René Taphoorn is auditor bij de interne auditafdeling van de Dienst Justitiële Inrichtingen en recent geslaagd voor de opleiding Internal Auditing & Advisory aan de EUR.

Rubriek
Tekst Drs. Paul van der Zwan RO EMIA
Beeld Adobe Stock

Youssef El Baouchi:

"Met uitdaging komt groei"

In de rubriek De overstap dit keer Youssef El Baouchi, die van KPN overstapte naar Deloitte om aan de slag te gaan als internal auditmanager.

Waarom bent u overgestapt van KPN naar Deloitte?
"Ik geloof dat uitdaging belangrijk is voor groei. Deloitte biedt qua omvang en internationale aanwezigheid veel mogelijkheden om mij te kunnen blijven ontwikkelen. Zowel professioneel als persoonlijk. Ook heeft Deloitte een brede variëteit aan bedrijfsonderdelen die bijzonder en divers van aard zijn. Denk aan de verschillende soorten dienstverlening die we aan klanten bieden op het gebied van accountancy, consulting, risk advisory, digitalisering en overige gerelateerde dienstverlening. Er is veel kennis en je kunt direct impact hebben.
Ook het auditen van een auditor is een interessante uitdaging. Je moet van goede huize komen om een auditrapport te verdedigen tegenover mensen die in veel gevallen dagelijks hetzelfde type werk doen bij klanten. Bovendien krijg ik bij mijn afdeling voldoende ruimte om mee te denken over innovatieve oplossingen en om invulling te geven aan het verder professionaliseren van een relatief jonge afdeling. Ik word uitgedaagd op mijn kwaliteit en toegevoegde waarde. Daarom past Deloitte momenteel beter bij mij."

Wat waren uw eerste indrukken in de nieuwe werkkring?
"Mijn eerste indruk is positief. Er is veel diversiteit, in zowel mensen als afdelingen. Daarbij zorgt het internationale karakter voor een extra dimensie bij het uitvoeren van audits. Je moet hier ook wendbaar zijn en steeds in vrij korte tijd de elementen van de organisatie goed kunnen begrijpen. Het vraagt dus wel wat van je aanpassingsvermogen en communicatieve vaardigheden.
Wat me ook opvalt is dat Deloitte veel energie en tijd steekt in het individu, met persoonlijke ontwikkelingstrajecten, groepstrainingen en opleidingen. Evaluatie en reflectie worden systematisch en structureel georganiseerd. Er is tijd en aandacht voor en dat spreekt me aan. Ik vind investeren in je mensen belangrijk om kwaliteit te kunnen blijven leveren en om groei te realiseren. Als internal auditor is dit punt belangrijker dan ooit door het snel veranderende risicolandschap en de veranderende rol van de internal auditor binnen de organisatie."

Wat zijn opmerkelijke verschillen tussen beide organisaties?
"In mijn ogen is het voornaamste verschil dat de dynamiek tussen stakeholders hier anders is dan bij een corporate

Over Deloitte

Deloitte is een van de grootste aanbieders van professionele dienstverlening op het gebied van accountancy, belasting- en juridisch advies, consultancy, risk management en financiële advisering. Deloitte heeft ruim 5500 medewerkers en 15 kantoren verspreid over heel Nederland.

business als KPN. Bij Deloitte heb je te maken met een partnergerichte organisatiestructuur. De eigenaren van het bedrijf zitten dichter op wat er gebeurt. Zij werken zelf ook binnen de organisatie. Volgens mij is dit positief omdat je dan sneller tot actie kunt komen als er processen verbeterd moeten worden. Verder kan ik me voorstellen dat het een stuk uitdagender is om de belangrijkste stakeholders voldoende mee te krijgen in bepaalde standpunten, zeker als zij binnen die organisatie zoveel verschillende belangen en rollen hebben."

Hoe ziet de interne auditafdeling eruit?

"De internal auditfunctie maakt gebruik van een ruime community van zo'n 25 Deloitte-professionals die regelmatig meedraaien in audits. Het kernteam dat hier sturing aan geeft bestaat uit de chief audit executive, een senior manager en een manager. Mijn collega's hebben een ruim kennisniveau en een groot netwerk binnen Deloitte. Dat is handig en ook belangrijk om efficiënt audits uit te kunnen voeren. Het maakt je wendbaar, maar het is ook fijn omdat ik via mijn collega's snel met verschillende mensen in contact kan komen. Iedere week leer ik nieuwe gezichten kennen."

Wat wilt u mensen meegeven die een overstap overwegen?

"Besteed aandacht aan een visie. Vorm je vooraf een goed beeld van je toekomst en hoe je werkgever hierbij past. Natuurlijk zijn er ideaalbeelden over hoe je carrière kan lopen en kan verandering best eng zijn. Maar als je een overstap overweegt, is het belangrijk dat je koers helder is en je niet bang bent voor verandering. Verandering en uitdaging zijn nodig om te kunnen groeien. Dus: heb een duidelijke visie, wees niet bang voor verandering en werk toe naar realiseerbare doelen."

Over...

Youssef El Baouchi is internal audit manager bij Deloitte en verantwoordelijk voor het plannen en uitvoeren van interne audits binnen Deloitte Nederland. Hij draagt bij aan het verbeteren van bedrijfsprocessen en de beheersing van veranderende risico's binnen de organisatieonderdelen. In het verleden werkte hij onder meer op de internal auditafdeling van KPN. Zijn andere grote passie is voetbal en hij houdt van culturele reizen.

RSG AUDIT•RISK& COMPLIANCE
HUMAN KEY SOLUTIONS

GEZOCHT: TALENTVOLLE PROFESSIONALS

RSG Audit, 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.

HUMAN KEY SOLUTIONS

ACCOUNTANT? EN NU?

Heb jij al scherp wat de beste route is naar jouw ambitie? RSG bemiddelt al ruim 8 jaar voor Accountants, Financial Controllers, Business Controllers, GRC-Specialisten en CFO's bij Werving & Selectie, Detachering en Interim Management (zzp) opdrachten. Wij hebben de voor- en de nadelen van de verschillende alternatieven voor je op een rijtje gezet.

RSG Audit, Risk & Compliance ondersteunt interne accountantsdiensten, accountantskantoren, banken en verzekeraars en Corporate Organisaties op het gebied van Audit&Assurance, Enterprise Risk Management en Compliance.

Leer van de keuzes van onze financials en kom eens met ons praten. RSG helpt je met het maken van de juiste keuzes.

RSG Audit • Risk & Compliance
Vestdijk 57a
5611 CA Eindhoven
The Netherlands

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

■ Business Continuity Management
■ Crisismanagement

Artikel
Tekst Drs. Abderrahman Kaouass
Drs. Iwan Drost
Mr. Saida Nhass CIPP/E
Beeld Adobe Stock

Het is van belang dat internal audit de eigen organisatie actief toetst op business continuity management (BCM) én crisismanagement. De third line of defense kan hiermee een belangrijke en actieve bijdrage leveren aan het verminderen van kwetsbaarheden bij een incident of crisis en aan het vergroten van de veerkracht van de organisatie.

Waarom BCM en *crisismanagement* belangrijk is

Het voorkomen van risico's staat bij de meeste organisaties hoog op de agenda. De aandacht hiervoor komt voort uit de dynamiek en complexiteit waarin organisaties opereren én uit een toename van eisen vanuit de omgeving. Bijvoorbeeld de steeds complexer wordende toeleverancierskeken door globalisering, een toename van eisen op het gebied van wet- en regelgeving (zoals de privacywetgeving) of een toename aan eisen die door klanten worden gesteld (duurzaamheids-, leverbetrouwbaarheids- en kwaliteitseisen). Organisaties proberen het hoofd te bieden aan deze ontwikkelingen door in control te zijn en te blijven.

In control

Voor veel organisaties wordt het in control zijn voornamelijk toegespitst op het inrichten van een adequate governancestructuur, een planning & controlcyclus en de implementatie van het three-lines-of-defensemodel. Hierbij wordt een focus aangebracht op het mogelijk voorkomen van risico's. Met andere woorden, het voorkomen van onvoorziene gebeurtenissen die kunnen leiden tot onaangename verrassingen of, erger nog, die het voortbestaan van de organisatie bedreigen.

Echter, de praktijk wijst uit dat niet alle risico's kunnen worden voorkomen. Geen enkele organisatie is incidentvrij. Er kan namelijk altijd iets misgaan. Soms met verstrekkende gevolgen voor individuen, de financiële situatie of zelfs het voortbestaan van de organisatie. In iedere organisatie vinden nu eenmaal incidenten plaats waarop niet vooraf is en kan worden geanticipeerd. Dit kan leiden tot een verstoring van de bedrijfscontinuïteit en in sommige gevallen zelfs tot een crisis.

Binnen het risicomanagement zien wij (beroepsmatig) dan ook een ontwikkeling naar een meer integrale toepassing van risicomanagement, te weten de 'resiliencegedachte'. Vanuit deze resiliencegedachte wordt structureel gewerkt aan het verminderen van kwetsbaarheden én het vergroten van de veerkracht van organisaties indien risico's zich toch

voordoen (de wat-als vraag). De twee disciplines die zich daar voornamelijk op richten zijn BCM en crisismanagement. Om deze twee disciplines op een juiste wijze in te zetten en te borgen, gaan we in op de belangrijke rol die de auditpraktijk hierbij, in onze optie, kan en hoort te spelen.

Wat is BCM én crisismanagement?
Organisaties werken dagelijks aan hun weerbaarheid. Dit doen ze deels door te voorkomen dat risico's ontstaan. Werken aan weerbaarheid vraagt ook om goed en tijdig te reageren op risico's die toch ontstaan. Dit noemen we 'veerkracht en weerbaarheid'. Maar hoe organiseer je nu veerkracht en weerbaarheid? In de kern bestaan er twee disciplines voor veerkracht: BCM in een situatie waarbij de bedrijfscontinuïteit bedreigd kan worden en crisismanagement bij een grote crisis waarin het bestaansrecht van de organisatie afneemt. We lichten beide disciplines kort toe.

BCM
Bedrijfscontinuïteit is het vermogen van de organisatie om na een bedrijfsverstorend incident producten of diensten te kunnen blijven leveren, binnen van tevoren gedefinieerde en geaccepteerde serviceniveaus. Om dit te kunnen bereiken richt een organisatie BCM in. BCM identificeert potentiële bedreigingen en de impact die deze bedreigingen hebben op de continuïteit van de bedrijfsvoering. Deze discipline voorziet in een structuur voor het realiseren van organisatorische weerbaarheid en veerkracht. Dit door vooral gericht te investeren in de bekwaamheid van de organisatie om een tijdig en voldoende herstel te realiseren. Herstel door de juiste prioritering, snelheid en capaciteit, zodat de belangen van stakeholders, de reputatie, het merk en waardecreërende activiteiten optimaal worden beschermd. De belangrijkste norm voor BCM is de certificeerbare norm NEN ISO 22301:2012. Deze norm is een richtlijn en geeft duiding aan hoe de verschillende eisen van BCM moeten worden geïnterpreteerd en toegepast.

Crisismanagement
Een crisis is een van de ernstigste uitdagingen waarvoor een organisatie zich gesteld kan zien. Een crisis is een abnormale en buitengewone verstoring, impactvol, en gekenmerkt door een onstabiele en complexe situatie die een mogelijke bedreiging vormt voor de strategische doelstellingen, veiligheid van medewerkers of omgeving, reputatie en, uiteindelijk, de continuïteit en het voortbestaan van een organisatie. Crisismanagement richt zich op de brede impact die een groot scala aan ernstige gebeurtenissen (denk aan fraude, datalekken, brand, ernstige ongevallen, et cetera) kan hebben op de reputatie en het voortbestaan van de organisatie.
Momenteel zijn er twee normen voor crisismanagement: de British Standard 11200:2014 en de Europese norm CEN/TS 17091 'Crisis management – Guidance for developing a strategic capability'. Beide normen voor crisismanagement bieden organisaties handvatten voor het ontwikkelen van hun bekwaamheden om met crisissituaties om te gaan en deze te verbeteren. Niet elke uitdaging op het gebied van bedrijfscontinuïteit is een crisis en niet elke crisis gaat alleen over het herstellen van producten en/of diensten. De impact bij een crisis is dan breder dan alleen bedrijfscontinuïteit. Wanneer bijvoorbeeld een gebouw uitbrandt vindt uitwijk van de productie plaats, er kunnen slachtoffers zijn die tevens veel media-aandacht genereren en er is zorg voor familieleden en collega's.

