AUDIT MAGAZINE

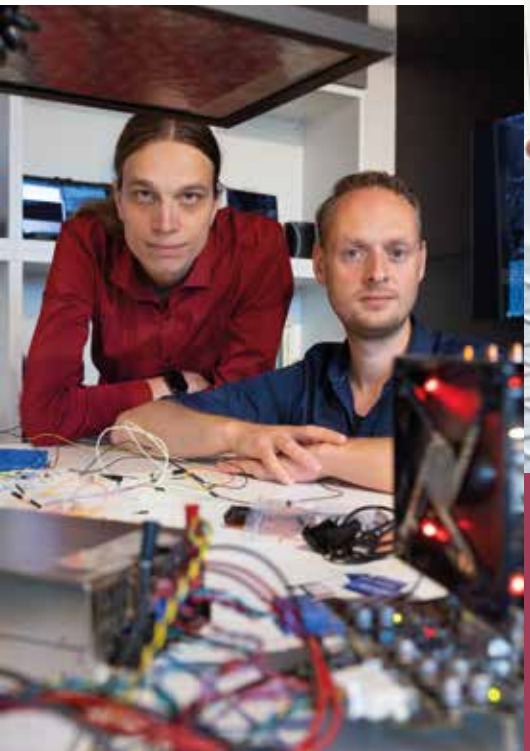
VAKBLAD VOOR DE INTERNAL AUDITOR

2022 JAARGANG 21

Agile auditing @ Jumbo: **a good practice**

“**Wijzig** in *hemelsnaam* je wachtwoord **niet**”

Waarheidsvinders: **DOELGERICHT** en met open vizier



Ketenrisicobeheersing moet **volwassen discipline** worden

It is something that only happens to other companies...

Until it happens to yours.

Is your company ready for a cyber attack?

Connect with us via
+31.20.346.0400 or
cybersecurity@protiviti.nl

protiviti.nl

protiviti®
Global Business Consulting

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
Nick Bartman CIA CISA
Femke Dik MSc
Sander Diks CIA
Liane Lambert Mendez-van Eerde MSc RO
Drs. Nicole Engel-de Groot RA
Drs. Margot Hovestad RO
Bas de Jong MSc RA
Max Lodder CISA
Sierd Stapersma RO EMITA
Drs. Marc van der Veen RA RO CIA RMFI
Fong-Chi Wai MSc RO
Raymond Wondergem MSc RO
E-mail

Instituut van Internal Auditors Nederland

auditmagazine@iia.nl
IIA Nederland
Burgemeester Stramanweg 105F, 1101 AA Amsterdam
tel.: 088-0037100
iia@iia.nl, www.iia.nl

SVRO Stichting Verenigde Register Operational Auditors

Burgemeester Stramanweg 105F, 1101 AA Amsterdam
svro@iia.nl, www.iia.nl

Eindredactie
Ria Harmelink Journalistieke Producties

Uitgever
Verloop uitgeverij
Arjan Verloop
info@verloop.nl
tel.: 078-6912899

Vormgeving
ViaMare grafisch ontwerp, Marijke Maarleveld

Druk
Verloop drukkerij, Alblasserdam

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. Leden woonachtig in het buitenland en niet-leden verwijzen wij naar ons online magazine op www.auditmagazine.nl.

Audit Magazine verschijnt 1 maal per jaar.

ISSN: 1570-856X

We zijn **online!**

Vorig jaar was het dan eindelijk zover. Na een lange periode van voorbereiding ging *Audit Magazine* in maart 2021 online (auditmagazine.nl). Sindsdien publiceerden we meer dan vierhonderd pagina's aan artikelen, interviews, rubrieken en columns op ons online platform. En dat los van de jaargangen 2016-2020, die we met terugwerkende kracht online hebben gezet. Dit alles om ervoor te zorgen dat auditmagazine.nl snel kon verworden tot waar het voor bedoeld is: dé kenniswaterplaats voor internal auditors in Nederland. We zijn dan ook blij dat we de bezoekersaantallen sinds de lancering van auditmagazine.nl hard zien groeien!

Ondanks de vele extra mogelijkheden die online biedt begrijpen we het nostalgische gevoel dat sommige lezers hebben wanneer ze terugdenken aan het fysieke blad. Dat hebben we zelf namelijk ook! Daarom valt *Audit Magazine* voortaan rond iedere kerst – in extra dikke vorm – bij u op de mat. In deze jaarlijkse uitgave vindt u een greep van de dat jaar online veelgelezen (en veelgeprezen) bijdragen.

In het nummer dat voor u ligt vindt u dan ook de pareltjes van het afgelopen jaar. Zo zetten zowel Thijs Smit als Bob van Kuijck voor u uiteen hoe lang een chief audit executive ongeveer meekan. Ook voelen we de waarheidsvinders Nicole den Hartigh en Xavier Zielinga stevig aan de tand over liegen en bedriegen. En natuurlijk ontbreekt de online meest gelezen bijdrage van het afgelopen jaar, Agile auditing @ Jumbo, in dit nummer niet. Een bijdrage die u (nog) niet online zag verschijnen is het interview met securityspecialisten Daan Keuper en Thijs Alkemade. Zij gaan in op de gevaren die organisaties op digitaal gebied lopen en beantwoorden bovendien de vraag waarom je je wachtwoord juist *niet* moet wijzigen.

Ook komend jaar mag u weer het nodige van *Audit Magazine* verwachten. Vanzelfsprekend vindt u op auditmagazine.nl regelmatig tal van interessante bijdragen over relevante thema's voor internal auditors, zoals ESG en human capital. Daarnaast gaan we ook de jaargangen 2014 en 2015 op ons online platform publiceren. En last but not least, vanaf volgend jaar kunt u luisteren naar podcasts op auditmagazine.nl!

De redactie wenst u veel leesplezier en ziet u graag volgend jaar online weer terug!

Björn Walrave
Hoofdredacteur *Audit Magazine*

“Een wachtwoord wijzigen dat nooit gelekt is? Niet nodig!”

Hoe veilig zijn onze data en systemen eigenlijk? Securityspecialisten Thijs Alkemade en Daan Keuper (Computest) onderzoeken met de researchafdeling producten en zaken die maatschappelijk relevant zijn. Over actieve handel in inloggegevens, phisingsimulaties en de onzin van een wachtwoordpolicy. **Pag. 6**

Auditen vanuit de bedoeling

De toeslagenaffaire is een bekend voorbeeld waarbij de bedoeling uit het zicht is geraakt. Als auditors leren we om te starten bij de opzet, dan volgt het bestaan en tot slot de werking. Met het risico te blijven hangen bij de papieren wereld. **Pag. 12**

Blik op 2023

Voorzitter van IIA Nederland Linda Post blikt vooruit op welke speerpunten – gebaseerd op de IIA-missie dat internal auditors wereldwijd erkend worden als een essentiële schakel – van belang zijn het komende jaar. **Pag. 17**

“Ik geloof heilig in een houdbaarheidsdatum voor de CAE”

Dat zegt Thijs Smit, auditconsultant en voorzitter van Kwaliteitstoetsingen IIA Nederland. “Ik vind dat de roulatie van de CAE opgenomen zou moeten worden in de Corporate Governance Code.” **Pag. 18**

Vervang de chief audit executive tijdig

Het functioneren van de CAE is geen constante factor en in een dynamische omgeving kunnen ook de verwachtingen ten aanzien van de rol wijzigen. Dit artikel gaat in op de bedreigingen voor het goed functioneren van de CAE en op zijn houdbaarheid. **Pag. 22**

Is angst voor cultuuraudits terecht?

Organisatiecultuur is een breed omvattend begrip dat geen begin of eind kent, zoals een inkoopproces. Dat kan voor angst zorgen, omdat deze veranderingen niet zo makkelijk te koppelen zijn aan concrete processtappen. Wat betekent dat voor de auditor? **Pag. 27**

Audit van integriteitscultuur bij fusies en overnames

Fusies en overnames pakken niet altijd goed uit. Internal audit kan bijdragen aan de kans dat fusies en overnames slagen door de integriteitscultuur van targets te onderzoeken, gericht op het verder ontwikkelen van de onderneming ná de transactie. **Pag. 30**

“Zoek elkaar op en deel je uitdagingen”

Jan Rodenburg, hoofd Interne Audit bij Saxo Bank MER, aan het woord over het werken met een kleine auditdienst, ondernemen, bouwen, ontwikkelen en meeademen met de organisatie. **Pag. 34**

Auditen met meer toegevoegde waarde door effectieve communicatie

Vaak passen internal auditors dezelfde vorm toe voor het presenteren van de auditresultaten: het stellen van normen en uitsluitend de tekortkomingen ten opzichte hiervan melden. Maar de acceptatie van de auditresultaten neemt toe als er in de communicatie rekening wordt gehouden met de persoonlijkheidsvoorkeuren van de ontvanger. **Pag. 38**

Waarheidsvinders: doelgericht en met open vizier

Nicole den Hartig en Xavier Zeilinga (denhartigh & partners) over liegen en bedriegen, desinformatie, profilingtechnieken, deepfake en de kunst van het waarheidsvinden. **Pag. 42**

Wat is inzicht en wat moet je ermee?

Het IIA wil de internal auditor ontwikkelen tot de trusted advisor van het management om zo bij te dragen aan het inzicht binnen de organisatie. Maar wat is precies de rol en de bijdrage van de internal auditor met betrekking tot inzicht? **Pag. 48**

De auditor als antropoloog

De Algemene Rekenkamer voerde een oorzaakanalyse, gericht op gedrag, uit naar een hardnekkig probleem: het gebrekkige munitiebeheer van het ministerie van Defensie. De gehanteerde methode is echter geen typische auditmethode: er is geobserveerd zonder normenkader. **Pag. 54**

Ketenrisicobeheersing moet volwassen discipline worden

Steeds meer organisaties zijn voor hun functioneren in grote mate afhankelijk van derde partijen, waardoor ze kwetsbaarder zijn voor verstoringen of informatiebeveiligingsincidenten. Ketenrisicobeheersing wordt dan ook steeds belangrijker voor de continuïteit en kwaliteit van de organisatie. **Pag. 58**

Meer effect met data-analyse

De snelle ontwikkeling van DDA roept vragen op: hoe volwassen zijn we als internal auditors in het toepassen van DDA? Hoe hoog leggen we de lat? En, hoe komen we daar? Het DDA-volwassenheidsmodel biedt houvast. **Pag. 62**

Agile auditing @ Jumbo: a good practice

Van rapport in de la naar acties op de vloer: hoe Jumbo internal audit het agile-gedachtegoed implementeerde in haar werkwijze. Van log en weinig draagvlak naar wendbaar met een brede acceptatie met behulp van een kwartaalplanproces en een kernteam. **Pag. 66**

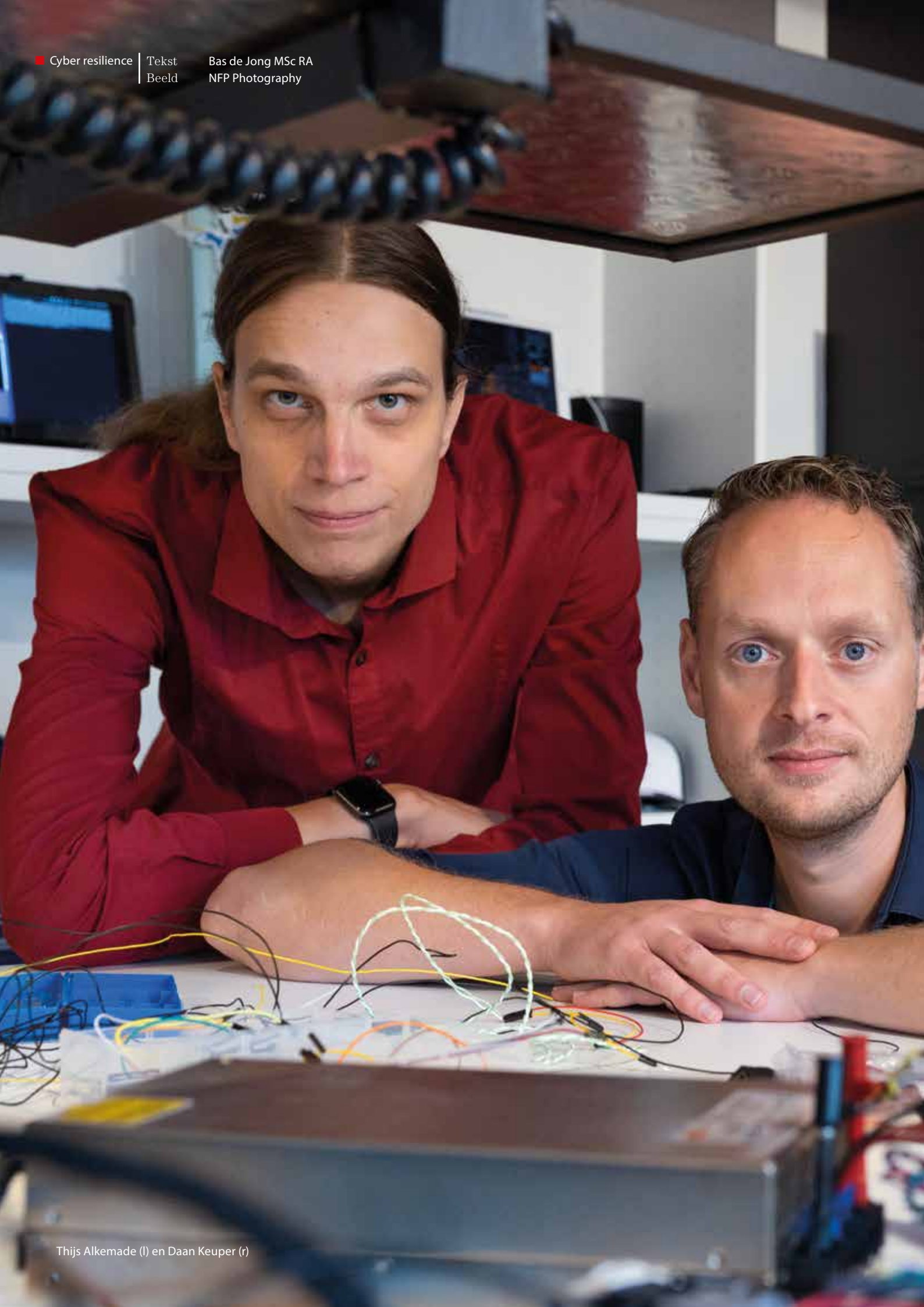
De trusted advisor: verdiept inzicht door rust en focus

Een verkenning naar de rol van de trusted advisor. Van het begrip counsel, het gedachtegoed van Maister, randvoorwaardelijke factoren voor de audifunctie tot socratische gespreksvoering. **Pag. 70**

Enkelvoud

Klinisch psycholoog Michael Tophoff over wat inclusiviteit problematisch maakt. **Pag. 74**

Tekst Bas de Jong MSc RA
Beeld NFP Photography



Thijs Alkemade (l) en Daan Keuper (r)

“Een **wachtwoord** wijzigen dat nooit ***gelekt*** is? **Niet nodig!”**

Hoe veilig zijn onze data en systemen eigenlijk? Prijswinnende hackers Thijs Alkemade en Daan Keuper van Computest geven het antwoord.

Wat doet Computest eigenlijk?

Daan Keuper (DK): “Computest heeft meerdere disciplines, maar vanuit Computest Security helpen wij klanten van begin tot eind. Wij hebben een preventieve cybersecurityafdeling waar wij kwetsbaarheden en risico’s beoordelen en trainingen verzorgen. Verder hebben wij een detectieafdeling waar wij de systemen van klanten kunnen monitoren om te beoordelen of er verdachte activiteiten zijn, en een incident-responseafdeling die komt invliegen als het toch een keer misgaat, bijvoorbeeld bij een ransomware-incident. Tot slot hebben we een governancetak waarbij we het beleidsmatige stuk als service aanbieden.”

En Sector 7?

DK: “Sector 7 is onze researchafdeling. Met Sector 7 werken wij niet voor klanten. Wij hebben ook geen winstoogmerk, maar doen securityonderzoek naar zaken die wij maatschappelijk relevant achten. Dat is ooit begonnen met auto’s, waarbij wij kwetsbaarheden vonden in de auto’s uit de Volkswagengroep. Wij hadden een visie op security van IoT-items (Internet of Things, apparaten die verbonden zijn met internet – red.) en hebben onderzoek gepubliceerd over een van de meest voorkomende apparaten waar wij op dat moment aan konden komen, een auto uit de Volkswagengroep dus. Door dit onderzoek werd er naar ons geluisterd. Sindsdien pakken wij producten en zaken op die maatschappelijk relevant zijn.”

Hoe komen jullie aan jullie expertise?

Thijs Alkemade (TA): “Ik heb wiskunde en informatica gestudeerd en had veel interesse in het ontwerpen van programmeertaal tijdens mijn studie. Na mijn studie ben ik de security ingerold.”

DK: “Ik ben hier eigenlijk altijd al mee bezig geweest. Op jonge leeftijd wist ik al dat ik de IT in wilde, ik ben ook jong begonnen met security. Ik was vrij slecht in gamen en wilde liever weten hoe het werkte, daarna wilde ik weten hoe je het ‘kapot’ kon maken. Ik heb een master IT-security gedaan, maar daar leer je meer de theoretische kant en het echt praktische, dat komt pas na de studie. Ik ging als PEN-tester (penetratietester – red.) aan de slag en via wat omwegen ben ik uiteindelijk hier terechtgekomen.”

Nooit ergens voor vastgezeten? Ik vraag het maar even

DK: “Ha, nee zeker niet. Je hebt in deze sector een Verklaring Omtrent Gedrag (VOG) nodig en een strafblad kan je dan goed in de weg staan.”

Over

Daan Keuper is hoofd van de securityresearchafdeling van Computest. Deze afdeling is verantwoordelijk voor diepgaande security research op veelgebruikte systemen en IT-omgevingen.

Thijs Alkemade studeerde wiskunde en informatica. Hij werkt op de securityresearchafdeling van Computest. Alkemade won twee keer de Pwn2Own-competitie, onder meer door kwetsbaarheden in Zoom aan te tonen.

Wat hebben jullie recentelijk bekeken?

DK: “Vorig jaar hebben wij gekeken naar de beveiliging van Zoom, wat natuurlijk ineens door de pandemie op grote schaal werd gebruikt. Maar we hebben ook naar de CoronaCheck-app gekeken en de examenmonitoringssoftware die studenten verplicht moesten installeren om thuis examens te kunnen maken. Dit jaar hebben we ons gericht op industriesoftware, zoals software die wordt gebruikt in fabriekshallen, kerncentrales en sluizen. Daar speelt een grote IT-securitybehoefte. Deze operationele technologie (OT) is heel anders dan een standaard IT-landschap.”

Doen jullie onderzoek op aanvraag of op eigen initiatief?

DK: “Dat kan allebei, maar vooral op eigen initiatief. We kijken naar wat er speelt in de markt of de samenleving en wat we leuk vinden om te onderzoeken. Maar het kan ook op verzoek en dat verzoek komt dan vaak van een van de afdelingen van Computest. Het zou bijvoorbeeld kunnen dat het incident-responseteam nieuwe malware tegenkomt of een van de andere teams heeft een klant die met nieuwe technologie werkt waar weinig over bekend is. Dat zijn zaken waar wij op aanvraag onderzoek naar kunnen doen.”

Wat levert jullie onderzoek op?

DK: “Het doel is dat we kwetsbaarheden die wij zien rapporteren, zodat deze dichtgezet kunnen worden voordat de buitenwereld daar lucht van krijgt. Maar wij publiceren ook technische details van kwetsbaarheden – nadat deze zijn verholpen – zodat andere securityonderzoekers daarvan kunnen leren en eventueel op kunnen voortbouwen. We proberen de wereld een stukje veiliger te maken.”

Met alles wat jullie zien, waar verbaas je je het meest over?

TA: “Soms vraag je je af hoe dingen in elkaar zitten en waarom dat zo is. En als je dan goed kijkt, blijkt het niet zo robuust te zijn ontworpen als je eigenlijk zou verwachten.”

DK: “Soms ziet iets er op het eerste gezicht heel complex uit, maar blijkt het niet zo moeilijk als ik op voorhand had verwacht. Software blijft uiteindelijk mensenwerk. Mensen programmeren en mensen maken fouten.”

Jullie hebben prijzen gewonnen

TA: “We hebben twee keer meegedaan aan de internationale competitie Pwn2Own. Dat is een hackwedstrijd waarbij van tevoren een aantal targets bekend wordt gemaakt. Vorig jaar was dat bijvoorbeeld Zoom. We hebben die wedstrijd beide keren gewonnen.”

DK: “Je moet dan binnenkomen in de applicatie via tot dan toe onbekende kwetsbaarheden en vervolgens het systeem volledig overnemen. We zijn ontzettend blij dat we die wedstrijd nu twee keer achter elkaar hebben gewonnen.”

Waren ze bij Zoom ook blij?

DK: “Jazeker, de kwetsbaarheid die in de software zat, zat er sowieso in. Wij hebben die aangetoond, zodat ze in staat zijn die te verhelpen.

Daan Keuper: "Soms ziet iets er op het eerste gezicht heel complex uit, maar blijkt het niet zo moeilijk als ik op voorhand had verwacht. Software blijft uiteindelijk mensenwerk. Mensen programmeren en mensen maken fouten"

TA: "Die kwetsbaarheid is daarna ook snel opgelost. Het idee van die competitie is dat je na het vinden van het probleem in contact komt met de organisatie om details uit te wisselen, zodat ze het kunnen herstellen. Pas nadat het opgelost is mogen wij erover praten."

Onlangs waren jullie in Las Vegas. Wat hebben jullie daar gedaan?

TA: "Ik heb in augustus 2022 een presentatie gegeven op het hackerscongres Def Con in Las Vegas over kwetsbaarheden in macOS. Dat was een grote vondst met best verstrekkende gevolgen. Het heeft geleid tot een wereldwijde update van de systeemsoftware van Macs en aanpassingen in applicaties die op macOS draaien."

Als je dan toch gehackt wordt, wat dan?

DK: "Een responseteam komt naar je toe om je te ondersteunen. Zij onderzoeken wat er precies is gebeurd, hoe ze zijn binnengekomen en welke systemen er precies zijn geraakt. Ze proberen een totaalbeeld te krijgen van het incident en de impact daarvan. Vervolgens wordt er gekeken naar de herstelopties, omdat de klant zo snel mogelijk terug wil naar een normale situatie, of in ieder geval naar een situatie dat de meest kritieke systemen weer operationeel zijn. Wij onderzoeken hoe de aanvallers zijn binnengekomen, wat er is gestolen en wat je herstelopties zijn.

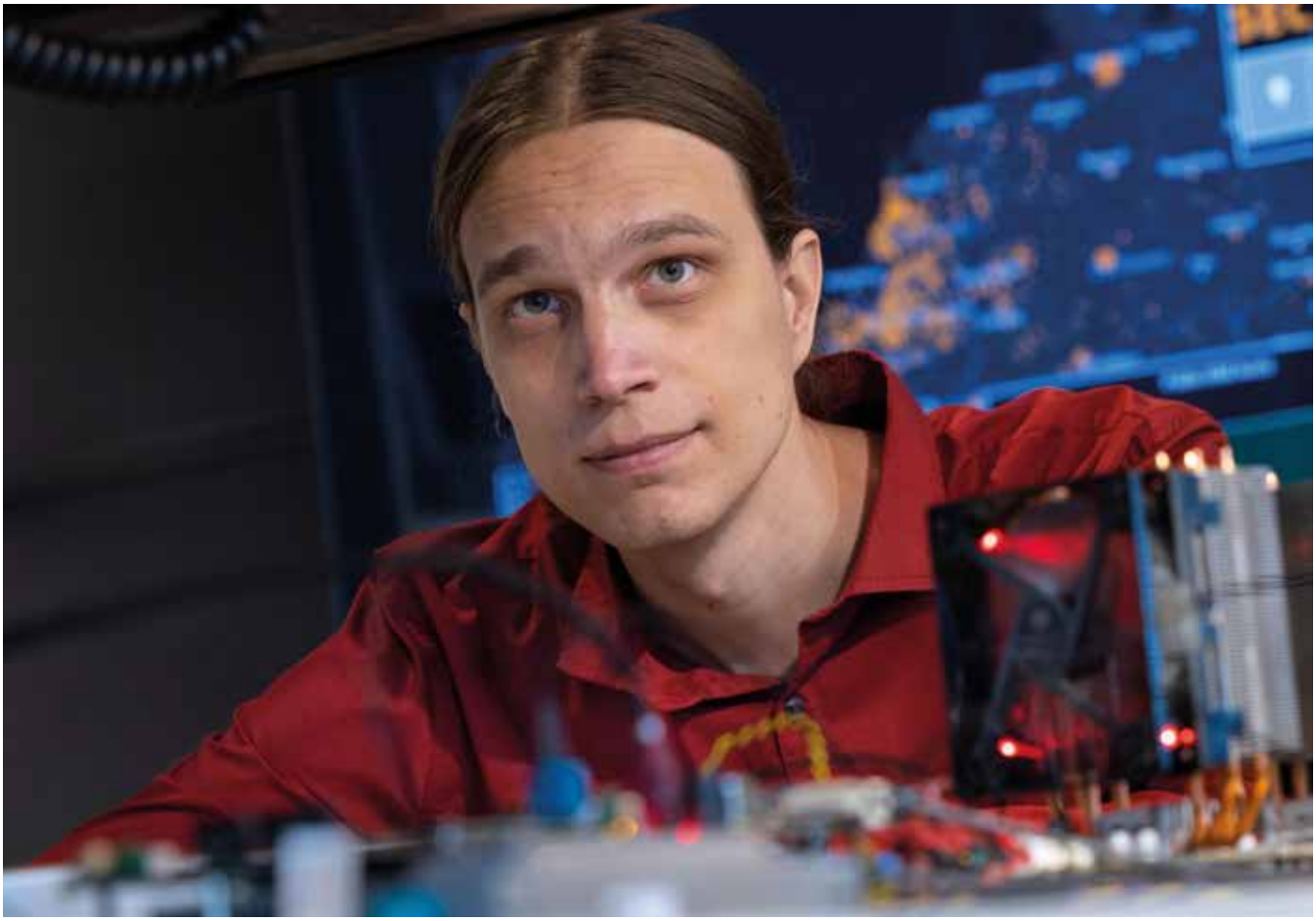
Back-up herstellen en weer door?

DK: "Het herstellen van back-ups is een mogelijke oplossing als je niet bij je data kunt (mits de back-up niet ook versleuteld is door de hacker), maar niet als je data gestolen is. Ook kan het een probleem zijn als de back-up verouderd is of niet snel genoeg te herstellen valt."

TA: "Als je nooit getest hebt je hele netwerk te herstellen vanaf een back-up kan het best dat dit twee weken duurt of helemaal niet lukt. Dan is je back-up dus niets waard."

Hoe ga je om met gestolen of geblokkeerde data?

DK: "Wij nemen contact op met de criminelen en openen het contact voor onderhandelingen over het losgeld. Maar er moet van alles geregeld worden op zo'n moment. De medewerkers moeten worden ingelicht, de belangrijkste partners moeten op de hoogte worden gesteld en mogelijk moeten getroffen personen worden geïnformeerd of gemeld worden bij de Autoriteit Perspoonsgegevens. Er komt heel wat op je af, mensen verkijken zich vaak op hoeveel impact zoiets heeft op je bedrijfsvoering en op je medewerkers."



Onderhandelen met criminelen?

DK: “Het hele businessmodel van de hacker is erop gericht dat jij betaalt en dat jouw problemen daarna zijn opgelost. Als dat niet zo is, dan betaalt niemand meer. Dus hoe gek het ook klinkt, zij zijn erbij gebaat dat hun ‘klant’ enigszins tevreden blijft. Maar ze zitten er wel voor het geld. Men heeft dus geen zin in ellenlange onderhandelingen. Ze draaien op snelheid en volume. Niet betalen is ook prima, maar dan ben jij alles kwijt en gaan zij door naar de volgende.”

Kan je iets zeggen over de oorzaak van hacks?

DK: “Vaak zijn het updates die niet worden gedraaid, of wachtwoorden die worden hergebruikt of phising. Mensen hebben de neiging wachtwoorden op meer dan een plek te gebruiken en als een van die plekken gehackt wordt ligt je wachtwoord dus op straat. Je moet een wachtwoord zien als een geheim tussen jou en de partij aan wie je dat wachtwoord geeft. Met hoe meer partijen je dat deelt, hoe groter het risico dat het geheim een keer verklapt wordt.”

En het beheer van rechten binnen de organisatie zelf?

DK: “Wij testen veel op toegangsrechten in interne netwerken. Los van dat gebruikers soms te veel rechten krijgen, zijn er veel trucjes om van lage rechten naar volledige rechten te gaan. Dat lukt tot nu toe eigenlijk altijd wel. De partij die die initiële rechten heeft, is vaak een andere partij dan de uiteindelijke aanvaller die de ransomware installeert. De eerste groep noemen we de Initial Access Broker en het enige wat zij doen, is bij bedrijven binnenkomen. Zij verkopen die toegang vervolgens op allerlei online forums, gesorteerd per sector, grootte van bedrijf en jaaromzet. Groeperingen die die toegang kopen proberen vervolgens de rechten om te zetten naar een systeembeheeraccount, zodat ze data naar buiten kunnen kopiëren, virusscanners kunnen uitzetten en ransomeware in het hele netwerk kunnen plaatsen. Vaak onderzoeken ze die data ook en weten ze bijvoorbeeld of je een cybersecurityverzekering hebt en tot welk bedrag je verzekerd bent. Hackers zijn soms een paar maanden binnen voordat ze toeslaan.”

Is het een balans tussen gemak en beveiliging?

DK: “Bij security is het een beetje een ongelijke race, omdat de verdediging alles goed geregeld moet hebben terwijl de aanvaller maar één manier hoeft te vinden. Maar je kunt het ook omdraaien. Als die aanvaller eenmaal binnen is, zijn er veel manieren om de aanvaller te detecteren. Dan hoeft de aanvaller maar één keer verkeerd te klikken en dan weet je dat hij er zit. En dan kun je er wat mee. Maar de meeste klanten investeren wel in de preventieve kant, maar niet of nauwelijks in het detecteren van aanvallen. Partijen kunnen veel winnen door meer te investeren in detectie.”

Zit het ook voor een deel in het bewustzijn van mensen?

DK: “Ik vind zelf dat we de schuld niet bij de gebruikers moeten leggen, maar dat we technische oplossingen moeten ontwerpen waarmee we de gebruiker van minder groot belang kunnen maken. Gedrag zou er idealiter niet toe moeten doen. Als je nu veilig wilt werken vraag je heel veel van je medewerkers. Zij moeten allerlei dingen nalaten of juist wel doen om op een veilige manier te kunnen werken. In de praktijk werkt dat niet. Een gebruiker wil gewoon zijn werk doen en wil helemaal niet bezig zijn met security. Dat is

Thijs Alkemade: "Er is een zeer actieve handel in inloggegevens. Dat maakt het risico van het hergebruiken van wachtwoorden of het gebruiken van dezelfde wachtwoorden bij verschillende accounts erg groot"

ook niet zijn expertise. Ik zie veel bedrijven die investeren in phisingsimulaties, maar als ik kijk naar de incidenten die we zien dan zijn moderne phising mails niet van echt te onderscheiden. We moeten naar een wereld toe waarin IT-security het echte werk niet in de weg staat."

Zeg je dat awareness niet belangrijk is?

DK: "In bepaalde mate niet nee. Je hebt wel iets van awareness nodig, maar ik zou liever zien dat we naar technische maatregelen gaan die ervoor zorgen dat we minder van gebruikers vragen. Of, wanneer een gebruiker toch op een phising mail klikt, het effect hiervan beperkt is tot alleen die gebruiker en zijn systeem. Eén groot securityincident is niet hetzelfde als twintig kleintjes die in een half uur per keer zijn opgelost. Daar moeten we naartoe. Als je ervan uitgaat dat je je bedrijf kunt beschermen door ervoor te zorgen dat gebruikers niet op linkjes klikken, dan kom je van een koude kermis thuis. Een awarenesstraining is een relatief goedkope oplossing, maar biedt misschien meer schijnzekerheid dan echte security."

En de combinatie van techniek en gedrag?

DK: "Ja, als we het hebben over awareness hebben we eigenlijk al een beetje verloren. Het zit in meer dan alleen het gedrag van mensen. De techniek kan ervoor zorgen dat dingen simpelweg niet mogelijk zijn, het gedrag moet ervoor zorgen dat die techniek goed wordt toegepast. En gedrag raakt aan cultuur, dat is moeilijk snel te veranderen, maar in sommige gevallen heel relevant. Als je gedragsverandering wilt, moet je dat vanaf het bestuur/de directie uitrollen en afdwingen. Maar ja, hoeveel board members ken jij die fanatiek met een wachtwoordmanager aan de slag gaan? Daar zit een uitdaging."

Welke ontwikkelingen zien jullie op dit moment?

DK: "We zien dat via sociale platformen mensen worden benaderd om een deel van hun zakelijke accountgegevens te verkopen. Maar ook dat inloggegevens actief worden verhandeld."

TA: "Er is een zeer actieve handel in inloggegevens. Dat maakt het risico van het hergebruiken van wachtwoorden of het gebruiken van dezelfde wachtwoorden bij verschillende accounts erg groot."

DK: "We zien ook een trend dat multifactor authenticatie wordt gecombineerd met phising mails of notificaties via apps. Aanvallers loggen honderd keer in en er is altijd wel een gebruiker die op de mail klikt ter bevestiging. Dan zijn ze ook binnen. Dus multifactor is absoluut goed voor de beveiliging, maar het is niet zo dat je daardoor 100% veilig bent."

Geldt dit alleen voor zakelijke gebruikers of ook voor particulieren?

DK: "Voor particulieren geldt dat ze hun IT eigenlijk volledig hebben uitbesteed en niet in eigen beheer hebben. Wat je als particulier moet doen is 1) installeer updates tijdig; 2) gebruik een wachtwoordmanager; 3) zet multifactor authentication aan waar mogelijk. En met betrekking tot detectie: schaf een virusscanner aan."

Is een wachtwoordmanager niet een groot risico?

DK: "Als een hacker daar toegang toe krijgt ligt alles op straat. Maar als je een wachtwoordmanager hebt die wachtwoorden alleen op je computer opslaat, dan kan het goed werken. Heeft een aanvaller toegang tot die computer, dan is het sowieso al game over, los van de wachtwoordmanager. Een wachtwoordmanager gebruiken is beter dan hetzelfde wachtwoord hanteren bij verschillende accounts, want je kunt niet honderd verschillende wachtwoorden onthouden. De kans dat een webshop waar jij je gegevens hebt achtergelaten wordt gehackt, is groter dan een wachtwoordmanager die zijn businessmodel hiervan heeft gemaakt."

Nog tips voor bedrijven?

TA: "Eerste tip: zoek naar technische maatregelen om de impact van aanvallen te beperken en zorg dat je minder afhankelijk bent van gedrag. Een tweede tip is dat je een incident oefent. Als het gebeurt is namelijk iedereen in rep en roer en komt er veel op je af. En als derde: maak een business continuity plan en vergeet daarbij je leveranciers niet."

TA: "Ik wil bij de technische maatregelen toevoegen dat je rekening houdt met hoe je mensen werken en dat het werkzaam blijft. Je wilt security die voor mensen werkt en niet tegen ze. Als bijvoorbeeld attachments standaard worden verwijderd gaat men actief op zoek naar manieren om dat te omzeilen."

Nog meer wat je juist niet moet doen?

DK: "Ik ben geen fan van phisingsimulaties. Wat mij betreft heb je dan sowieso al verloren. En een wachtwoordpolicy dat een minimumlengte, hoofdletter, speciaal teken en iedere-dertig-dagen-wijzigenregels oplegt: stop daarmee."

TA: "Ja, wij zien dan dat het vorige keer op 03 eindigden dus laten we nu eens 04 proberen. Het maakt wachtwoorden onveiliger, omdat het niet past in de praktijk van de gebruiker. Waarom zou je een wachtwoord dat nooit gelekt is moeten wijzigen?"

DK: "Gebruik desnoods een wachtwoordmanager of neem een zin in plaats van een woord, maar laat de vrijheid bij de gebruiker en zet het niet vast in een beleid." <<

Tekst Gerben Korevaar MSc RO
Drs. Roos Kalker RO
Illustraties Roos Kalker
Beeld Belinda Fewings

Auditen *vanuit de* BEDOELING

Als auditors leren we om te starten bij de opzet, dan volgt het bestaan en tot slot de werking. Vaak is dit geschikt, maar we lopen wel het risico om te blijven hangen bij de papieren wereld. Met auditen vanuit de bedoeling draaien we dit om.

De toeslagenaffaire is een bekend voorbeeld waarbij de bedoeling uit het zicht was geraakt. Bij de toeslagenaffaire zijn naar schatting 26.000 ouders en 70.000 kinderen in de problemen geraakt. Ouders raakten in de schulden, sommigen verloren hun baan, moesten hun huis uit of kregen psychische problemen.

De plank misslaan

Adviescommissie Donner concludeerde dat de strenge toepassing van de wet door de afdeling Toeslagen gesteund werd met jurisprudentie van de Raad van State. Wettelijk mocht de harde aanpak, maar was dit wel de bedoeling? Achteraf bleek dat niet zo te zijn. De adviescommissie schrijft in de samenvatting van haar eerste rapport: 'De gesignaleerde vooringenomenheid kreeg een plek in werkinstructies en werkte door in bezwaar- en beroepstrajecten, bij de inzet van invorderingsmaatregelen alsook bij nieuwe aanvragen kinderopvangtoeslag van deze ouders. Uitvoerders kenden alleen de instructies maar niet de achtergrond en bedoeling daarvan, waardoor men zich niet meer bewust was van het onderscheid tussen de goeden en kwaden.'

Dit patroon, waarbij niet meer wordt nagedacht over de werkelijke bedoeling zou zich op meer plekken kunnen voordoen, zowel binnen de overheid als binnen het bedrijfsleven. Met de theorie 'werken vanuit de bedoeling' zijn er mogelijkheden om in ons werk als auditor hier meer oog voor te hebben. Zo kun je voorkomen dat je als auditor een verlengstuk wordt van een systeem dat niet werkt.

Werken vanuit de bedoeling

Als auditors leren we om te starten bij de opzet: zijn de processen wel beschreven? Daarna onderzoeken we het bestaan: zijn die processen dan ook wel echt aanwezig? En tot slot kijken we naar de werking: worden de processen in de praktijk ook uitgevoerd conform de beschrijving? Deze methode is vaak heel geschikt, maar we lopen wel het risico om de papieren opzet leidend te maken voor de echte mensenwereld. Voor je het weet richten we de meeste aandacht op de procesbeschrijving en niet op wat er in de praktijk gebeurt.

Wouter Hart, auteur van twee boeken over het thema 'werken vanuit de bedoeling', beschrijft dat auditors professionals tot uitvoerders van regels maken als we hen enkel vragen naar hun kennis en uitvoering van de beschreven opzet. In de auditwereld is dit ook al eerder onderkend. Van Twist constateerde bijvoorbeeld al overmatige auditaandacht voor de papieren werkelijkheid, waarna de Korte en Otten hebben opgeroepen om vaker te starten bij de werking (*Audit Magazine*, 4-2020).

Figuur 1. Werken vanuit de bedoeling
(Bron: Wouter Hart, Verdraaide Organisaties, 2012)

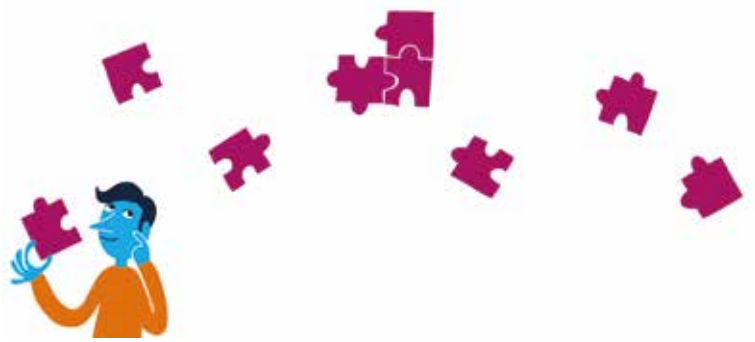
Professionele buikpijn

De theorie 'werken vanuit de bedoeling' draait het model van opzet, bestaan en werking om (zie *figuur 1*). Eerst kijk je naar wat de grotere bedoeling van de geldende regels eigenlijk is, waarom is het proces ooit bedacht en welk hoger doel wordt ermee gediend? Hierna observeer je hoe mensen eigenlijk werken in de leefwereld: wat doen ze in de praktijk en waar lopen ze tegenaan? Tot slot kun je onderzoeken hoe de systeemwereld ondersteunt, op welke manier dragen bijvoorbeeld procesbeschrijvingen en de IT-systemen bij aan het behalen van de bedoeling? Een belangrijk begrip hierbij is professionele buikpijn, wanneer de regels worden gevolgd, maar je toch het gevoel krijgt: 'dit kan toch echt niet de bedoeling zijn?!'

Intern verbetertraject

Met de theorie 'werken vanuit de bedoeling' hebben we binnen de ADR de afgelopen periode een audit en een intern verbetertraject uitgevoerd, daarnaast hebben we er diverse workshops over gegeven. Hierbij hebben we gemerkt dat de theorie goed aansluit op de methodieken van Design Thinking. Design Thinking wordt gebruikt om complexe problemen op te lossen door je te verplaatsen in betrokkenen, het probleem te definiëren, ideeën voor oplossingen te verzamelen en daarna een prototype-oplossing te maken die je gaat testen.

In dit artikel reiken we vier principes aan die toegepast kunnen worden bij audits met als uitgangspunt 'werken vanuit de bedoeling'. Bij ieder principe geven we eerst een beschrijving, vervolgens wat dit van de auditor vraagt en tot slot beschrijven we een praktijkvoorbeeld van de pilotaudit die we hebben uitgevoerd.



Principe 1 – Denk groot voor de bedoeling

De eerste stap is om bij een audit bewust stil te staan bij de bedoeling. Dit lijkt makkelijk maar is lastiger dan je denkt. Iedere betrokkene denkt vanuit zijn eigen perspectief. De oorspronkelijke bedoeling wordt vertaald in taken en die taken worden vervolgens als de bedoeling gezien. Zo raakt de werkelijke bedoeling verder uit het zicht.

Bij dit principe gaat het om uit te blijven zoomen en je af te blijven vragen wat de toegevoegde waarde is van het deel voor het geheel. Voor auditors is het een cruciale vaardigheid om breder te kijken. Hart: "Dit vraagt om lef want de hele wereld is ingezoomd. Er zijn enorm veel belangen gekoppeld aan de eigen taken en handelingen. De bedoeling ligt meestal een stap verder dan ons perspectief daarop."[1]

Stilstaan bij de bedoeling en groot denken vraagt met name aan de voorkant van het onderzoek een actieve rol van de auditor. Door al bij de intake of de start van een onderzoek uit te zoeken wat de bedoeling en de grotere context is, kun je betere onderzoeksvragen formuleren en zullen je onderzoeksresultaten waardevoller zijn voor de opdrachtgever.

In theorie is het voor ons als auditor makkelijker om uit te zoomen, omdat wij niet veel eigenbelangen hebben bij het onderzoeksobject, de specifieke taken of handelingen. Maar het is niet vanzelfsprekend dat we nadenken over de grotere bedoeling van de te onderzoeken organisatie of het proces. In onze opleiding leren we juist om de onderzoekscope zo goed mogelijk af te bakenen. Hiermee lopen we zelf het risico om in te zoomen op een specifiek afgebakend deel. Met een afgebakende scope is natuurlijk niets mis, maar we moeten dan wel bewust tijd en aandacht besteden aan de grotere context waarin dit zich afspeelt.

Bij de pilotaudit naar een toezichtproces betrokken wij bewust alle spelers van het proces waarop toezicht werd gehouden. Ook maakten we een tijdlijn van het proces waarbij we begonnen bij het echte begin en pas ophielden bij het echte einde. Dit maakte het onderzoek groter, maar bracht zo wel de grotere bedoeling aan het licht. Daarbij hebben we alle betrokkenen geïnterviewd en specifiek gevraagd naar de grotere bedoeling, het eigen belang en hun eigen succesfactoren. In de praktijk bleek het lastig voor iemand die betrokken is bij een deelproces om het geheel te overzien. Hierdoor werd de genoemde bedoeling verkleind naar het deelproces. Door het proces van begin tot eind te onderzoeken, werden de grotere bedoeling van het proces en kleinere deelbelangen aan het licht gebracht.

Principe 2 – Maak de praktijk klein

Na het groter denken is de tweede stap om je te verdiepen in concrete voorbeelden uit de praktijksituatie, zodat je onderzoekt hoe er echt gewerkt wordt en welke invloed processen en systemen hebben. Zo vind je de werkelijke informatie voorbij het papier. Hierdoor krijg je als professional niet alleen meer informatie, maar geef je jezelf ook de kans om 'geraakt' te worden (professionele buikpijn). Immers, in de praktijk wordt duidelijk waar de systeemwereld botst met de leefwereld en worden de directe effecten daarvan voor betrokkenen zichtbaar.

Door naar praktijk te kijken gaan we in feite direct naar de werking. Een traditionele audit is deductief, vanuit de regel (norm) onderzoeken we hoe de opzet, het bestaan en de werking verloopt. De werkwijze die we nu bespreken is inductief. Vanuit praktijksituaties onderzoeken we welke gemeenschappelijke regels er zijn. Het is wel belangrijk dat we die gemeenschappelijke regels dan nog testen, daar komen we later op terug.

Auditors kunnen dit tweede principe toepassen door een aantal casussen te selecteren en echt op zoek te gaan hoe medewerkers in de praktijk invulling geven aan de grote bedoeling.

Met 'werken vanuit de bedoeling' kun je voorkomen dat je als auditor een verlengstuk wordt van een systeem dat niet werkt

Hierdoor is het ook mogelijk om met behulp van storytelling onderbouwing te geven aan bevindingen. Dat geeft ook de lezer de mogelijkheid om professionele buikpijn te ervaren: het kan toch niet de bedoeling zijn, dat… Hart zegt hierover: "De auditor moet dus niet de controleur zijn, maar horen hoe in de organisatie antwoord wordt gegeven op werkelijke vraagstukken en welke mechanismen daarbij helpen of in de weg staan."[2]

Bij de pilotaudit zoomden we in op vijf concrete casussen. In de praktijk bleken werkzaamheden en processen heel anders te lopen dan het beeld dat betrokkenen hadden. Een casus waar een positief beeld over was, bleek bij het opstellen van een concrete tijdlijn veel vertragingen te kennen. Ook andersom vond dit plaats, er was een negatief beeld over een casus, terwijl het in de praktijk vlot was gegaan. Door in te zoomen konden we heel gerichte voorbeelden geven bij elke bevinding die we rapporteerden. Doordat de gevolgen van de bevindingen duidelijk werden, werd het gesprek met de opdrachtgever verrijkt.

Principe 3 – Breng betrokkenen samen

Na het groot denken en klein maken, volgen nog twee principes die helpen om een onderzoek goed te laten landen. Het principe om samen te brengen kan bijdragen aan een cultuur van verantwoordelijkheid, door op zoek te gaan naar mechanismen waardoor mensen stelselmatig wel of geen antwoord kunnen geven op wat de praktijk van hen vraagt. Dit kan door alle verschillende perspectieven die stakeholders hebben op de bedoeling samen te brengen. Zo kun je leren van elkaars perspectief en samen aan een oplossing werken.

Hart stelt in zijn boek *Anders Vasthouden* dat het vergroten van het eigenaarschap een belangrijke voorwaarde is om te kunnen werken vanuit de bedoeling. Hij beschrijft dat er vaak oplossingen worden bedacht voor mensen die er straks echt wat mee moeten gaan doen. Daarom is het belangrijk te beseffen dat de oplossing van de ander is. De oplossing kun je vormgeven door naast de ander te gaan staan en samen met de ander over de oplossing na te denken. Door de oplossing van, naast en met de ander tot stand te laten komen ontstaat oplossend vermogen. Het gaat om in co-creatie werken aan de oplossing.

Design Thinking kent verschillende methodieken om samen aan een probleem te werken. De empathy map is in het kader van werken vanuit de bedoeling interessant. Een empathy map helpt om dieper inzicht te krijgen in de belevingswereld van de betrokken spelers, door op één plaat visueel te maken wat de bedoeling en belangen zijn van iedere betrokkene.

Concreet vraagt dit van de auditor om bij iedere stap van het onderzoek na te denken wie de spelers zijn. De vervolgvraag is dan of het samenbrengen van alle spelers van toegevoegde waarde kan zijn voor het laten landen van het onderzoeksresultaat en het ontwikkelen van oplossingen.

In de pilotaudit organiseerden we na alle individuele interviews een workshop voor alle betrokkenen. Tijdens deze workshop deelden we een empathy map waarop alle belangen en succesfactoren van betrokkenen stonden. In de workshop stonden we expliciet stil bij de verschillen en de overlap tussen de verschillende bedoelingen en belangen. Dit leverde naast nieuwe onderzoeksresultaten ook meer begrip op tussen de betrokkenen onderling. Ook bespraken we met alle spelers de bepalende momenten in de tijdlijn van de casus. En tot slot verkenden we samen mogelijke verbeteropties.

Principe 4 – Test de uitkomst

In het laatste principe staat testen van de uitkomsten van het praktijkonderzoek centraal. Dit raakt aan de bedoeling van de audit zelf, niet zomaar het opleveren van de bevindingen, maar verder zoeken naar de betekenis van de gevonden inzichten. Het testen van uitkomsten is een belangrijke stap bij Design Thinking en is wat ons betreft erg belangrijk. We noemden eerder al dat het onderzoek inductief is opgezet: vanuit casussen zoeken we naar gemeenschappelijke regels. Door te testen kom je te weten of bevindingen of oplossingen ook breder toepasbaar zijn. Daarnaast stelt het je in staat om nuance aan te brengen.

Concreet vraagt dit van de auditor om niet te snel aan te nemen de wijsheid in pacht te hebben. Blijf aannemen dat het waardevol is om uitkomsten terug te leggen bij de mensen waar het echt om gaat, die er straks echt wat mee gaan doen. Daarnaast kun je als auditor de organisatie aan het denken zetten hoe ze zelf een lerende omgeving creëren over het onderzochte onderwerp.

Bij de pilotaudit hebben we de uitkomsten van individuele interviews aan de hele groep voorgelegd voor hoor en wederhoor en reflectie. Vooraf hadden we ook aangeboden om bevindingen te testen, omdat er terughoudendheid was om enkele casussen te onderzoeken. Achteraf bleek dit niet nodig, omdat de bevindingen herkend werden.

Bijdragen aan een bewuste organisatie

Wanneer zet je de vier principes voor auditen vanuit de bedoeling in? Wij denken dat je deze principes in variërende mate kunt implementeren in audits om meer aandacht te schenken aan de bedoeling.

Zo kun je de principes beperkt toepassen in een reguliere audit om tot een effectiever resultaat te komen. Of je kunt de hele audit naar de principes inrichten, zodat het onderzoek echt specifiek is gericht op de bedoeling. Dan ben je als auditor geen verlengstuk van het systeem, maar draag je bij aan een bewuste organisatie.

Hart zegt hier nog over: “Dus niet meer kijken of mensen zich aan de regels houden, maar hoe mensen de regels hanteren in het licht van de werkelijke bedoeling. En dan kan dus soms het adviseren om regels af te schaffen een uitstekende conclusie van de audit zijn.” <<

Noten

1. Interview Wouter Hart in Jaarplan Auditdienst Rijk 2020.
2. Jaarplan Auditdienst Rijk 2020.

Roos Kalker is auditmanager bij de Auditdienst Rijk. Haar specialisaties zijn onderzoeken op het gebied van gedrag, verandermanagement en procesverbetering. Naast onderzoeker is Roos ook facilitator en illustrator.

Gerben Korevaar is auditmanager bij de Auditdienst Rijk. Zijn specialisaties zijn onderzoeken op het gebied van gedrag, governance en project- en programmamanagement.

INTERNATIONAL CONFERENCE

AMSTERDAM • 10-12 JULY 2023

WHAT: INTERNATIONAL CONFERENCE 2023 • **WHERE:** AMSTERDAM
DATE: 10-12 JULY 2023 • **HOTEL:** RAI AMSTERDAM

theiia.org/IC

Column
Tekst Linda Post

Blik op 2023

Als bestuur zijn we afgelopen tijd volop bezig geweest met het bepalen van de speerpunten voor 2023. Deze speerpunten zijn gebaseerd op de IIA-missie 'Het ontwikkelen en promoten van de internal auditfunctie, waarbij een toegevoegde waarde wordt geboden aan alle belanghebbenden'. De ambitie van het IIA is dat internal auditors wereldwijd erkend worden als een essentiële schakel voor effectieve governance, risk management & control, waarbij het IIA het primaire aanspreekpunt is voor de internal auditberoepsgroep.

Voor 2023 zijn vier thema's gedefinieerd. De eerste twee thema's zijn gericht op het bieden van een toegevoegde waarde, met name door het aanbod af te stemmen op de wensen en behoeften van onze leden, wat afhankelijk is van de omvang of de branche van de organisatie. Daarnaast wordt ook aandacht besteed aan overige belanghebbenden door via advocacy de bekendheid van de internal auditfunctie verder te vergroten. Onder meer door contacten met raden van commissarissen, audit committees en andere beroepsgroepen die eveneens kennis over het internal auditvakgebied kunnen verspreiden en promoten.

De overige twee thema's zijn meer gericht op het versterken van de interne organisatie. In 2023 wordt verder geïnvesteerd in de automatisering. Het is belangrijk dat leden informatie snel kunnen vinden, zich makkelijk kunnen inschrijven voor trainingen en permanente educatie eenvoudig kunnen registreren. Daarnaast wordt onze vereniging door een grote groep van ruim honderd vrijwilligers ondersteund via diverse commissies en werkgroepen, bijvoorbeeld de commissie voor young professionals, de commissie professional practices en PAS (professionele auditors at small audit shops), een commissie voor kleinere auditafdelingen. Als bestuur willen we onze waardering voor deze vrijwilligers blijven tonen en de professionele inzet van gemotiveerde vrijwilligers waarborgen.

Bij het bepalen van de meer inhoudelijke prioriteiten voor 2023 is gebruikgemaakt van het document *Risk in Focus 2023* dat recent is verschenen. Ieder jaar werken de Europese instituten voor Internal Auditors samen om de belangrijkste risico's te inventariseren voor het daaropvolgende kalenderjaar. De resultaten van *Risk in Focus 2023* zijn bedoeld als hulpmiddel voor het opstellen van de auditplannen voor 2023 en geven bestuursorganen goed zicht op welke uitdagingen hen komend jaar te wachten staan.

De resultaten van het onderzoek *Risk in Focus 2023* laten zich samenvatten in de volgende vijf 'hot topics':
1. cybersecurity en datasecurity;
2. macro-economische en geopolitieke risico's;
3. klimaatverandering en environmental sustainability;
4. human capital, diversiteit en talentmanagement;
5. digitale disruptieve en nieuwe technologieën.

Als bestuur hebben we deze topics meegenomen bij het bepalen van de vaktechnische onderzoeken en publicaties voor 2023. Met name op het gebied van environmental, social & governance (ESG) verwachten we dat de internal auditor toegevoegde waarde kan hebben. Een van de speerpunten is dan ook om op basis van aanvullend onderzoek de rol van de internal auditor verder uit te werken en te promoten. Daarnaast staan cybersecurity en datasecurity op nummer een in de hot topics, onder meer door de ransomware-aanvallen, die met 80 procent zijn toegenomen.

IIA Nederland
Linda Post is voorzitter van IIA Nederland

Tekst Naeem Arif EMIA RO
Femke Dik MSC
Beeld NFP Photography

Over

Thijs Smit is auditconsultant en docent internal auditing aan de universiteit van Amsterdam. Daarnaast voert hij namens het IIA kwaliteitstoetsingen op auditfuncties uit. Voorheen was hij voorzitter van het IIA, president van ECIIA en CAE bij PostNL, Corus, Ahold, SNS Reaal en SHV.

“Ik geloof ***heilig*** in een **houdbaarheidsdatum** voor de CAE”

Thijs Smit vervulde in het verleden als vrijwilliger diverse functies binnen IIA Nederland en was van 2003 tot 2008 voorzitter. Tegenwoordig is hij voorzitter van KIN (Kwaliteitstoetsingen IIA Nederland). Een gesprek over de houdbaarheid van een CAE.

Wie is Thijs Smit?
“Je zou kunnen zeggen dat ik van geboorte internal auditor ben. Direct na de heao ben ik gestart bij de interne accountantsdienst van de toenmalige PTT (nu PostNL). In die tijd heb ik het internal auditvak zien ontstaan. Daar heb ik ruim negentien jaar gewerkt. Vervolgens heb ik als chief audit executive (CAE) gewerkt bij Hoogovens, Corus, Ahold, SNS Reaal en SHV. Ten tijde van de grote crisis bij Ahold in 2003 was ik in dienst bij Ahold. De afgelopen vier jaar ben ik werkzaam als consultant. Ik geef trainingen en colleges over ons mooie vak en voer kwaliteitstoetsingen uit namens het IIA.”

Bent u al lang verbonden aan het IIA?
“In 1998 kwam ik, vlak na oprichting, in het bestuur van IIA Nederland. In het eerste jaar was ik voorzitter van de commissie Vaktechniek. Daarna kwam ik in het bestuur, dat heb ik tien jaar gedaan. In 2003 tot 2008 in de rol van voorzitter. Van 2009 tot 2013 zat ik in het bestuur van IIA Global in Amerika. Bij de ECIIA (Europese IIA) ben ik vijf jaar bestuurslid geweest waarvan de laatste twee jaar als president. Ik heb in de jaren dat ik betrokken was bij het IIA het nodige gezien, waaronder de fusie tussen de VRO – de rechtsvoorganger van het huidige SVRO – en het IIA NL.”

Was de term internal audit al in zwang toen u begon?
“Nee, je was assistent interne accountant. Ik heb jarenlang jaarrekeningen gecertificeerd, interne certificering noemden we dat. Een fenomeen dat in het bedrijfsleven niet of nauwelijks meer voorkomt. De ontwikkeling naar internal audit heb ik meegemaakt. De focus verschoof van volledig gericht op financiële gegevens naar operational audits en compliance.”

Bestaat er zoiets als de houdbaarheid van een CAE?
“Ja, dit bestaat en daar geloof ik heilig in. Hier heb ik vijftien jaar geleden al eens een artikel over geschreven. Ik sluit me graag aan bij de praktijk van de externe accountant: na vijf tot zeven jaar rouleren. Zelf vind ik een termijn van zes jaar het mooist. Vertrekken in de eerste twee jaar is zonde van alle energie die je als CAE en organisatie steekt in het leren kennen van het bedrijf. Je hebt die jaren nodig om een bedrijf goed te leren kennen. Je moet de cultuur van een organisatie volledig doorgronden, dat wil zeggen: de onderstroom van de organisatie kennen. De onderstroom is cruciaal voor het functioneren van een CAE. Na twee jaar word je pas effectief. Het management moet namelijk het gevoel hebben dat jij het bedrijf door en door kent.”

Hoe doe je dat als CAE?
“Een voorbeeld: wanneer je CAE bij een supermarktbedrijf bent, zou je een tijdje in een filiaal van de supermarkt moeten werken. Ik heb bij Ahold in totaal in mijn eerste jaar vier weken in een filiaal gewerkt. Hierdoor leer je wat er écht speelt in een bedrijf. Die investering doe je in de eerste twee jaar. Dit is een zware periode, want je moet naast diepgaande kennis opdoen van de basisprocessen ook bouwen aan de internal auditfunctie, visie ontwikkelen en auditjaarplannen schrijven. Na de twee ontwikkelingsjaren heb je een raad van bestuur en een auditcommissie die in je geloven. In de twee jaren die hierna volgen, kunnen audits gedaan

worden die echt waarde toevoegen. Hierbij kunnen de audits soms best een beetje pijn doen. Het zou niet goed zijn als auditors al acht á tien jaar ergens werken en nog nooit op de tenen hebben gestaan van een directeur of manager, dan heb je hoogstwaarschijnlijk je rol niet goed ingevuld. De auditor moet spreekwoordelijk 'het kiezeltje in de schoen zijn'."

Hoe hebt u dit aangepakt?
"Altijd als ik in mijn rol als CAE over cultuur begon, met name over cultuurelementen die niet zo goed zijn, worden mensen ongemakkelijk. Na vijf tot zeven jaar is de magie vaak verdwenen. Daarna is het wat mij betreft tijd voor iets anders, en dit idee heb ik verder uitgewerkt. De start zou zijn dat de definitie van internal audit veel beter omschreven zou moeten worden in de Corporate Governance Code. Internal audit zou een meer onafhankelijke rol moeten krijgen. Tegenwoordig heeft vrijwel elke auditafdeling een lijn naar de auditcommissie, maar dit blijft meestal wat vrijblijvend. Het is eigenlijk raar dat de auditcommissie niet de opdrachtgever is voor de vijfjaarlijkse kwaliteitstoetsing van de internal auditfunctie (IAF)."

Moet de auditcommissie toezicht houden op de IAF?
"Ja, dat vind ik wel. Daarnaast vind ik dat de roulatie van de CAE opgenomen zou moeten worden in de Corporate Governance Code, net als bij de externe accountants. Ik zou willen pleiten voor een maximale termijn van de CAE van 6 jaar. In het nieuwe systeem zou het functioneren van de CAE beoordeeld moeten worden door de directe lijnbaas (vaak CEO) en de voorzitter van de auditcommissie samen. De primaire rapportagelijn moet wel naar de CEO blijven."