De voorbereidingen op crises zijn vaker een eigen keuze en tegelijkertijd is ook compliance steeds vaker een reden om te investeren in de voorbereiding op crises

Waarom noodzakelijke verbreding van risicomanagement?
Een studie uitgevoerd onder meer dan vierhonderd business executives toont aan dat organisaties steeds meer het belang inzien van het verbreden van risicomanagement naar het reeds genoemde resilienceconcept, waarbij risicomanagement, BCM en crisismanagement met elkaar verbonden worden.[1] Het overgrote deel van de business executives (80%) is ervan overtuigd dat resilience zelfs een absolute prioriteit is om op langere termijn te overleven.
Het door Aon uitgevoerde onderzoek, genaamd 'Global Risk Management Survey 2019', laat zien dat bedrijven minder goed voorbereid zijn op risico's. Reputatieschade wordt genoemd als de op een na grootste zorg. Opvallend is dat de risicomanagers melden dat zij nog nooit zo weinig voorbereid zijn op risico's, omdat veel van de toprisico's, zoals economische teruggang en toenemende concurrentie, onverzekerbaar zijn.[2] Naar onze mening komen bij een juiste focus op de onverzekerbare risico's de onderwerpen discontinuïteit en crises meer tot hun recht.

Sinds 2015 wordt door COT, Instituut voor Veiligheids- en Crisismanagement (onderdeel van Aon) onderzoek verricht, waaruit blijkt dat de kwetsbaarheid voor crises toeneemt. Ook is gebleken dat bedrijven/organisaties steeds vaker en eerder een daadwerkelijke crisis ervaren. De voorbereidingen op crises zijn vaker een eigen keuze en tegelijkertijd is ook compliance steeds vaker een reden om te investeren in de voorbereiding op crises.[3]

Is de internal auditpraktijk voldoende voorbereid?
Deze belangrijke verbreding van risicomanagement naar BCM en crisismanagement heeft consequenties voor de reikwijdte van de auditpraktijk. Internal audit vervult immers een essentiële rol om een onafhankelijk en objectief oordeel te vellen over het in control zijn van de organisatie. Hierbij is het verminderen van kwetsbaarheden binnen de organisatie en het vergroten van de veerkracht van organisaties een belangrijk onderdeel. Wij zien in onze adviespraktijk dat deze veranderende rol voor internal audit een uitdaging kan vormen. Dit komt door de volgende factoren:

1. *In de meeste control frameworks ontbreken duidelijke normen voor BCM en crisismanagement* – Het uitvoeren van audits kent een zekere cyclus, te weten de audit en de opvolgaudit. De thema's zijn in eerste instantie meer gericht op compliance en het meer klassieke risicomanagement. De bredere kijk op resilience – waar BCM en crisismanagement onderdelen van zijn – wordt daarom nog niet altijd toegepast. Daarnaast wordt om de auditagenda vast te stellen veel gebruikgemaakt van richtlijnen en informatie zoals door (internationale) auditorganisaties worden gepubliceerd. In deze richtlijnen wordt niet of nauwelijks gewezen op het belang van een BCM- en crisismanagementaudit. Wij zien dat er meer aandacht is voor gerelateerde onderwerpen zoals cybersecurity en dataprotectie die door het IIA als hot topic worden beschreven. Tot slot ligt er nog een uitdaging om BCM en crismanagement binnen het opleidingscurriculum van internal auditors te plaatsen, zodat auditors zelf over voldoende kennis en vaardigheden beschikken om onafhankelijk en adequaat te kunnen toetsen en het topmanagement van de juiste adviezen te kunnen voorzien.

2. *De toename van wet- en regelgeving zorgt voor regeldruk* – De toename van wet- en regelgeving vanuit de EU zorgt ook voor regeldruk bij internal audit. Vanuit de EU wordt steeds vaker opgelegd dat periodieke audits verplicht zijn, wat leidt tot een toename van wettelijk verplichte audits. In onze adviespraktijk zien we dat regeldruk leidt tot meer verplichte audits, waardoor er minder ruimte is voor audits naar complexe onderwerpen als BCM en crisismanagement. In de meeste gevallen worden eerst de wettelijk verplichte audits op de agenda geplaatst, pas daarna komen eventuele andere onderwerpen in beeld.

3. *De rol van de diverse stakeholders bij de auditplanning* – Welke rol de directie c.q. het bestuur speelt bij de bepaling van de auditagenda verschilt per organisatie. In ieder geval levert de internal auditor een aanzet hiertoe en houdt hij hierbij rekening met eventuele specifieke opdrachten. De internal auditor is zich niet altijd bewust van het belang om BCM en crisismanagement als onderwerp op de agenda te plaatsen. Dit wordt ook nog eens gevoed door het strategische niveau dat zich ook niet altijd bewust is van de noodzaak om BCM en crisismanagement te laten toetsen.
In veel gevallen vertrouwt het strategische niveau te veel op het operationele vermogen van organisaties om met ernstige calamiteiten om te gaan en zijn ze zich onvoldoende bewust van hun eigen rol en verantwoordelijkheid. Immers, het wel of niet overleven van een ernstige crisis is in een grote mate afhankelijk van het op dat moment getoonde leiderschap. In veel gevallen komen BCM en

Wolters Kluwer

When you have to be right

TeamMate+

The future of Audit & Internal Controls

One Language. One Voice. One View.

Direct insight in your risks & controls and improve audit efficiency by implementing TeamMate+ for Audit & Internal Controls

Voor meer informatie, bezoek **TeamMatesolutions.com** of bel ons via **+31(0)6 – 25695737** of onze partner **BR1GHT** via **+31(0)6 – 15396270**

crisismanagement pas op de agenda nadat de betreffende organisatie een ernstig(e) incident/crisis heeft meegemaakt, of omdat er een directe eis ligt uit hoofde van compliance. Hier ligt dus een mooie uitdaging voor de risicomanager in samenwerking met internal audit.

Beoordelen en adviseren

Uit het hiervoor genoemde blijkt dat de internal auditfunctie een belangrijke rol kan en – in onze optiek – behoort te spelen in het beoordelen van veerkracht en weerbaarheid en het adviseren hierover. Om deze redenen stelt de NBA-LIO in samenwerking met Aon/COT in 2019 een handleiding op die bedoeld is als praktische gids en hulpmiddel voor internal auditors om hun organisaties te toetsen op BCM en crisismanagement.[4] Op basis van de constateringen hiervoor komen wij tot de volgende aanbevelingen die ertoe bij kunnen dragen dat BCM en crisismanagement veel meer in beeld komen bij internal audit:

1. *Ontwikkel als internal auditor kennis van BCM en crisismanagement en hanteer de relevante normen als toetsingskader voor de audits* – Beide onderwerpen hebben normen die door internal auditors gebruikt kunnen worden om de eigen organisatie te toetsen. IIA heeft bijvoorbeeld de Practice Guide business continuity management ontwikkeld. In 2018 is een Europese norm gepubliceerd die richtlijnen bevat voor crisismanagement, de CEN/TS 17091 'Crisis management – Guidance for developing a strategic capability'. Deze norm beoogt organisaties handvatten te bieden om hun bekwaamheid om met crisissituaties om te gaan, te ontwikkelen en te verbeteren.

2. *Breng het control framework op een lijn met het brede risicoprofiel* – In de huidige basis voor het beoordelen van de risico's en maatregelen dienen ook continuïteits- en crisisrisico's opgenomen te worden. Op deze manier worden in het control framework zowel onderwerpen meegenomen die over preventie als over herstel/repressie gaan.

3. *Agendeer BCM en crisismanagement bij de riskmanager en RvC/RvT* – Neem als internal audit het initiatief om het control framework te verbreden naar BCM en de crisismanagement. Ga in gesprek met de riskmanager en de RvC/RvT om het belang te benadrukken van deze verbreding in het licht van alle noodzakelijke maatregelen om risico's te voorkomen én deze risico's tijdig en adequaat te beheersen en te herstellen. Is de auditagenda vol? Maak dan gebruik van een externe partij. <<

Noten

1. 'Organisational Resilience: Building an enduring enterprise', *The Economist Intelligence Unit*, 2015.
2. Aon voert de 'Global Risk Management Survey' sinds 2007 elke twee jaar uit. In het laatste kwartaal van 2018 ondervroeg Aon 2672 risicomanagers, CRO's, CFO's en andere verantwoordelijken in 60 landen en 33 bedrijfstakken. https://www.aon.com/netherlands/grms-2019.jsp
3. COT voert sinds 2015 periodiek een onderzoek uit naar crisismanagement in het bedrijfsleven. http://www.cot.nl/pdf/COT-Aon-Benchmark-Crisismanagement-Bedrijfsleven.pdf
4. Deze richtlijn is toepasbaar binnen elke organisatie en zal in het najaar van 2019 beschikbaar zijn voor internal auditors. Zodra de handleiding is afgerond,wordt dit bekendgemaakt op onder andere de website van NBA, Aon en COT.

Abderrahman Kaouass is managing consultant bij COT (onderdeel van Aon) en gespecialiseerd in strategische organisatievraagstukken rond crisismanagement. Hij adviseert organisaties bij de professionalisering van het crisisvermogen.

Iwan Drost is managing consultant bij Aon Global Risk Consulting en adviseert organisaties bij de implementatie van risicomanagement en in het bijzonder BCM. Hij is lid van de NEN BCM-commissie.

Saida Nhass is managing consultant bij Aon Global Risk Consulting en is in haar hoedanigheid van practice lead compliance consulting verantwoordelijk voor de advisering van organisaties op het gebied van compliance.

■ Financial Chaos Engineering
■ Cybercrime

Artikel
Tekst Eric J.H.J. Mantelaers RA AA CISA CISO
Dr. Ing. Martijn M. Zoet
Beeld Adobe Stock

Financial CHAOS engineering

Maken uw bestuurders, net zoals de bestuurders van Pathé, 19 miljoen euro over wanneer ze daarover worden gebeld en gemaild door de accountant? Ofwel, wanneer een medewerker een e-mail van de baas krijgt, maakt hij dan het geld over? En hoeveel nepfacturen worden er door uw organisatie betaald?

Als het goed is komen de voorbeelden in het intro bij u niet voor. Maar werkt uw financiële systeem 100% foutloos? Dat is waarschijnlijk ook niet het geval. Er zijn altijd zaken die kunnen worden verbeterd. Veel managers en organisatieadviseurs beschouwen een organisatie te veel als een verzameling van bewust gemaakte en goed onderhouden afspraken. Het zelfordeningsmechanisme uit de chaos- en complexiteitstheorie laat evenwel zien dat die veranderingen juist niet altijd kunnen worden beheerst, maar 'vanzelf' ontstaan en een eigen dynamiek hebben. Het is daarom belangrijk dat uw financiële systeem veerkracht toont en kan blijven functioneren. Het is wenselijk om een goed optimum te vinden tussen enerzijds de natuurlijke wil om een organisatie te beheersen en anderzijds de durf om een organisatie haar eigen dynamiek te laten hebben.

Toetsen van de veerkracht

Binnen informatie- en communicatietechnologie is er een discipline die de veerkracht van hard- en software toetst, genaamd chaos engineering. Chaos engineering is door Netflix geïntroduceerd en als volgt gedefinieerd: 'Chaos engineering is the discipline of experimenting on a distributed system in order to build confidence in the system's capability to withstand turbulent conditions in production'. In dit artikel introduceren wij het concept van financial chaos engineering, hetgeen we baseren op de principes zoals deze zijn gedefinieerd voor chaos engineering binnen het informatietechnologiedomein. Wij definiëren financial chaos engineering als volgt: 'Financial chaos engineering is de discipline van experimenteren op het financieel systeem binnen de organisatie om vertrouwen te hebben dat het financiële systeem fraude en turbulente condities kan weerstaan tijdens dagelijkse werkzaamheden'.