Waarom dan?
"In mijn tijd bij Corus (met one-tier board) heb ik meegemaakt dat de effectiviteit van de CAE afneemt als de primaire directe rapportagelijn de voorzitter van de auditcommissie is. Hierdoor werd ik als CAE op een te grote afstand gehouden door het bedrijf, omdat ik een te grote invloed had. De IAF zou onderdeel moeten zijn van het bedrijf en dichtbij het managementteam moeten staan. Dit is een waarborg voor de goede verstandhouding tussen de CAE en raad van bestuur. Uit ervaring kan ik zeggen dat het niet goed afloopt met de CAE die een conflict krijgt met zijn eigen raad van bestuur."

Kunt u iets meer vertellen over deze ervaring?
"Dit heb ik in de praktijk meerdere malen zelf ondergaan en van andere CAE's gehoord. In het geval van geconstateerde evidente misstanden of grote risico's moet je een lastige boodschap brengen aan je raad van bestuur. Het kan gaan om misstanden die om direct ingrijpen vragen. Dergelijke boodschappen kunnen binnen de raad van bestuur 'slecht vallen'. Ik heb deze situatie zowel bij Ahold, SNS als SHV meegemaakt. Overigens in totaal verschillende situaties. Bij Ahold was er sprake van verkeerd handelen door de raad van bestuur zelf (side letters), bij SNS verkeerd beleid in de onroerend-goeddivisie (Property Finance) en bij SHV van onrechtmatige transacties bij dochterbedrijven (omkoping). Zolang je rapporteert over zaken die een caissière, CFO van een dochteronderneming of een filiaalmanager aangaan, vindt iedereen het prima. Het wordt pas spannend als de bevindingen de voorzitter van de raad van bestuur persoonlijk kunnen raken. Dán moet je als internal auditor nog steeds je werk goed kunnen doen."

Hoe kun je deze rol als CAE toch op je nemen?
"De rapportagelijn zou primair naar de raad van bestuur moeten zijn. De auditcommissie moet toezicht houden op de IAF. Het aanstellen, beoordelen van het functioneren en de beloning van de CAE hoort daar zeker bij. Om als CAE professioneel onafhankelijk te zijn, zou het ook goed zijn een incentive beloning toe te kennen die na het verstrijken van de termijn (idealiter zes jaar) wordt uitgekeerd."

"Het zou niet goed zijn als auditors al acht á tien jaar ergens werken en nog nooit op de tenen hebben gestaan van een directeur of manager, dan heb je hoogstwaarschijnlijk je rol niet goed ingevuld"

Na de termijn? Waarom?
"Het is niet wenselijk om CAE's mee te laten doen aan de jaarlijkse programma's voor variabele beloning. De onafhankelijkheid en professionaliteit kunnen in het gedrang komen wanneer een 40-jarige CAE met een hypotheek en een jong gezin zijn baan dreigt te verliezen. De CAE kan in een dergelijk gevallen mogelijkheden zoeken om zijn baan te redden die de onafhankelijkheid bedreigen. Een variabele beloning na het verstrijken van de termijn zorgt ook voor een buffer om de tijd te overbruggen. Het zou goed zijn om deze variabele beloning van CAE te verankeren in de Corporate Governance Code."

Hebt u zelf ook de eerder besproken termijn van zes jaar toegepast?
"Ja. Behalve bij SHV, toen was het zeven jaar. De termijn van zes jaar heb ik niet bewust gevolgd, het is zo gelopen. Toen ik CAE van (nu) PostNL was, was ik daar na vijf jaar wel klaar. Ik ging daar weg om 'de wereld te veroveren'. Bij andere werkgevers is het ook op natuurlijke wijze gebleven bij maximaal zes jaar. Bij Ahold heb ik zes jaar gewerkt. Drie jaar voor de crisis en drie jaar erna."

Hoe kun je als auditor bijdragen aan een cultuurverandering?
"Bij SNS heb ik dit gedaan samen met de externe hulp van KPMG. Als IAF moet je niet de illusie hebben dat je de hele cultuur van een organisatie kunt doorgronden en onderzoeken. Ik heb geleerd dat je het proces voor een cultuurverandering moet laten faciliteren door een buitenstaander. Die kan de cultuurverandering makkelijker overbrengen. Het kan provocerend overkomen als de CAE dat doet. Bij echte fundamentele cultuurproblemen zou ik iemand inhuren als procesbegeleider. Dat werkt als een katalysator. Het gaat namelijk niet alleen om wat je zegt, maar ook wie het zegt. Bij SNS heeft dat heel goed uitgepakt."

Hoe belangrijk is een goed proces?
"Een goed proces van kwaliteitstoetsingen binnen de IAF kan daarnaast ook helpen om de positie van de IAF, vooral ten opzichte van het audit committee, goed te waarborgen.

In het ideaalmodel verricht een IAF in het eerste jaar een zelfassessment die wordt gedeeld met de raad van bestuur en het audit committee. In het tweede jaar ook weer een zelfassessment, maar dan met een beoordeling van een externe partij en in het derde jaar een externe toetsing. Daar zijn we nog lang niet aan toe, maar je ziet wel dat het karige systeem van eens in de vijf jaar een externe toetsing op zijn retour is. Er is een beweging gaande dat IAF's zich frequenter laten toetsen. Er zijn meerdere auditafdelingen in de financiële sector die zich nu eens in de drie jaar extern laten beoordelen. Wat mij betreft een goede ontwikkeling, want belangrijke processen binnen een onderneming beoordelen we ook jaarlijks en niet eens in de vijf jaar."

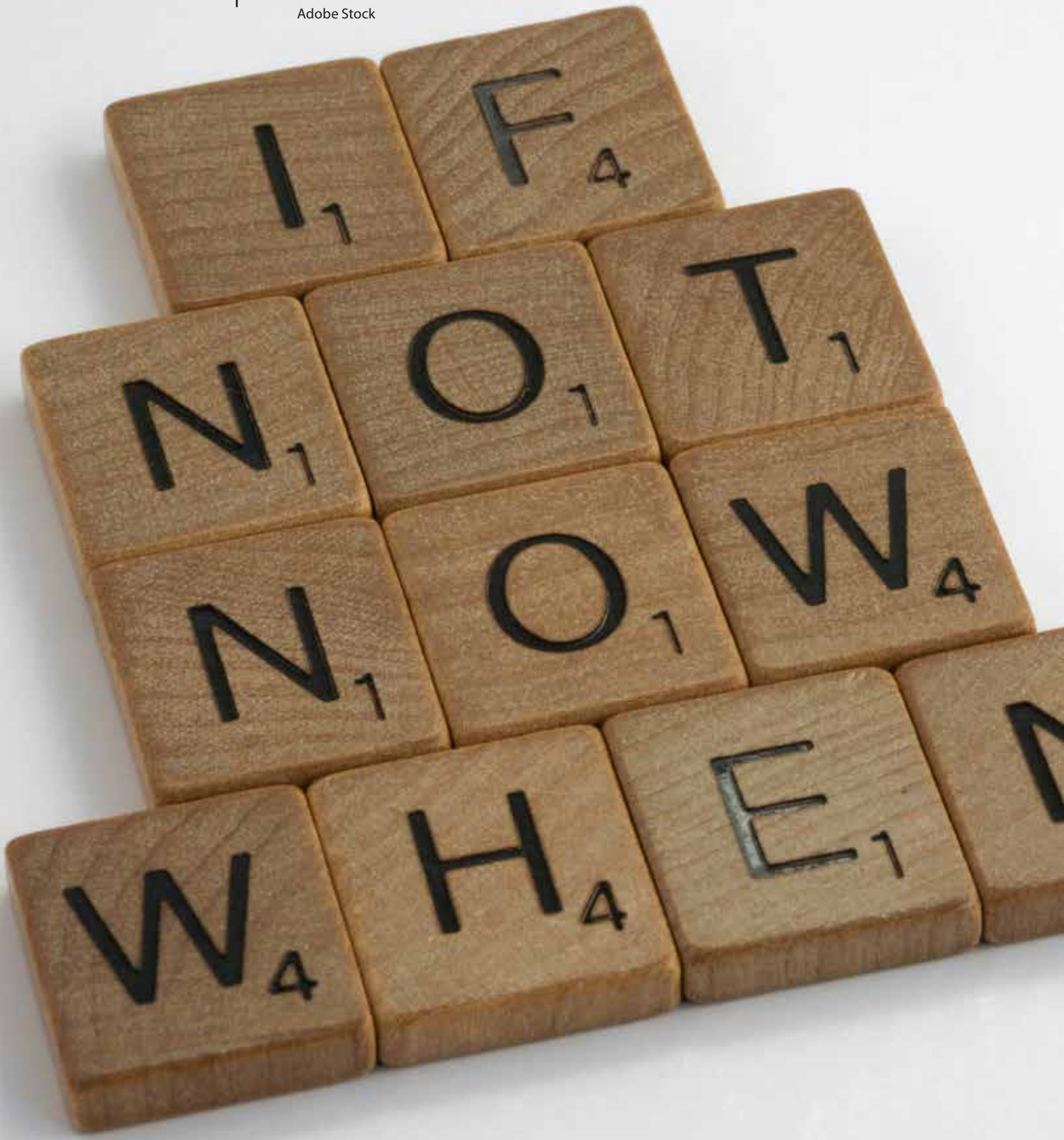
Wat gebeurt er als een CAE over de houdbaarheidsdatum is?
"Dat varieert sterk. Soms zal de CAE defensief gedrag gaan vertonen om zijn IAF te beschermen tegen aanvallen van partijen als het management van decentrale eenheden, bijvoorbeeld divisies/business units. Ook kan het omgekeerde gebeuren en kan de CAE te veel onderdeel worden van de cultuur van de organisatie waardoor een effectieve derdelijnsfunctie in gevaar komt. Uiteraard zijn er ook CAE's die na zes jaar nog prima functioneren."

Wat zeggen de internationale standaarden over de termijn van een CAE?
"Die zeggen daar niets over. Het is geen wetmatigheid. Sommige CAE's zitten wat langer en doen hun werk goed. Echter, de tegenwerkende krachten in een organisatie worden op een gegeven moment heel sterk, daarom zou ik een maximum van zes á zeven jaar willen aanhouden. In een deel van de wereld zijn de IIA Standaarden gedeeltelijk tot wet verheven. Als wij standaarden gaan veranderen, zoals bijvoorbeeld een maximumtermijn voor een CAE, dan moeten dergelijke landen de wet veranderen. Veranderingen van standaarden is een heel intensief traject. In Nederland is de Corporate Governance Code heel belangrijk, dat heeft internal audit veel meer power gegeven. Daar zou ik op inzetten als IIA Nederland."

Ziet u al verandering de afgelopen jaren?
"Ja, het rouleren is toegenomen in de afgelopen jaren. Dat juich ik toe. Natuurlijk zijn er in Nederland meerdere CAE's die tien jaar of meer op hun positie zitten. Op zich geen ramp, want degenen die ik ken werken nog prima. Nog meer rouleren van CAE's zou een goede zaak zijn. Er zou wel een goed financieel vangnet moeten komen voor CAE's, zodat ze ergens op terug kunnen vallen (de eerdergenoemde buffer, rechtspositie, et cetera – red.). Het IIA zou bijvoorbeeld een pool chief auditors kunnen maken."

Is het raadzaam dat een CAE na zijn termijn een andere – eerste of tweedelijns – functie gaat bekleden?
"Dit is niet ondenkbaar. Dat kan zeker als je hart daar ligt. Maar je vraagt het eigenlijk aan de verkeerde persoon. Ik heb dit wel één keer gedaan in het begin van mijn carrière. Bij PostNL ben ik na vijftien jaar CAE anderhalf jaar CFO geweest bij een Belgisch distributiebedrijf dat net was gekocht. Ik heb toen veel geleerd over internal audit. Bijvoorbeeld hoe goed gerapporteerd kan worden. Voor ieder probleem dat je aanlevert, moet een oplossing aangedragen worden. Je zou als auditor een handelingsperspectief moeten bieden. Ik vind het zelf lastig, maar begrijp wel dat er veel draagvlak is als een CAE uit de business komt." <<

Tekst Dr. J.R.H.J. van Kuijck RA RC
Beeld Brett Jordan
Adobe Stock



Vervang de chief audit *executive* tijdig!

In 2006 schreef ik in *Audit Magazin*e de column ‘Leiderschap en het succes van een interne auditafdeling’. Daarin werd met een uitroepteken gesteld dat de uiterste houdbaarheidsdatum van een chief audit executive (CAE) beperkt is.

Daarnaast deed ik in deze column een oproep aan ondernemingen om het functioneren van de CAE periodiek te evalueren. Het functioneren van de CAE is geen constante factor en in een dynamische omgeving kunnen ook de verwachtingen ten aanzien van de rol wijzigen. Deze bijdrage gaat in op de bedreigingen voor het goed functioneren van de CAE. In dit kader wordt ook ingegaan op de houdbaarheid van een CAE.

Ethisch leiderschap CAE

De resultaten van het onderzoek van Van Staden en Steyn (2009) gaven al aan dat het profiel van de CAE een positieve invloed heeft op de kwaliteit van de interne auditfunctie. Een belangrijke rol die de CAE speelt is uiteraard het voor een organisatie realiseren van de doelstelling van interne auditing, namelijk ‘an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.’

Daarbij zijn de ethische houding en het professioneel kritisch gedrag van de auditors van cruciaal belang. De leider van de interne auditafdeling speelt daarin een prominente rol. Hij bepaalt niet alleen voor zichzelf hoe om te gaan met ethische kwesties, maar ook hoe de overige interne auditors binnen de afdeling daarmee omgaan.

Bedreigingen

Het is belangrijk dat de CAE het hoofd biedt aan allerlei bedreigingen die op de loer liggen. Bedreigingen die de professioneel kritische instelling en de ethische oordeelsvorming van de interne auditfunctie als geheel mogelijk aantasten:

- druk van het management;
- invloed carrièreperspectief;
- tijdige voltooiing van audits en follow-up;
- bewaking onafhankelijkheid en integriteit;
- transparantie en openbaarmaking onjuiste informatie.

Druk van het management
In de praktijk worden interne auditors geconfronteerd met situaties waarin het management probeert druk uit te oefenen op de CAE. Dat kan heel direct, maar ook indirect of heel subtiel. Soms zien we dat rechtstreeks druk wordt uitgeoefend om de inhoud van een rapport of – op een hoger geaggregeerd niveau – de rapportage naar de auditcommissie aan te passen. Daarbij gaat het er dan om dat het management de inhoud gunstiger wil voorstellen. Bijvoorbeeld door bewoording af te zwakken, verzachtende omstandigheden toe te voegen of issues zelfs helemaal niet te vermelden. Alles zogenaamd in het belang van de mensen of de organisatie. Maar de uiteindelijke gedachte is dat het management daarop minder kan worden aangesproken.

Naast deze rapportagedruk is er bij interne auditfuncties met veel expertise ook sprake van een druk op interne auditors om de organisatie te ondersteunen in operationele taken. Denk daarbij aan het adviseren bij het opzetten van processen, het meehelpen oplossen van acute problemen of om – uit kostenoverweging – omvangrijke adviesopdrachten uit te voeren. Bij terughoudendheid of weigering van de CAE om urencapaciteit van interne auditors daarvoor beschikbaar te stellen, wordt dit vaak gezien als niet-coöperatief.

De CAE zal daarom een balans moeten vinden tussen het weigeren en het accepteren van dergelijke adviesopdrachten. Niet alleen in het licht van de realisatie van de jaarplanning en ad-hocverzoeken van toezichthouders, maar ook om het onafhankelijk functioneren van de afdeling te beschermen. We weten allemaal dat het belangrijk is voortdurend zorgvuldige afwegingen te maken om collisiegevaar te voorkomen.

Invloed carrièreperspectief
In veel organisatie wordt de functie van de interne auditafdeling ook gezien als kweekvijver voor toekomstig management. Interne auditors krijgen namelijk de gelegenheid om diep in de keuken van de organisatie te kijken. Zo kunnen zij bedrijfsprocessen doorgronden en de relaties leren zien tussen operationele processen en de weerslag daarvan in de cijfers. Het helpt in het ontwikkelproces van interne auditors en maakt hen bovendien waardevolle medewerkers die in de toekomst elders in de onderneming functies kunnen gaan bekleden. In sommige organisaties worden medewerkers als onderdeel van hun carrièrepad gedurende een korte tijd gestationeerd bij de interne auditfunctie. Daarmee krijgen zij ook een beter begrip van de functie en het belang ervan in hun latere carrière elders in de onderneming.

In het personeelsbeleid moeten uiteraard wel goede randvoorwaarden zijn geschapen. Daarbij gaat het om beloning in lijn met andere functies en voorwaarden voor doorstroming. Ervaren interne auditors hebben namelijk vaak veel kennis van de organisatie en processen en kunnen dan ook wellicht beter betaalde banen in andere bedrijfsonderdelen krijgen. Echter, een te snelle doorstroming kan een interne auditfunctie ook verzwakken. In de praktijk blijken meer en meer organisaties overigens nadrukkelijk bij de aanname van een interne auditor te kijken of hun profiel geschikt is om langduriger betrokken te kunnen zijn bij de organisatie.

Een kweekvijver heeft ook een keerzijde. Een CAE die veelvuldig de vinger op de zere plek legt maakt geen vrienden binnen de organisatie, zeker als er koppen rollen als gevolg van rapportages. In het licht van het veiligstellen van het carrièreperspectief kunnen er dan ook prikkels zijn die ervoor zorgen dat de CAE minder professioneel kritisch is of minder ethisch oordeelt. Hoe langer een CAE betrokken is, hoe meer dit een bedreiging vormt voor het goed functioneren van de CAE.

Tijdige voltooiing van audits en follow-up
Een van de doelstellingen van een interne audit is om probleempunten zichtbaar te maken en vast te stellen of management adequate maatregelen neemt om deze tijdig op te lossen. De doorlooptijd van een audit kan echter in het gedrang komen wanneer voor de audit relevante gegevens niet tijdig worden vrijgegeven of het management beantwoording van vragen onnodig uitstelt. Soms kan het management zelfs essentiële informatie achterhouden of vrijgave uitstellen met vertrouwelijkheid of gevoeligheid als argument. Een CAE zal dan krachtig moeten optreden.

Een CAE die veelvuldig de vinger op de zere plek legt maakt geen vrienden binnen de organisatie, zeker als er koppen rollen als gevolg van rapportages

In de fase waarin het conceptrapport moet worden afgewikkeld zal het management gevraagd worden acties te definieren op de geconstateerde issues. Een niet tijdige reactie daarop of het geven van niet adequate of onvoldoende scherp geformuleerde managementacties kunnen tot vertraging leiden. Dit soort bewust traineren leidt uiteindelijk tot uitstel van de rapportage en de vrijgave van het definitieve auditrapport.

Als laatste noemen we de follow-up monitoring. Een CAE moet optreden als follow-upacties door het management niet tijdig of onvoldoende zijn. In dit soort situaties zal de CAE mogelijk stuiten op weerstand van het management. Een CAE moet dan een adequate houding hebben en zich daarbij gesterkt voelen door topmanagement en interne en externe toezichthouders. Als er in een organisatie overigens sprake is van lang openstaande punten, dan is dat wel een aandachtspunt. Het is een indicatie dat de issues opgeworpen

door de interne auditors onvoldoende belangrijk zijn of dat de spelers in het governance spectrum onvoldoende hun rol hebben gepakt.

Bewaking onafhankelijkheid en integriteit
De IIA Code of Ethics wijst de interne auditors op hun verantwoordelijkheden en de naleving van deze regels. De persoonlijke belangen mogen de onafhankelijkheid en de integriteit van interne auditors niet aantasten. Naast de eerdergenoemde bedreiging van de druk van het management blijken interne auditors in de praktijk bewust of onbewust vertrouwelijke informatie vrij te geven aan onbevoegden binnen de organisatie.

Ook het buiten de organisatie bespreken van gevoelige informatie of het bewust lekken zijn uit den boze. In de dagelijkse werkzaamheden hebben interne auditors namelijk toegang tot veel vertrouwelijke informatie. Deze informatie kan onder andere gebruikt worden voor persoonlijk gewin, het beschadigen van collega´s of het bevoordelen van anderen. Het is de verantwoordelijkheid van de CAE om preventieve maatregelen te nemen om integer handelen te bevorderen en krachtig op te treden tegen auditors die niet integer omgaan met informatie.

Transparantie en openbaarmaking onjuiste informatie
De maatschappelijke ontwikkelingen van de afgelopen decennia hebben ertoe geleid dat het merendeel van de organisaties verplicht is om transparant te zijn en financiële en/of niet-financiële informatie te openbaren. Om de vereiste zekerheid te verschaffen voordat deze wordt vrijgegeven, worden interne auditors betrokken in de beoordeling van processen die leiden tot die informatie of de informatie zelf.

Als een organisatie niet transparant is over misstanden of onjuiste informatie publiceert, getuigt het van moed als een interne auditor toch stelling durft te nemen en dit via de geëigende kanalen binnen de organisatie escaleert.

Als ook de raad van commissarissen meegaat met de beslissing van de organisatie, dan staat de interne auditor in de kou. Op grond van zijn ethische houding zal deze een ultieme afweging moeten maken of een continuering van het dienstverband nog mogelijk is. Immers, organisaties hebben in de regel een strikt beleid om (het vermoeden van) criminele activiteiten of wetsovertredingen te melden aan externe instanties. Dit betekent dat als de CAE eigenstandig een melding doet, dit kan worden gezien als overtreding van het bedrijfsbeleid, en de CAE kan daarvoor gestraft worden. In het recente verleden hebben we gezien dat klokkenluiders maar al te vaak de wrange vruchten plukken.

In de wereld van de externe accountants geeft de regelgeving ten aanzien van non-compliance with laws and regulations (NOCLAR) houvast en de mogelijkheid om de interne escalatieprocedure te doorbreken. Deze regelgeving is wereldwijd geïmplementeerd. Een dergelijke standaard ontbeert het international professional practices framework van het IIA (IPPF) anno 2022 en is wellicht een waardevolle aanvulling om de ethische rol van de interne auditor te versterken.

Houdbaarheid
De wereld van de externe auditors is sinds het Enron-debacle in 2001 sterk veranderd. De zelfregulering is danig op de schop gegaan en vervangen door stringentere regelgeving die nauwlettend wordt gevolgd door toezichthouders. In de huidige samenleving is de zorg om de onafhankelijkheid van accountants groot. Dit heeft ook geleid tot het instellen van termijnen aan de betrokkenheid van auditors bij een cliënt. Dit in de gedachte dat een te nauwe betrokkenheid leidt tot 'verkleving' die de ethische houding en professioneel kritische instelling aantast. Een maximumtermijn aan de aanstelling zou de kwaliteit van externe audits bevorderen.

Bij de interne auditors komen we dit soort bepalingen in de IPPF niet tegen. Veelal ook niet in de interne audit charters. Het beroep van interne auditor kent op dit gebied – en vele andere terreinen – nog een hoge mate van zelfregulering. Kennelijk is er zoals bij de externe auditors geen urgentie om wel regelgeving die de kans op 'verkleving' verkleint te introduceren. Feit is wel dat er een grote hoeveelheid onderzoek aantoont dat de onafhankelijkheid van externe auditors wordt aangetast als de relatie langdurig is. Als er onderzoek naar zou worden gedaan bij interne auditors zal waarschijnlijk blijken dat dit ook geldt voor CAE's. Immers, de prikkels die beschreven zijn in het voorgaande maken duidelijk dat de CAE ethisch en professioneel kritisch moet zijn.

Bij ondernemingen van openbaar belang is bepaald dat – naast interne roulatie van partners – een accountantskantoor na maximaal tien jaar moet roteren. Maar wat zou nu de norm voor de CAE moeten zijn? Naar mijn idee zal dat van geval tot geval moeten worden beoordeeld. Mij lijkt dat voor tien jaar – als niet eerder – de vervanging van de CAE aan de orde is. Ofschoon niet alle CAE's hetzelfde zijn zal wetenschappelijke literatuur op het gebied van effectief leiderschap en 'social bonding'-theorieën aanknopingspunten kunnen bieden voor een dergelijke beoordeling.

Conclusie
Het voorgaande maakt duidelijk dat de ethische houding van de CAE van cruciaal belang is voor het goed functioneren van de interne auditafdeling in het governance spectrum. Daarbij speelt het risico op verkleving een factor van betekenis die mogelijk de ethische houding en de professioneel kritische instelling van de CAE bedreigt. En mogelijk zelfs de kwaliteit van de interne auditfunctie als geheel aantast. Het advies aan organisaties is dan ook om de houdbaarheid van de CAE expliciet intern periodiek op dit gebied te evalueren. In het gesprek tussen de C-suite en de auditcommissie moet dit een onderwerp van gesprek zijn. Ook is dit een thema dat aan de orde komt bij externe quality assurance reviews van de interne auditfunctie. <<

Dr. Bob van Kuijck RA RC is een onafhankelijk finance & auditprofessional die voor het IIA quality-assuranceopdrachten uitvoert.

Tekst Svetlana Vrubleuskaya MSc RO
Beeld M.T. Elgassier
Pexels

Is *angst* voor **cultuuraudits** terecht?

Cultuuraudit klinkt nog vaak te spannend in de oren van een auditee. Je krijgt als interne auditor al snel de tegenvraag: 'Wat is er mis met onze cultuur en het gedrag?' Waar komt deze angst vandaan en is het wel terecht?

Als ik in 'het jasje' van een interne auditor of een onderzoeker de organisatie binnenstap en vragen begin te stellen over organisatiecultuur en welk effect bepaalde culturele normen en waarden hebben op het gedrag van medewerkers, zijn mensen minder bereid om met mij te praten. Dit in tegenstelling tot meer operationele onderwerpen, zoals standaardprocessen van inkoop, verkoop en voorraden. Deze terughoudende of voorzichtige houding van een auditee riep bij mij de volgende vraag op: in hoeverre heerst bij organisaties angst voor audits naar cultuur en gedrag en is dit wel terecht?

Observaties

In dit artikel deel ik een aantal observaties die ik bij de beantwoording van deze vraag ben tegengekomen. Deze observaties heb ik geformuleerd op basis van gesprekken met meerdere interne auditors, riskmanagers en compliance officers, werkzaam bij diverse organisaties. Deze gesprekken gingen niet over het belang van 'cultuuraudits', dat is over het algemeen wel bekend en onderkend in de interne auditwereld. Het ging juist over het 'hoe' en de angst vanuit de organisatie om dit type onderzoeken uit te kunnen voeren.

Het is van belang om voor de uiteenzetting van deze observaties en de beschouwing daarop uiteenzet, eerst kort bij de begrippen van 'cultuur' en 'gedrag' stil te staan en toe te lichten wat de verbanden tussen beide begrippen zijn.

Breed begrip
De focus in dit artikel ligt op de organisatiecultuur. Als ik het met mijn netwerk van interne auditors heb over cultuur, kom je al snel tot de conclusie dat het een breed omvattend begrip is. In het rapport dat Chartered Institute of Internal Auditor (CIIA, 2022) over het belang van cultuuraudits in post-COVID-tijd, wordt organisatiecultuur als volgt omschreven: '…defined as being the shared attitudes, behaviours, principles, and values that drive action and purpose within an organisation and its people' … 'the way things are done around here'.

Aangeleerd gedrag
Antropologen en organisatiepsychologen zien organisatiecultuur als aangeleerd gedrag. Organisatiecultuur kent ook de definitie van 'shared meaning and learned behaviour'. Organisatiecultuur zou dan gaan over hoe medewerkers hun dagelijkse werkelijkheid percipiëren en welke betekenis ze daaraan geven. Het gedrag van deze medewerkers is dan een 'logisch' gevolg van deze percepties en betekenissen. Hieruit blijkt dat de cultuur en daarmee het gedrag niet statisch is. Beide kunnen in de loop van de tijd veranderen door nieuwe inzichten en nieuwe ervaringen.

Antropologen stellen dat een cultuurverandering zonder gedragsverandering niet mogelijk is. Als interne auditor willen we juist het gedrag aanpakken, dus de voorgaande stelling draai ik graag om: gedragsverandering is niet mogelijk zonder een cultuurverandering. Toch zien we juist die veranderingen vaak niet zo zitten.

Angst voor cultuurverandering is niet zo gek
We vinden stabiliteit erg fijn, maar dromen vaak van uitdagingen en nieuwe ervaringen. Het onbekende verkennen hoort bij onze nieuwsgierige en ontdekkende aard. De angst die gepaard gaat met de veranderingen is voor ieder van ons herkenbaar. Het is alleen niet de verandering zelf waar we angstig voor zijn, maar we ervaren angst om het bekende te verlaten en om het niet weten wat de verandering precies gaat brengen.

Als een interne auditfunctie (IAF) een auditee informeert over een audit naar een inkoopproces, weet een auditee eigenlijk al dat na het bespreken van het rapport hoogstwaarschijnlijk een aantal verbeteracties doorgevoerd moeten worden. De verandering is al een feit, en uit mijn ervaring blijkt dat een auditee zelfs al het vermoeden heeft welke aanbevelingen in het rapport gaan komen te staan.

Als een IAF met een cultuuraudit aankomt, bestaat bij een auditee ook hier het vermoeden dat veranderingen eraan zitten te komen. Toch is de angst, zoals blijkt uit de gesprekken, hier groter omdat deze veranderingen niet zo makkelijk te koppelen zijn aan concrete processtappen. Organisatiecultuur is zoals eerder omschreven een breed omvattend begrip dat geen begin of eind kent, zoals een inkoopproces. Een auditee ervaart angst voor het 'onbekende' dat dit begrip met zich meebrengt.

Begin klein en ga zeker niet met een uithangbord in de organisatie rondlopen dat jij met cultuuraudits 'iets bijzonders' gaat doen, want in werkelijkheid doe je gewoon je werk

Verschil tussen cultuuraudits en audits met de focus op cultuur en gedrag
Dat de organisatiecultuur een plek moet krijgen in de auditwerkzaamheden is een feit dat de meeste interne auditors niet betwisten. Wanneer je internal auditors de vraag stelt waarom in reguliere audits nog weinig aandacht wordt besteed aan cultuur en gedrag, komt het antwoord vaak op het volgende neer: het kost nog te veel energie om uit te moeten leggen dat auditors vaardig genoeg zijn om dit soort audits uit te voeren. Een aantal gesprekspartners gaf me daarbij aan dat het bestuur en audit committee nog te veel vraagtekens plaatsen bij de onderliggende onderzoeksmethode.

De praktijk van IAF's laat zeker zien dat je bij dit soort audits uitvoerig stil moet staan bij de methodologische verantwoording, maar ik ben van mening dat je als interne auditor niet de nadruk moet leggen dat je 'iets bijzonders' gaat doen. Je gaat namelijk naast de harde aspecten de zachte (culturele) aspecten meenemen als object van het onderzoek. Het meenemen van deze culturele risico's is absoluut uit te leggen. Het onderzoek van *Risk in Focus* (2022) laat zien dat organisatiecultuur als aandachtsgebied van internal audit een substantiële stijging heeft doorgemaakt ten opzichte van het voorgaande jaar. In plaats van 20% vindt nu 27% van de CAE's dit een Top-5-risico voor de organisatie. Maar hoe leg je dat uit aan de organisatie? Een voorbeeld uit mijn praktijk.

Verborgen cultuuraudits
Ik werk momenteel parttime voor de afdeling Concern Auditing (CA) van de gemeente Rotterdam. Ons team heeft als motto: 'Audits die leiden tot verbetering'. Daarmee impliceren we dat de audits die we uitvoeren een toegevoegde waarde leveren. Deze waarde uit zich in verbetering. En elke verbetering is al een verandering op zich, op kleine of grote schaal, afhankelijk van het onderwerp. We stappen bij de auditee niet naar binnen met de boodschap dat we daar 'de boel komen veranderen'.

Onze boodschap is dat de uitkomsten van audits de organisatie handvatten biedt voor het verbeteren van het functioneren van de organisatie en daarmee mogelijk ook van de medewerkers. Gedrag is immers het resultaat van culturele normen en waarden in combinatie met de vastgestelde systemen (beleid, protocollen, et cetera) in een organisatie. We ontkomen er dus niet aan om in de audits naar de culturele aspecten van de auditee te kijken. De vraag over hoe wij het als auditors doen, wordt niet altijd gesteld.

Ik moet hierbij wel opmerken dat het bij CA helpt dat ongeveer de helft van audits die we uitvoeren op verzoek zijn en dus geen onderdeel uitmaken van het vastgestelde auditprogramma. De stap waarin we uitleggen waarom deze audit noodzakelijk is, is in deze gevallen overbodig.

Gedragsbeïnvloedende factoren
Mijn boodschap is dat de audits naar cultuur en gedrag geen op zichzelf staande audits hoeven te zijn. Je hebt als auditor de taak om in de reguliere audits inzichtelijk te maken aan welke knoppen de auditee zou kunnen draaien om de eigen processen te optimaliseren. Die knoppen zijn gedragsbeïnvloedende factoren. Deze factoren zijn vaak verborgen in de patronen van de organisatiecultuur. Denk aan de acht soft controls van het model ontwikkeld door Muel Kaptein. Dit model helpt een auditor om aan de hand van deze acht elementen te onderzoeken waar de aandachtspunten liggen als het gaat om culturele aspecten. Zo zijn er uiteraard ook andere modellen en benaderingen die handvatten kunnen bieden.

Onderzoek specifieke regeling
Graag deel ik nog één sprekend praktijkvoorbeeld. Ik was als externe onderzoeker gevraagd om een evaluerend onderzoek uit te voeren naar de implementatie van een specifieke regeling. Het ging om een organisatie die vanuit diverse regio's opereert. De aanleiding voor dit onderzoek was dat het management signalen had gekregen dat regio's al jaren op eigen wijze invulling gaven aan de betreffende regeling, wat ten koste ging van de eenduidigheid van de uitvoering van beleid.

In eerste instantie lijkt dit onderzoek de kenmerken te hebben van een toetsend onderzoek. Je hebt normen, vastgelegd in deze regeling (de SOLL-positie), en je hebt de praktijk (de IST-positie). De vraag luidt: wat zijn de verschillen tussen de SOLL- en de IST-positie? Al gauw kom je er als interne auditor, of in dit geval als onderzoeker, achter dat de dieperliggende waaromvraag leidt naar de culturele aspecten van de regio's in scope. Waarom heeft regio A voor deze specifieke regeling toch een andere invulling, of wijkt het zoveel af van de invulling van regio B? Culturele aspecten als leiderschap, samenwerking en zelfsturing kwamen al snel aan bod tijdens de eerste voorbereidende gesprekken van dit onderzoek. Het toetsend onderzoek had een beschrijvend karakter gekregen, waarbij de cultuur en zeker het gedrag, van de medewerkers centraal zijn komen te staan.

Conclusie
Ik heb nog geen eenduidig antwoord op de vraag: in hoeverre heerst bij organisaties angst voor audits naar cultuur en gedrag en is dat wel terecht? De onzekerheid en voorzichtigheid voor dit type audits is wel voelbaar en aanwezig bij interne auditors, onderzoekers en interne opdrachtgevers. Aan de ene kant terecht, omdat verandering van cultuur voelt als iets ongrijpbaars. Aan de andere kant hoeft een audit met de focus op cultuur en gedrag niet als iets groots of nieuws te worden gebracht.

Op basis van mijn ervaring en gesprekken die ik hierover heb gevoerd, kan ik stellen dat interne auditors geen behoefte hebben aan uitleg over wát de toegevoegde waarde is om culturele of gedragsaspecten in reguliere audits mee te nemen. Interne auditors stellen vooral de vragen: 'Hoe neem ik deze aspecten mee in mijn audits?, 'Hoe overtuig ik de opdrachtgever dat ik over de vaardigheden beschik om gesprekken over cultuur en gedrag te voeren?', en 'Hoe rapporteer ik?' Er is dus meer behoefte aan een praktische handreiking. Mijn advies is: begin klein en ga zeker niet met een uithangbord in de organisatie rondlopen dat jij met cultuuraudits 'iets bijzonders' gaat doen, want in werkelijkheid doe je gewoon je werk. In de adviezen over noodzakelijke verbeteringen kan een interne auditor of onderzoeker namelijk niet voorbij de organisatiecultuur. <<

Svetlana Vrubleuskaya MSc RO is zelfstandige op het gebied van auditeren en onderzoeken naar cultuur en gedrag. Daarnaast werkt ze als auditor bij de gemeente Rotterdam waar zij audits continu vanuit de 'zachte aspecten' voorbereidt en uitvoert.

Tekst Nathalie Voortman MBA
Prof.dr. Ronald Jeurissen
Beeld Tara Winstead
Pexels

Audit van *integriteitscultuur* bij fusies en overnames

Fusies en overnames pakken niet altijd goed uit: beoogde synergievoordelen worden niet behaald en aandeelhouderswaarde wordt niet of onvoldoende gecreëerd. Soms is onvoldoende oog voor integriteit in de organisatiecultuur van de over te nemen onderneming (de target) de oorzaak.

Aandacht voor de integriteitscultuur van de target draagt bij aan het creëren van waarde voorafgaand, tijdens en ná de fusie of overname

Een integere organisatiecultuur is een effectieve internal-controlmaatregel. Deze helpt organisaties bij het realiseren van de doelstellingen en is onlosmakelijk verbonden aan risicobeheersing. Integriteit is een meetbare kritische succesfactor voor de waardecreatie van organisaties. Internal audit kan bijdragen aan de kans dat fusies en overnames slagen door de integriteitscultuur van targets te onderzoeken, gericht op het verder ontwikkelen van de onderneming ná de transactie. Hiervoor bestaan wetenschappelijk onderbouwde meet- en ontwikkelinstrumenten.

Weinig aandacht voor integriteitscultuur
Je zou verwachten dat integriteit dus een belangrijk onderdeel is bij de due diligence in het kader van fusies en overnames. Dit is echter niet het geval. Waarom niet? Onderzoek van Nyenrode Business Universiteit laat zien dat private-equitypartijen die betrokken zijn bij fusies en overnames zich enerzijds wel bewust zijn van het belang van aandacht voor integriteitsrisico's voor de huidige en toekomstige ondernemingswaarde.

De verwachting is dat transacties verbeteren door de integriteitscultuur van de target te onderzoeken. Anderzijds heeft men toch moeite om de integriteitscultuur operationeel te betrekken in de due diligence van targets. Ook na het afronden van het fusie- of overnametraject lijkt hier onvoldoende aandacht voor te zijn. Een drietal redenen hiervoor kwam uit het onderzoek naar voren.

1 – Integriteit is ongrijpbaar en complex
De belangrijkste reden voor het niet toepassen van systematische aandacht voor integriteitscultuur is dat men niet weet hoe integriteit te onderzoeken en bespreekbaar te maken. Zoals een respondent zei: 'Je kunt ook niet vragen: ben je integer?' Integriteit wordt gezien als een materie die niet meetbaar, moeilijk te operationaliseren en bovendien subjectief is. Daardoor vindt men het onderzoeken van integriteitscultuur moeilijk in de praktijk te brengen en gebeurt het dus niet. Ondanks het erkende belang ervan. Over duidelijke integriteitskwesties is iedereen het wel eens, maar in het grijze gebied vindt men integriteit een ongrijpbare materie.

2 – Men verwacht dat het veel moeite kost
De tweede reden van het uitblijven van expliciet integriteitsonderzoek is de verwachting dat het erg veel werk is. Een respondent: 'Integriteitscultuuronderzoek vraagt extra inspanning: het is een breed gebied, het is niet tastbaar, zoals financials'. De respondenten ervaren een hoge mate van inspanning voor het doen van integriteitscultuuronderzoek.

De verwachte moeite die geassocieerd wordt met het doen van een dergelijk onderzoek wordt veroorzaakt doordat men onvoldoende begrip heeft hoe integriteit te duiden. Als je iets niet als dusdanig herkent en niet kunt meten, kun je je geen beeld vormen van de huidige cultuur en niet sturen op mogelijke verbeteringen. En zo blijft de systematische aandacht voor integriteitscultuur op een laag pitje staan.

3 – Lage inpasbaarheid door gebrek aan bewegingsvrijheid
Het Nyenrode-onderzoek brengt ook aan het licht dat de fusie- en overnamesector het gebrek aan bewegingsvrijheid in de werkwijze zoals controlled auctions, het gebruik van virtuele datarooms en het delicate karakter van de voorgenomen transactie, als belemmering ziet om een expliciet onderzoek naar de integriteitscultuur te doen. Als alternatief worden in een fusie- of overnametraject de intuïtieve voelsprieten ingezet en wordt er op een impliciete, subjectieve en indirecte manier onderzoek naar de integriteitscultuur gedaan.

Door het aanvoelen van de integriteitscultuur via het beluisteren van het topmanagement tot het raadplegen van openbare bronnen voor background checks probeert men een beeld te krijgen van de integriteitscultuur. Of men gaat totaal voorbij aan de aandacht voor de integriteitscultuur van de target. Dit is helaas een gemiste kans, aangezien bij een impliciete manier van onderzoek het ontbreekt aan een betrouwbare en valide meting, waardoor het onderzoeken van de integriteitscultuur niet mogelijk is.

Integriteitscultuur is te onderzoeken
Het impliciete karakter van het in kaart brengen ligt niet in lijn met de genomen zorgvuldigheid in het expliciet onderzoeken van de financiële, operationele, juridische en strategische risico's.

Het is ook helemaal niet nodig om onderzoek naar de integriteitscultuur toe te vertrouwen aan impliciete en intuïtieve bevindingen. De integriteitscultuur is juist heel goed te meten en vormt een betrouwbare en belangrijke voorspeller van het al of niet integer handelen binnen de organisatie. Dat is uitvoerig aangetoond in het internationaal vooraanstaande onderzoek van Nederlandse wetenschappers als Ellemers, van der Toorn, Paunov & van Leeuwen (2019), Kaptein, Rozekrans & de Groot (2005), Kaptein (2012), en Zaal (2013).

Gebrek aan aandacht voor integriteit vergroot het risico op fraude en het weglekken van waarde

Het Nyenrode-onderzoek toont nu aan dat er in de fusie- en overnamesector behoefte is aan een praktisch inzetbaar instrument dat de integriteitscultuur kan meten. Dergelijke instrumenten bestaan. Een voorbeeld is de Belevingsmonitor Integriteit, onderdeel van een ontwikkelmodel voor organisatie-integriteit genaamd Stimuleringskader Integere Organisatie (SIO). De Belevingsmonitor Integriteit wordt al door veel organisaties in de profit- en non-profitsectoren uitgevoerd.

Het meetinstrument brengt de perceptie van de medewerkers in kaart aan de hand van kenmerken die onder meer van belang zijn voor het meten van de ontwikkeling van de integriteitscultuur. De cultuur wordt bepaald door (direct) leidinggevenden. Een voorbeeld van een concrete stelling die aan medewerkers wordt voorgelegd is 'in de organisatie houden mensen zich aan gemaakte afspraken' en aanvullend wordt gevraagd naar de gepercipieerde frequenties van een aantal verschillende integriteitsschendingen gerelateerd aan verschillende stakeholders zoals collega's, toezichthoudende instanties en externe partijen.

Dit meetinstrument kan in de pre-acquisitiefase door de kopende partij als expliciet onderzoeksinstrument ingezet worden om de gepercipieerde sterkten (kansen) en zwakten (risico's) in de integriteitscultuur te identificeren. Het meten van de reflectie van de individuele beleving levert een beeld op dat de werkelijkheid benadert. Organisaties hechten belang aan dit soort onderzoeken om zo inzage te krijgen, dit levert belangrijke informatie op.

Voorkomen van weglekken van waarde na de overname
Een meetinstrument waarmee de integriteitscultuur wordt gediagnostiseerd geeft, zoals eerder beschreven, een vollediger beeld van de target voordat de transactie plaatsvindt, én biedt ook handvatten hoe te handelen na de transactie. Bijvoorbeeld in de beheerfase. In deze post-acquisitiefase worden de bouwstenen gelegd voor de strategische waardecreatie.

De eerste 100 dagen na de transactie maken deel uit van deze beheerfase. Het zogeheten '100 dagen plan', staat in het teken van de post due diligence issues en het creëren van operationele rust (zoals het behouden van de belangrijkste klanten en belangrijkste medewerkers) en het minimaliseren van het weglekken van waarde. Een uitgelezen kans om integriteitsrisico's te identificeren door het diagnosticeren van de integriteitscultuur, mocht dit niet expliciet gedaan zijn tijdens de due diligence.

En om deze risico's te reduceren door als internal auditor de voorbeeldrol te pakken, te fungeren als het morele bewustzijn van de onderneming, deze te challengen en handvatten voor interventies ter stimulering van de integriteitscultuur te bieden. Hierbij kan gedacht worden aan het verstevigen van management control door een integrale integriteitsaanpak zoals de integratie van integriteitsbevorderende procedures en maatregelen in het hr-beleid. En inzicht geven en bewustwording bevorderen de wijze waarop de tone at the top door medewerkers wordt beleefd.

Goed onderbouwde diagnose
Aandacht voor de integriteitscultuur van de target draagt bij aan het creëren van waarde voorafgaand, tijdens en na de fusie of overname. Een grondige en wetenschappelijk goed onderbouwde diagnose van de integriteitscultuur mag bij een fusie- en overname niet ontbreken. Het identificeren van integriteitsrisico's in de cultuur van de target wordt bovendien binnen het ESG-beleid onder het thema governance geadresseerd. Interne audit, mits goed geschoold in het management van integriteit, is de aangewezen functie om dit onderzoek uit te voeren. De rol van de ethics and integrity officer is gericht op het opzetten en coördineren van het integriteitsmanagement. De interne auditfunctie verschaft assurance en advies op dit punt.

Het wegvegen van de blinde vlek die men beleeft rondom integriteit, is een stap die de auditor kan maken door het inzetten van een instrument om de integriteitscultuur meetbaar en zo inzichtelijk te maken. Op deze manier levert de auditor inzicht in de zwakke en sterke punten in de organisatiecultuur en is de auditor voor de organisatie van toegevoegde waarde. Aan deze inzichten wordt samen met de eerste lijn een juiste interpretatie gegeven om een juiste vertaalslag te kunnen maken naar de praktijk. Samenspel met een ethics en integrity officer voor de coördinatie, borging, verankering en continue verbetering is hierbij cruciaal.

Aanbevelingen voor de internal auditor

De resultaten van het Nyenrode-onderzoek pleiten voor het doen van expliciet integriteitscultuuronderzoek, als onderdeel van de due diligence rondom de transactie. Voorafgaand, tijdens en na de transactie ligt hier een schone taak voor de internal auditor om hier zijn rol in te pakken. Het advies is het hoofd bieden aan de ervaren belemmeringen zoals hiervoor opgesomd. Een stappenplan helpt hierbij.

Stap 1 – Maak integriteit 'grijpbaar en begrijpbaar' door te werken aan begripsvorming en bewustwording, het inzetten van meetinstrumenten en te werken aan bewustwording door actualiteiten zoals 'het debacle van The Voice' in de organisatie in openheid organisatiebreed te bespreken: zie jij wat er speelt? Wat kunnen wij als organisatie hiervan leren? Zo zijn er 'handen en voeten' te geven aan integriteit, gedrag en cultuur.

Stap 2 – Doordat integriteit grijpbaarder wordt, zal de verwachting dat het moeite kost ook afnemen. Reductie van de complexiteit rondom het begrip integriteit bevordert de intentie tot het doen van integriteitscultuuronderzoek.

Stap 3 – Het afnemen van de verwachting dat het moeite en inspanning kost, zal de inpasbaarheid van het doen van expliciet integriteitscultuuronderzoek bevorderen. De beperkte tijd en toegang tot de target en informatie en ook de vertrouwelijkheid van de voorgenomen transactie worden minder als belemmerend gezien om aandacht te geven aan de zachte aspecten in de M&A. Denk bijvoorbeeld aan het doen van een nulmeting 'belevingsonderzoek' via een online survey onder medewerkers bij het verkoopklaar maken, voorafgaand aan de transactie of in de beheerfase, het doen van een (self) assessment tone at the top onder medewerkers, het ondernemingsbestuur en andere stakeholders, en het signaleren van tekortkomingen in de governance, zoals het ontbreken van een heldere visie op integriteit, basiswaarden en een gedragscode. De aanwezige maatregelen in de structuur en cultuur versterken elkaar. <<

Literatuur

- Psychology of Morality: A Review and Analysis of Empirical Studies Published From 1940 Through 2017', *Personality and Social Psychology Review*, pp. 1-35, 2019.
- Kaptein, M., 'De integriteit van organisaties: 7 handvatten uit de sociaalpsychologie', in *Integriteit Jaarboek* (Zweegers, M. en E. Karssing – red.), BIOS, Bureau Integriteitsbevordering Openbare Sector, pp. 34-41, 2012.
- Kaptein, M., Rozekrans, R. en R. de Groot, 'Integriteitsklimaat als auditobject', *Maandblad voor Accountancy en Bedrijfseconomie*, vol.79, no. 10, pp. 466-474, 2005.
- Zaal, R., *Manieren van bankieren. Over bankiers, bonussen en effectief beinvloeden van onethisch gedrag* (1e ed.), Koninklijke Van Gorcum, 2013.

Nathalie Voortman MBA is consultant/interim-manager via JUST business consulting, gericht op duurzame organisatieontwikkeling. nathalie@just-bc.nl

Prof.dr. Ronald Jeurissen is als hoogleraar bedrijfsethiek verbonden aan Nyenrode Business Universiteit. r.jeurissen@nyenrode.nl

Tekst Liane Lambert Mendez-van Eerde MSc RO
Beeld Towfiqu Barbhuiya

Jan Rodenburg: *"Zoek elkaar op en deel je uitdagingen"*

Jan Rodenburg, hoofd Interne Audit bij Saxo Bank MER, aan het woord over het werken in en met een kleine auditdienst, ondernemen, bouwen, ontwikkelen en meeademen met de organisatie.

Kunt u iets over Saxo Bank en BinckBank vertellen?
"Ik ben twaalf jaar geleden begonnen bij BinckBank. In 2018 is BinckBank overgenomen door Saxo Bank. De afgelopen jaren waren we dus flink bezig met de integratie van BinckBank in Saxo Bank. We opereren nu naar buiten als Saxobank. Alhoewel onze legal entity nog Binckbank is en wij hierop ook de bankvergunning hebben."

Hoe ziet de auditafdeling eruit?
"Onze auditafdeling bestaat uit vier auditors en wij auditen de Mid European Region (MER). Naast deze functie kent Saxo Bank nog een auditfunctie: 'Group Internal Audit', die bestaat uit achttien auditors op het hoofdkantoor in Kopenhagen. Omdat wij een aparte bankvergunning hebben, dienen wij zelfstandig audits uit te voeren. We hanteren wel dezelfde templates en procedures, maar we stellen onafhankelijk onze auditplanning en rapportages op."

Brengt zo'n kleine auditfunctie uitdagingen met zich mee?
"Dat ervaar ik niet zo. We zijn bovendien sinds 2010 al drie keer succesvol gecertificeerd door het IIA. Daarnaast kunnen we ook, als het nodig is, expertise gebruiken vanuit Group Internal Audit. We maken daarom eigenlijk ook nooit gebruik van externe inhuur. Mijn eigen auditors zijn allround, ik heb mensen nodig die multidisciplinair kunnen opereren. Iedereen moet een groot deel van de audits uit kunnen voeren in zo'n klein team. Het allerbelangrijkste voor een auditfunctie is dat je goed gepositioneerd bent. Bij een bank is dat goed gewaarborgd in verband met wet- en regelgeving. Ik rapporteer aan de voorzitter van het audit committee en wij zijn gepositioneerd onder de raad van commissarissen."

Welk type onderzoeken voert de IAF uit?
"Wij doen zowel procesgerichte audits, IT-audits als audits op functies. Bij functies kun je denken aan tweedelijnsfuncties zoals finance, risk management, compliance, hr en legal. Bij grote projecten voeren wij ook audits uit, bijvoorbeeld naar aanleiding van implementaties, verandering in wet- en regelgeving en verbetertrajecten."

Hoe voegen jullie waarde toe als auditfunctie?
"Wij verschaffen inzichten en zijn gericht op het continu verbeteren van de organisatie. Onze bevindingen worden echt op waarde geschat. We hebben een kritisch opvolgingsproces van bevindingen. We volgen deze maandelijks op met de raad van bestuur en bovendien worden deze meegenomen in de beoordeling van bestuursleden. Belangrijk is dat je de hoofd- van de bijzaken kunt onderscheiden. Je dient jezelf te vraag te stellen: waar ligt men nu echt wakker van? Alleen dan kun je je kernboodschap goed overbrengen en hiermee impact creëren. Al het andere leidt af van de kernboodschap."

Denkt u dat er een houdbaarheidsdatum aan een hoofd Interne Audit zit?
"Ik denk dat er zeker een bepaalde houdbaarheid aan een hoofd Interne Audit zit. Hoewel het erg van de omgeving af hangt. Ik werk natuurlijk al bijna twaalf jaar voor dezelfde organisatie, maar je kunt wel zeggen dat ik sinds de overname in 2018 voor een ander type organisatie werk. We zijn nu onderdeel van een groter concern. De BinckBank van vroeger is niet meer de BinckBank van nu. De omgeving, de mensen en de board zijn deels gewijzigd. Ik heb daarom met andere mensen en situaties te maken, met name de relatie met het hoofdkantoor van Saxo Bank is een volledig nieuw element."

Maar als een organisatie stabiel is?
"Ik kan me voorstellen dat als een organisatie stabiel blijft je na een jaar of vijf, zes wel klaar bent. Dan ben je onderdeel van de organisatie geworden. Je kunt zeggen dat je dan het merendeel hebt gezien en vaker dezelfde issues besproken hebt. Het wordt dan steeds lastiger om bepaalde thema's wederom aan te snijden. Het toevoegen van waarde wordt dan minder makkelijk."

Wat is uw belangrijkste les geweest in deze twaalf jaar?
"Je groeit als mens. Ik ben relaties steeds belangrijker gaan vinden. Een auditor wil graag onderzoeken, analytische vaardigheden inzetten, aan waarheidsvinding doen en zijn punt maken. Je kunt wel gelijk hebben, maar gelijk krijgen in de organisatie is heel wat anders. Ik ben gaandeweg een veel groter belang gaan hechten aan de menselijke relaties en geleidelijk aan meer gaan leren om ook gelijk te krijgen. Ik heb ook veel geleerd door met vakgenoten buiten de organisatie te spreken, bijvoorbeeld binnen het IIA (PAS) of bij interbancair overleg. Over het algemeen denk ik dat we nog meer kunnen samenwerken met auditfuncties van andere organisaties, bijvoorbeeld in dezelfde branche. Ook kleine auditfuncties kunnen hier baat bij hebben. Het kan soms best eenzaam zijn als hoofd Interne Audit, dus zoek elkaar op en deel je uitdagingen met elkaar."

Blijft u voor altijd in de financiële sector werken?
"Ik denk dat banken een goede leerschool zijn waar alle elementen voorkomen die een rol spelen binnen audit. De bancaire sector is flink gereguleerd en daarom zijn processen veelal eerder volwassen dan in andere branches. Een belangrijk element voor mij is ook het ondernemen, bouwen en ontwikkelen binnen een organisatie. Dat is juist het leuke van deze organisatie, er heerst nog echt een wil om te ondernemen."

Hebt u een ondernemende rol als auditor?
"Niet echt hé, zou je zeggen. Maar ik mag zeker als hoofd meedenken en ik mag ook wat van de strategie vinden. Of ik ooit het auditberoep loslaat? Ik weet het niet. Ik kom uit een ondernemersgezin, maar ik ben geen visionair. In een bestuur zou ik waarschijnlijk eerder de COO zijn. Misschien in de toekomst. Je weet niet wat er op je pad komt. Ik had vroeger ook nooit gedacht dat ik interne auditor zou worden. Ik had er überhaupt nog nooit van gehoord tijdens mijn studietijd. Toch heb ik mijn plekje wel gevonden in deze auditfunctie."

Wat zijn uw ambities voor de auditfunctie?
"Ik wil voornamelijk blijven meeademen met de organisatie en die zaken auditen die er echt toe doen. En erg belangrijk voor mij is het bieden van een ontwikkelpad aan de mensen in mijn team. Het bieden van kansen, het verder opleiden en de mogelijkheid geven om een nog betere auditor te worden dan ze al zijn." <<

Over...

Jan Rodenburg is sinds augustus 2021 hoofd Interne Audit bij Saxo Bank MER (voorheen Binck Bank) waar hij al bijna twaalf jaar werkt. Hij behaalde zijn RE- en RO-titel en volgde daarna een executive MBA Business en IT. Daarnaast is hij actief lid van de PAS Commissie van het IIA.

IIA CONGRES 2022
MOED & VEERKRACHT


WAT IS JOUW MOMENT?

Tekst Lisanne Frijling MSc RO
Beeld Adobe Stock

Auditen met meer **toegevoegde waarde** ***door effectieve*** **communicatie**

Effectieve communicatie door de internal auditor speelt een belangrijke rol in de acceptatie van de auditresultaten. De mate van acceptatie en het opvolgen van aanbevelingen heeft een direct verband met de effectiviteit van de internal auditfunctie. Effectieve communicatie door interne auditors is essentieel voor de kwaliteit van internal audits en dus voor de kwaliteit van internal auditfuncties.

In de rubriek De afgestudeerde presenteert een recent afgestudeerde van de post-initiële RO-opleidingen in Amsterdam of Rotterdam zijn of haar onderzoeksresultaten en geeft hierop een reflectie.

Signalen van slecht nieuws, zoals de bevindingen van de internal auditor, kunnen worden afgezwakt of zelfs niet worden gehoord door leidinggevenden binnen organisaties. Dit fenomeen wordt ook wel het 'deaf effect' genoemd. Het deaf effect vermindert de acceptatie van de auditresultaten. De wetenschap is duidelijk over de oplossing voor het deaf effect: creëer een samenwerkend partnerschap door middel van effectieve communicatie.

Effectieve communicatie
Vaak wordt door internal auditors een en dezelfde vorm toegepast voor het presenteren van de auditresultaten, namelijk het stellen van normen en vervolgens uitsluitend de tekortkomingen ten opzichte van deze norm melden. Echter, er zijn diverse wetenschappelijke methoden ontwikkeld waarin wordt uitgelegd dat de effectiviteit van communicatie toeneemt wanneer er rekening wordt gehouden met de persoonlijkheidsvoorkeuren van de ontvanger. De bron van de communicatie en de manier waarop het nieuws wordt gepresenteerd zijn namelijk bepalend voor de aandacht die de ontvanger hieraan zal geven.

- **Vurig rood** – extravert denken. De extraverte denker werkt resultaat- en actiegericht. Hij kan overtuigend zijn in zijn aanpak en is in staat het team richting te geven.
- **Stralend geel** – extravert voelen. De extraverte voeler heeft aanleg voor creatief en interactief samenwerken. Hij wordt vaak gezien als inspirerend en is in staat het team te enthousiasmeren.
- **Zachtgroen** – introvert voelen. De introverte voeler heeft talent voor zorgvuldig en mensgericht werken. Hij richt zich op het belang van het hele team en kan hierdoor harmonie in de teamsfeer te brengen.

Communicatiestijlenmodel
Het communicatiestijlenmodel is gebaseerd op het social stylesmodel van Merril en Reed. Het adviesbureau GITP introduceerde het communicatiestijlenmodel. Dat is een

"Het is niet nodig dat vrouwen veranderen, maar mannen moeten wel beter leren luisteren naar wat vrouwen zeggen"

Onderzoek
Het doel van mijn onderzoek was om vast te stellen hoe de internal auditpraktijk effectiever kan communiceren en hoe de internal auditor zijn communicatie kan aanpassen aan de ontvanger. De centrale onderzoeksvraag hierbij was: hoe kunnen de persoonlijkheidsvoorkeuren van de ontvanger toegepast worden in de communicatie van internal auditresultaten om de acceptatie te verhogen?

Om deze vraag te beantwoorden is in dit onderzoek het insights discoverymodel gekoppeld aan het communicatiestijlenmodel. Het insights discoverymodel is van de organisatie Insights, die is gestart door vader en zoon Andi en Andy Lothian in 1993.

Insights discoverymodel
Het insights discoverymodel is gebaseerd op het werk van Carl Gustav Jung. Het doel van het model is mensen meer inzicht te geven in zichzelf en anderen. Het model toont persoonlijkheidsvoorkeuren aan de hand van vier kleuren:

- **Helderblauw** – introvert denken. De introverte denker is onderzoekend en accuraat. Hij kan objectief zijn en neemt weloverwogen beslissingen. In een team bewaakt de introverte denker de logica en de feiten in het werkproces.

praktisch toepasbaar model waarmee men de eigen communicatiestijl en die van anderen kan herkennen.

Het model bestaat uit twee elementaire gedragsdimensies, namelijk: 1) wijze van beïnvloeding (ruimte geven versus ruimte nemen), 2) openheid over gevoelens (inhouden versus uiten). Met deze twee assen zijn vervolgens vier verschillende communicatiestijlen te herkennen: 1) de beschouwende stijl, 2) de expressieve stijl, 3) de coöperatieve stijl en 4) de directieve stijl.

Op basis van de gemaakte koppeling tussen de vier voorkeurskleuren van het insights discoverymodel en de vier communicatiestijlen van het communicatiestijlenmodel, zijn vier verschillende auditresultaten geformuleerd. Tevens zijn vier stellingen geformuleerd over de communicatie gedurende het auditproces. Deze auditresultaten en stellingen zijn gebaseerd op een casus rondom de implementatie van een nieuw IT-systeem. Zie tabel 1 voor de formulering van de auditresultaten en de stellingen.