In normaal Nederlands staat hier het opzettelijk doorbreken van onderdelen van de financiële systemen binnen de organisatie, zijnde de administratieve organisatie en de interne beheersing, zowel geautomatiseerd als niet-geautomatiseerd. Wanneer onderdelen van deze administratieve organisatie en/of de interne beheersing worden doorbroken, dan dient bepaald te worden wat er moet gebeuren, de impact dient

gemeten te worden en de problemen dienen verholpen (gecorrigeerd) te worden, zodat de interne organisatie veerkrachtiger wordt voor de toekomst.

Experimenten op het financieel systeem
De gedachte om experimenten vanuit risk management, compliance en/of accountancy uit te voeren op het financieel systeem van een organisatie is relatief nieuw. Desondanks voeren organisaties al experimenten uit om onderdelen van de organisatie te toetsen. Een voorbeeld van een onderdeel dat vaker getoetst wordt, is de ICT-omgeving en met name de ICT-beveiliging. Een chaos monkey is een voorbeeld van zo'n experiment. Het verschil tussen de chaos monkey en de financial chaos monkey (FCM) is het gebied waarop de aanval wordt uitgevoerd. Bij de FCM is dit het financiële systeem van het bedrijf of de organisatie waarbinnen dit experiment wordt uitgevoerd. In het vervolg van dit artikel wordt de manier waarop financial chaos engineering geïmplementeerd kan worden nader toegelicht.

Implementatie financial chaos engineering
We onderkennen in het algemeen vier verschillende stappen bij de implementatie van financial chaos engineering:
1. Definieer de 'steady state' als een meetbare output hoe het systeem optimaal functioneert.
2. Definieer events (aanvallen) die het systeem van deze steady state kunnen afbrengen en definieer voor elk van deze aanvallen ook de risico's.
3. Automatiseer de experimenten.
4. Voer de experimenten uit in de live-omgeving, maar minimaliseer de impact op de financiële huishouding.

Om de hiervoor genoemde vier stappen te concretiseren, beschrijven we deze inclusief een voorbeeld, namelijk een spookfactuur. Andere typen en complexere aanvallen zijn natuurlijk ook mogelijk. Hierbij kan onder andere gedacht worden aan: 1) het verzoek tot het (ongeoorloofd) muteren van een bankrekeningnummer, 2) het aanmelden van een nieuwe medewerker (deadman on the payroll), 3) een 'besmette' usb-stick aanleveren met een administratie van een klant, 4) aanvraag van een ongeoorloofde wijziging van een bankrekeningnummer van een klant, 5) het onterecht aanmaken van een creditfactuur.

1. Definieer de steady state als een meetbare output van het systeem dat een normaal gedrag definieert
In een normale organisatie is er sprake van een sluitende 'three-way-match', wat betekent dat de inkoopfactuur van bestelde en ontvangen onderdelen pas betaald mag worden nadat (in functiescheiding) is vastgesteld dat de bestelde

Chaos engineering is door Netflix geïntroduceerd

hoeveelheid onderdelen correct ontvangen is en de bijbehorende inkoopfactuur juist is voor wat betreft: 1) het soort onderdelen, 2) de prijs ervan. Een voortdurend sluitende 'three-way-match' – waarvan een 'correcte' inkoopfactuur een belangrijk onderdeel is – is een weergave van de zogenaamde steady state.

2. Definieer events (aanvallen) die het systeem van deze steady state kunnen afbrengen en definieer voor elk van de aanvallen ook de risico's

Om de werking van de organisatie met betrekking tot de 'three-way-match' te toetsen, kunnen als aanval facturen worden ingebracht met onjuiste aantallen of onjuiste prijzen, zogenaamde spookfacturen. Om zoveel mogelijk aan te sluiten bij de werkelijkheid moeten dergelijke testfacturen op dezelfde wijze als de normale facturen (zoveel mogelijk geautomatiseerd) worden ingevoerd in het systeem. Mochten deze spookfacturen er overigens doorheen glippen, dan is op deze testfactuur een 'eigen' bankrekeningnummer vermeld, zodat het geld niet verloren gaat. Omdat deze beschrijving voor een specifieke aanval te vaag is, kan er gebruikgemaakt worden van een template om een concrete aanval te definieren. Deze template bestaat uit zeven onderdelen, namelijk: a. doelwit, b. experimenttype, c. hypothesen, d. 'blast radius', e. status vóór aanval, f. status na aanval en g. bevindingen van de aanval.

a. doelwit

Het doelwit van een aanval kan alle essentiële en vitale onderdelen van een financiële organisatie betreffen. In het geval van de spookfactuur betreft het doelwit de werking (het functioneren) van de inkooporganisatie en in het bijzonder de crediteurenadministratie.

b. experimenttype

Het experimenttype deelt de experimenten op in vooraf gedefinieerde categorieën. Echter, omdat er vooralsnog geen standaardstructuur bestaat, beschrijven we hier geen specifiek voorbeeld.

c. hypothesen

Het 'inschieten' van een spookfactuur is zoals beschreven een vereenvoudigd voorbeeld van financial chaos engineering. Op basis hiervan kunnen twee (H0 en H1) hypothesen worden geformuleerd.

H0 – de spookfactuur krijgt een factuurnummer toegekend, wordt het proces ingeschoten en wordt geblokkeerd door de controleur van de inkooporganisatie die de prijzen, hoeveelheden, kwaliteiten en dergelijke moet controleren.
H1 – de spookfactuur krijgt een factuurnummer toegekend, wordt het proces ingeschoten en wordt uiteindelijk onterecht betaald.

d. blast radius

Onder blast radius wordt verstaan de impact die een aanval op de organisatie kan hebben. Hierbij wordt gestreefd naar een zo groot mogelijke impact, waarbij de organisatie zo min mogelijke schade wordt toegebracht. Hoever reiken de gevolgen van deze spookfactuur? Als de in de interne organisatie opgenomen administratieve organisatie en interne beheersing (AO/IB) niet naar behoren functioneren, dan wordt uiteindelijk de spookfactuur ten onrechte betaalbaar gesteld en betaald. Geld verlaat de organisatie zonder dat er een tegenprestatie tegenover staat. Daaraan voorafgaand wordt natuurlijk de inkooporganisatie (crediteurenadministratie) geraakt, waardoor de werking van dit deel van de AO/IB ter discussie komt te staan. De werking van de AO/IB is primair van belang voor het bedrijf zelf. De leiding van dit bedrijf streeft immers een betrouwbare informatievoorziening na.

Onder 'blast radius' wordt verstaan de impact die een aanval op de organisatie kan hebben

e. status vóór aanval

Bij de status vóór aanval wordt beschreven hoe de organisatie functioneert voordat de aanval heeft plaatsgevonden. De verantwoordelijke leiding van het bedrijf waarbinnen de FCM wordt toegepast, heeft de interne organisatie zodanig opgebouwd dat de gewenste taken worden uitgevoerd, rekening houdend met de vereiste controletechnische functiescheidingen. Dit betekent bijvoorbeeld dat iemand die onderdelen bewaart (magazijn) niet de bevoegdheid heeft om te beschikken over de bankrekening en dus de inkoopfactuur niet kan betalen. Door een adequate inrichting (opzet) van de AO/IB en een constant functioneren hiervan (bestaan en werking) mag de leiding erop vertrouwen dat de taken correct worden uitgevoerd en de processen naar behoren functioneren, waardoor de informatievoorziening ook adequaat zal functioneren. Concreet is dit voor de leiding van het bedrijf de basis om erop te vertrouwen dat betaalde inkoopfacturen hebben geleid tot de ontvangst van bestelde onderdelen die aan de eisen voldoen. De accountant die namens het toezichthoudend orgaan of de leiding van het bedrijf wordt ingeschakeld voor de controle van de jaarrekening zal – afhankelijk van zijn controleaanpak – waar mogelijk willen steunen op en gebruikmaken van de in de interne organisatie opgenomen AO/IB. Als we kijken naar de eerdergenoemde hypothesen, lijkt het geoorloofd dat de accountant in geval van H0 steunt op die interne organisatie.

f. status na aanval
Bij de status na aanval wordt beschreven hoe de organisatie functioneert nadat de aanval heeft plaatsgevonden. In geval van H1 is de spooknota ten onrechte betaald en heeft geld (zonder tegenprestatie) de organisatie verlaten. Het vertrouwen in bepaalde medewerkers en dus in de werking van de AO/IB (inlooporganisatie en de crediteurenadministratie) is geschaad. Wanneer de accountant na verloop van tijd constateert dat zijn vertrouwen wordt geschaad omdat H1 van toepassing is en gebleken is dat de vermeende adequate AO/IB niet naar behoren functioneert, dan zal hij zijn controle-aanpak moeten wijzigen. Of, nog erger, zal hij zijn opdrachtcontinuering moeten heroverwegen. Immers, de integriteit van de leiding staat mogelijk ter discussie.

g. bevindingen
Bij de sectie bevindingen wordt zodra de aanval is afgerond, beschreven wat de eventuele gevolgen zijn voor de opzet, het bestaan en de werking van de interne organisatie. Deze gevolgen dienen te worden geëvalueerd en omgezet te worden in acties, die vervolgens geffectueerd dienen te worden. Indien de aanval met goed gevolg is afgeweerd, dan wordt dit ook hier geconstateerd en gedocumenteerd.

3. Automatiseer de experimenten
Om de aanvallen met minimale inspanning en herhaalbaar te kunnen uitvoeren, dienen zij zoveel mogelijk te worden geautomatiseerd. In ons voorbeeld kan een server elke maand een of meerdere spookfacturen inschieten. Belangrijk is dat het beheer van deze server onder verantwoordelijkheid staat van de allerhoogste bedrijfsleiding.

4. Voer de experimenten uit in de live-omgeving maar minimaliseer de impact op de financiële huishouding
De organisatie is erbij gebaat de experimenten zo waarheidsgetrouw mogelijk uit te voeren. Daarom dienen experimenten in een live-omgeving plaats te vinden. In sommige gevallen zal dit niet mogelijk zijn. Bijvoorbeeld bij een aanval met een flash-crash of een beurscrash, omdat de aanval dan mogelijk een grote schade toebrengt aan de organisatie. Dergelijke aanvallen kunnen dan beter worden gesimuleerd.

Three lines of defense
In het kader van de interne beheersing onderkent men binnen organisaties de zogenaamde first, second en third line of defense. De eerste lijn betreft de proceseigenaren. De tweede lijn zijn de mensen die verantwoordelijk zijn voor compliance of risk management. De derde lijn betreft de interne accountantsdienst. Normaliter zullen de mensen in de first line vooraf niet op de hoogte zijn van financial chaos engineering, al zullen ze na verloop van tijd wel bekend zijn met het fenomeen spookfacturen en het feit dat deze kunnen opduiken. Dit zou een preventieve werking kunnen hebben. Afhankelijk van de omvang van het bedrijf en de diverse afdelingen, kunnen zowel de tweede als de derde lijn betrokken zijn bij het voorbereiden van bewuste chaosacties. De interne accountantsdienst zal gebruikmaken van de bevindingen van deze acties.
Traditioneel gezien maken accountants uit het oogpunt van efficiency (waar mogelijk) gebruik van de AO/IB die aanwezig is in de interne organisatie. In dit kader voeren deze accountants een interimcontrole en een eindejaarscontrole uit. Tijdens deze laatste controle wordt normaliter de balans 'dichtgevinkt', terwijl tijdens de interimcontrole de opzet, het bestaan en de werking van de organisatie wordt getoetst. In het licht van de beoordeling van de betrouwbaarheid van de informatievoorziening hebben zowel de leiding van het bedrijf (intern) als ook de externe accountant (extern) gelijke belangen. Normaliter wordt vastgesteld of de organisatie werkt zoals die zou moeten werken. Het is daarbij (nog) niet gebruikelijk om de organisatie 'voor de gek te houden' en te kijken of men (door of namens de accountant) gemaakte fouten eruit weet te halen. <<

Eric Mantelaers is hoofd Bureau Vaktechniek en auditpartner bij RSM Nederland Accountants nv, docent accountantsopleiding Maastricht University, lid van het lectoraat van Zuyd Hogeschool 'Optimaliseren Kennisintensieve Bedrijfsprocessen' en PhD fellow Open Universiteit.

Martijn Zoet is als lector verbonden aan het lectoraat van Zuyd Hogeschool 'Optimaliseren Kennisintensieve Bedrijfsprocessen'. Tevens is hij als managing partner verbonden aan EDM-Competence Centre.