Vervolgens zijn surveys uitgezet bij zowel auditors als niet-auditors. Aangezien in dit onderzoek is gekeken naar psychologische processen, is de survey breed uitgezet. Door middel van de survey is de score per insights discoverykleur per respondent gemeten. Hierna is aan de hand van een case

Voorkeurs-kleur*	Effectieve communicatie**	Omschrijving auditresultaat	Omschrijving stelling
Blauw	Beschouwend	Er is een aanzienlijk risico dat het IT-systeem gaat falen, aangezien het systeem niet getest is. Bij andere bedrijven worden soortgelijke IT-systemen minstens x-aantal keren getest en wordt tevens een testbeleid voor continue monitoring en testwerk opgesteld. In de bijlage van dit rapport is een lijst opgenomen met daarin gedetailleerde voorbeelden van testprocedures die bij andere bedrijven worden gehanteerd. Tevens is in de bijlage een lijst opgenomen met risico's die ontstaan als u het IT-systeem niet laat testen.	Ik waardeer het als de internal auditor in zijn communicatie de details en feiten van zijn testwerk bespreekt. Daarnaast vind ik het van belang dat de internal auditor systematisch te werk gaat en heldere afspraken met mij maakt over de follow-upacties. Ik wil graag dat naar mijn ideeën wordt geluisterd.
Rood	Directief	Het IT-systeem is niet getest, dit betekent dat er een groot risico is dat het IT-systeem zal falen met als gevolg dat sommige operaties stopgezet moeten worden en het bedrijf omzet mist. Het is aan te raden het IT-systeem te testen, met als voordeel dat de kans op slagen en de toegevoegde waarde van het systeem toeneemt.	Ik wil geen details zien maar graag meteen horen wat ik moet doen om tot het gewenste resultaat te komen. Ik waardeer het als de bevinding en aanbeveling kort en bondig zijn geformuleerd. Ik wil graag dat de internal auditor de voor- en nadelen aantoont voor het wel of niet doorgaan met het IT-project.
Geel	Expressief	Ik heb geobserveerd dat uw projectteam bereid is om hard te werken en dat de doelstelling van het team is om succesvol te zijn. Echter, het IT-systeem is momenteel niet getest, waardoor er een groot risico ontstaat dat uw project en het IT-systeem zullen falen. Dit is niet in lijn met de doelen van het team. Het uitvoeren van testprocedures zal u helpen een competent IT-systeem te implementeren.	Ik wil niet te veel details zien, maar op grote lijnen inzicht krijgen in de tekortkomingen van het IT-project. Ik zou graag met de internal auditor in gesprek gaan over mijn ideeën en afwegingen voor het opvolgen van de aanbevelingen. Ik vind een goede, leuke en doelgerichte samenwerking erg belangrijk.
Groen	Coöperatief	Het belang dat het IT-systeem voor de deadline geïmplementeerd moet worden, wordt begrepen. Echter, er is een groot risico dat het IT-project kan falen aangezien het systeem niet getest is. Het gevolg hiervan is dat het bedrijf omzet mist en daardoor de medewerkerstevredenheid en de betrokkenheid afneemt. Als u besluit deze risico's aan te pakken dan werk ik graag met u samen om een geschikte partij te vinden die het IT-systeem voor u kan testen.	Ik wil graag gehoord worden en steun krijgen in mijn afwegingen rondom het voortzetten van het IT-project. Daarnaast wil ik samen met de internal auditor en het management de planning vastleggen voor het opvolgen van de aanbevelingen van de internal auditor. Ik waardeer een informele samenwerking.

Tabel 1. Formulering van de auditresultaten en de stellingen
(* Bron: Insights Discovery ** Bron: Désar, 2005)

Voorkeurskleur en communicatiestijl	Formulering auditresultaat/communicatie gedurende auditproces	Significant verband vastgesteld?
Blauw en beschouwende stijl	Formulering auditresultaat	Ja
Blauw en beschouwende stijl	Communicatie gedurende auditproces	Ja
Rood en directieve stijl	Formulering auditresultaat	Nee
Rood en directieve stijl	Communicatie gedurende auditproces	Ja
Geel en expressieve stijl	Formulering auditresultaat	Ja
Geel en expressieve stijl	Communicatie gedurende auditproces	Ja
Groen en coöperatieve stijl	Formulering auditresultaat	Nee
Groen en coöperatieve stijl	Communicatie gedurende auditproces	Nee

Tabel 2. Samenvatting resultaten van het onderzoek

Een coöperatieve communicatiestijl en dus empathie en een informele samenwerking met de internal auditor wordt van belang gevonden

getoetst welke van de vier formuleringen van het auditresultaat het meest geaccepteerd wordt door de respondent. Dezelfde vraag is daarna gesteld voor de vier verschillende stellingen over de communicatie tijdens het auditproces. Hierna zijn eventuele verbanden tussen de scores per insights discoverykleur en de keuze voor de formuleringen van auditresultaten en stellingen geanalyseerd.

Bewijs

In deze studie is bewijs gevonden dat wanneer de internal auditor in de communicatie van de auditresultaten en in de communicatie gedurende het auditproces rekening houdt met de persoonlijkheidsvoorkeuren van de ontvanger, de acceptatie van de auditresultaten wordt vergroot. Zie tabel 2 voor de samenvatting van de resultaten van het onderzoek.

Zoals in tabel 2 is weergegeven, blijkt uit de resultaten dat iemand met de voorkeurskleur blauw eerder geneigd is om de internal auditresultaten te accepteren als bij de formulering van de auditresultaten en gedurende het auditproces aan de communicatievereisten van de beschouwende stijl wordt voldaan.

Iemand met de voorkeurskleur rood is eerder geneigd om de internal auditresultaten te accepteren als gedurende het auditproces aan de communicatievereisten van de directieve stijl wordt voldaan. Er is echter geen verband gevonden tussen de directieve formulering van de auditresultaten en de acceptatie van iemand met de voorkeurskleur rood.

Iemand met voorkeurskleur geel is eerder geneigd om de internal auditresultaten te accepteren als bij de formulering van de auditresultaten en gedurende het auditproces aan de communicatievereisten van de expressieve stijl wordt voldaan.

In dit onderzoek is geen positief verband vastgesteld tussen de voorkeurskleur groen en de coöperatieve manier van communiceren gedurende het auditproces en in de formulering van de auditresultaten. Respondenten geven echter vaak de voorkeur aan de coöperatief geformuleerde auditresultaten en stelling. Op basis van deze resultaten kan gesteld worden dat een coöperatieve communicatiestijl en dus empathie en een informele samenwerking met de internal auditor van belang wordt gevonden.

Tevens is onderzocht of het geslacht van de ontvanger een rol speelt in de voorkeur voor een bepaalde communicatiestijl van de internal auditor. Hiervoor is enkel voor de expressieve communicatiestijl een significant verschil tussen mannen en vrouwen in de mate van acceptatie vastgesteld. Bij de overige formuleringen is geen verschil in de mate van acceptatie door mannen en vrouwen.

Praktische adviezen

Op basis van de resultaten van dit onderzoek zijn drie praktische adviezen tot stand gekomen voor de internal auditors.

1. Als internal auditors bij het formuleren van de auditbevindingen rekening houden met de persoonlijkheidsvoorkeuren van de ontvanger, kan de acceptatie en de effectiviteit van de internal audits toenemen. Dit is afhankelijk van de voorkeurskleur van de ontvanger en geldt voor de blauwe en de gele voorkeurskleur.

2. Als internal auditors in hun communicatie gedurende het auditproces rekening houden met de persoonlijkheidsvoorkeuren van de ontvanger, kan de acceptatie en de effectiviteit van de internal audits toenemen. Dit is afhankelijk van de voorkeurskleur van de ontvanger en geldt voor de blauwe, rode en gele voorkeurskleur.

3. Internal auditors hoeven in hun manier van communiceren gedurende het auditproces en in de manier van het formuleren van de auditbevindingen geen rekening te houden met het geslacht van de ontvanger. Enkel bij de gele voorkeurskleur is een verschil tussen de voorkeur van communicatie bij mannen en vrouwen.

Ter afsluiting

Dit onderzoek toont aan dat de effectiviteit van communicatie toeneemt wanneer er rekening wordt gehouden met de persoonlijkheidsvoorkeuren van de ontvanger. Daarom is het van belang dat internal auditors meer rekening houden met de psychologische omstandigheden van de ontvanger als persoon in de formuleringen van de auditresultaten en de communicatie gedurende het auditproces.

Communicatie van de internal auditor in relatie tot de acceptatie en de kwaliteit van de internal audits is nog niet vaak onderwerp geweest van onderzoeken. Het onderwerp rondom psychologische aspecten in de communicatie door de internal auditor verdient meer aandacht. <<

Lisanne Frijling is senior consultant binnen de afdeling Governance, Risk & Compliance Services bij KPMG. In mei 2021 studeerde zij af met haar onderzoek *Communicatie als middel voor het vergroten van de acceptatie van de internal auditresultaten* aan de executive master of internal auditopleiding aan de Universiteit van Amsterdam.

Tekst Sander Diks CIA
Beeld NFP Photography
Adobe Stock

Nicole den Hartigh: *"Liegen is noodzakelijke smeerolie in het sociale verkeer. Als je liegt maar je weet niet dat je liegt, dan lieg je overigens niet"*

Waarheidsvinders: **DOELGERICHT** en met open vizier

In hun knusse Zutphense kantoor voelt *Audit Magazine* Nicole den Hartigh en Xavier Zeilinga van denhartigh & partners aan de tand over liegen en bedriegen, desinformatie en de kunst van het waarheidsvinden.

Jullie noemen jezelf waarheidsvinders en 'profilers'. Wat maakt een goede waarheidsvinder?

Nicole den Hartigh (NdH): "Het begint allemaal met oprechte interesse voor de kwestie waarvoor je gevraagd wordt onderzoek naar te doen. Een waarheidsvinder is benieuwd naar de uitkomst van de te leggen puzzel, ongeacht de kleuren van de te leggen plaat. Die nieuwsgierigheid is een belangrijke eigenschap voor een waarheidsvinder. Onafhankelijkheid van geest en integriteit zijn daarnaast eigenschappen waar een professionele waarheidsvinder over moet beschikken. Met onafhankelijkheid van geest bedoelen we dat je de durf hebt om buiten de gebaande paden te zoeken naar antwoorden en in weer en wind een rechte rug toont."

Heeft een waarheidsvinder nog meer eigenschappen?

NdH: "Het is daarnaast heel erg belangrijk om zonder daderschapdenken een onderzoek te starten, je vooringenomenheid opzij te zetten en je bewust te zijn van je bias. Ook integer handelen, door je bijvoorbeeld niet te laten leiden door omzetdruk of een andere vorm van druk bij het accepteren van een opdracht, is van belang. De vrijheid om nee te zeggen tegen een opdracht, bijvoorbeeld als er vraagtekens bestaan bij het motief van de opdrachtgever, is een groot goed voor een waarheidsvinder."

En wat doet een profiler?

Xavier Zeilinga (XZ): "Om te begrijpen wat een profiler doet is het goed om eerst te kijken naar enkele verschillende profilingdisciplines die er bestaan. Profiling heeft zijn oorsprong in het werk van Darwin, die zich in de 19e eeuw bezighield met het leren lezen van gedrag van dieren op basis van nauwgezette observaties. Je zou hem een 'animal profiler' kunnen noemen. Jung en Freud waren in de 20e eeuw binnen de psychiatrie bekende 'human profilers' die de gedragingen van patiënten met psychische aandoeningen observeerden om in die tijd gepaste behandelingen te kunnen bepalen. Dr. Paul Ekman zette in de 20e eeuw het werk van Darwin voort en deed onderzoek naar emoties en gelaatsexpressies bij mensen. Hij ontdekte dat er zeven universele gelaatsexpressies bestaan zoals blijheid, angst en minachting. Inzichten die in belangrijke mate hebben bijgedragen aan het vakgebied van profiling."

Zijn er sinds die tijd nog ontwikkelingen?

XZ: "In de jaren zeventig ontwikkelde de FBI criminal profiling waarbij gedragingen van verkrachters en moordenaars door een eerste behavioral science unit in kaart werden gebracht. De Netflix-serie *Mindhunter* is hierop gebaseerd. De term seriemoordenaar is pas in 1974 binnen deze behavioral science unit ontstaan en bestaat dus nog niet eens zo lang.

Over

Nicole J. den Hartigh EMIA RO CPI CGBL RPP CPE CIS is directeur/eigenaar van denhartigh & partners bv | waarheidsvinders & profilers in Zutphen.

Xavier Y. Zeilinga RPP CPE CPI is als onderzoeker, gedragsdeskundige en trainer aan dit bureau verbonden. Samen met een team van professional partners geven zij met deskundigheid, plezier en enthousiasme invulling aan integriteitgerelateerd onderzoek, advies en training.

Xavier Zeilinga: "Ik vond het in het begin best lastig om mij te realiseren dat er iemand glashard tegen mij zat te liegen, zeker als ik het bewijs hiervan in mijn tas had zitten"

Sinds de jaren zeventig proberen overheden en veiligheidsdiensten in situaties van (mogelijke) dreiging, zoals een aanslag op een vliegveld, met 'predictive profiling' tijdig afwijkingen in gedrag – ten opzichte van een veronderstelde contextuele norm – te signaleren en daarop te anticiperen."

Hoe zetten jullie profiling in?

XZ: "Wij gebruiken de diverse profilingtechnieken bijvoorbeeld tijdens interviews, hoor en wederhoor. We beginnen altijd met het maken van een zogenoemde 'baseline'. Dat is het gedrag en de lichaamstaal van iemand in een (redelijk) ontspannen situatie. Zoals tijdens een gesprekje bij de koffie en voorafgaand aan het daadwerkelijke interview. Vervolgens gaan we het formele gesprek aan. Afwijkende gedragingen ten opzichte van die eerder gemaakte baseline kunnen weergaven zijn van spanning (stress of angst). Wij letten dus op lichaamstaal. In feite kijken we of iemand comfortabel overkomt of tekenen vertoont van discomfort."

Wat betekent dat dan? Dat iemand liegt?

NdH: "Getoonde stress of menselijke reacties daarop betekent niet per definitie dat iemand liegt. Maar het getoonde gedrag kan wel onthullen of iemand terughoudend is om het hele verhaal te vertellen, het te verdraaien of toch glashard te liegen. Het is voor ons dus zaak om te achterhalen wat precies de redenen zijn voor hetgeen we signaleren."

Hebt u een voorbeeld?

XZ: "Een goed voorbeeld is een gesprek dat we hadden met een meneer in het kader van een zogenaamde 'MeToo-zaak'. Op een zeker moment en na flink doorvragen van onze kant, schoot hij opeens zichtbaar verhit omhoog, waarbij zijn stoel omviel. Hij probeerde zich nog te herstellen door zijn jasje uit te doen maar het was overduidelijk een 'flight response'. Dit is een specifiek voorbeeld. Vaak zijn de signalen subtieler, maar als je weet waarop je moet letten, zijn ze niet minder zichtbaar. Ieder mens kan zijn voordeel doen met het leren lezen van gedrag en lichaamstaal om de betrouwbaarheid van de gesprekspartner te helpen beoordelen. Dat geldt zeker ook voor auditors."

Krijgen jullie te maken met desinformatie/fake news tijdens jullie onderzoeken?

NdH: "Zeker! Juist als er belangen op het spel staan, bijvoorbeeld omdat er sancties dreigen, zijn mensen bereid om niet geheel of geheel niet de waarheid te vertellen. Hele en halve leugens zijn natuurlijk de meest basale vorm van desinformatie. Als mensen stoute of foute dingen hebben gedaan, kunnen ze er baat bij hebben om weg te blijven bij de waarheid. We krijgen dus veel en vaak te maken met desinformatie tijdens de gesprekken die we in het kader van het onderzoek voeren."

Zijn het altijd leugens die iemand vertelt?

XZ: "Nee hoor. Een andere vorm van desinformatie waar wij in ons werk mee te maken krijgen, is het vertellen van een waarheid die in de betreffende context niet van belang is. Dit noemen we ook wel misleiding. Wat maakt het dat iemand jou specifiek iets vertelt? Wat maakt dat jij als auditor juist dát document krijgt aangereikt? Of dat een auditee je dat ene voorbeeld voorschotelt? Waarom gebeurt dat? Het helpt om als auditor vaak de 'waaromvraag' te stellen teneinde te achterhalen waarom juist jij bepaalde informatie krijgt aangereikt. En het helpt ook om door te vragen om erachter te komen wat de precieze intentie van de aangever hierbij is."

Hoe gaan jullie daar mee om?
NdH: "Wij doen, net als auditors, heel feitelijk werk. En we stellen ook, net als auditors, een toetsingskader of normenkader op om de door ons waargenomen werkelijkheid tegen af te zetten. Denk hierbij bijvoorbeeld aan een gedragscode of een beleidsnorm. We maken bij het verzamelen van informatie gebruik van meerdere bronnen, zoals 'logs' van verschillende gesprekken en documenten als e-mails en sms'jes. Ook zetten we bevindingen af tegen andere verkregen antwoorden of stukjes informatie om zodoende de betrouwbaarheid te duiden of discrepanties te signaleren."

Betrouwbaarheid duiden?
NdH: "Iemand kan bijvoorbeeld wel vertellen tijdens een gesprek dat hij niet op kantoor was op een specifiek moment, maar logboeken, lijstjes of andere vastleggingen kunnen andere informatie geven. En over deze discrepanties stellen we weer aanvullende vragen, bijvoorbeeld tijdens hoor en wederhoor. Op deze wijze proberen we de feiten en de eventuele toedracht bloot te leggen. Feiten en analyse zijn onlosmakelijk verbonden met onze benadering. Een feit is een reden van wetenschap en het product dat wij opleveren is daarmee dan ook een feiten- of toedrachtrapport."

Naïef zijn is dus geen optie
XZ: "Ik ben van nature een naïef persoon. Dat is in ons werk behulpzaam. Naïviteit heeft mijns inziens ten onrechte een negatieve connotatie gekregen. Naïviteit stelt je in staat om zaken onbevangen tegemoet te treden. Mijn uitgangspunt is dat ik ervan uitga dat iemand de waarheid spreekt. En zo ga ik ook met mensen in gesprek. Ik vond het in het begin best lastig om mij te realiseren dat er iemand glashard tegen mij zat te liegen, zeker als ik het bewijs hiervan in mijn tas had zitten. Een professionele houding is cruciaal als je geconfronteerd wordt met desinformatie, draaierij en met leugens. Je realiseren wat er gebeurt, het in de context kunnen zien en aanvullende vragen stellen. Bijvoorbeeld door zogenaamde 'gewetensvragen' te stellen. Bijvoorbeeld of de betreffende persoon bij zijn verklaring wil blijven of niet, omdat er aanwijzingen zijn dat het mogelijk anders in elkaar zit."

Wat vindt u daarvan?
XZ: "Als gedragsanalist en onderzoeker veroordeel ik mensen niet. Natuurlijk vind ik persoonlijk iets van het gedrag van mensen, maar iedereen heeft redenen voor zijn gedrag en het heeft mijn interesse om die beweegredenen te achterhalen. Nicole en ik voeren veel gesprekken als duo en dat is heel effectief. Wanneer een van ons vragen stelt kan de ander observeren en visa versa. Daarnaast draagt het bij aan de dynamiek in een gesprek en dat maakt het interviewen dan ook erg leuk!"

Van welke technieken maken jullie gebruik tijdens jullie werk?
NdH: "Naast gesprekken (interviews) maken we ook gebruik van achtergrondonderzoek naar procesbetrokkenen en onderzoek van brondocumenten. Ook gebruiken we e-discovery-technieken om grote hoeveelheden informatie, zoals zakelijke bestanden, e-mails en WhatsAppberichten effectief en efficiënt te kunnen doorzoeken. Wij merken overigens dat auditors in hun onderzoeken soms de beschikking krijgen over informatie die ze nooit hadden mogen ontvangen. Denk aan privacygevoelige informatie over collega's. Als hier op een onzorgvuldige wijze mee om wordt gegaan, kan dit zeer verstrekkende gevolgen hebben voor de personen in kwestie. In potentie kun je iemands leven de vernieling in helpen als je niet precies weet wat je doet en wat er kan en mag op dit terrein."

Hoe zorg je voor zorgvuldigheid?
NdH: "Bij een auditor zouden er alarmbellen af moeten gaan als er privacygevoelige informatie over personen met je gedeeld wordt of als je gevraagd wordt om naar privacygevoelige informatie te kijken, zoals e-mails of personeelsgegevens van collega's. Plaats jezelf als auditor eens in de positie van iemand die onterecht wordt onderzocht en hoe jij je dan zou voelen. Zeker als je weet wat de potentiële consequenties van zo'n onderzoek kunnen zijn, zoals ontslag of andere sancties. Zelfs de schijn van betrokkenheid bij een onderzoek kan voor een mens schadelijke gevolgen hebben."

Voor de lezers die de Deepfake masterclass tijdens het IIA Congres van 2021 hebben gemist: wat is een 'deepfake'?
XZ: "Een deepfake is een voorstelling die gemaakt is om mensen bewust te misleiden. Het zijn veelal met een computer gemaakte beelden of geluiden die wel echt lijken, maar niet echt zijn. Deepfakes worden gemaakt voor amusement, grappige beelden en/of geluiden die bijvoorbeeld op Snapchat, TikTok of Facebook worden gezet. Ook worden deepfakes gemaakt die bedoeld zijn als politieke manipulatie of om fake news mee te maken. Bijna alle deepfakes zijn pornografisch, zo blijkt uit onderzoek van de Universiteit van Oxford. Dit kan zijn om gepersonaliseerde porno te maken, om bijvoorbeeld wraak op iemand te nemen, of om iemand mee te chanteren. Ook bestaan er audio-deepfakes waarbij bijvoorbeeld de stem van een CEO of CFO wordt geïmiteerd met de bedoeling iemand geld te laten overmaken naar een specifieke bankrekening in opdracht van de 'baas'. Ik kan iedereen aanraden eens de site van Siri Beerends te bekijken. Hier is veel informatie terug te vinden over artificial intelligence en deepfakes."

Kun je een deepfake herkennen?
XZ: "Deepfakes worden steeds beter en daardoor wordt het ook steeds lastiger om ze te herkennen. Zaken waar je op kunt letten zijn een afwijkende kwaliteit van beelden in het oorspronkelijke beeld en door gesproken teksten af te zetten tegen de bewegingen die iemand maakt. Jezelf vragen stellen (past dit binnen de context?), helpen om er kritischer naar te kijken. Het belangrijkste devies voor het achterhalen van misleiding, al dan niet door deepfake, is echter:
1. neem waar met aandacht;
2. wees kritisch op wat je aangeboden krijgt;
3. vraag om verifieerbare bronnen;
4. wees eerlijk naar jezelf als het gaat om welke informatie je accepteert."

Waar moet je als auditor op letten om te weten of iemand liegt of de waarheid spreekt?
NdH: "Het achterhalen of iemand de waarheid spreekt, verdraait of liegt, kan zeker nuttig zijn voor een auditor. Het vergt echter wel kennis, training en onderhoud. Weten waar je op moeten letten in een gesprek en de basisbeginselen

onder de knie krijgen, zijn belangrijk. Letten op de lichaamstaal van je gesprekspartner en deze lichaamstaal op de juiste wijze weten te interpreteren, is essentieel."

Kun je überhaupt wel vaststellen of iemand liegt?

NdH: "Het is wetenschappelijk aangetoond dat een mens in ongeveer de helft van de geteste gevallen kan vaststellen of iemand liegt. Het vergelijk met 'kop of munt' is dan vlug gemaakt. Uit onderzoek blijkt dat met het onder de knie krijgen van de basisbeginselen je die kans al aanzienlijk kunt vergoten naar 70 en zelfs 90%. Dit kan door training, door het lezen over gedrag, door oprechte interesse te tonen in het gedrag van mensen. Een nadeel is wel dat als je hier erg goed in wordt en vrienden en familie weten dat, je mogelijk niet meer uitgenodigd wordt op feestjes."

Hoe breiden jullie zelf jullie kennis uit?

NdH: "Xavier is druk bezig met zijn tweede jaar van de master Behaviour Analysis, Communication and Credibility Assessment door de EIA Group verbonden aan de Manchester Metropolitan University, waar Ekman de grondlegger van is. Ik ben recentelijk begonnen met de leer van Criminal profiling, een opleiding verzorgd door een van de grondleggers van de Behavioral Science Unit van de FBI, Joe Navarro. Ik merk dat het lezen van lichaamstaal, in combinatie met het kunnen detecteren van leugens, wetenschappelijk beschouwd twee hoofdkampen kent."

Vertel

NdH: "Er zijn mensen die stellen dat je leugens als zodanig kunt herkennen. En ook mensen die hier fel tegen ageren, onder wie Navarro. Vanuit de leer van Ekman en zijn team wordt mijns inziens nogal 'makkelijk' gedaan omtrent leugendetectie. Zo is er de Netflix-serie Lie to me waar Ekman als wetenschappelijk adviseur bij betrokken is geweest. Hier zie je de hoofdpersoon – Cal Lightman – die zich presenteert als een menselijke leugendetector. In bijna iedere aflevering hangt hij eerst met een verveelde blik in een freezepose. Plots schiet hij dan in standje 'flight', rennend naar een persoon die volgens hem niet de waarheid heeft gesproken. Die kijkt hij dan ongegeneerd een poosje van veel te dichtbij aan om hem vervolgens vanuit een fightstandje toe te schreeuwen: 'Je liegt!'"

Bijzonder…

NdH: "Het is jammer dat het gedachtegoed van Darwin en Ekman op deze manier wordt vermarkt en verkracht. Immers, lichaamstaal, waaronder micro- en macro-expressies, vertellen een geoefend oog veel over hoe iemand zich werkelijk voelt ten opzichte van wat hij zegt of doet. Maar als iemand bijvoorbeeld zweet of bibbert, dan wil dat niet zeggen dat iemand liegt. Je dient je beschouwingen dus te verifiëren in het gesprek met de persoon. En dat vergt kennis, extreem veel oefening en bovendien talent op dit terrein. Ik vind het bijzonder gaaf dat we binnen ons bureau zoveel verschillende kennis op dit mensgerichte gebied vergaren en het nog heel erg leuk vinden ook. De mens maakt immers het verschil."

Klopt het dat integere mensen nooit liegen en geen desinformatie verspreiden?

NdH: "Dit is onzin. Ieder mens liegt, behalve een net geboren baby! Dat kunnen kleine leugens zijn, zoals: 'Wat zie je er goed uit!', terwijl je iets anders denkt. Of grote leugens. Het met opzet geven van verkeerde informatie, het achterhouden van informatie, dat gebeurt overal. We kunnen als mensen ook niet functioneren zonder te liegen. Het is noodzakelijke smeerolie in het sociale verkeer. Als je liegt maar je weet niet dat je liegt, dan lieg je overigens niet."

Welk advies willen jullie auditors meegeven?

XZ: "Stel je als auditor steeds de vraag: waarom bereikt deze informatie mij? Ga op zoek naar de intentie van je gesprekspartners en realiseer je altijd dat gedrag een resultante is. In meer algemene zin: Breid je toolbox uit met kennis over menselijk gedrag, ook dat van jezelf en bekwaam je in gesprekstechnieken." <<

Tekst Frank Schuiten MA
Ron de Korte RA RE RO CIA
Beeld Andre George
Adobe Stock

Wat is *inzicht* en Wat moet je *ermee?*

Het Instituut voor Internal Auditors (IIA) wil de internal auditor ontwikkelen tot de trusted advisor van het management om zo bij te dragen aan het inzicht binnen de organisatie. Maar wat is precies de rol van de internal auditor met betrekking tot inzicht?

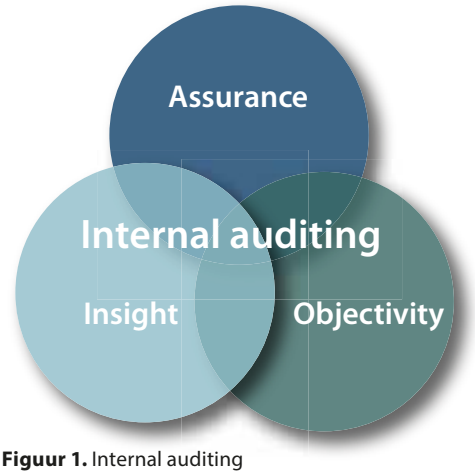
Om organisatorische waarde te creëren en te beschermen, heeft management inzicht nodig. Inzicht in de gang van zaken op de werkvloer, in de marktontwikkeling en concurrentie, in de belevingen van de organisatieleden, et cetera. Het is de kerntaak van iedere internal auditfunctie (IAF) om hieraan bij te dragen.

We zien voor de internal auditor zowel een rol als onderzoeker en een rol als counselor of 'trusted advisor' (zie ook: De Korte, Otten & Schuiten, 2021). Deze bijdrage bekijkt de gestelde vraag vanuit een onderzoekersperspectief.

Insight binnen het IIA
Binnen het Innovatieplatform van het IIA wordt 'insight' benoemd als een thema voor innovatie. Inzicht wordt in de missie voor de IAF genoemd naast assurance en advies, maar wordt binnen de Standaarden niet gedefinieerd. Uit een latere studie (2011) van het IIA blijkt dat inzicht als product wordt neergezet. Het belang van inzicht en de rol van de auditor is daarmee al een decennium onder de aandacht van het IIA. In deze bijdrage onderschrijven wij het belang van inzicht voor het succes van de organisatie en schetsen wij nader de rol van de auditor.

Nader vormgeven en positioneren
Om antwoord te kunnen geven op de hiervoor geformuleerde vraag, zetten wij eerst uiteen wat al bekend is over inzicht in de auditcontext. Vervolgens beschrijven wij een drieluik dat volgens ons de term inzicht binnen de auditwereld en het auditproces omschrijft. Dit drieluik beschrijft drie vormen van inzicht: inzicht van anderen (input), inzicht van de auditor (output) en inzicht bij de opdrachtgever (outcome). Wij lichten de keuze voor dit drieluik toe op basis van (audit)methodologische overwegingen. Met deze bijdrage willen wij dus de enigszins onduidelijke definitie van het IIA van inzicht nader vormgeven en positioneren binnen het auditwerkveld, met de daarbij behorende methodologische overwegingen.

Insight in de internal auditcontext
Voor de betekenis van inzicht binnen internal audit kijken we allereerst naar het IIA. In de missie van de IAF treffen we inzicht aan, naast assurance en advice. Dit roept enigszins verwarring op. Immers, de IAF levert assurance en consulting activities aan de organisatie. Waar komt inzicht dan vandaan?



Figuur 1. Internal auditing

Dit heeft te maken met de definitie van het IIA waarbij inzicht een product is dat de auditor levert aan de opdrachtgever, naast aanvullende zekerheidsgerichte en adviesgerichte producten. Het IIA heeft in 2011 een studie gepubliceerd waarin inzicht in een bollenfiguur (zie *figuur 1*) wordt gepresenteerd in samenhang met assurance en objectivity. Men verwijst ook naar de IIA-definitie met de begrippen assurance- en consultingactiviteiten.

Perspectieven op insight
In een eerder artikel stelt een van ons (De Korte, 2019) kritische vragen bij het neerzetten van inzicht als product en geeft daarbij aan dat inzicht niet van dezelfde orde is als de termen assurance en consulting actvities uit de IA-doelstelling (1999).

Internal auditors moeten inzicht eerder interpreteren als de resultante bij de opdrachtgever: het spreekwoordelijke kwartje dient te vallen. Inzicht is dus niet langer de output van de activiteiten van de IAF, maar de outcome dankzij de activiteiten van de IAF. Beide perspectieven zien we terug in woordenboeken.

Definities
In The Cambridge Dictionary vinden we een tweetal definities van insight die het waard zijn om met elkaar te vergelijken:
- a clear, deep, and sometimes sudden understanding of a complicated problem or situation;
- the ability to have such an understanding.

Allereerst is insight dus het hebben van een begrip over een bepaalde situatie; we hebben er een bepaalde interpretatie van, we snappen hoe iets werkt. Daarnaast is insight ook het vermogen om een dergelijke situatie te bevatten. Laat het duidelijk zijn dat beide definities onvermijdelijk met elkaar verbonden zijn, maar wel degelijk verschillend zijn. Het kúnnen kopen van een brood is immers iets wezenlijks anders dan het kópen van een brood. Ten derde zien we ook dat insight in de spreektaal wordt gebruikt als duiding; een nadere invulling door iemand, waardoor het dicht bij een doordachte mening komt.

Ontwikkelpad
Binnen het auditwerkveld zien we in een publicatie van PwC (2014) een getrapt ontwikkelpad voor de IAF. Achtereenvolgens zijn deze stappen: assurance provider, problem solver, insight generator and trusted advisor (p. 5). Het genereren van inzicht ten behoeve van de organisatie wordt daar als (noodzakelijke) opstap gezien om de stap naar de begeerde trusted advisor te kunnen maken. En dat het twee stappen verder is dan de IAF die louter assurance afgeeft over de interne beheersing. De term problem solver

past bovendien niet binnen het three lines model dat het IIA als basis hanteert voor de rolinvulling van de internal auditor.

Als we de interpretatie van PwC plaatsen in het spectrum van output versus outcome, zijn beide interpretaties mogelijk. Immers, de IAF kan inzichten genereren als product vanuit de auditactiviteiten, maar het is ook mogelijk dat de IAF inzicht creëert bij de opdrachtgever als uitkomst. Dat is ook de clou: het een sluit het ander niet uit. Sterker nog, het een heeft het ander nodig. Daar komen wij later in deze bijdrage op terug.

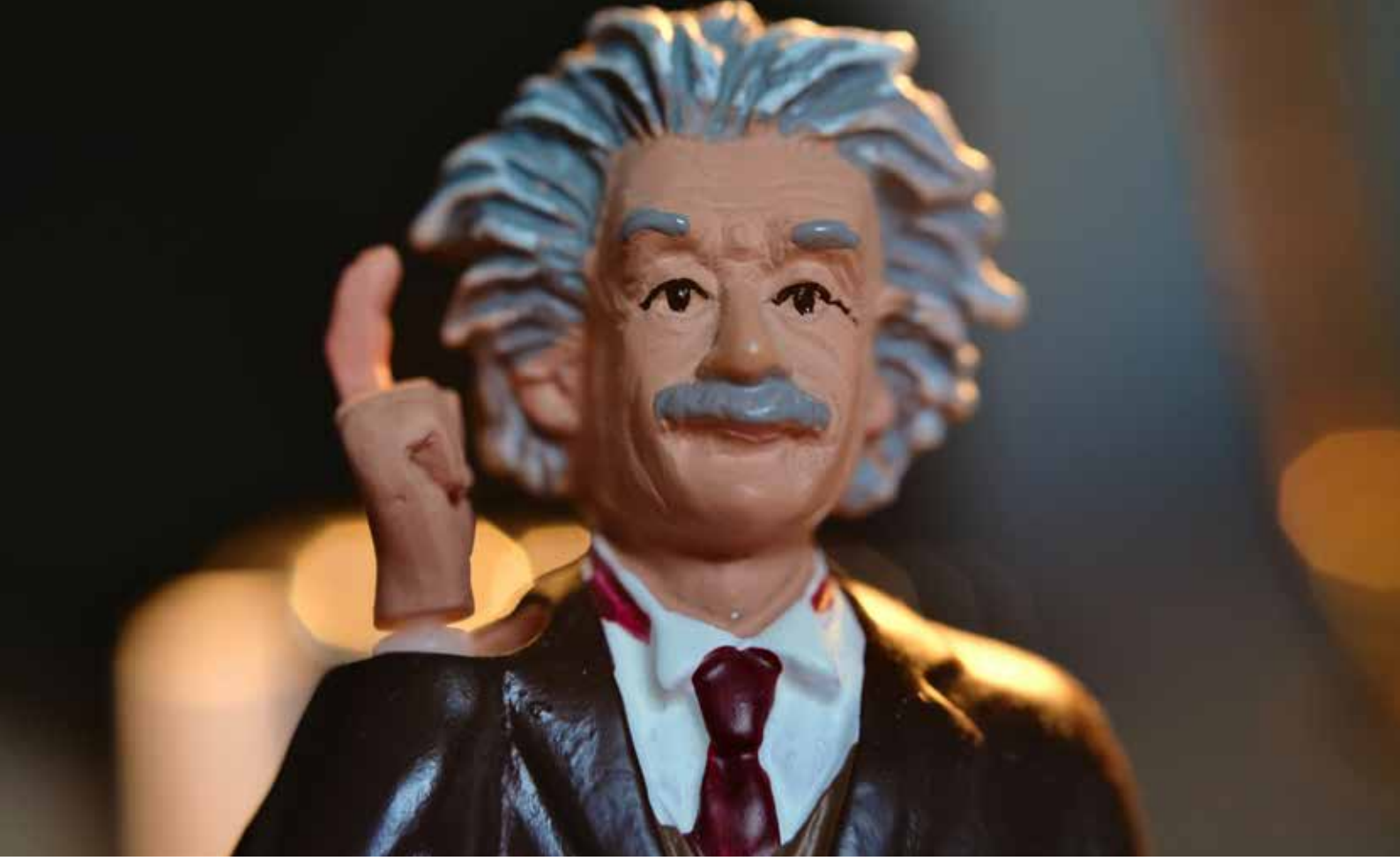
Drieluik van insight

Inzicht bij de opdrachtgever
Laten we beginnen met de stelling dat inzicht bij de opdrachtgever het uiteindelijke, ideale doel is van iedere activiteit die de IAF onderneemt. Het uiteindelijke doel (outcome) is dat de opdrachtgever komt tot een eurekamoment en op basis van auditresultaten (output) verdere keuzen kan maken. Het behoeft ook geen verder betoog dat dit uiteindelijke doel niet mag ontbreken in de centrale auditdoelstelling (zie ook: Bos, De Korte & Otten, 2017; De Korte, Otten & Schuiten, 2021). Deze aha-erlebnis bij de opdrachtgever is de katalysator voor verdere managementactie in het beschermen en creëren van organisatorische waarde (zie ook: IIA, 2011).

Er zijn drie vormen van inzicht: inzicht van anderen (input), inzicht van de auditor (output) en inzicht bij de opdrachtgever (outcome)

Inzicht van de auditor
Zoals hiervoor aangegeven komt het inzicht bij de opdrachtgever onder meer voort uit auditresultaten. Laten we ons voor nu richten op de bijdrage van auditresultaten aan het inzicht bij de opdrachtgever. Tijdens de audit heeft de auditor allerlei gegevens verzameld, verwerkt en geanalyseerd. Dat doet de auditor op basis van goed onderzoek, gestoeld op zorgvuldige methodologische overwegingen. Op basis van deze gegevens formuleert de auditor bevindingen. Anders gezegd: de auditor formuleert diens interpretatie van de situatie, getoetst aan een vooraf opgesteld normenkader. Of, nog anders gezegd: het inzicht van de auditor wordt geformuleerd.

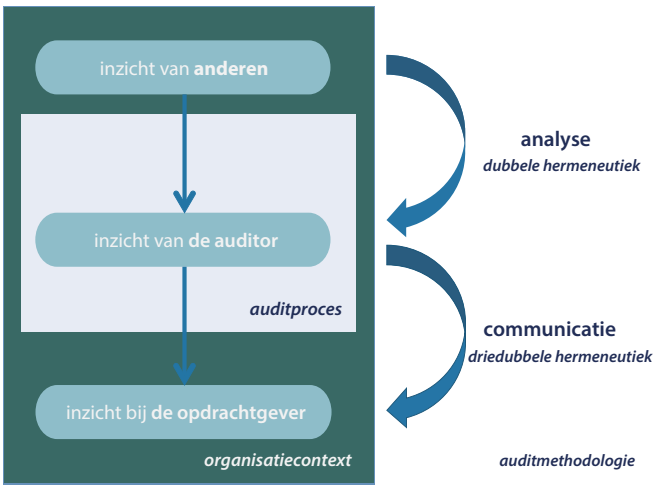
Inzicht van anderen
Dit inzicht van de auditor is gestoeld op zorgvuldig uitgevoerd onderzoek. De meestgebruikte combinatie van methoden is documentenstudie en interviews/enquêtes.



Bij die laatste methoden gaat het om het verzamelen van gegevens afkomstig van personen. Zij delen hun ervaringen en belevingen over een bepaalde situatie met de auditor. Zij formuleren daarin hun inzichten, die de auditor gebruikt. In de gegevensanalyse gebruikt, interpreteert en weegt de auditor dus inzicht van anderen.

Drieluik en de uitwerking in het auditproces – analyses en communicatie

Figuur 2 laat zich als volgt lezen: het inzicht van de auditor in het gekozen auditobject wordt vormgegeven in het auditproces, op basis van het inzicht van anderen. De auditor communiceert dit dusdanig dat het inzicht bij de opdrachtgever ontstaat.



Figuur 2. Drieluik van inzicht

Dat inzicht van de auditor wordt niet in een vacuüm vormgegeven; dat gebeurt binnen de context van de organisatie. Net zomin bestaat het inzicht van anderen, noch het inzicht bij de opdrachtgever zonder deze in de bedrijfscontext te plaatsen. Het is bovendien onderhevig aan (inter)subjectiviteit. Het interpreteren van de bedrijfscontext is daarmee randvoorwaardelijk voor inzicht binnen welke organisatie dan ook. Zonder begrip van de bedrijfscontext kan de auditor geen audit uitvoeren.

De analysetaak

De auditor heeft twee taken binnen het auditproces wat betreft inzicht: een analyse- en een communicatietaak. Dit lichten we kort toe. Allereerst dient de auditor goed en zorgvuldig, methodologisch onderbouwd, onderzoek uit te voeren om zo het inzicht van de auditor te creëren, (mede) op basis van de analyse van het inzicht van anderen. Dit kan op de bekende manieren ter borging van betrouwbaarheid van een onderzoek: het bijhouden van bronnen- en datamatrices, het borgen van triangulatie op het gebied van methoden, bronnen en auditors, het toepassen van hoor en wederhoor, et cetera.

We herhalen hier graag de kritische noot geplaatst bij een definitie van inzicht van de auditor als mening van de auditor (De Korte 2019). Dat is geenszins hoe wij inzicht van de auditor willen definiëren binnen diens onderzoekersrol. Het inzicht van de auditor moet hier methodologisch worden onderbouwd. Als dat onvoldoende gebeurt, spreken we niet over een inzicht van de auditor, maar over een mening van de auditor. Ook die kan heel relevant zijn, maar voor de ontvanger is juist de kennis over de mate van onderliggend onderzoek van belang om de audituitspraak aanvullende zekerheid te kunnen gebruiken voor zijn managementtaak.

Wanneer de drie vormen van inzicht staan als een huis, kan de IAF tot inzicht bijdragen, zodat de organisatie kan bouwen op de IAF

De communicatietaak
Ten tweede ligt er een communicatietaak voor de auditor binnen het auditproces. Dit betreft het communiceren van de auditresultaten naar de opdrachtgever. Het is een verre van simpele taak, maar ook een van de belangrijkste voor de auditor. Immers, niets is kwalijker dan gebrekkige communicatie, waardoor de opdrachtgever niet in staat is om de auditresultaten te bevatten. En er zijn meerdere manieren om auditresultaten te communiceren. Het kan schriftelijk in een rapportage, maar ook met een presentatie of faciliterende groepssessie. Tevens zijn er goede ervaringen opgedaan met tekeningen, fotorapportages, video, hoorspelen, et cetera.

Alles staat of valt met de vaardigheid om het inzicht van de auditor over te brengen, zodat inzicht bij de opdrachtgever ontstaat op basis van auditresultaten. Nu komen wij ook terug op onze eerdere stelling dat inzicht als output en outcome elkaar nodig hebben: zonder een duidelijk gecommuniceerd inzicht van de auditor komt het met de audit gevraagde inzicht bij de opdrachtgever niet. We benadrukken dat het inzicht bij de opdrachtgever niet door inzichten van de auditor alleen tot stand komt. Wel kan het inzicht van de auditor een (wezenlijke) bijdrage daaraan leveren.

Drieluik gezien vanuit hermeneutiek en de interpretatieve onderzoekstraditie
Dan resteren nog drie paragrafen voor de liefhebber van (audit)methodologie en wetenschapsfilosofie voordat we naar de conclusie gaan. Binnen de interpretatieve traditie van onderzoek staat de methodologie van hermeneutiek hoog in het vaandel. Daarmee staat interpretatie van fenomenen centraal in onderzoek. Veelal wordt ook gesproken over de dubbele hermeneutiek (zie onder andere Giddens, 1987).

Dubbele hermeneutiek
Dubbele hermeneutiek stelt dat iedereen een situatie of fenomeen altijd op persoonlijke wijze tot zich neemt en interpreteert. Wanneer een onderzoeker hier onderzoek naar doet, verzamelt deze gegevens door onder andere interviews te houden met die personen. Vervolgens interpreteert de onderzoeker zelf nogmaals de verzamelde gegevens in de analyse van onderzoeksresultaten. Daarmee vindt een dubbele interpretatiecyclus plaats: dubbele hermeneutiek. Dit benadrukt het belang van het terugkoppelen van ontvangen inzichten met samenvattingen (wederhoor): het is een interpretatie van iemands interpretatie. De bevestiging van jouw samenvatting vormt de borging van de betrouwbaarheid van je onderzoek.

Driedubbele hermeneutiek
Binnen het drieluik zit deze dubbele hermeneutiek ook verborgen. Deze bevindt zich in de analysefase van het auditproces: de plek waar de auditor het inzicht van anderen weegt en interpreteert om zo tot het inzicht van de auditor te komen. Binnen ons drieluik is er nog een interpretatiecyclus. De opdrachtgever interpreteert immers ook de auditresultaten. Daarom spreken wij binnen het drieluik van een driedubbele hermeneutiek: de interpretatiecycli tussen de inzichten van anderen (no 1), van de auditor (no 2) en bij de opdrachtgever (no 3).

Inzicht als voorwaarde voor en opmars naar trusted advisor
Inzicht heeft in deze bijdrage voor de auditor drie verschillende betekenissen gekregen. We hebben gesteld dat het belangrijkste inzicht bij de opdrachtgever ligt: die moet immers met de auditresultaten aan de slag! De auditresultaten representeren het inzicht van de auditor, dat veelal gestoeld is op inzicht van anderen binnen de organisatie. Daarmee is inzicht dus zowel input, als output als de outcome van het auditproces (throughput).

De drie vormen van inzicht stoelen op twee activiteiten die de auditor in het auditproces uitvoert: analyse en communicatie. De analyse van de internal auditor als onderzoeker moet stoelen op goed en zorgvuldig, methodologisch onderbouwd, onderzoek, waarin is geborgd dat het inzicht van de auditor passend is in relatie tot het inzicht van anderen. De communicatie moet passend zijn, zodat de opdrachtgever de clou van het verhaal snapt; zodat het inzicht van de opdrachtgever indaalt.

Om deze bijdrage af te ronden: wanneer de drie vormen van inzicht staan als een huis, kan de IAF tot inzicht bijdragen, zodat de organisatie kan bouwen op de IAF. Auditors kunnen zich vervolgens verder ontwikkelen tot een trusted advisor voor belangwekkende managers binnen de organisatie. Zo kun je nog meer waarde voor de organisatie beschermen én creëren. Dan transformeert kennis tot inzicht. <<

Literatuur

- Bos, P., De Korte, R. en J. Otten, *Management Control Auditing: bijdragen aan doelrealisatie en verbetering*, Auditing.nl, 2017.
- De Korte, R., 'Auditor: Zó lever je inzicht', *Audit Magazine*, 2019.
- De Korte, R., Otten, J. en F. Schuiten, 'Wendbaarheid met internal audit(deel)producten', *Audit Magazine*, 2021.
- Giddens, A., *Social Theory and Modern Sociology*, Cambridge: Polity Press, 1987.
- IIA, *Insight: delivering value to stakeholders*, 2011.
- PWC, *The eight attributes: delivering internal audit excellence as stakeholders expect more*, 2014.

Frank Schuiten MA werkt bij de Auditdienst Rijk en daarvoor bij de Europese Rekenkamer. Hij heeft een achtergrond in internationale betrekkingen bestuurskunde en Europese publieke zaken.

Ron de Korte RA RE RO CIA is partner van ACS Partners. Hij begeleidt hoofden audit risicomanagement en control en hun medewerkers met training counseling en ondersteuning in hun professionalisering.

Onderzoek
Tekst Dr. Sjoerd Keulen
Virginie de Rooij MSc RO
Beeld Ministerie van Defensie
Adobe Stock
Pexels

De auditor als antropoloog

In het op 18 mei 2022 gepresenteerde verantwoordingsonderzoek van de Algemene Rekenkamer is dit jaar een oorzaakanalyse opgenomen van het munitiebeheer bij Defensie dat zich specifiek richt op gedrag.

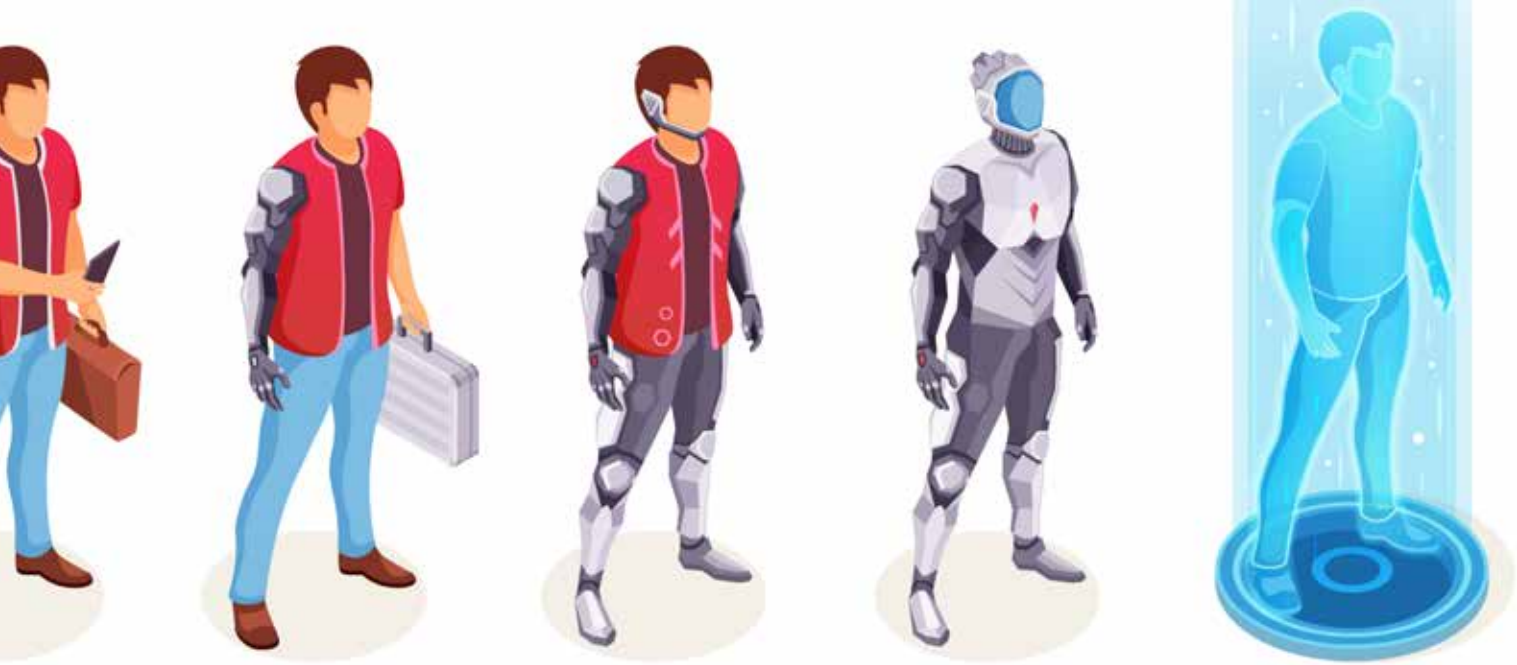
Anders dan meer bekende gedragsaudits wordt niet gewerkt met een vooraf opgesteld normenkader van gewenst gedrag, maar wordt participerend geobserveerd hoe procedures in de praktijk uitwerken. Met deze vernieuwende uitbreiding van het auditpalet, gebaseerd op methoden uit de antropologie, wil de Algemene Rekenkamer meer inzicht bieden in hardnekkige problemen.

Hoe het werkt in de praktijk

In oktober 2020 nam Mark van Twist afscheid als collegelid in buitengewone dienst bij de Algemene Rekenkamer. In Audit Magazine kruiste hij toen de degens met Ron de Korte en Jan Otten met zijn pleidooi voor meer operational auditing – meer onderzoeken naar de werking in de praktijk. Onderzoeken die Van Twist ook mistte bij de Algemene Rekenkamer zelf. In dit artikel laten wij zien hoe we deze handschoen hebben opgepakt door een oorzaakanalyse, gericht op gedrag, uit te voeren naar een hardnekkig probleem: het gebrekkige munitiebeheer van het ministerie van Defensie. De gehanteerde methode is echter geen typische auditmethode en zal wellicht wat wenkbrauwen bij auditors doen fronsen: we hebben geobserveerd zonder normenkader.

Oordelen op Verantwoordingsdag

De Algemene Rekenkamer presenteert ieder jaar elke derde woensdag in mei haar bevindingen over de rechtmatigheid van de uitgaven van het rijk en over de stand van de bedrijfsvoering op de departementen. Zaken in de bedrijfsvoering die niet voldoen worden als 'onvolkomenheden' aangemerkt. Vaak gaat het hierbij om papieren beheersprocessen en de mate waarin het departement in control is.



Sommige van deze onvolkomenheden zijn hardnekkig. Zo constateert de Algemene Rekenkamer sinds 2016 dat de aantallen van de opgeslagen munitievoorraden van het ministerie van Defensie niet kloppen en dat de beheersprocessen niet altijd worden gevolgd. Een werkelijke oplossing voor dit probleem is ondanks diverse verbeterprogramma's in al die jaren niet gevonden.

Dit was reden om ook naar onszelf en onze manier van auditen te kijken: als we blijven doen wat we altijd deden, helpen we de auditee niet verder. In een analyse van onze eigen onderzoeken zagen we dat we bij lang openstaande onvolkomenheden dezelfde typen financial audits verrichten en ook dezelfde conclusies blijven herhalen: men werkt niet volgens het vastgestelde beleid en de werkinstructies. Met als aanbeveling: ga dit wel doen.

De waaromvraag werd niet gesteld

De vraag waarom de procedures niet worden gevolgd, wordt in deze onderzoeken niet altijd beantwoord. Als gevolg daarvan wordt het eventuele antwoord niet gebruikt in de formulering van aanbevelingen. Hardnekkige problemen kunnen meerdere soorten oorzaken hebben. Er kunnen problemen zijn in de organisatie (bedrijfsvoering en governance) en/of met de middelen (geld en capaciteit). Op deze terreinen doet de Algemene Rekenkamer vaak onderzoek.

Een ander belangrijk type oorzaak is gedrag. Aan dit type oorzaak besteedt de Algemene Rekenkamer nog weinig aandacht. Cultuur wordt nog weleens als restvariabele opgenomen die de afwijking verklaart, maar is geen onderdeel van de aanbeveling: cultuur en gedrag hebben we namelijk niet onderzocht. Dit terwijl processen door mensen worden uitgevoerd. Tijd dus om naar de mens achter het papieren proces te kijken. Niet alleen in een voorbereid interview, maar juist door werk, werkdruk, instructies, keuzen en afwegingen zelf te ervaren in de praktijk.

Een oorzaakanalyse naar gedrag

Oorzaakanalyse (ook wel root cause analysis genoemd) is een verzameling methodieken die de auditor helpt om niet alleen vast te stellen dat een risico bestaat, maar vooral ook waarom dit gebeurt. Hiermee kan de auditor aanbevelingen doen die de tekortkomingen daadwerkelijk opheffen.

Vaak worden interviews of enquêtes gebruikt om gedrag te begrijpen. De meest bekende is TRIPOD BETA, een zeer systematische onderzoeksmethode afkomstig uit het ongevallen- en incidentenonderzoek (Turksema, Postma & De Haan, 2007). Andere technieken als de Five why's of de visgraatdiagrammen helpen wel bij het bepalen of je met doorvragen echt bij de oorzaak (de root cause) van een probleem bent, maar niet hoe je die in gedrag kunt vaststellen (IIA, 2017).

Niet altijd de 'juiste' antwoorden

De kwalitatieve methoden vanuit Learning Histories van Kleiner & Roth (1997) die binnen behavioural auditing worden gebruikt, helpen om na te denken over 'sensitizing concepts' en onderstrepen het belang van validatieworkshops en het gebruik van quotes om de essentie van auditees weer te geven. Respondenten geven dan als het ware een eigen analyse van hun gedrag. Echter, respondenten geven niet altijd de 'juiste' antwoorden. Zij weten zelf niet altijd waarom zij op een bepaalde manier handelen of zij kunnen zich situaties niet meer helemaal herinneren. Doordat wij door ons eerder onderzoek verwachten dat gedrag een belangrijke verklaring kon zijn voor de langdurige onvolkomenheid met betrekking tot munitiebeheer, wilden wij in onze oorzaaksanalyse vooral hier aandacht voor hebben. Daarom kozen wij voor participerende observatie in combinatie met diepte-interviews.

Observeren in vier stappen

Stap 1 – Opzet, vraag en 'norm'

De munitieketen is een omvangrijk proces dat bij verschillende bedrijfsonderdelen van defensie wordt uitgevoerd. Daarom hebben we het onderzoek zoveel mogelijk ingericht als een 'product journey', waarbij we 'één patroon' volgden (Howard, 2014). Zo konden we alle bewegingen, handelingen en registraties van munitie observeren. Het patroon was bovendien een gemakkelijke kapstok om aan alle medewerkers van Defensie concreet uit te leggen waar ons onderzoek over ging.

We wisten bij aanvang van het onderzoek dat het munitiebeheerproces niet aan de 'norm' voldeed. Voor het gewenste gedrag hadden we geen 'norm': we wilden juist zien wat er gebeurde, wat leidde tot het afwijken van de norm. Op die manier gingen wij dus blanco het onderzoek in. Iets wat niet vaak gebeurt in audits, maar wel in gedragsonderzoek dat wordt uitgevoerd door antropologen.

Binnen het onderzoeksteam hebben we veel disciplines bij elkaar gebracht om de methode van de grond te krijgen: van operational auditors tot (gepromoveerde) antropologen. Op die manier werd kennis van oorzaakanalyse verbonden met kennis van observatie. Onze collega-antropologen waren niet alleen onderdeel van het auditteam, maar hebben de reguliere defensieauditors getraind in het doen, registreren en het op een gestructureerde wijze analyseren van observaties (Emerson, Fretz & Shaw, 2007).

Stap 2 – Observatie
We wilden zo dicht mogelijk bij participerende observatie komen: een beproefde methode uit de antropologie waarin

de onderzoeker door ervaring kennis opdoet. Bij participerende observatie 'doet' de onderzoeker letterlijk 'mee' in de wereld van de onderzochte groep. Op die manier kan de onderzoeker de gemaakte keuzen begrijpen. Ook worden de interacties zichtbaar die zich rondom de keuze afspelen en kan de onderzoeker direct gerichte vragen stellen over de situatie, op een detailniveau die in een setting van alleen gesprekken onhaalbaar is.

Door veiligheidseisen voor het omgaan met munitie was dit niet volledig mogelijk. We hebben de methode daarop aangepast: door meerdere malen te observeren bij het verstrekken van munitie en het verbruiken van munitie tijdens oefeningen, probeerden de onderzoekers zo dicht als mogelijk bij de dagelijkse gang van zaken te komen. Dat betekende onder meer in de brandende zon lege hulzen rapen en met geluidsdempers op de oren – op veilige afstand – achter schietende militairen aanlopen. Tijdens de oefeningen maakten de onderzoekers aantekeningen (field notes) en foto's. Vanwege de kans op beïnvloeding van gedrag zijn de observaties niet gefilmd.

Als risico van deze methode wordt vaak subjectiviteit genoemd. Wij hebben dit risico ondervangen door in de opzet van ons onderzoek een aantal maatregelen te nemen: onderzoekers zijn getraind in het doen van observaties en het uitvoeren van diepte-interviews. Tijdens de observaties is gebruikgemaakt van intersubjectiviteit: de observaties worden door meer dan één onderzoeker gedaan en verschillen worden besproken.

Stap 3 – Analyse
De auditors die hebben geobserveerd, bespreken hun observaties in groepsdiscussies en komen tijdens de discussies tot patronen. Deze worden gedeeld met collega's die de observaties niet hebben uitgevoerd om zo een subjectief perspectief te voorkomen en actief tegendenken in het onderzoeksproces in te bouwen.

Stap 4 – Validatie
In een focusgroep met vele verschillende eenheden van één krijgsmachtsonderdeel hebben we onze resultaten en observaties voorgelegd en gevraagd of deze rode draden herkend werden. Komt het door ons geobserveerde gedrag breder binnen de krijgsmacht voor? Daarnaast helpt deze werkwijze om biases in de observaties te voorkomen. Als triangulatie hebben wij daarnaast een documentstudie gedaan en gesproken met de diverse inspectiediensten die toezicht houden op het transporteren, behandelen en opslaan van munitie om te verifiëren of zij de observaties herkenden.

De methode toegepast: de uitkomsten
Defensie heeft zeven centrale munitiemagazijncomplexen van waaruit munitie wordt geleverd aan de operationele commando's, zoals de marine en de luchtmacht. Voor deze decentrale voorraad munitie heeft het ministerie van Defensie 47 opslaglocaties die munitie voor oefeningen op schietterreinen uitgeven. Vanwege bijvoorbeeld de veiligheid en om vermissing of diefstal te voorkomen, wordt de voorraad munitie periodiek geteld om te vergelijken met de hoeveelheid die in het beheersysteem staat. In opzet een goed doordacht en goed lopend proces.

Vanwege de veiligheid is het munitieproces sterk gereguleerd. Er gelden tal van verplichtingen voor opslag en transport. De meerwaarde van het (vele) papierwerk dat hierbij hoort is voor de gebruikers van munitie niet altijd duidelijk. Veel militairen zien dit als 'papieren bevrediging'. Ze houden omvangrijke administraties bij waar nooit naar wordt gevraagd en die geen onderdeel vormen van een controlecyclus. Tijdens onze observaties constateerden we dat deze ervaren papieren last leidt tot ongewenst gedrag.