De auteurs hebben dit artikel geschreven op persoonlijke titel.

Rubriek
Tekst Raymond Wondergem MSc RO
Beeld Adobe Stock

Wilbert Kooiman:

"De grootste uitdaging is om de schaarse capaciteit op de juiste onderwerpen in te zetten"

PAS op de plaats is een rubriek waarin auditors van kleine auditdiensten aan het woord komen. Dit keer Wilbert Kooiman, manager Operational Audit en Risk bij de Detailresult Groep.

Algemene informatie	
Aantal fte organisatie	circa 22.000
Aantal fte IAF	5
Rapporteert aan	CFO/auditcommissie

Kunt u iets vertellen over de interne auditfunctie (IAF) van de Detailresult Groep?

"De Detailresult Groep (DRG) is voortgekomen uit een fusie in 2008 tussen twee familiebedrijven, die van de familie Kat en die van de familie Van den Broek. DRG voert de supermarktformules DekaMarkt en Dirk en heeft in totaal 203 filialen. DekaMarkt bevindt zich voornamelijk in Noord-Holland en richt zich op het middensegment (full service). Dirk bevindt zich voornamelijk in Noord- en Zuid-Holland, is een prijsvechter (discounter) en is onlangs door de Consumentenbond én door Kassa bekroond als de goedkoopste supermarkt.
In 2013 ben ik gestart bij DRG als manager Operational Audit. Mijn opdracht was het opzetten van een IAF, met de focus op operational audit. Hiervoor had DRG geen IAF. De auditgerelateerde werkzaamheden lagen op het gebied van verbijzonderde interne controle en financial audit. Na een aantal maanden kwam ik erachter dat het risicomanagement niet op het gewenste niveau lag. In samenspraak met het bestuur hebben we besloten om onder mijn verantwoordelijkheid eerst het risicomanagement verder op te zetten. Gedurende deze exercitie hebben we de belangrijkste processen geïdentificeerd voor het opzetten van het risico control framework. Op basis van interviews met de eerste lijn en de beschikbare AO/IC-beschrijvingen zijn de risico control matrices per proces vastgesteld. Dit hele traject heeft ongeveer twee jaar geduurd. De verantwoordelijkheid van het actueel houden van de risico control matrices ligt in de lijn en wij beheren de matrices."

Hoe was de IAF gepositioneerd?

"In eerste instantie onder de concerncontroller. Dat werkte voor mij niet optimaal. Ik kreeg namelijk niet rechtstreeks feedback vanuit het bestuur. Dat maakt ook het anticiperen op deze feedback minder gemakkelijk. Na een jaar vertrok de concerncontroller bij DRG en dat was voor mij het natuurlijke moment om de positie van de IAF bespreekbaar te maken. Sindsdien vallen we hiërarchisch onder de CFO. Wij zijn gestart met twee fte en inmiddels zijn we doorgegroeid naar vijf fte. In ons team zitten senior, medior en junior auditors. Ik zie de IAF als kweekvijver voor DRG. Voor de medewerkers bestaat de mogelijkheid om door te stromen naar de business."

Welke type onderzoeken voert de IAF uit?
"We zijn na het opzetten van de risico control matrices gestart met het uitvoeren van operational audits. Allereerst hebben we het winkelproces geaudit. Met deze operational audit zijn we ruim vijf maanden bezig geweest. Het was een veelomvattende audit met circa vijftig bevindingen. Een belangrijke bevinding was het harmoniseren van verschillende werkprocessen van de DekaMarkt en Dirk supermarkten op bijvoorbeeld het gebied van de geldstromen en veiligheid. Voorafgaand aan een operational audit sturen wij de risico-controlmatrix naar de auditee. De auditee krijgt vervolgens de tijd om te beoordelen of de risico-controlmatrix actueel is en/of er grote wijzigingen hebben plaatsgevonden. Op basis van deze informatie (de actuele risicomatrix) voeren wij de audit uit. Voor ICT-onderwerpen (bijvoorbeeld cybersecurity) huren wij een externe partij in."

Voeren jullie tweedelijnstaken uit?
"Niet echt. Zoals ik eerder benoemd heb, sturen wij vooraf de risico-controlmatrices naar de auditees om een actueel beeld te krijgen. Aan de hand van de actuele informatie doen wij aanpassingen en wij beheren de matrices voor de organisatie. Ik heb er bewust voor gekozen om risk in onze afdelingstitel te houden, zodat er binnen DRG aandacht voor risk blijft."

Met welke uitdagingen krijgt een kleine IAF te maken?
"De grootste uitdaging is om de schaarse capaciteit op de juiste onderwerpen in te zetten. Daarnaast is het een uitdaging om goede mensen binnen te halen. We hebben ervoor gekozen om jonge medewerkers met potentie een kans te bieden om binnen onze afdeling aan de slag te gaan. We leren ze de basisprincipes van het auditvak en daarnaast krijgen zij de mogelijkheid om de RO-opleiding te volgen. Tevens is het een uitdaging om kennis en vaardigheden binnen de afdeling te hebben ten aanzien van nieuwe ontwikkelingen zoals data-analyse."

Hoe blijft u op de hoogte?
"Ik ga jaarlijks naar diverse bijeenkomsten, zoals het IIA Congres en de PAS-conferentie. Daarnaast houd ik de IIA-site in de gaten. Verder maak ik goed gebruik van mijn netwerk. Intern spreek ik tweewekelijks de CFO, waarbij wij een vast agendapunt hebben omtrent de ontwikkelingen binnen DRG. Daarnaast spreek ik regelmatig met diverse mensen uit de business (inclusief de businessdirecteuren)."

Wat haalt u uit de PAS-commissie?
"Ik zie de PAS-commissie als een netwerk om kennis uit te wisselen en op te halen over hoe andere kleine IAF's zaken georganiseerd hebben. Daarnaast heeft het IIA ervoor gezorgd dat er een specifieke rondetafel wordt georganiseerd voor de verschillende retailbedrijven."

Hoe vindt kwaliteitsborging plaats?
"Dit jaar laten wij de externe kwaliteitstoetsing uitvoeren. Wij hebben ons er eerst op gericht om de basis op orde te krijgen. Dit hebben wij gedaan door het maken van templates voor het uitvoeren van audits, het formuleren van archiveringsvoorschriften, het invoeren van collegiale review en het inzetten van evaluaties na het uitvoeren van de audits. In 2018 hebben we een zelfevaluatie uitgevoerd (QAIP). Aan de hand van de uitkomsten van de zelfevaluatie zijn er nog een aantal verbeteringen doorgevoerd, met als doel om in 2019 te voldoen aan de IIA Standards en daarmee de kwaliteitstoetsing met een positief resultaat af te ronden."

Wat is de ambitie van de IAF op de langere termijn?
"Dit jaar met goed resultaat de kwaliteitstoets afronden. Daarnaast een kweekvijver voor de business en een afdeling te zijn die door de business gevraagd wordt een specifieke audit uit te voeren (audits op verzoek)."

Over...

Wilbert Kooiman RO is manager Operational Audit en Risk bij de Detailresult Groep. Daarvoor was hij hoofd Internal Audit bij de Telegraaf Media Groep. Het auditvak leerde hij bij PriceWaterhouseCoopers.

Dit artikel is eerder gepubliceerd (14-12-2018) op deitauditor.nl. https://www.deitauditor.nl/informatiebeveiliging/focus-op-essentiele-zaken-in-it-audits/

UIT DE IT-AUDITOR

Focus op essentiële zaken in IT-audits

Robert Metsemakers

Waar let je op als je de kwaliteit van informatiebeveiliging wilt verbeteren of op het reeds hoge niveau wilt houden? Let je op het ontbrekende deel in de beheersmaatregelen of juist op wat wél aanwezig is? Focus is meestal goed, maar richt daarbij de aandacht dan wel op de juiste onderwerpen.

Britse vliegtuigen bombardeerden en beschoten in de Tweede Wereldoorlog steden in nazi-Duitsland. Ze werden zelf ook geraakt, door vliegtuigen en luchtafweergeschut – de nazi's verdedigden immers hun burgers, militairen, handel en industrie tegen deze aanvallen. Alle Britse vliegtuigen werden daarom bij terugkeer op de vliegvelden in het Verenigd Koninkrijk nauwkeurig onderzocht en de bepantsering werd verstevigd. Maar de geallieerden hadden er enige tijd plus het inzicht van wiskundige, statisticus en econoom Abraham Wald voor nodig, om in te zien dat het verstevigen juist moest gebeuren op de plaatsen waar de vliegtuigen niet geraakt waren. Want de geraakte plaatsen, zichtbaar aan de kogelgaten of aan de geheel weggeschoten delen, waren duidelijk niet essentieel om terug te kunnen keren naar de vliegbasis. Juist de niet-geraakte delen hadden het teruggekeerde vliegtuig gedragen.

Hel en verdoemenis… niet dus

Laten we nu eens een te auditen afdeling of proces vergelijken met het vliegtuig, en de auditor oneerbiedig met het luchtafweergeschut. De auditor raakt in zijn audit of onderzoek het vliegtuig en zet een flink aantal bevindingen als kogelgaten op papier. Die bevindingen verschillen onderling in omvang, plaats, invloed op het 'vliegtuig' en daarmee in hun belang. Elke auditor weet dat bij gerapporteerde bevindingen die niet urgent, dringend, of belangrijk worden genoemd, de aandacht van de lezer al snel verslapt. Zeker als de auditee toch al te weinig tijd heeft of neemt om het hele rapport te lezen en zich daarom beperkt tot de aanbevelingen op de bladzijde met de managementsamenvatting. De belangrijkste bevindingen komen immers in de managementsamenvatting en de enigszins belangrijke halen enkel het rapport zelf.

De (interne) auditor bespreekt het conceptrapport met de bevindingen met de auditee, er worden per oplosactie realisatiedata en verantwoordelijke personen bepaald en dit alles wordt vastgelegd binnen een actielijst. Sommige bevindingen zijn urgent en moeten snel, binnen drie maanden, worden opgelost. Zo niet, dan gaat het licht uit. Andere zijn iets minder dringend en moeten over zes maanden of een jaar klaar zijn.

Vaak duurt het echter langer, veel langer dan de vooraf afgesproken periode, om bevindingen op te lossen. Toch blijft het licht ondertussen branden, gaat de tent niet failliet en komen er geen enorme boetes van de toezichthouder. Werkend aan de auditeekant dronk ik ooit champagne omdat een tot urgent bestempelde bevinding, die dus binnen drie maanden opgelost moest worden, reeds zes volledige jaren 'open' op de actielijst stond, terwijl de onderzochte afdeling nog steeds succesvol draaide. Met andere woorden, het vliegtuig vloog nog steeds! Het door de auditor gevonden 'gat' was weliswaar een tekortkoming, maar niet essentieel. De auditor achtte de kans dat het op dat punt fout zou gaan zo groot, dat de bevinding geen drie maanden meer open kon blijven. De auditee hoorde daarin echter alleen de tijdsdruk en prioriteit en niet de mogelijke impact. Als de auditee erin slaagt om toch jarenlang in de lucht te blijven, zonder die urgente bevinding ooit aan te pakken, gaat het tijdsdrukgevoel echter verloren. 'The thrill is gone', zou bluesgitarist B.B. King zingen, want 'the sense of


Adobe Stock

urgency for the auditee' heeft te veel lettergrepen. Het mooiste is wanneer auditor en auditee gezamenlijk de prioriteit van oplossen bepalen en daarbij rekening houden met de impact én de kans op een bedreigende gebeurtenis.
Urgentie van issues in soorten en maten
Er kunnen goede en minder goede redenen zijn waarom een auditor vindt dat bepaalde bevindingen urgent zijn en dus als eerste opgelost moeten worden, namelijk omdat ze:

a. zeer riskant zijn door een hoge impact als het fout gaat;
b. zeer riskant zijn door een hoge kans van optreden;
c. noodzakelijk zijn om daarna andere bevindingen goed, goedkoop of snel (slechts twee van de drie zijn tegelijkertijd mogelijk) op te kunnen pakken;
d. niet veel tijd hoeven te kosten en de auditee het gevoel kunnen geven 'dat zijn medewerkers meters maken' met de noodzakelijke verbeteringen.