Grijze voorraden
Defensie is de afgelopen jaren vaak in het nieuws gekomen vanwege tekorten aan munitie, personeel en (werkend) materieel. Wij merkten in onze observaties dat er bij de gevechtseenheden een gevoel van munitieschaarste was, dat ook werd uitgesproken. Daarnaast zagen we dat oefeningen door materieelstoringen niet (volledig) doorgingen, waardoor er minder goed geoefend kon worden. Om al die redenen wordt na een oefening niet altijd alle munitie (veelal losse flodders, ofwel blanks) ingeleverd bij de munitiedepots. Deze achtergehouden patronen worden de 'grijze voorraden' genoemd.

Deze munitie wordt in de kazernes op daarvoor niet ingerichte plekken en dus onveilig bewaard. Op deze manier hebben eenheden eigen reserves voor het geval munitie bij

de complexen niet voorradig is, of kan gemakkelijk een oefening worden geïmproviseerd als een oefening in een simulator niet door kan gaan vanwege een storing. Wij hebben dit gedrag breed binnen de krijgsmacht geconstateerd.

Deze grijze voorraad kan binnen het munitieproces bestaan, omdat munitie uitgegeven aan eenheden voor oefeningen in het systeem wordt beschouwd als 'verschoten'. Dit brengt een veiligheidsrisico met zich mee, omdat er niet wordt bijgehouden hoeveel er wordt verschoten en hierdoor dus geen controle is op wat er al dan niet retour wordt gebracht. Hierdoor bestaat ook het risico dat door munitiecomplexen uitgegeven munitie ontvreemd wordt. Tot slot werkt dit systeem verspilling in de hand, doordat grijze voorraad soms alsnog opduikt bij de munitiecomplexen en dan vernietigd moet worden.

Munitie inleveren is een last

Na een oefening wordt vaak niet-verschoten munitie van eerdere oefeningen gevonden. Ook vinden militairen na de oefening ondanks controles nog weleens een paar patronen in hun tassen of bezittingen. Vroeger stonden hiervoor anoniem te gebruiken containers op de kazernes. Nu dienen deze te worden ingeleverd en met behulp van formulieren in het administratiesysteem SAP te worden ingevoerd. In de praktijk worden de formulieren voor het retourneren van gevonden munitie nauwelijks gebruikt, ook niet door de munitiespecialisten. Bij de eenheden lijken militairen deze munitie te laten liggen of 'in de grond te trappen'. Verspillend gedrag zien we ook na oefeningen. Vanwege de administratieve last zijn er eenheden die liever de munitie opschieten dan inleveren.

Vanwege het personeelstekort binnen de munitieorganisatie vinden niet alle controles gestructureerd plaats. Zo werd bij de jaarlijkse telling een bunker niet bevroren waardoor tijdens het tellen munitie binnenkwam en vertrok. Ook werken medewerkers in de munitiedepots door het tekort soms op andere plaatsen, waardoor onbedoeld vier ogenprocedures of tweedelijnscontroles wegvallen. Bij sommige gevechtseenheden hadden logistieke ondersteuners zoveel 'rechten' binnen het systeem dat zij in de praktijk niet werden gecontroleerd.

Van oorzaak naar verbetering

De Algemene Rekenkamer constateert dat het huidige munitieproces gedrag in de hand werkt waardoor veiligheidsrisico's ontstaan. Alleen door te observeren wat er in de praktijk gebeurt en door gesprekken te voeren, konden wij het wijdverbreide probleem van grijze voorraad en het lastig inleveren van gevonden munitie constateren én begrijpen. Pas door observaties konden wij vaststellen welke gevolgen en mogelijkheden het als 'verschoten' boeken van verdwenen munitie heeft. Dit besef hadden wij niet tijdens onze eerdere onderzoeken naar munitiebeheer die vooral gericht waren op de beheersingskant.

Het doel van een oorzaakanalyse is het komen tot aanbevelingen die het probleem oplossen. De Algemene Rekenkamer heeft de minister van Defensie daarom aanbevolen na te gaan of er manieren zijn om gevonden munitie gemakkelijker in te leveren en of hiermee 'grijze' voorraadvorming kan worden voorkomen. Ten tweede heeft de Algemene Rekenkamer aanbevolen om te bekijken of de administratieve last verminderd kan worden, bijvoorbeeld door toepassing van (nieuwe) technologie in het munitiebeheer en het doorlichten van de omvangrijke regelgeving op nut, noodzaak en tegenstrijdigheid. Hiermee zullen de medewerkers van Defensie hopelijk minder prikkels voelen om onveilig gedrag te vertonen.

Gedragsverandering vraagt tijd

Daarnaast heeft de Algemene Rekenkamer aanbevolen om vanuit het gehele munitiedomein de verbeteracties verder te synchroniseren en onder één eindverantwoordelijke te plaatsen en verantwoordelijkheden als monitoring beter vast te leggen. Op deze manier kunnen verbeteringen van het munitiebeheer voor de hele keten worden aangebracht. Hiernaast is ook aandacht voor gedrag noodzakelijk. Dit kan uiteindelijk alleen als er voldoende medewerkers zijn in de munitiebunkers om munitie veilig uit te geven en de voorraden bij te houden. De tekortkomingen zijn in de loop der jaren ontstaan, het zal dan ook een meerjarige inzet vragen die op te pakken. En dit geldt nog sterker bij gedragsveranderingen. <<

Literatuur

- Emerson, R. M., Fretz, R. I. en L.L. Shaw, *Participant observation and fieldnotes. Handbook of ethnography*, Sage, Londen, 352-368, 2007.
- Howard, T., 'Journey mapping: A brief overview', *Communication Design Quarterly Review*, 2(3), 10-13, 2014.
- IIA, *Toepassingen van oorzaakanalyses bij audits: handvatten en ervaringen voor root cause analyses*, 2017.
- Kleiner, A. en G. Roth, 'How to make experience your company's best teacher', *Harvard Business Review*, 75(5), 172-178, 1997.
- Turksema, R., Postma, K. en A. De Haan, *Tripod Beta and Performance Audit. Paper for the International Seminar on Performance Auditing*, Oslo, 2007.

Virginie de Rooij MSc RO is operational auditor bij de Algemene Rekenkamer. Zij is gespecialiseerd in methodologie en oorzaakanalyse.

Dr. Sjoerd Keulen is expert Defensie en Methoden bij de Algemene Rekenkamer.

Dit artikel is op persoonlijke titel geschreven.

Tekst Bram Ketting
Jelle Groenendaal
Beeld Adobe Stock

Ketenrisicobeheersing moet **volwassen discipline** worden

Grote en kleine organisaties worden steeds meer afhankelijk van (ICT-)diensten van derden, maar zijn nog maar beperkt bezig met de beheersing van risico's die daardoor kunnen ontstaan. Auditors kunnen een belangrijke aanjagende rol vervullen bij het (verder) professionaliseren van deze risicodiscipline binnen organisaties.

In dit artikel vijf redenen waarom ketenrisicobeheersing volwassen(er) moet worden. We zullen deze redenen larderen met ICT-gerelateerde voorbeelden, al zien we in onze praktijk dat ze ook van toepassing zijn op proces- en productieketens. Tot slot geven we enkele tips hoe auditors concreet kunnen bijdragen aan een verdere professionalisering van de ketenrisicobeheersingsdiscipline.

Langere en complexere ketens

Steeds meer organisaties zijn voor hun functioneren in grote mate afhankelijk van derde partijen. Neem bijvoorbeeld verzekeraars. Volgens De Nederlandsche Bank (DNB) besteden verzekeraars ICT-oplossingen ondersteunend aan een of meerdere kritieke bedrijfsprocessen steeds vaker uit. Daarnaast kiezen zij ervoor om (delen) van hun primaire bedrijfsproces volledig uit handen te geven, zoals de schadeafhandeling, het onderhouden van klantrelaties en de administratie.
Deze toegenomen afhankelijkheid van en verwevenheid met derde partijen maakt dat organisaties kwetsbaarder worden voor verstoringen of informatiebeveiligingsincidenten ergens in de keten. Ketenrisicobeheersing wordt daarmee belangrijker voor de continuïteit en kwaliteit van de dienstverlening.

Bovendien worden de uitbestedingsketens steeds langer (en daardoor) complexer. Serviceproviders die diensten leveren aan organisaties besteden zelf vaak ook een deel van het werk uit aan derde partijen. Dit betekent dat uitbestedingsketens van kritieke bedrijfsprocessen uit meerdere schakels kunnen bestaan. Een complicerende factor is dat deze schakels zich veelal in verschillende landen begeven met andere wet- en regelgeving.
Inzicht in en beheersing van ketenrisico's wordt dus steeds ingewikkelder. Dit vraagt daarom om meer inspanning vanuit organisaties en de juiste ondersteunende technologie om dit voor elkaar te krijgen.

Toename van incidenten
Volgens het Europees Agentschap voor Cyber Security (ENISA) zijn ketenaanvallen of supply chain attacks een van de grootste cyberdreigingen van dit moment. SolarWinds is wellicht een van de meeste bekende ketenaanvallen van de afgelopen jaren. Aanvallers voegden een kwaadaardige code toe aan een software update van SolarWinds. Hierdoor kregen de aanvallers toegang tot alle klanten van SolarWinds die deze update hadden uitgevoerd. Onder de klanten van SolarWinds bevonden zich de Amerikaanse overheid, het Europese Parlement en vele grote internationale bedrijven.

Een ander en meer recentelijk voorbeeld is de Okta-aanval. Aanvallers wisten de systemen van Okta binnen te komen door middel van een gecompromitteerd systeem van een derde partij die de klantenservice verzorgde. Eenmaal binnen hadden de aanvallers weer toegang tot een deel van de systemen van twee klanten van Okta.

Beide voorbeelden laten zien dat organisaties zeer kwetsbaar kunnen zijn voor aanvallen die plaatsvinden via een derde partij en dat deze risico's actief beheerst moeten worden. Ook al heb je in dergelijke gevallen als organisatie geen directe invloed op het incident- en crisismanagement van de gecompromitteerde derde partij, wel kun je zelf risicobeperkende maatregelen nemen zoals het afsluiten van netwerkverbindingen met de derde partij en het proactief informeren van klanten en medewerkers.

Bestaande en aanstaande wet- en regelgeving
Organisaties die gebruik (willen) maken van buitenlandse ICT-dienstverleners moeten nu al anticiperen op bestaande wet- en regelgeving (denk aan de Amerikaanse Patriot Act) en de risico's hiervan beoordelen en mitigeren. Daarnaast worden er op Europees niveau verschillende nieuwe initiatieven ontplooid om organisaties te bewegen om meer aandacht te besteden aan ICT-ketenrisicobeheersing.

NIS-2
In de in 2022 door het Europese Parlement goedgekeurde Network and Information Security (NIS-2) directive wordt nadrukkelijk aandacht besteed aan ketenrisicobeheersing. Artikel 43 stelt bijvoorbeeld dat organisaties die essentiële maatschappelijke diensten leveren, moeten beoordelen of de cybersecurity van derde partijen en serviceproviders voldoende is. Artikel 45 eist van dezelfde organisaties dat zij de cybersecurity van derde partijen die data verwerken (bijvoorbeeld voor analyticsdoeleinden) grondig beoordelen en indien nodig passende maatregelen (laten) nemen. Onderdeel van de voorgestelde NIS-2 directive is om lidstaten de mogelijkheid te geven om boetes uit te delen aan organisaties die niet voldoen aan de vereisten. Medio 2024 wordt de NIS-2 directive doorgevoerd in Nederlandse wetgeving.

DORA
Specifiek voor financiële instellingen is de Digital Operational Resilience Act (DORA) aanstaande. Deze voorgestelde wet bevat maar liefst veertien artikelen waarin tot in detail wordt beschreven wat financiële instellingen moeten doen om ICT-risico's van derde aanbieders te beheersen. Hieronder valt onder andere een uitgebreid due diligence assessment bij aanvang van het contract en risicogestuurde monitoring om te beoordelen of derde partijen blijven voldoen aan de in het contract vastgelegde afspraken.

Regelmatige audits
Voor auditors is het goed te weten dat beide wetgevingen voorschrijven dat ketenrisicobeheersing onderworpen moet worden aan regelmatige audits. Artikel 29 van NIS-2 spreekt bijvoorbeeld over regelmatige audits en gerichte beveiligingsaudits. Artikel 5.7 van DORA stelt dat auditors regelmatig (dat wil zeggen afhankelijk van de ICT-risico's van de

Vacatures

Wij groeien, groei jij met ons mee?

Vanberkel Professionals is dé financieel en juridisch expert in interim- en advies opdrachten binnen de brede publieke sector. Om ons kernteam van 130 professionals te versterken en aan onze klantvragen te voldoen zoeken wij adviseurs, auditors, controllers, juristen en managers met kennis op het gebied van Finance of Legal.

Wij zijn op zoek naar: **(Interim) Professionals en Consultants in Finance en Legal**

Wij komen graag in contact met bevlogen en deskundige professionals met ervaring in Bestuursrecht, (IT)-Audit, Bedrijfsvoering, Control, Data, Financieel Advies en/ of Subsidies die inzetbaar zijn binnen Lokaal bestuur, Rijksoverheid en/of Woningcorporaties.

Voel jij je thuis in een omgeving waar zelfstandigheid en teamspirit samengaan? Waar vertrouwen en openheid tot het DNA behoort? Zoek je een betrokken werkgever die persoonlijke aandacht combineert met vakinhoudelijke en beroepsmatige ontwikkeling en waar je aan verschillende opdrachten kunt werken? Dan pas jij goed in ons team!

Wij bieden goede primaire en secundaire arbeidsvoorwaarden waaronder een vast contract na het succesvol doorlopen van je proeftijd, een auto- en bonusregeling en ruime ontwikkelingsmogelijkheden op het gebied van opleidingen en trainingen met een onbeperkt opleidingsbudget.

Voor meer informatie kun je contact opnemen met onze Corporate Recruiters: Désirée van der Kruk (**06 22 91 15 09**), Ilse Stokman (**06 29 48 22 24**) en Corina Minguel (**06 22 53 95 02**) of **recruitment@vbprofs.nl**

Ook voor W&S ben je bij ons aan het juiste adres!

Laten we samenwerken aan ambities!

financiële entiteit) moeten controleren of financiële instellingen effectief ICT-risico's beheersen, waaronder risico's geïntroduceerd door derde partijen.

Toenemende kosten
Nu de regeldruk rond derde-partijenrisico's vanuit verschillende kanten toeneemt, zullen organisaties moeten accepteren dat de kosten voor (keten)risicobeheersing zullen stijgen. Onze stelling is echter dat organisaties die investeren in een volwassen ketenrisicobeheersingsorganisatie onder de streep voordeliger uit kunnen zijn dan organisaties die dit nalaten en maar blijven 'doormodderen'.

Third party risk management
Uit onderzoeken van Deloitte en KPMG blijkt dat third party risk management bij veel organisaties nog in de kinderschoenen staat. Zo ontbreekt volgens deze onderzoeken in veel gevallen een goed geëquipeerde organisatie voor ketenrisicobeheersing, zijn rollen en verantwoordelijkheden binnen de organisatie onduidelijk belegd en wordt er onvoldoende gebruikgemaakt van technologie die inzicht geeft en delen van het (repetitieve) werk automatiseert.
Het gevolg is dat hoogopgeleide en schaarse professionals veel tijd kwijt zijn aan vrij simpel werk, zoals het opstellen en versturen van vragenlijsten, het vinden van de juiste verantwoordelijke collega's binnen de organisatie, het najagen van reacties en het bijhouden van spreadsheets. Werkzaamheden die in hoge mate geautomatiseerd kunnen worden zodat risk professionals zich kunnen richten op het daadwerkelijk mitigeren van onacceptabele risico's. Bij een hogere volwassenheid van ketenrisicobeheersing hoort ook een meer slimme samenwerking tussen organisaties. Zo zou op sectorniveau meer samengewerkt kunnen worden om kosten van individuele organisaties te drukken en de kwaliteit van bijvoorbeeld de assessmentvragenlijsten te verbeteren.

Krapte op de arbeidsmarkt
Het behoeft geen toelichting dat er momenteel sprake is van een enorme krapte op de arbeidsmarkt. Deze krapte maakt het noodzakelijk dat het beschikbare risicomanagementtalent in organisaties zo effectief en efficiënt mogelijk wordt ingezet. Dit geldt ook voor ketenrisicobeheersing. Heldere doelstellingen en strategie, duidelijk omschreven rollen en verantwoordelijkheden, en goede ondersteunende technologie maken ketenrisicobeheersing meer volwassen. Bovendien maken ze de discipline veel aantrekkelijker voor de toch al zo schaarse risicoprofessional.

Tot slot: Wat kunnen auditors doen?
Auditors kunnen een belangrijke rol vervullen bij het verder professionaliseren van ketenrisicobeheersing binnen organisaties. Bijvoorbeeld door op het volgende te letten:

• *Actueel overzicht* – Ketenrisicobeheersing begint met een gedegen en actueel inzicht in de keten. Auditors moeten er dus op toezien dat de juiste randvoorwaarden gecreëerd zijn om tot dit complete en actuele overzicht te komen. Daarbij is het cruciaal dat bekend is welke derde partijen toegang hebben tot het bedrijfsnetwerk en wie de contactpersoon binnen de securityafdeling is.

• *Data triangulatie* – Enkel data verkregen uit self-assessmentvragenlijsten van derde partijen geeft onvoldoende zekerheid over eventuele risico's. Daarom is het belangrijk dat auditors aansturen op het gebruik van verschillende databronnen, bijvoorbeeld cybersecurityscores, nieuwsbronnen en fysieke inspecties. Bovendien zouden auditors kritisch moeten zijn op de frequentie van self assessments – namelijk gebaseerd op het risico van de derde partij en ook op basis van kritieke dreigingen zoals zero days

• *Risicogebaseerde opvolgingen* – Soms komen organisaties niet verder dan het identificeren van risico's uit due diligence assessments. Echter, een volwassen ketenrisicobeheersingsorganisatie zorgt ervoor dat er ook goede opvolging gegeven wordt. Hier zouden auditors op moeten sturen.

• *Frictieloze klantreis voor derde partije*n – Steeds meer organisaties voeren due-diligenceactiviteiten uit wanneer ze zaken willen doen met een derde partij. Het gevolg is dat de gemiddelde organisatie heel wat tijd spendeert aan het invullen van deze vragenlijsten. Hoe gemakkelijker en leuker je dit werk kunt maken, hoe hoger de betrouwbaarheid en kwaliteit van de antwoorden. Auditors zouden daarom kritisch moeten zijn op hoe de klantreis voor derde partijen is vormgegeven.

• *Aansturen op het gebruik van standaarden* – Hoe meer organisaties gebruik gaan maken van internationale standaarden (denk aan ISO 27001, NIST, CIS of SOC2), hoe gemakkelijker ingevulde vragenlijsten in de toekomst uitgewisseld kunnen worden. Dit zou een enorme winst betekenen voor het hele ecosysteem. Auditors zouden daarom kunnen aansturen op het volgen van internationale standaarden bij het opstellen van due-diligence-assessmentvragenlijsten. <<

Organisaties die investeren in een volwassen ketenrisicobeheersingsorganisatie kunnen voordeliger uit zijn dan organisaties die maar blijven 'doormodderen'

Bram Ketting is medeoprichter en CEO van 3rdRisk.
Jelle Groenendaal is chief product owner (CPO) bij 3rdRisk and senior associate onderzoeker bij Crisislab. Tevens is hij verbonden aan de IT Audit Compliance & Advisor- opleiding van de Vrije Universiteit Amsterdam.

Tekst Henriette van Vugt
Beeld Adobe Stock
Claudio Schwarz

Meer *effect* met DATA-ANALYSE

Data-analyse wordt steeds belangrijker in de auditwereld. Ook binnen Audit Rabobank, waar we onder andere data driven assurance (DDA) verschaffen. De snelle ontwikkeling van DDA roept wel nieuwe vragen op: hoe volwassen zijn we als internal auditors in het toepassen van DDA? Hoe hoog leggen we de lat? En, hoe komen we daar? Het DDA-volwassenheidsmodel biedt houvast.

Steeds meer auditafdelingen van organisaties hebben DDA als belangrijk speerpunt aangewezen. Het vertrekpunt, in welke mate DDA nu al wordt toegepast en effect heeft in de audit, verschilt sterk tussen deze afdelingen. Echter, zowel auditafdelingen die op lagere als auditafdelingen die op hogere DDA-volwassenheidsniveaus presteren, hebben er baat bij om te bepalen wat werkt en waarom.

Deze kennis maakt het mogelijk om DDA-werk te systematiseren en om het echt onderdeel te maken van het DNA van de auditafdeling. Ook kan, ongeacht de huidige DDA-activiteiten in een auditafdeling, het vergroten van het begrip en zelfbewustzijn over DDA-volwassenheid de kwaliteit van het DDA-werk verbeteren. Uiteindelijk vergroot dit de impact van een auditafdeling op de hele organisatie.

DDA in de Rabobankorganisatie

Binnen Audit Rabobank hebben we gekozen voor een gespecialiseerd team van data-analisten, -scientists en -consultants, het zogenoemde audit data excellence team (ADET). Dit team heeft de opdracht om de auditteams te transformeren en het toepassen van data-analyse te versnellen. En dit in alle domeinen en wereldwijd, zoals credit, compliance, IT en Retail.

ADET werkt daarbij samen met een auditor in elk domein, die de opdracht heeft om DDA in de auditopdrachten van het eigen domein tot een succes te maken. Binnen Audit Rabobank wordt dit de dedicated product owner of DPO genoemd. Afhankelijk van het auditteam en het type audit, wordt DDA steeds vaker in verschillende fasen van de audit toegepast, van planning tot veldwerk en rapportage. Denk hierbij aan op signalen gebaseerde risicobeoordeling, het scopen van de audit, het bepalen van een risicosteekproef en het geautomatiseerd testen van de werking van controls. Het meten van het volwassenheidsniveau van DDA in de interne auditfunctie is belangrijk om te weten waar we staan én om te bepalen waar we naartoe willen.

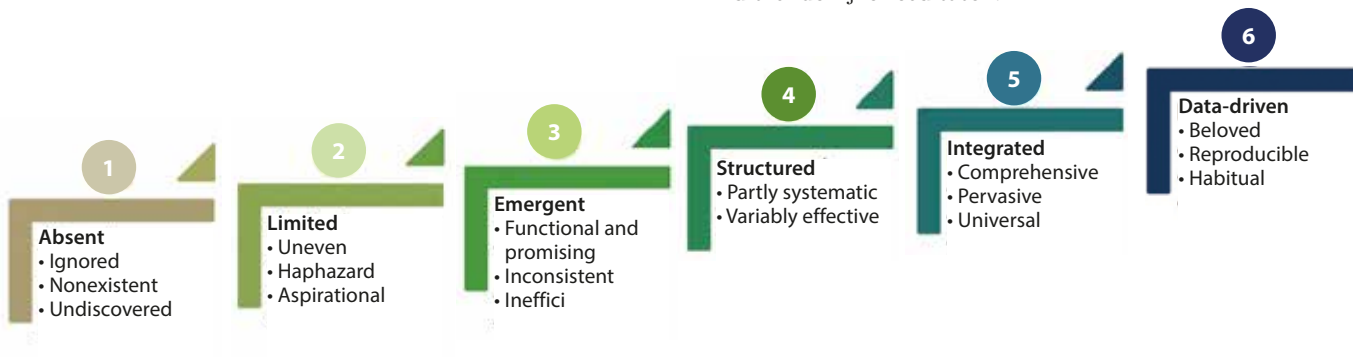
Het meten van DDA-volwassenheid
Het veelgebruikte en bekende IIA-ambitiemodel wordt gebruikt om de kwaliteit te meten van allerlei aspecten van een interne auditfunctie en om de ambities voor de toekomst te formuleren. Een van de vele aspecten in dit model is data-analyse, dat met zeven andere topics (waaronder role and authority, governance and risk management, strategy en soft sontrols) wordt geschaard onder het thema: services and role of internal auditing.

Dit grotere thema wordt gescoord op een volwassenheids-schaal. Echter, wij voelden de behoefte om gedetailleerder te kijken naar de volwassenheid van DDA in de organisatie dan het IIA-ambitiemodel doet. Data-analyse omvat vele aspecten en het is de moeite waard om dieper naar deze aspecten te kijken om het huidige volwassenheidsniveau gedetailleerder vast te stellen, ambities beter te kunnen bepalen en te versnellen in de toepassing van aspecten.

Uitgangspunten van een meer gedetailleerde meting van de volwassenheid van DDA zijn:
1. het gebruik van verschillende volwassenheidsniveaus;
2. het onderscheiden van verschillende aspecten om tot een eindoordeel te komen;
3. de bruikbaarheid in de Audit Rabobankomgeving: het DDA-volwassenheidsmodel als meetinstrument en communicatiemiddel om de toepassing te versnellen.

DDA-volwassenheidsniveaus
Het denken over volwassenheid is een hot topic dat relevant is voor verdere professionalisering van de auditfunctie. Het is al langer een gedachtegoed in de software engineering (capability and maturity model), en je ziet het ook terug in de accountancy (zoals bijvoorbeeld blijkt uit een special van het *Maandblad voor Accountancy en Bedrijfseconomie* uit 2020).

Bij de ontwikkeling van ons DDA-volwassenheidsmodel zijn we uitgegaan van een bestaand gedetailleerd model: het UX-volwassenheidsmodel.1 We hebben dit model aangepast voor DDA en uitgebreid. Het model onderscheidt zes volwassenheidsniveaus (zie *figuur 1*):
1. Afwezig – DDA wordt genegeerd of bestaat niet.
2. Beperkt – DDA-werk is zeldzaam, wordt ad hoc gedaan en is niet belangrijk.
3. Opkomend – het DDA-werk is functioneel en veelbelovend, maar wordt inconsistent en inefficiënt uitgevoerd.
4. Gestructureerd – de organisatie heeft een semisystematische DDA-gerelateerde methodologie die wijdverbreid is, maar met een verschillende mate van effectiviteit en efficiëntie.
5. Geïntegreerd – DDA-werk is veelomvattend, effectief en alomtegenwoordig.
6. Data driven – systematisch gebruik van DDA op alle (organisatie)niveaus leidt tot diepgaande inzichten en uitzonderlijke resultaten.



Figuur 1. De zes volwassenheidsniveaus van DDA

DDA-aspecten
We onderscheiden zeven DDA-aspecten die elk kunnen worden gescoord op deze zes niveaus. De aspecten zijn: ADET-ondersteuning, efficiëntie, waarde-focus, DDA-activiteiten, hergebruik, advies en kwaliteit. De combinatie van aspecten en volwassenheidsniveaus levert een 7x6 matrix op (zie *figuur 2*).

Bruikbaarheid: meetinstrument
De 7x6 matrix is praktisch toepasbaar gemaakt door middel van een vragenlijst. Over elk aspect (bijvoorbeeld, efficientie) wordt één vraag gesteld. De antwoordcategorieën beschrijven de zes volwassenheidsniveaus (bijvoorbeeld, van 'No DDA applied' tot 'Efficiency gains are accelerating; The audit process is redefined'). Dit maakt het invullen makkelijk: welke beschrijving past het best?

Als alle zeven vragen zijn ingevuld kan worden bepaald wat het gemiddelde DDA-volwassenheidsniveau is (alle scores/7) of welk niveau de overhand heeft (bijvoorbeeld, vier van de zeven vragen worden gescoord in niveau 2). Elk team binnen een auditafdeling kan de vragenlijst zelfstandig invullen om te zien waar het staat. Binnen Audit Rabobank zijn er teams met een dominant 'beperkt' volwassenheidsniveau en anderen met een dominant 'gestructureerd' volwassenheidsniveau.

Het ambitieniveau
Een volgende stap is het bepalen van het ambitieniveau. Een afdeling met een beperkt volwassenheidsniveau kan de ambitie hebben binnen een bepaalde periode te komen tot een 'opkomend' volwassenheidsniveau. Hierna wordt bedacht wat er nodig is om dit niveau te bereiken. Denk aan

Het meten van het volwassenheidsniveau van DDA in de interne auditfunctie is belangrijk om te weten waar we staan én om te bepalen waar we heen willen

DDA-trainingen voor specifieke tools of methoden, DDA-brainstormsessies om te komen tot relevante ideeën en hypothesen, het hergebruiken van bestaand DDA-werk zoals dashboards en het van elkaar leren.

Om de versnelling te realiseren is ook het bespreken en doorbreken van belemmeringen van cruciaal belang. Veelgehoorde belemmeringen zijn het niet op tijd verkrijgen van relevante data, het niet weten waar te beginnen en daardoor het blijven gebruiken van de traditionele auditmethoden en het geen tijd vinden om analyses uit te voeren. Meer aandacht kan gegeven worden aan die aspecten die achterlopen op de rest of die als lastig worden ervaren. Bijvoorbeeld, het is mogelijk dat analyses gedaan worden binnen audits met behoorlijke impact, maar dat buiten de audits niemand elkaars DDA-werk en dashboards kent en 'hergebruik' dus achterloopt.

	Absent 1	Limited 2	Emergent 3	Structured 4	Integrated 5	Data-driven 6
ADET support	Pool does not do DDA, even with ADET support.	Pool needs ADET support for all DDA activities (data-driven mindset, finding data, analyses).	Pool needs ADET support for most DDA activities (e.g., data-driven mindset, analytics) except finding relevant data.	Pool needs ADET support for advanced analyses only.	Pool is almost self-sufficient. Limited ADET support needed.	Pool is self-sufficient. No ADET support needed.
Efficiency	No DDA applied.	No efficiency gains.	Small efficiency gains in some audits due to DDA usage in planning, fieldwork, or reporting.	Substantial efficiency gains in some audits due to DDA usage in planning, fieldwork, or reporting.	Impressive efficiency gains in most audits due to DDA usage in planning, fieldwork, or reporting.	Efficiency gains are accelerating; The audit process is redefined.
Value focus	No focus on any aspect of DDA.	Focus on awareness and encouraging to learn to use DDA.	Focus on strengthening the DDA skills of pool analysts.	Focus on applying DDA structurally, mainly by pool analysts. Less focus on the added value of DDA for the audit.	DDA is applied structurally. Focus on the added value of DDA for the audit, i.e. increased effectiveness or compliance.	Focus on outperforming with DDA; Optimizing value for the audit universe.
DDA activities	No DDA activities.	First pilots e.g. statistical sampling. Ideation for applying analytics.	Piloting and ad hoc, mostly basic, analytics. applied mainly by pool analysts. Ideation on more advanced analytics.	Both basic and advanced analytics, applied mainly by pool analysts. Ideation on full range of analytical methods.	Both basic and advanced analytics applied by all auditors in the pool. Ideation on full range of analytical methods.	The full range of analytical methods including predictive analytics is used to optimally support all audits.
Reuse	No reuse of DDA dashboards and workflows.	Exploring usage of existing dashboards and workflows.	Usage of existing dashboards; Occasional reuse of workflows.	Reuse of dashboards and workflows as much as possible; Build on top of existing DDA work.	Dashboards used extensively; Automatic reperformance through continuous data pipelines.	Smart integration of dashboards and automatic analyses; Seamless collaboration with other pools.
Advise	Poor DPO advise.	DPO advise of mediocre quality (lacking clear hypotheses, methods, and/or data need).	DPO advise of good quality (clear hypotheses, methods, data need), but not always followed up.	DPO advise of good quality, and is generally followed up. Advice not always integrated in the announcement letter.	DPO advise of good quality, and is always followed up. Advice integrated in the announcement letter.	DPO advise serves as example for other pools because of high quality. Advise gives clear direction to the audit and is always followed up.
Quality	Not applicable (No DDA).	Variable DDA quality; peer reviews by ADET needed to repair flaws or increase trust in analyses performed.	Reasonable DDA quality; peer reviews by ADET show no real flaws but help to alter the DDA work.	Good DDA quality; Peer reviews are done within the pool. DDA work serves as an example for other pools.	Consistent high DDA quality. Pool performs peer reviews on DDA work of other pools.	Pool is seen as expertise centre that produces high quality DDA work.