Reden (a) is de beste motivatie en ook goed te onderbouwen met een inschatting van de mogelijke schade bij optreden. Maar dit onderbouwen moet de auditor dan wel expliciet doen in zijn managementsamenvatting, want anders denkt de auditee dat de bevinding urgent is om reden (b).

Reden (b) is ook een goede, maar de auditor moet daarvoor wel beschikken over een kristallen bol van uitzonderlijke kwaliteit of gewoon uit de losse pols zelf de toekomst kunnen voorspellen. De ingeschatte kans van optreden kun je met statistisch goochelen omrekenen naar een periode waarin de vervelende impact naar verwachting zal gaan optreden, maar wanneer die periode inmiddels meerdere jaren verstreken is (zie het champagnevoorbeeld) worden voortgangsgesprekken over de actielijst tussen auditor en auditee wel een beetje ongemakkelijk. Zeker wanneer de prioritering puur van de kant van de auditor komt en de auditee, achteraf, 'de kans altijd al te hoog had gevonden'.

Reden (c) is misschien wel de beste, maar uiteindelijk ook gebaseerd op een niet al te harde inschatting.

Reden (d) is de politieke of verkoopmotivatie. Wat verkocht wordt is het 'laaghangend fruit' dat misschien niet zo voedzaam of lekker of gezond is als de hoger hangende vruchten, maar je kunt er wel gemakkelijker bij. Het motiveert de plukker dat hij/zij het eerste mandje al snel gevuld heeft. Bijkomend nadeel is dat zo de moeilijke en tijdrovende issues overblijven, wat vervolgens de eerder via deze truc opgebouwde motivatie bij de auditee weer teniet kan doen. Niet de allerbeste reden dus.

Hoe dan wel?
Begrijp me goed: auditors moeten blijven auditen (lees: schieten op vliegtuigen) en daarbij letten op zaken die niet voldoen aan een voorafgaand vastgestelde set normen. Ook moeten ze die 'foute' zaken en bijkomende urgentie blijven melden. Maar ik zou er graag een lans voor breken onze audits te verrijken door nadrukkelijk ook aandacht te geven aan de niet-geraakte delen van het onderzochte vliegtuig (de wel onderzochte aspecten waar echter geen bevindingen waren). Dat betekent analyseren wat er juist wél goed gaat in de uitvoering van precies die vitale, dus onmisbare delen en daar lessons learned en best practices uit te halen. Want andere auditees met hetzelfde proces kunnen dat proces daarmee vaak verbeteren

en/of tijd en geld besparen. Hierbij ga ik uit van de situatie dat een (interne) auditor een proces een aantal keren onderzoekt, zoals in een thema-onderzoek, waarbij hetzelfde proces bij meerdere afdelingen wordt beoordeeld. Er zijn natuurlijk ook audits of onderzoeken gericht op de oorzaak van een groot incident, of met een forensisch karakter waar een dader van een eerdere (moedwillige) foutieve actie moet worden opgespoord. Daar zijn de bevindingen anders van aard en is het lastiger, ook door de noodzakelijke vertrouwelijkheid, om tot elders toepasbare lessons learned te komen.

'Voorspellen is moeilijk, vooral als het om de toekomst gaat', zoals natuurkundige Niels Bohr ons al waarschuwde. Als onafhankelijke buitenstaander kan een auditor soms beter het belang of de prioriteit van een aanbeveling inschatten dan de auditee die verantwoordelijk is voor uitvoering of implementatie ervan. Maar als tegenhanger hiervan moeten we als auditor wel conclusies trekken uit het gegeven dat het 'vliegtuig', ondanks alle in de audit ontdekte werkelijke gaten en tekortkomingen, nog steeds vliegt en terugkeert op de basis.

Natuurlijk moeten we als auditors de auditee blijven helpen door voor en het liefst samen met hem, de bevindingen te prioriteren naar hun belang en ernst. Maar laten we daarbij ook de durf hebben om na enige tijd die inschatting te heroverwegen en dan een nieuwe inschatting en dus nieuwe selectie voor de actielijst te maken: hoe zit het zes jaar later eigenlijk met die destijds tot urgent bestempelde bevindingen, waren die echt allemaal zo urgent? Dat er al die tijd niets vervelends is gebeurd, betekent niet per definitie dat de urgentie aanvankelijk was overschat, maar het stemt wel tot nadenken of het in de audit aangetroffen 'gat' inderdaad een vitaal of essentieel punt in het proces of de onderzochte organisatie is. Dat is waar ik de focus zou willen leggen.

R. (Robert) Metsemakers | IT-auditor en informatiebeveiligingsexpert.
Robert is een ervaren IT-auditor en informatiebeveiligingsexpert. Hij gaat graag uitdagingen aan op gebieden als de inrichting van informatiebeveiliging, security advies en schrijfopdrachten op verschillende terreinen.
Robert is te bereiken via:
Robert.metsemakers@gmail.com.

Een andere kijk op **waardecreatie**

Duurzaamheid is niet nieuw maar wel actueler dan ooit. Veelal zal gepoogd worden om economische groei gepaard te laten gaan met het realiseren van duurzaamheidsdoelstellingen. De rol van de auditor op het gebied van duurzaamheid is ook niet nieuw. In 2011 verrichtte het IIA samen met de vakgroep Interne accountants van het NBA een studie naar de rol van internal audit op het gebied van corporate social responsibility (CSR). De conclusie was dat internal audit veel toegevoegde waarde kan leveren. Er zijn al diverse standaarden om duurzaamheid in te richten en dus ook te toetsen. Het meest toegepast is het global reporting initiative (GRI), waarbij een organisatie naar economische, ecologische en sociale normen is ingericht. Economische groei is daarin het leidende criterium.

De donuteconomie breekt met het dogma van eeuwige economische groei.[1] Het gedachtegoed van de donuteconomie stoelt op het als maatschappij, land of organisatie, vinden van de balans tussen een minimum sociale ondergrens en een maximum ecologische bovengrens. Een organisatie die de donuteconomie omarmt, richt zich op distributieve en regeneratieve systemen. Distributief betekent dat welvaart gelijk verdeeld wordt; dit is gestoeld op het concept van sociale rechtvaardigheid. Regeneratief houdt in dat de productiefactor natuur maximaal wordt hergebruikt en dat de aangerichte schade aan de natuur wordt hersteld. Economische groei is daarin geen randvoorwaarde, noch een doel op zich.

De interne auditor dient inzicht en aanvullende zekerheid te geven aan het management en de bestuurders over de interne beheersing. Wat nu als laatstgenoemden geen enkele intentie hebben om de organisatie circulair in te richten en aandacht te geven aan gelijke verdeling van welvaart? En wees nu eerlijk: wat kan het bestuur doen als de aandeelhouder uitsluitend financieel rendement op zijn investering wil? Maar, zonder inzicht geen verandering. In het kader van ongevraagd advies belet niets de internal auditor om inzicht te geven in onderwerpen als: wat is onze ‘carbon foot print’? Wat kan in onze processen anders zodat er meer hergebruikt wordt? Kunnen we kennis meer verspreiden? Wanneer de organisatie duurzaamheid als kernwaarde propageert, heeft de internal auditor ook nog eens een objectieve grond om dergelijke inzichten te geven en op deze manier een steentje bij te dragen aan de grote verandering waar we als mensheid voor staan.

Het gaat daarbij dus niet om het identificeren van besparingsmogelijkheden voor de organisatie. Het gaat om de vraag wat de sociale en ecologische impact is van het productieproces, hoe het product vervoerd en verkocht wordt. De vraag: hoe kan dit product of deze dienst meer bijdragen aan de welvaart van de maatschappij?, staat centraal. Die vraag kan gesteld en beantwoord worden door de auditor.

Circulariteit en gelijke distributie van welvaart zijn wellicht de onderscheidende factoren voor de consument van de toekomst. Dus stel de vragen (en beantwoord ze), voor de aarde, voor ieders welzijn en voor de organisatie.

Noot
1. Zie AM onderzoek, *Audit Magazine*, nr. 2, 2019.

■ Internal auditfunctie
■ Data science

Artikel
Tekst Drs. Margot Hovestad RO
Raymond Wondergem MSc RO
Beeld 123RF

Cybergeddon, een reëel gevaar?

Peter Zinn is expert op het gebied van cybersecurity en was spreker op het IIA Congres afgelopen juni. In dit interview passeerden de gevaren van cybercrime, de kans op een Cybergeddon en de weerbaarheid van organisaties om dit te voorkomen, de revue.

Over...

Peter Zinn studeerde informatica. Na een standaard IT-carrière stapte hij over naar het hightech crime team van de Nationale Politie. In 2016 startte Zinn zijn eigen bedrijf op het gebied van cybersecurity.

Vertel eens iets over uzelf

"Ik heb informatica gestudeerd en daarnaast wat psychologie. Overdag was ik IT-er en 's avonds deed ik aan toneel. Na drie jaar in Canada maakte ik de overstap naar cybersecurity. Daar werd ik strategisch adviseur bij de politie bij het net opgerichte hightech crime team. Daar heb ik mijn twee kanten in balans gebracht, de technische IT-kant en de communicatiekant. Belangrijk in deze rol was het communiceren met de buitenwereld, bijvoorbeeld om mensen duidelijk te maken dat je wel aangifte kunt doen op het gebied van cybercrime. Daarnaast heb ik mij sterk gemaakt voor een cyberteam in iedere regio. Dat heb ik tien jaar gedaan. Het team is in die periode gegroeid van 15 naar 120 medewerkers.
Vervolgens ben ik voor mijzelf begonnen. Ik vind spreken leuk en geef lezingen over cybersecurity en -crime. En ik train specialisten op het gebied van cybersecurity om betere sprekers te worden. Deze specialisten hebben vaak veel kennis, maar niet de vaardigheden om deze kennis goed over te brengen. Mijn belangrijkste doel is Nederland veiliger te maken op het gebied van cybersecurity, daar wil ik aan bijdragen."

Wat kunnen we doen om cybercrime risico's te verminderen?

"Over het algemeen is het bewustzijn bij mensen er wel, alleen weten ze niet waar ze op moeten letten en wat ze moeten doen om een cyberaanval te voorkomen. De meeste mensen zijn van goede wil en moeten handvatten krijgen om te leren omgaan met cybercrime. Als iedereen in de keten zijn eigen verantwoordelijkheid neemt, dan kan 99% van de problemen voorkomen worden en is er niet eens zoveel aan de hand. Het begint bij het ontwikkelen van 'patches' door bijvoorbeeld Microsoft, vervolgens moet de IT-afdeling van een organisatie deze patches tijdig uitvoeren en de

eindgebruiker zorgt voor zijn digitale hygiëne. Deze hygiëne bestaat onder andere uit het:

- aanstaan van automatische updates;
- aanzetten van de screensaver, zodat als je van je werkplek weggaat anderen niet kunnen meekijken;
- gebruiken van fatsoenlijke wachtwoorden (lange wachtwoorden, bijvoorbeeld vier woorden);
- gebruiken van verschillende wachtwoorden voor verschillende domeinen.

Ik vergelijk het altijd met gordels in de auto. Toen die werden ingevoerd was er veel tegenstand. Mensen vonden het vreemd en onwennig. Nu is het raar wanneer je geen gordel draagt. Dat is precies hetzelfde met het aanleren van nieuwe gewoonten op cybergebied. Het is niet fijn, want we moeten onze werkwijze veranderen. Maar als je de gewoonte eenmaal hebt, kost het geen extra tijd en voelt het niet meer vreemd.
Het doel van organisaties moet zijn om cybersecurity als onderdeel van hun risicobeheersing te zien. Welke risico's willen organisaties lopen op het gebied van cybersecurity? Het heeft geen zin om alles 'dicht' te zetten, want dan kunnen medewerkers hun werk niet doen. Als een organisatie vervolgens het slachtoffer wordt van ransomware is het belangrijk dat er een back-up is. Dus is het verstandig te zorgen voor een goed back-upbeleid, waarbij de back-ups ook periodiek getest worden. Er zijn bedrijven failliet gegaan door ransomware."

Kun je cybercrime voorkomen?
"Nee, nooit helemaal. Er blijven altijd slimme criminelen die nieuwe manieren bedenken om toch binnen te komen. Cybercriminelen zijn ontzettend creatief als het gaat om geld verdienen. Een maand geleden had ik een bijeenkomst met een groep CISO's (chief information security officers). Het onderwerp was dat de cybersecuritydijken steeds hoger worden. Maar wat gaan we doen als de dijken het begeven? Wat betekent het als een groep cybercriminelen ervoor zorgt dat je organisatie niet meer functioneert? Organisaties moeten een plan hebben als dit gebeurt, als de dijk overstroomt. Heb je dan een fall-backsysteem, ben je dan robuust genoeg om nog te functioneren als organisatie? Een van de uitkomsten was: we kunnen de dijken wel verhogen, maar ze zijn lek. Cybercriminelen zoeken naar lekken in de dijken en denken out of the box. Daar zit ook een kans voor auditors, niet om de dijken te verhogen, maar om de lekken te vinden."

Op het IIA Congres sprak u over cybergeddon. Wat is dat?
"Cybergeddon is een woordspeling op armageddon en gaat over het einde van de wereld. De redenatie is dat we sinds

de jaren zestig steeds meer afhankelijk zijn geworden van IT en dat groeit nog steeds. Door schaalvergroting van IT wordt de impact van een calamiteit ook groter. Het betekent dat je niet alleen meer aangevallen kunt worden door iemand uit je eigen omgeving, maar ook door een Russische crimineel die 2000 km verder op zit. De aanvalsoppervlakte is vergroot. De multinational Maersk is hier een goed voorbeeld van. Een aanval van Russische hackers op de IT-infrastructuur van Oekraïne leidde ertoe dat Maersk een tijdlang 'out of business' was."

Hoe groot is de kans op een cybergeddon?

"Ik denk dat de kans klein is dat er een cybergeddon gaat plaatsvinden, maar het is niet onmogelijk. Als je bijvoorbeeld kijkt naar artificial intelligence, dan ben ik niet bang dat robots de wereld gaan overnemen. We zijn nu wel in de 'narrow-artificial-intelligencefase' beland, de fase dat robots één handeling ontzettend goed kunnen. Alleen zijn robots nog steeds afhankelijk van de aansturing door mensen. Kwaadwillenden kunnen enorme schade aanrichten met dit nieuwe gereedschap. Autorijden daarentegen wordt veiliger door artificial intelligence, want mensen zijn niet de beste chauffeurs. Maar er is ook de mogelijkheid om het artificial-intelligencesysteem negatief te beïnvloeden.
Om de kans op een cybergeddon te verkleinen, is het van belang om de security en de robuustheid van de samenleving te vergroten. Dat begint in je organisatie. Wat ga jij als organisatie doen als alle digitale gegevens weg zijn? Alleen kost robuustheid een organisatie veel geld. Er moet een terugvaloptie zijn en dat is ook logisch, ook als mens hebben we twee longen, twee nieren, twee ogen."

De mens is vaak de zwakste schakel, waarom?

"Daar kan ik uren over vertellen. Voor software heb je updates, maar ons brein is al eeuwenlang niet geüpdatet. Wij hebben bepaalde patronen waar cybercriminelen gebruik van maken. Het is makkelijk om misbruik te maken van het vertrouwen van mensen om fysiek of digitaal binnen te komen. Wat doe je eraan? In ieder geval elkaar blijven vertrouwen. Anders worden de medewerkers paranoïde en werkt je organisatie niet meer. Het gaat om het aanpassen van patronen en gewoonten om de veiligheid vergroten. Bijvoorbeeld het aanzetten van een screensaver. Een ander belangrijk onderdeel is de cultuur van de organisatie. Vroeg of laat wordt een organisatie gehackt. Het is belangrijk dat medewerkers dit open en eerlijk kunnen vertellen. Er moet de mogelijkheid zijn dat medewerkers leren van hun fouten en ze er niet voor worden gestraft. Een open cultuur zorgt ervoor dat medewerkers hun gewoonten aanpassen."

Wat is de rol van de top van een organisatie?

"Bewustwordingsprogramma's hebben ook een plek in het voorkomen van cybercrime, maar daar moet het niet bij

"We kunnen de dijken wel verhogen, maar ze zijn lek. Daar zit ook een kans voor auditors, niet om de dijken te verhogen, maar om de lekken te vinden"

blijven. Cybersecurity is vooral een verantwoordelijkheid van de raad van bestuur, dus ook de bewustwording is dat. Op de werkvloer zijn best goede ideeën om cybercrime aan te pakken, maar de sturing hoort vanuit de top te komen. Top-down moet aangegeven worden dat cybersecurity belangrijk is. De raad van bestuur moet ook de opdracht geven om het IT-landschap in kaart te brengen en om de IT-afdeling op voldoende sterkte te brengen om cybercrime het hoofd te bieden. Dan hebben bewustwordingsprogramma's toegevoegde waarde."

Is er een standaardprofiel van de cybercrimineel?

"Er is geen standaardprofiel van de cybercrimineel. Het begint bij de tophackers. Ik deel ze grofweg in een aantal categorieën in, aan de hand van een berg:

- statelijke hackers (China, Rusland, Amerika, et cetera) en de tophackers;
- carrièrecriminelen;
- script kiddies die online tooltjes gebruiken zonder te weten wat ze doen.

Net zoals bij een berg het smeltwater naar beneden stroomt, stroomt bij deze indeling de informatie en het gebruik van de technologie ook naar beneden. De tophackers bedenken en schrijven nieuwe methoden om te hacken en wat later maakt de volgende groep hier gebruik van. Overigens zijn de tophackers niet meer zichtbaar. Je kunt het vergelijken met de kopstukken van de maffia. Die zijn ook niet in beeld.

Naast deze categorieën kun je hackers ook indelen naar motieven. Deze motieven zijn: geld (businessmodel); politiek; vandalisme; bekendheid; uitdaging. Het is belangrijk om te beseffen dat 90% van de hackers niet crimineel is. De meesten staan aan de goede kant en doen het voor de sport. Zij waarschuwen vervolgens de organisaties dat er een 'lek' is ('responsible disclosure'). Het is daarom van belang dat organisatie de regels voor responsible disclosure op hun website zetten. Organisaties moeten dit serieus nemen, het lek dichten en de hacker hiervan op de hoogte te brengen. In Nederland zijn we hier al heel ver mee."

Wat kunnen auditors leren van cybercriminelen?

"Creatief en lateraal denken. Denk als auditor vooral out of the box en probeer eens een andere techniek als de huidige niet werkt. Je hebt soms meerdere plannen nodig om je doel te bereiken. Dan heb je ook een back-upplan als het nodig is. Wees niet bang om een keer af te wijken van standaardpatronen, wees flexibel. Richt ook ruimte in om te pionieren en te klooien." <<

Artikel
Tekst Linda Poort
Beeld Elisabeth Beelaerts

Terugblik IIA Congres 2019: Intelligence & *Impact*

Afgelopen 13 en 14 juni vond in Amersfoort het jaarlijkse IIA Congres plaats over data analytics, algoritmes, ons brein en het einde van de wereld. Het congres was weer een groot succes met 7 keynotes, 18 parallelsessies, 4 verschillende workshops, een talkshow, een satirische nieuwsshow en een gezellige feestavond. Een terugblik.

5 Lessen voor de moderne auditor
Hoe ga jij straks 2020 in? Welke dingen ga jij volgend jaar anders doen? **Martijn Aslander** heeft wel een paar tips. 1) Mensen enthousiasmeren is je belangrijkste uitgangspunt. 2) Sommige dingen kun je alleen leren door ze te doen. 3) Technologie is perfect om dingen in beweging te krijgen. 4) Je kunt bureaucratie omzeilen met easycratie. 5) Innovatie is onvermijdelijk, dus innoveer mee. Zorg ervoor dat je als auditor niet overbodig wordt!

Auditing met Artificial Intelligence
Mona de Boer ziet de toekomst van de auditfunctie als een Formule 1-race: “Je hebt de auditor, een mens, plus heel veel data, en met die combinatie worden grote doelen bereikt. ‘Data-centricity is changing what we audit, how we audit and when we audit.’ Het centraal staan van data verandert langs meerdere lijnen het auditvak. Terugkijken verandert in vooruitkijken. De internal auditfunctie is aan het automatiseren, zodat we ons kunnen gaan richten op de inhoudelijke analyse van de resultaten. Een luxepositie.”

De menselijke aspecten van AI
"Bedenk niet hoe de wereld er over vijf tot tien jaar uit kan zien met behulp van technologie, maar kijk naar wat de technologie van vandaag kan betekenen voor morgen", aldus **Wouter Siepman**. "Hiervoor moeten we leren hoe wij, als mensen, onze processen uitvoeren. Dan kunnen we die daarna misschien in AI omvatten. Dat moet ons doel zijn: onze intelligentie in de computer zien te krijgen. De robot kan dan de aantekeningen maken, zodat de werknemer een echt gesprek kan voeren met de klant. Automatiseren is mensen empoweren in plaats van overnemen of vervangen!"

De auditor als stuntpiloot
Mensen maken ontzettend veel fouten. Dat is niet te voorkomen, maar dat is ook niet de bedoeling. Van (andermans) fouten, kun je namelijk ontzettend veel leren", zegt **Frank Versteegh** (piloot en kunstvlieger). Hij geeft vijf tips voor de auditor die zijn risico's goed wil managen. 1) Een goede voorbereiding is het halve werk. 2) Wees je bewust van de risico's. 3) Weet wat je moet doen in onverwachte situaties. 4) Hoe meer je weet, hoe beter werk je kunt leveren. 5) Praat over je fouten zodat deze als les kunnen dienen.

ICT zorgt voor de ondergang van de wereld
"We gaan er allemaal aan. We weten alleen nog niet hoe. Mijn 'guess': cybergeddon." **Peter Zinn** legt uit hoe onze ICT ervoor gaat zorgen dat we er allemaal aan gaan én hoe we dit kunnen voorkomen. ICT de zwakste schakel? Snelle ontwikkeling de zwakste schakel? Nee! De mens is de zwakste schakel. In drie stappen kunnen we deze zwakke schakel versterken: 1) Doe aan cyberhygiëne. 2) Leer denken als hacker. 3) Leg de cyberverantwoordelijkheid bij de CEO. Vroeg of laat komen ze binnen. En dan is de vraag: ben je daarop voorbereid?

Auditor redt de wereld in 3 stappen
Leen Zevenbergen spreekt gepassioneerd over het belang van duurzaamheid en de rol van de internal auditor in het voortbestaan van de wereld. "'Don't try to be successful, but try to be of value.' De mensheid bestaat maar een snippertje van de tijd dat de aarde bestaat. De natuur zal altijd overleven. De mens niet." De drie manieren om als auditor de wereld te redden: 1) Wees blijvend creatief. 2) Werk aan de duurzame ontwikkelingsdoelstellingen. 3) Geef jouw bedrijf een 'purpose'. "Zolang je organisatie waarde biedt, heeft deze betekenis voor de wereld. Inspireer jezelf." <<

Meer weten...

Lees het hele congresverslag: http://bit.ly/ConVe19
Bekijk alle foto's: http://bit.ly/FotoIIACon19
Bekijk de impressiefilmpjes: http://bit.ly/ConVid2019

VOLLEDIG DATA-GEDREVEN AUDIT?
ONTDEK INTELLIGENT BUSINESS CLOUD

- Reconstrueer de daadwerkelijke processen met feitelijke data
- Vind de oorzaak van tegenstrijdigheden en 'compliance issues' met enkele muisklikken
- Anticipeer op toekomstige bedreigingen en voorkom problemen
- Meet en kwantificeer de impact van uw audit-activiteiten

100%

Volledig transparante bedrijfsprocessen

+37%

Hogere snelheid in auditproces

+30%

Hogere efficiëntie in auditproces

celonis

Column
Tekst Prof.dr. Mark van Twist

Niet weten *wat* **niet weten**

Het zal aan mij liggen, maar ik krijg de indruk dat het verkennen van de toekomst op dit moment weer ongelooflijk populair is in auditland. Na een periode waarin de belangstelling hiervoor wat afnam, is elke zichzelf respecterende organisatie of instelling er opnieuw druk mee. Met wat gevoel voor ironie zou je kunnen spreken over een 'terugkeer van de toekomst' in de auditpraktijk.

Nu is de wens om de toekomst te verkennen ook buiten het vakgebied bepaald niet nieuw. Integendeel, het past in een traditie die duizenden jaren teruggaat. De mens is altijd al op zoek geweest naar mogelijkheden om meer over de toekomst te weten te komen. Vandaar dat er door de eeuwen heen diverse pogingen zijn gedaan om de stand van de sterren te interpreteren, de ingewanden van kippen en schapen te lezen, in kristallen bollen te kijken, tarotkaarten te leggen of zieners en orakels in te schakelen. Methoden als deze mogen in onze tijd wat in onbruik zijn geraakt, de wens om de toekomst te kennen en te verkennen is blijven bestaan.

In de recente opleving van de belangstelling voor de toekomst valt naar mijn idee ondertussen wel een duidelijke verschuiving waar te nemen in de ambitie die hiermee verbonden wordt. Inhoudelijke trefzekerheid van de toekomstvoorspellingen wordt minder belangrijk geacht. Niet de vraag of de voorspellingen in de toekomstverkenning wel precies zo uitkomen staat centraal in de oordeelsvorming over de opbrengsten. De nadruk ligt eerder bij de interactieve dan bij de instructieve waarde van de toekomstverkenningen, ingegeven door de even indringende als intrigerende vraag: draagt de trendanalyse uiteindelijk (vooral ook) bij aan een breed in de organisatie gedeeld en gedragen beeld van de toekomstige auditpraktijk?

De veronderstelling is hier dat toekomstverkenningen sterker doorwerken in de organisatie wanneer mensen via intensieve interactie bij de totstandkoming ervan betrokken zijn en de verkenning mede als hun 'eigen' product beschouwen. De waarde van een dergelijke 'participatieve' aanpak is bovendien dat het inzicht over thema's en trends die kunnen spelen in de toekomst niet pas aan het eind van het traject beschikbaar komt, maar al gedurende het totstandkomingsproces wordt uitgewisseld.

Tegelijkertijd zijn hier natuurlijk kanttekeningen bij te plaatsen. Intensivering van de interactie en het streven naar breed gedeelde en gedragen toekomstbeelden is niet zonder keerzijde. Dat wordt direct duidelijk bij een duiding van de toekomst in termen van het 'onbekende onbekende'. Hoe zei Donald Rumsfeld het ook alweer? "There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know."

Het gaat er bij toekomstverkenningen niet alleen om in kaart te brengen wat we weten dat we het weten en wat we weten dat we het nog niet weten. Waar het vooral om draait is gevoel te ontwikkelen over wat we zelfs niet weten dat we het niet weten over de toekomstige auditpraktijk. Dat is de categorie van het 'onbekende onbekende'.

Juist om grip te krijgen op die laatste categorie is het goed om bij het verkennen van de toekomstige auditpraktijk niet te veel te vertrouwen op de 'insiders' in het vak, die immers niet zomaar weten wat ze niet weten. Nodig is juist een aanpak die volop ruimte laat voor ongezochte ontmoetingen en onverwachte opbrengsten, ter voorkoming van de anders toch eigenlijk weer vrij 'voorspelbare verrassingen' achteraf.

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.

Artikel
Tekst Drs. Martine de Zeeuw RO
Dr. Paul van den Brink MBA
Beeld Martine de Zeeuw

Kennisdelen: *wat werkt?*

Dit artikel beschrijft hoe auditors organisaties kunnen helpen om kennisdeling te verbeteren. Met een inventariserend waarderend onderzoek kun je inzicht geven in die factoren die mensen helpen om kennis te delen. Met het inzicht in wat goed werkt, kan de organisatie gericht kennismanagement verbeteren.

Bij een krappe arbeidsmarkt, een vergrijzende arbeidsbevolking, of bij het inkrimpen van het personeelsbestand vanwege bezuinigingen, wordt het behouden van de juiste kennis een steeds grotere uitdaging voor organisaties. Het wordt dan belangrijker om medewerkers te motiveren om gewenste kennis te ontwikkelen en om kennis met elkaar te delen. Door kennis te delen kan de aanwezige kennis effectiever gebruikt worden.

Hoe stimuleer je het delen van kennis?

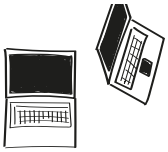
Het delen van kennis kan worden bevorderd door een omgeving in te richten die dit stimuleert. Cruciaal daarbij is dat kennisdelen tussen mensen niet afgedwongen kan worden. Er kan alleen een omgeving gecreëerd worden die kennisdelen stimuleert en faciliteert.
De in dit artikel beschreven onderzoeksmethode is gebaseerd op een proefschrift (Van den Brink) en is in de praktijk doorontwikkeld in een onderzoek naar kennismanagement bij Rijkswaterstaat (RWS). Bij dit onderzoek is bewust gekozen voor een waarderende, positieve aanpak. De verwachting van RWS was namelijk dat als je het accent

legt op de dingen die goed gaan, dit energie geeft om te verbeteren. Ook is gekozen voor het gebruik van visuals tijdens het hele onderzoek om bij te dragen aan een open en positieve sfeer tijdens het onderzoek. Hierna worden drie stappen beschreven van een waarderend onderzoek naar motiverende factoren voor het delen van kennis.

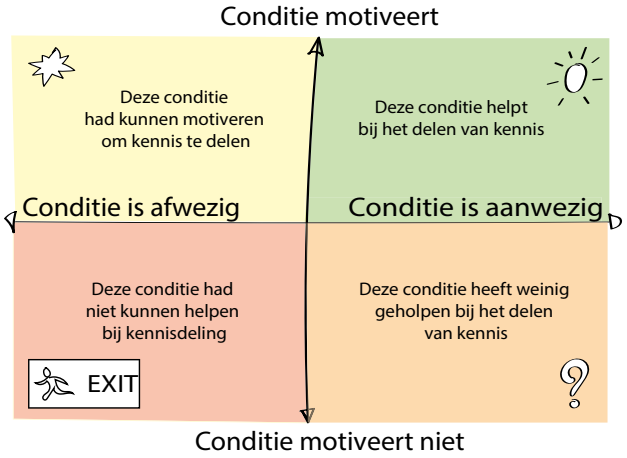
Stap 1 – Inventarisatie van motiverende factoren voor kennisdeling
In de eerste stap van het onderzoek worden interviews gehouden met functionarissen op sleutelposities in de organisatie. Hen wordt gevraagd om verschillende factoren in een matrix te plaatsen. Zo kunnen ze aangeven of motiverende factoren aan- of afwezig zijn en of factoren daadwerkelijk als motiverend of faciliterend worden ervaren (zie *figuur 1*).

Er worden in de gesprekken drie typen factoren voorgelegd. De sociale factoren zijn met name bedoeld om de motivatie, houding, competentie en vaardigheden van de mens te beïnvloeden, er dient immers een gedragsverandering bewerkstelligd te worden.

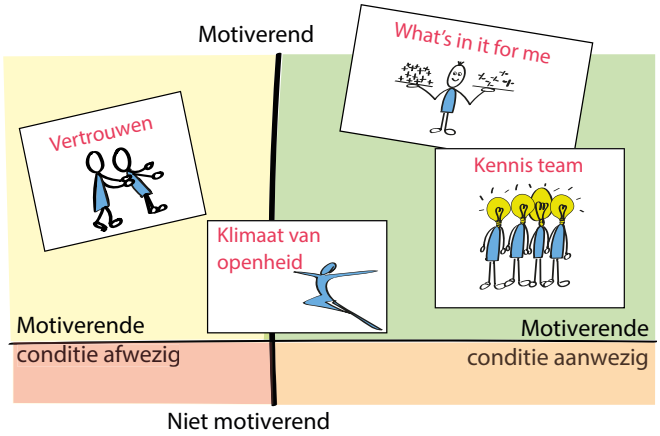
De organisatorische factoren staan voor de dimensies van een organisatie die kunnen helpen bij het kennisdelen in de (dagelijkse) praktijk.



Technologische factoren kunnen helpen bij het verbinden van mensen met elkaar of met expliciete kennis of informatie.



Figuur 1. Matrix ten behoeve van de inventarisatie van motiverende factoren



Figuur 2. Voorbeeldmatrix met motiverende factoren

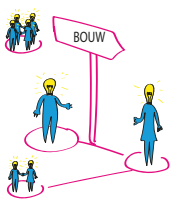
Stap 2 – Overzicht motiverende factoren als startpunt voor verbetering

Door de inventarisatie van motiverende factoren ontstaat een beeld van de mate waarin factoren aan- of afwezig zijn en daadwerkelijk motiveren en faciliteren om kennis te delen, of niet. Deze onderzoeksresultaten worden gevalideerd, bijvoorbeeld door middel van een groepsworkshop, waarna de auditor ze kan opnemen in een rapportage.

Het overzicht met motiverende factoren vormt het startpunt om te bepalen hoe het delen van kennis verder verbeterd kan worden. Wanneer men kiest voor een waarderende aanpak, zoals in het onderzoek bij RWS, zal in deze stap het accent gelegd worden op de factoren die door de geïnterviewden daadwerkelijk als motiverend ervaren worden. De insteek is dan om deze motiverende en faciliterende factoren te behouden en te versterken (zie *figuur 2*).

Stap 3 – Verbeteracties formuleren

Op basis van de geïnventariseerde motiverende en faciliterende factoren, die in meerdere of mindere mate aanwezig zijn, formuleert de opdrachtgever verbeteracties om te zorgen voor een werkomgeving die nog meer motiveert en faciliteert. Bij het formuleren van verbeteracties is het goed om eerst stil te staan bij de vraag welk type producten of diensten de organisatie levert. Wanneer een organisatie gestandaardiseerde producten en diensten levert is het belangrijk om de kennis van de medewerkers vast te leggen en toegankelijk te maken. De herbruikwaarde van kennis is namelijk hoog. Verbeteracties zullen gericht zijn op het vastleggen en toegankelijk maken van kennis. Deze acties horen bij de zogenaamde 'codificeringsstrategie'.



Bij een organisatie die op maat gemaakte producten of diensten levert, is het belangrijk dat mensen elkaar (en elkaars kennis) goed kunnen vinden, zodat ze de benodigde kennis kunnen uitwisselen. Acties gericht op het koppelen van mensen om uitwisseling van kennis gemakkelijk te maken horen bij de 'personalisatiestrategie'.

Praktijkervaring bij RWS

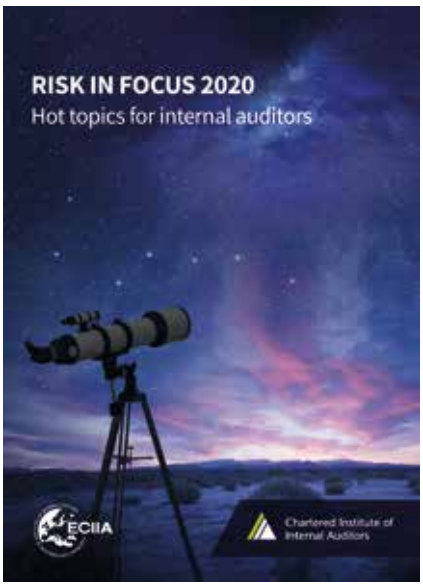
RWS heeft goede ervaringen opgedaan met een dergelijke wijze van onderzoek. De factoren uit het model van Van den Brink hebben de organisatie veel houvast geboden om gericht te sturen op het laten stromen van kennis. De visuals hebben bijgedragen aan het creëren van een open, positieve sfeer.

Het onderzoek is bij één doelgroep uitgevoerd. Om een tipje van de sluier op te lichten: voor deze doelgroep vormden de vele vormen van samenwerking tussen vakgenoten binnen en buiten RWS een belangrijke motiverende factor. De vele mogelijkheden om kennis vast te leggen in informatiesystemen hadden hen geholpen om kennis te delen. Naar aanleiding van het onderzoek zijn er verbeteracties geformuleerd. Door positieve insteek van het onderzoek waren mensen niet alleen enthousiast om deel te nemen aan het onderzoek, maar ook om de volgende stap te maken: het daadwerkelijk verbeteren van het delen van kennis. <<

Paul van den Brink is partner van het adviesbureau On The Brink Kennismanagement. Hij schreef een proefschrift over factoren die kennismanagement mogelijk maken.

Martine de Zeeuw werkt bij de Auditdienst Rijk. Zij paste het denkmodel van Van den Brink in de praktijk toe en zette deze om in visuals. Dit artikel is op persoonlijke titel geschreven en door De Zeeuw voorzien van illustraties.

Risk in Focus 2020: Hot topics voor internal auditors



In deze snel veranderende wereld heeft elke organisatie te maken met risico's, die ook weer veelvuldig veranderen. Internal audit jaarplannen zijn gebaseerd op inschattingen van deze risico's. Het is dus een uitdaging om de aandacht te blijven richten op de risico's die het belangrijkst zijn. Voor het vierde achtereenvolgende jaar hebben diverse Europese instituten van internal auditors, waaronder IIA Nederland, onderzocht wat de 'hot topics' zijn voor de auditplanning voor het komend jaar. Het rapport *Risk in Focus* geeft gerichte input om de specifieke risico's in de eigen organisatie te evalueren.

Op basis van surveys en interviews met chief audit executives van toonaangevende ondernemingen uit verschillende bedrijfstakken worden tien belangrijke topics besproken. Denk hierbij aan cybersecurity en gegevensbescherming, de disruptie van businessmodellen naar aanleiding van digitalisering, maar ook aan merkwaarde en reputatie en het aantrekken en inzetten van menselijk kapitaal. Daarbij spelen externe risico's als geopolitieke instabiliteit en klimaatverandering een steeds grotere rol.
https://bit.ly/RiskFo20

Winnaar Internal Audit Scriptie Award

Tijdens het jaarcongres van IIA Nederland is de Internal Audit Scriptie Award uitgereikt aan Lieke Franken-Pullen. Zij heeft met een experiment onder ruim tweehonderd auditors laten zien dat het oordeel van auditors daadwerkelijk beïnvloed wordt door gender. Winnares Franken-Pullen: "Er zijn twee effecten zichtbaar. Allereerst zie je dat auditors auditees van hetzelfde gender positiever beoordelen dan auditees van een ander gender. Ten tweede geldt dat je bij mannelijke auditors ziet dat ze vrouwelijke auditees negatiever beoordelen dan mannelijke auditees. Andersom zie je dit niet." De jury: "Deze scriptie heeft de hoogste score op onderwerpkeuze, originaliteit en wetenschappelijke onderbouwing."
http://bit.ly/IASAwi19

IIA feliciteert de geslaagden

Nieuwe RO's: Bram Bouwman, Jos Gelderblom, Peter de Guchteneire, Leon Hendriks, Simone Hoonakker, Wim Koorenneef, Ilse ter Linden, Charlotte van de Loo, Jack Mills, Marco Nieuwenhuis, Dick van Oort, Hay-Tie Tjiang, Daisy Vijgen, Marjolein van der Vlugt
Nieuwe CIA: Michal Trzebski
Nieuwe CRMA: Ksenia Kondratenko

E-learning standaarden met serious game SARA

Wat zijn de belangrijkste competenties van een internal auditor? Ontdek het terwijl je kennis op een unieke manier test met deze serious game. Maak kennis met SARA, een zeer speciale collega die een paar weken in je telefoon 'woont' en je dagelijks uitdaagt met situaties waarmee elke internal auditor geconfronteerd kan worden. Welke vaardigheden heeft een goede internal auditor en hoe breng je deze in praktijk? Ontdek alles wat je moet weten over de standaarden om het werk naar een hoger niveau te tillen. €100, 4 PE-punten.
http://bit.ly/iiaSARA

Uitgegeven certificaten Kwaliteitstoetsing

De internal auditafdelingen van de volgende organisaties ontvingen sinds de publicatie van het vorige *Audit Magazine* een Certificaat Kwaliteitstoetsing: Aegon Nederland, NWB Bank, Royal BAM Group, Schiphol Group, Triodos Bank.

NIEUWS VAN DE UNIVERSITEITEN

Internal Audit Scriptie Award 2019

Lieke Franken-Pullen heeft de Internal Audit Scriptie Award 2019 gewonnen met haar onderzoek *Gender bias bij auditors*. Zij onderzocht in hoeverre sprake is van gender bias bij auditors en hoe deze bias kan worden verklaard. Met een experiment onder ruim tweehonderd auditors toonde zij aan dat het oordeel van auditors daadwerkelijk beïnvloed wordt door gender. Het uiteindelijke doel is auditors bewust maken van het effect van gender bias op hun oordeel en daardoor gender bias te verminderen.

Franken-Pullen schreef haar referaat ter afsluiting van de post-masteropleiding Internal Auditing & Advisory aan Erasmus School of Accounting & Assurance. Ze heeft van de jury de hoogste score gekregen op onderwerpkeuze, originaliteit en wetenschappelijke onderbouwing. Het referaat is te downloaden op www.esaa.nl.

ESAA Erasmus School of Accounting & Assurance

Masterclass Digital Governance, vrijdag 6 december 2019

Veel directeuren en commissarissen worden met grote regelmaat geconfronteerd met digitale vraagstukken. Aanstaande december organiseren we rondom dit onderwerp een masterclass in samenwerking met prof. dr. Joe Peppard, MIT Sloan School of Management. Voor meer informatie en aanmelden verwijzen wij u naar de website.

Universiteit van Amsterdam

Amsterdam Business School

Ontwikkelingen in het vakgebied

Het vakgebied is de afgelopen jaren sterk in ontwikkeling met de opkomst van agile auditen, het toepassen van data & analytics in audit en het auditen van robotic process automation. Dankzij het sterke docentencorps met een mix van aansprekende thought leaders vanuit het bedrijfsleven en promovendi/hoogleraren, zijn wij in staat deze ontwikkelingen bij te houden. Onze focus ligt het komende jaar op twee punten: het vasthouden en verder vernieuwen van het huidige hoge niveau van de opleiding, met name op het gebied van ontwikkelingen zoals data science, soft controls, robotisering, agile auditen; en het behalen van de SVRO-accreditatie.

Opening academisch jaar

Op vrijdag 30 augustus 2019 opent de EMIA-opleiding het academisch jaar formeel met een lezing door Marco Rozenberg, vicepresident en chief audit officer bij Bookings Holdings. Hij gaat in op de ontwikkelingen in het vakgebied, deelt ervaringen bij Booking.com en reflecteert op de toekomst van de internal auditor. Aansluitend is er een borrel.

Algemene informatie

De EMIA-opleiding is een parttime programma voor ambitieuze internal auditors aan de Universiteit van Amsterdam. Tevens is het de enige internal auditopleiding (wereldwijd) waarbij je de MS-titel kunt verkrijgen bij het succesvol afronden van de opleiding. 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 één jaar RO te worden.

Column
Tekst Drs. Laszlo Nagy EMIA RO

De interne **algoritme-** functie in 2025

Eerder stond ik stil bij de ontwikkelingen van 'online' en de toegevoegde waarde van de auditor. Waar je ook komt, het lijkt wel of tegenwoordig alles een IT-sausje heeft. Alles wordt geautomatiseerd of 'geappificeerd'. Print verdwijnt in rap tempo. Brieven schrijven we allang niet meer, maar ook communiceren met de overheid doen we steeds vaker elektronisch. Afkortingen als RPA en AI zijn al behoorlijk ingeburgerd. En welke IAF heeft nog niet met data-analyse kennisgemaakt? Die biedt interessante kansen om het ouderwetse handwerk over te laten aan systemen en sneller en met grotere onderzoekspopulaties te werken. Kortom, voor auditors is IT een onontbeerlijk terrein.

Maar wat als IT niet helemaal je ding is? Als je denkt in de driehoek mensen, systemen, processen? Gelukkig hebben we dan nog Mensen. En dan specifiek het gedrag, de wereld van de soft controls. Daar heeft IT nog geen vat op. Of toch wel? Ook gedrag is een gebied waar het inmiddels – en steeds meer – wemelt van systemen. Systemen die gedrag analyseren, verklaren en voorspellen. Algoritmen voorspellen inmiddels een heleboel zaken sneller, maar ook nauwkeuriger dan de mens, zelfs deskundigen. De schaakcomputer die wint van de professionele schaker kennen we al. Algoritmen bepalen wat de passende baan is voor je, wat de passende kandidaat is voor de vacature maar ook welke partner het best past bij je. Ofwel, gedrag wordt steeds meer en beter voorspelbaar. Uiteindelijk zonder tussenkomst van een mens. En daar maken de nodige organisaties al flink gebruik van. Ze willen jou als consument, maar ook als mogelijke kandidaat of opdrachtgever, goed voorspellen én goed beïnvloeden zodat je doet wat ze willen. In een sollicitatieproces bepaalt al snel de computer en niet de recruiter of je überhaupt aan tafel komt. Ongetwijfeld efficiënt, maar is het ook integer? Zoals *Trouw* medio juni al kopte: 'Algoritmes zijn een vierde macht, waarvoor geen regels gelden'.

Wat is de rol van de internal auditor binnen deze ontwikkelingen? Dit laat zich lastig voorspellen. Mijn verwachting is dat het veel te maken zal hebben met de effectieve, maar ook integere inzet van algoritmen voor het voorspellen van processen en het gedrag van mensen. Zowel de mens als consument en klant, maar ook die als burger en werknemer. De interne auditor kan bestuurders dan ondersteunen bij de vraag of de steeds verder toegepaste algoritmen effectief en ook integer worden gebruikt. Hoe is de betrouwbaarheid van de gebruikte data gewaarborgd? Hoe is de integriteit van de toepassing gewaarborgd? Waarbij integer verder reikt dan compliance met de huidige en toekomstige wetten en regels. Integer reikt ook tot een gebruik dat maatschappelijk verantwoord en verantwoordbaar is en niet bedreigend is voor de reputatie van de organisatie. En daarmee kom je van het meer technische onderwerp van algoritmen weer terug bij het gedrag en het toezicht daarop: algoritmen ontstaan namelijk niet vanzelf, maar worden door mensen bedacht die er opdracht toe hebben gekregen. Inhoudelijk deskundigen en specialisten om precies te zijn. Het is interessant om te onderzoeken hoe zij werken en denken, met welke regels, kaders en doelen, hoe ze die interpreteren en toepassen en hoe het toezicht daarop is. En hoe biased ontwikkelaars en daarmee ook algoritmen wellicht zijn.

Een ding is zeker: met algoritmen kun je inmiddels meer voorspellen dan in de huidige maatschappij wenselijk is. Wellicht denken we daar in 2025 een stuk makkelijker over. Of hechten we tegen die tijd juist veel meer waarde aan onze privacy en vinden we het dan fijn niet al te voorspelbaar te zijn?

Laszlo Nagy adviseert en ondersteunt organisaties op het gebied van beheersen en verbeteren. Hij is director Business Risk Services bij adviesbureau Improven en voormalig hoofdredacteur van *Audit Magazine.*

EY
Building a better working world

The shift from reactive to proactive software compliance risk management starts now, not tomorrow

Many clients seek our help, reacting to vendor audits. Often, they already have a settlement claim from the vendor. We can still help them significantly reduce the financial claim. But, our advice is be proactive, invest today so you can save more tomorrow.

Contact us at: **ey.nl/sam**

Marco Boer
marco.boer@nl.ey.com
+31 6 21 25 14 01

Adil Modak
adil.modak@nl.ey.com
+31 6 29 08 46 51

Hoe kan internal audit het verschil maken, nu en in 2025?

In de huidige wereld is het voor een IAF bijna niet meer mogelijk om op alle inhoudelijke terreinen over voldoende kennis en ervaring te beschikken. Cognitieve technologieën zoals machine learning en artificial intelligence worden rap geïntroduceerd binnen organisaties. Cultuur en soft controls worden steeds belangrijker voor bestuurders en audit commissies.

Dit vraagt om een flexibele schil rondom uw IAF. Voor de nodige flexibiliteit, maar ook toegang tot actuele kennis op het gebied van cyberrisico's, soft controls, contract compliance, data & analytics tot dynamic risk assessments. Als een van de markleiders voor co-sourcing helpt KPMG uw IAF verder. Zo blijft de internal auditor waarde toevoegen voor de organisatie. Nu en in de toekomst.

Meer weten?

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

KPMG