Figuur 2. 7x6 matrix met combinatie van aspecten en volwassenheidsniveaus

Bruikbaarheid: communicatiemiddel
We merken dat het DDA-volwassenheidsmodel een veel meer open en meer resultaatgericht gesprek over de DDA-ambitie mogelijk maakt. Te denken valt aan hoe de zaken ervoor staan én wat er nodig is ambities te realiseren. Aan welke hulp is behoefte? Hoe kan het werk efficiënter worden met behulp van DDA? Welke bestaande dashboards worden nog te weinig hergebruikt en hoe kan hergebruik gestimuleerd worden? Wat is de kwaliteit van het DDA-advies aan de auditmanagers? Wat is er voor nodig om de kwaliteit van het DDA-werk te verhogen? Het model is dus niet alleen bruikbaar gemaakt doordat er een vragenlijst aan gekoppeld is, maar ook doordat het als communicatie(hulp)middel ingezet kan worden om de dialoog over DDA te ondersteunen.

De DDA-ambitie van Rabobank
De huidige ambitie van Audit Rabobank is om te komen tot het geïntegreerde volwassenheidsniveau: DDA-werk is veelomvattend, effectief en alomtegenwoordig. Naast de zeven aspecten zoals beschreven in de matrix, zoals toename in efficiëntie en kwaliteit, houdt dit concreet in dat we ons willen richten op:

- Op data gebaseerde auditplanning. Door data onderbouwde prioriteitsstelling in de risicoanalyse en auditplanning.
- Data-first audits – Audits worden 'by default' data driven uitgevoerd en zo niet moet worden uitgelegd waarom.
- Bijna-realtime auditing – Datasignalen leiden op vrijwel continue basis tot auditwerkzaamheden door gebruik van slimme algoritmes.
- Algorithm assurance – Er worden steeds meer geavanceerde methoden op basis van machine learning en artificial intelligence gebruikt in de organisatie. Audit wil in staat zijn om hier een goed oordeel over te vormen als opmaat naar algorithm assurance.

Dit is een hoge ambitie, en we zijn ons er terdege van bewust dat dit opschalen aanzienlijke moeite en tijd zal kosten. Ook verwachten we dat er niet altijd een lineaire progressie zal zijn; het kan zelfs uitdagend zijn om een bepaald niveau vast te houden. Belangrijke voorwaarden voor succes zijn de steun van het management, goede samenwerking met eerste en tweede lijn, en het geloof dat DDA een belangrijke plek zal (blijven) innemen in de toekomst.

Voorwaarden voor succes zijn de steun van het management, een goede samenwerking met eerste en tweede lijn, en het geloof dat DDA een belangrijke plek inneemt

Vervolg
Inmiddels is het vrij onomstreden dat DDA veel kansen biedt om auditafdelingen beter, sneller en toekomstgerichter te maken. DDA verdient het om genoeg aandacht te krijgen. Het DDA-volwassenheidsmodel helpt om meer diepte aan te brengen op het vlak van DDA-ambities van een auditafdeling. Het explicieter maken en communiceren van ambities op het gebied van DDA is belangrijk om bewuster te groeien en om het tempo van de ontwikkelingen in het vakgebied én van andere auditafdelingen, die zeker niet stilstaan op DDA-gebied, bij te houden.

Een vervolg kan zijn om dit model verder te integreren met het IIA-ambitiemodel, zodat nog scherper op groei in DDA-volwassenheid kan worden gestuurd naast de andere relevante factoren. <<

Noot
1. Pernice, K., Gibbons, S., Moran, K. and K. Whitenton, The 6 Levels of UX Maturity.

Henriette van Vugt werkt sinds 2019 als datascientist binnen Audit Rabobank. Ze promoveerde aan de VU Amsterdam op het gebied van mens-computerinteractie en werkte als onderzoeker en ontwerper bij Philips Research en Rabobank. Ook doceert zij DDA aan Tilburg University.

Tekst Drs. Annemarie van de Langenberg-de Reuver RC
Ing. Joost van Beijsterveld MSc RE CISA
Beeld Adobe Stock
Jumbo

Agile auditing @ Jumbo: a good practice

Van rapport in de la naar acties op de vloer: hoe Jumbo internal audit het agile-gedachtegoed implementeerde in haar werkwijze. Van log en weinig draagvlak naar wendbaar met een brede acceptatie met behulp van een kwartaalplanproces en een kernteam.

Hoe levert een internal auditafdeling toegevoegde waarde? Dit is de cruciale vraag ten aanzien van het bestaansrecht van het internal auditvakgebied. Als internal auditor wil je niet gezien worden als betweter, idealist of interne politieagent. Daarnaast wil je als internal auditor ook niet dat je doordachte analyses, verbeterplannen en actiepunten in een bureaula belanden. Hoe creëer je als internal auditafdeling commitment en draagvlak? Hoe zorg je ervoor dat verbeteringen worden doorgevoerd en hoe behoud je tegelijkertijd je onafhankelijkheid? In dit artikel is te lezen hoe Jumbo (motto: 'elke dag beter') de antwoorden op deze vragen succesvol heeft geïmplementeerd.

Beperkte opvolging van bevindingen
Als internal auditafdeling binnen Jumbo werden wij tot 2020 vooral gezien als een club slimme mensen die processen analyseerden en maanden hard werkten aan degelijke en lijvige rapporten. De vergelijking werd weleens gemaakt met een auto met een vermogen van 400 pk waarvan maar 100 pk werd gebruikt. Onze aanbevelingen waren objectief en feitelijk juist, maar werden beperkt opgevolgd.

Voor de operationeel verantwoordelijke afdelingen kwam de lijst met bevindingen vaak als een verrassing en bovenop al het andere werk. Hierdoor was er geen tijd en capaciteit beschikbaar om iets met de aanbevelingen te doen en volgde men de auditbevindingen beperkt op. Dit leidde tot frustratie bij het auditteam.

Hoe vergroten we de acceptatie?
Ons bestaansrecht is Jumbo 'elke dag beter' maken, maar het effect van onze audits was te klein. Dus moesten wij aan de slag met ofwel de kwaliteit ofwel de acceptatie van onze adviezen. Onze inschatting was dat de kwaliteit van de audits en de (vak)inhoudelijk kennis van het auditteam op orde waren, maar dat we een uitdaging hadden in het creëren van draagvlak. We constateerden dat onze werkwijze te rigide en zelfstandig was met te weinig tussentijdse afstemming en bijsturing met onze interne klanten. Dat leidde tot de vraag: hoe kunnen we ons proces aanpassen om de acceptatie van de auditbevindingen te vergroten?

De oplossing: agile auditing
We besloten om onze interne klanten, de operationeel verantwoordelijke collega's en controlling, nauwer bij ons proces te betrekken. Hiervoor hebben we een nieuwe werkwijze ontwikkeld die is gebaseerd op agile en die goed past bij het ondernemende karakter van Jumbo. De veranderingen hebben we (conform het agile-gedachtegoed) in kleine stapjes doorgevoerd. Dit was belangrijk, omdat het behoorlijk wat aanpassingsvermogen vereiste van de auditors zelf. Zekerheden kwamen op losse schroeven te staan en dit leidde tot discussies en wezensvragen over het auditvak. Naast het bereiken van meer toegevoegde waarde leidde dit ook tot meer werkplezier bij alle betrokkenen. Graag delen we onze werkwijze om inspiratie en handvatten te geven hoe agile auditing kan werken: ook in uw situatie!

In onze aanpak onderscheiden wij twee hoofdprocessen. Het kwartaalplanproces en het auditproces. We lichten beide toe en beschrijven hoe wij hieraan invulling geven.

Jumbo is een familiebedrijf dat de afgelopen jaren zeer snel is gegroeid door diverse overnames. Er werken op dit moment honderdduizend mensen in de bijna zevenhonderd supermarktwinkels in Nederland en België. Naast de supermarkten en de restaurants van La Place is er ook een groeiend online kanaal. De complexiteit is groot en de technologische en organisatorische veranderingen volgen elkaar in hoog tempo op.

De internal auditafdeling bestaat uit een manager en zeven medewerkers (zes auditors met verschillende RA-, RE- en RO-achtergronden en een fraude- en security-analist) en is direct gepositioneerd onder de raad van bestuur (RvB). Tevens rapporteert de manager Internal Audit aan de voorzitter van de audit committee. De werkzaamheden van de afdeling bestaan naast het uitvoeren van (operational) audits, uit het reviewen van self assessments op het internal control framework (ICF).

We geven geen assurance, doen geen werkzaamheden voor de accountant en we hebben geen terugkerende audits. Wel dragen we bij aan de doelstellingen van de organisatie en omarmen we het Jumbo DNA (Samen, Ondernemen en Winnen) in onze aanpak.

We voeren audits uit op onderwerpen die actueel zijn en waar de organisatie ook echt op zit te wachten, zoals de evaluatie van een organisatiewijziging of de executie van promoties op de winkelvloer in het licht van operational excellence. Op deze manier geven we advies en inzicht rondom actuele thema's.

Kwartaalplanproces: elke dag van een auditor is goud waard!

De cadans van ons planningsproces

Binnen onze 'agile auditing @ Jumbo'-aanpak is het kwartaalritme van groot belang. Ieder kwartaal voeren we drie audits uit. Alle audits beginnen en eindigen op hetzelfde moment.

Het voordeel hiervan is drieledig: 1) er is focus en transparantie, 2) de harde deadline dwingt tot keuzen en 3) na ieder kwartaal kan gemakkelijk gewisseld worden van teamsamenstelling.

De harde deadline maakt het extra belangrijk om de scope van de audit goed af te bakenen, te bewaken en af te stemmen. Tegelijkertijd heeft de praktijk ons geleerd dat een langere doorlooptijd (als gevolg van een bredere scope) niet per se leidt tot meer toegevoegde waarde.

Een dynamische auditbacklog

Wij werken in het kwartaalplanproces niet met een auditjaarplan, maar met een backlog. Hierop staan alle mogelijke auditonderwerpen gesorteerd per aandachtsgebied (vaak gekoppeld aan de directieportefeuille). De portefeuilles zijn verdeeld onder de auditors en naast de backlog bespreken we ieder kwartaal tevens de uitkomsten van het ICF en de voortgang op voorgaande audits.

Hoe komen we tot geschikte auditonderwerpen?

Iedereen kan auditonderwerpen aandragen. Wij stimuleren zowel de operationeel verantwoordelijke afdelingen als controlling om aan te geven waar ze risico's zien, waar ze zich niet helemaal comfortabel over voelen, of waar ze een onafhankelijke mening over willen hebben. Zeker processen die directieportefeuilleoverstijgend zijn, lenen zich bij uitstek goed voor een audit. Uiteraard denken we ook zelf na over mogelijke onderwerpen op basis van onze eigen risico-inschatting, of ze komen als verdiepingsslag uit een voorgaande audit.

Als de organisatie een audit-onderwerp niet ziet zitten doen we het niet

Prioritering
De onderwerpen op de backlog wegen en prioriteren we aan de hand van vijf verschillende criteria, waaronder de impact op de klant, het risicoprofiel en de mate waarin het proces onderhevig is aan veranderingen. Dit doen we zes weken voor aanvang van het kwartaal. Voor de Top-5 onderwerpen stellen we vast wat het meeste waarde oplevert voor de organisatie, of alle betrokkenen er voldoende tijd en aandacht aan kunnen besteden en of er voldoende spreiding zit in de onderwerpen.

Op deze manier gaan we altijd aan de slag met zaken die actueel zijn en waar de organisatie op dat moment behoefte aan heeft. Sterker nog, als er geen overeenstemming is en men ziet de toegevoegde waarde van de audit niet in, dan doen we het niet. Het is immers al vaak genoeg gebleken dat de audit dan moeizaam in beweging komt en dat er achteraf weinig opvolging plaatsvindt.

Afstemmen van onderwerpen en uitkomsten
Als de onderwerpen helder zijn, stemmen wij dit af met de RvB, de Jumbodirectie en het audit committee (van de raad van commissarissen) en maken we de ideale teamindeling gebaseerd op de persoonlijke voorkeur, kennis en ervaring van de teamleden en de benodigde (soft) skills. Vervolgens gaan de teams van start. Aan het eind van het kwartaal presenteren wij de bevindingen in een eindpresentatie aan de opdrachtgever en rapporteren wij de uitkomsten op hoofdlijnen aan het audit committee.

Auditproces: alleen ga je sneller, samen kom je verder!
Het succes van het kernteam
Het formeren van een kernteam met onze interne klant is de belangrijkste succesfactor om daadwerkelijk toegevoegde waarde te leveren, en te zorgen dat er iets met de uitkomsten van de audit gebeurt. Dit is de belangrijkste verandering ten opzichte van de traditionele aanpak. Zonder kernteam geen audit!

In dit kernteam zitten naast de auditors alle relevante personen uit de business die uiteindelijk een rol hebben in het uitvoeren van de gedefinieerde acties (vaak één niveau onder de directie). Vooraf weten we meestal wie in het kernteam hoort, soms vullen we tijdens de audit dit team aan mocht dat nodig zijn.

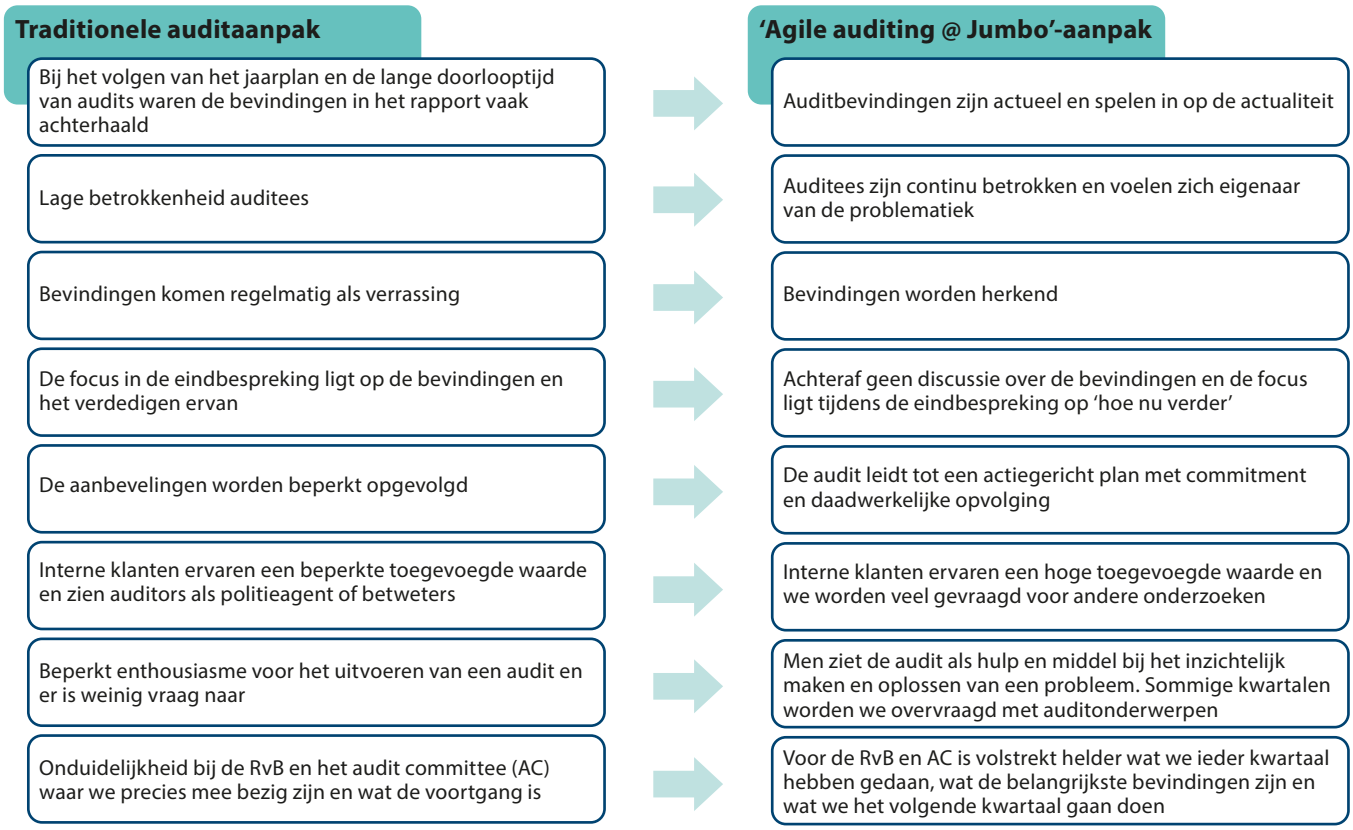
Voortdurende afstemming en bijsturing
Met het kernteam bespreken we tweewekelijks het verloop van de audit, maar ook de aanpak, voorlopige bevindingen, oplossingsrichtingen en waar nodig sturen we bij of escaleren we.

In overleg met het kernteam passen we tussentijds onze aanpak aan. Zo identificeren we tijdens de audit nieuwe risico's die het onderzoeken waard zijn en beslissen we samen welke zaken we niet meer kunnen doen. Andersom gebeurt ook regelmatig. Als een bevinding voldoende duidelijk is en men gaat hiermee aan de slag, dan onderzoeken we dit onderwerp niet verder. Op deze manier sturen we tweewekelijks (per sprint) bij, wat veel overbodig auditwerk voorkomt.

Alle disciplines aan tafel
Een ander voordeel van het formeren van een kernteam is dat alle relevante disciplines aan tafel zitten en meteen met elkaar in gesprek gaan over wat wel en niet werkt. Door deze collega's doorlopend te betrekken, komen de bevindingen achteraf niet als een verrassing en denken ze zelf mee in de oplossingsrichting. Zo creëren we direct draagvlak en komen we tot een gedragen actieplan. Bovendien ontstaat er verbinding tussen de kernteamleden. Dit voordeel komt ook terug in het artikel 'Wendbaarheid met internal audit deelproducten' van De Korte, Otten en Schuiten op auditmagazine.nl, dat daar een dubbele interventie wordt genoemd.

En onze onafhankelijkheid dan?
Deze aanpak kan vragen oproepen over onze onafhankelijkheid. Wij bewaken deze onafhankelijkheid te allen tijde. Alleen wij als auditors bepalen de definitieve aanpak, wij waarborgen dat de juiste discussies worden gevoerd en bepalen de inhoud van onze rapportages. Dit doen we het liefst zoveel mogelijk in samenspraak en met input van het kernteam, omdat we hebben geleerd dat je samen het meest bereikt!

Een actiegericht verbeterplan mét draagvlak
Door agile auditing worden tijdens de audit sommige bevindingen al opgelost door het kernteam. Deze oplossingen nemen we direct op in ons rapport. Voor de overige bevindingen bespreken we gezamenlijk met het kernteam wat de uiteindelijke oplossing is die voor alle partijen werkt. Dit vertaalt zich naar een overzicht met concrete acties, gecommitteerde eigenaren en heldere tijdslijnen. Daarmee gaan we een stuk verder dan het uitbrengen van theoretische adviezen zonder draagvlak die hoogstwaarschijnlijk niet opgevolgd worden.



Figuur 1. Overzicht wat 'agile auditing @ Jumbo' heeft gebracht

Eindbespreking
Dit actieplan laten we door de verantwoordelijken uit het kernteam presenteren in de eindbespreking met de opdrachtgever. Discussies vinden rechtstreeks plaats tussen opdrachtgever en verantwoordelijken. Wij auditors zitten de eindbespreking voor en luisteren en spreken kritisch mee.

Sinds de implementatie van onze agile-aanpak ligt de nadruk tijdens de eindbespreking vooral op 'hoe nu verder?' Na afloop van de eindbespreking ligt er een definitief actieplan met commitment vanuit de business. Wij monitoren in de toekomst of de afgesproken acties (tijdig) worden opgepakt en geïmplementeerd.

Retrospectie: 'elke dag beter'
Na afloop van de audit kijken we met het auditteam terug op het verloop van de audit. Enerzijds bespreken we de leerpunten vanuit de kwaliteitsreview. Anderzijds benoemt ieder teamlid wat goed en minder goed ging om hiervan te leren.

Daarnaast sturen we een korte tevredenheidsenquête naar het kernteam en de opdrachtgever. Waar nodig gaan we over de uitkomsten in gesprek. Op deze manier leren we ook vanuit het perspectief van de auditee wat we beter kunnen doen en wat men juist goed heeft ontvangen. Met deze feedback sleutelen we continu aan onze 'agile auditing @ Jumbo'-aanpak en aan onszelf.

Tot slot: effectiviteit = kwaliteit x acceptatie
Om meer toegevoegde waarde te leveren en de organisatie op basis van onze audits daadwerkelijk in beweging te krijgen, hebben wij de oplossing voornamelijk gevonden in het verhogen van het draagvlak en de acceptatie bij de auditee. We doen audits die op dat moment relevant zijn (kwartaalplanproces). En binnen de audits zelf betrekken we de verantwoordelijken continu en sturen we steeds bij (auditproces).

Vanuit de traditionele aanpak hadden we voorheen de neiging de auditaanpak tot in detail uit te werken. Het voelde vreemd om af te wijken van de aanpak die ons is aangeleerd en die we jarenlang hebben toegepast. De IIA Standaarden geven je echter de ruimte om het anders te doen. Het is juist krachtig en efficiënt om niet de hele aanpak vooraf tot in detail uit te werken, maar dit enkel op hoofdlijnen te doen en steeds bij te sturen op basis van nieuwe inzichten en veranderende behoeften vanuit het kernteam.

Samengevat hebben we met onze eigen variant op agile auditing veel bereikt en leveren we meer toegevoegde waarde voor Jumbo (zie *figuur 1*). Het agile-auditingproces wordt omarmd, zowel door het internal auditteam als door de organisatie als geheel. Wij willen echt niet anders meer. <<

Drs. Annemarie van de Langenberg-de Reuver RC is manager Internal Audit bij Jumbo en heeft naast controlling ook diverse jaren IT-managementervaring.
annemarie.vandelangenberg@jumbo.com

Ing. Joost van Beijsterveld MSc RE CISA is internal auditor bij Jumbo en heeft een achtergrond als IT-auditor bij BDO.
joost.vanbeijsterveld@jumbo.com

Meer weten? Schroom niet om contact op te nemen.

Tekst Ron de Korte RA RE RO CIA
Manja Knevelbaard MSc
Frank Schuiten MA
Beeld Adobe Stock

De trusted advisor: **verdiept** inzicht door **rust** en **focus**

Wat definieert de trusted advisor en hoe past deze rol in de auditfunctie? In dit artikel is te lezen wat het betekent om als trusted advisor te kunnen worden gezien.

In deze bijdrage verkennen we de rol van de trusted advisor allereerst door het te koppelen aan het begrip 'counsel' binnen de consultingactiviteiten van de internal auditfunctie (IAF). Dan benadrukken we wat Maister in 2000 met de term trusted advisor bedoelde. Vervolgens vertalen we dit naar randvoorwaardelijke factoren voor de auditfunctie. We bezien hoe de trusted-advisorrol past in de onderzoeksfunctie van de IAF. Ten vijfde belichten we de socratische gespreksvoering als een centrale techniek van de trusted advisor. We sluiten af met de stelling dat verdiept inzicht soms juist *niet* gebaseerd is op deugdelijk onderzoek. En met twee aanvullende eisen voor de trusted advisor: 'rust en focus'.

Vertalingen en definities

De bekende IIA-definitie van internal auditing is: 'Internal auditing is an independent, objective assurance and *consulting activity* (...)' 'Advies' wordt vaak als vertaling van consultingactiviteiten gebruikt, maar dit is te eenzijdig. Over *consulting activity* zegt het IIA immers: '(...) Examples include *counsel, advice*, facilitation, process design, and training' (De Korte, Otten & Schuiten, 2021).

Consulting activities zijn breder dan alleen 'advies'

Consulting activities omvatten dus advice. We benadrukken dat inhoudelijke adviezen in internal auditrapporten moeten zijn gebaseerd op adviesgericht of ontwerpgericht onderzoek. We stellen in diezelfde bijdrage voor (overeenkomstig het NOREA-studierapport Adviesdiensten, 2012) het onderscheid tussen assurance en consultingactiviteiten te baseren op wel of juist geen onderliggend onderzoek. In dit rapport wordt gesteld: 'Onderliggend aan assurance, audit én advies is "onderzoek" in brede zin. Praktisch gezien zal bij assurance de meeste nadruk wel liggen op normen(stelsels) en de toetsing daaraan, terwijl voor advies de meest "vrije" vormen van onderzoek mogelijk zijn en kunnen worden gekozen.'

Een definitie van counselor

Counsel wordt als eerste voorbeeld genoemd van consultingactiviteiten. De definitie vanuit de *Dikke van Dale* is: 'Iemand adviseren, helpen via het voeren van gesprekken, die hem inzicht proberen te geven in zijn moeilijkheden'. Een counselor is in dezen een adviseur, hulpverlener, raadsman. Deze vorm past uitstekend bij het repertoire van de trusted advisor. Let wel, een adviseur kan zichzelf niet als zodanig bestempelen. De ander (veelal een manager) bepaalt of de adviseur op zakelijk én persoonlijk vlak in vertrouwen wordt genomen, omdat er sprake is van 'chemie in de relatie', leidend tot verdiepende inzichten, innovaties en actiegerichtheid. En daarmee dus vertrouwd (trusted) is.

De trusted advisor conceptueel bekeken vanuit Maisters gedachtegoed

In zijn presentatie tijdens het IIA-seminar 2021 vergeleek De Korte de trusted advisor met een sportarts. Een sportarts is

geschoold in de anatomie van het menselijk lichaam, maar weet ook wat nodig is om daarmee lichamelijke én mentale topprestaties te verrichten. De sporter blijft zelf in de lead, maar leert te vertrouwen op onderzoeksuitslagen en interpretaties van de sportarts. Het vereist van de sporter vertrouwen om zijn trainingsarbeid hierop af te stemmen. En het vereist een persoonlijke band en soms zelfs het overwinnen van 'schaamte' voordat de sporter zijn shirt uittrekt en de koude stethoscoop op de rug accepteert. Dit geldt ook voor managers! De sportarts moet dat vertrouwen verdienen.

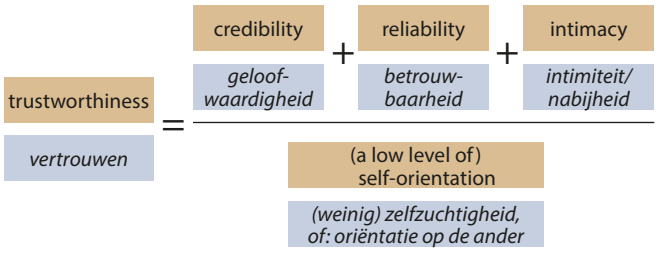
De formule van vertrouwen, geformuleerd door Maister

Maisters trusted advisor is de ideale uitwerking hiervan. Maar als auditor begrijp je nog lang niet voldoende van de complexe werkelijkheid van de manager. Laat staan diens psyche, opvoeding en (op ervaringen gebaseerde) mentale modellen. Des te meer reden om Maisters 'meesterwerken' toe te passen, waarbij je ook zijn definitie van vertrouwen – als formule weergegeven – goed op je moet laten inwerken (zie *figuur 1*).

De vier componenten van vertrouwen

We staan kort stil bij de componenten.

- *Geloofwaardigheid* klinkt waarschijnlijk bekend. Je bent eerlijk en wat je zegt is aannemelijk; iemand vertrouwt wat je zegt.
- *Betrouwbaarheid* is een logische vervolgstap: de mate waarin men op je kan bouwen, gebaseerd op ervaringen waarin jij je beloften nakomt. Iemand vertrouwt dat je doet wat je zegt.



Figuur 1. Maisters componenten van vertrouwen
(Bron: Maister's Components of Trust (2000))

- *Intimiteit* is wellicht een ongemakkelijke: intimiteit of – vrijer vertaald – nabijheid. Je bent een 'veilige haven voor pittige problemen' (Maister, et al., 2021, p. 103). Iemand vertrouwt je met iets waardevols.
- *Zelfzuchtigheid* of positiever geformuleerd: je bent georiënteerd op de ander. De internal auditor heeft zelfvertrouwen, is nieuwsgierig naar de ander, en is vooral niet met zichzelf bezig. Je bent met je volledige aandacht bij de ander. Die zal merken dat je werkelijk geïnteresseerd bent en je meer vertrouwen. Of, zoals Elke Wiss schrijft in haar bestseller *Socrates op sneakers*: 'Goede vragen gaan over de ander. Een goede vraag blijft dicht bij het verhaal, de ervaring van de ander en gaat niet stiekem over mij, mijn beleving, mijn mening.'

Randvoorwaarden voor de internal auditor als trusted advisor

De voormalig IIA-inc. president Chambers (in: Anderson, 2017) geeft enkele randvoorwaarden voor de internal auditor als trusted advisor:

1. *Positieve intentie* – Trusted advisors laten een positieve intentie zien. Het goede antwoord vinden staat voorop in plaats van het gelijk krijgen.

2. *Diplomatie* – Trusted advisors zijn bedreven in directe en open communicatievaardigheden (inclusief luisteren), hebben een politieke antenne en een goed gevoel voor de cultuur van de organisatie.
3. *Vooruitziendheid* – Trusted advisors kijken vooruit. Ze anticiperen op de behoeften van klanten en zien kwesties aankomen voordat ze zich voordoen.
4. *Betrouwbaarheid* – Trusted advisors doen wat ze zeggen en zeggen wat ze doen. Ze behouden het vertrouwen, handelen integer en doen er alles aan om hun geloofwaardigheid te behouden.
5. *Leiderschap* – Trusted advisors zetten vaak de toon voor de hele internal auditafdeling.
6. *Empathie* – Trusted advisors begrijpen de standpunten van stakeholders, en zijn zich bewust van diens behoeften en gevoelens.

Een verdieping op deze randvoorwaarden vinden we opnieuw bij Maister. Hij beschrijft in zijn boek *The Trusted Advisor* (2000) een vijfstappenmodel (zie *figuur 2*).

Het verschil tussen de expert en de adviseur…

Kunnen wij als internal auditors ons 'negatieve taaltje' en oordelende houding achterwege laten en als trusted advisor verdergaan, of is meer nodig? Maister redeneert niet vanuit

Figuur 2. Het vijfstappenmodel van Maister

Figuur 3. Verschillen tussen expert en adviseu
(Bron: Maister's Trusted Advisor (2000))

de oordelende auditor, maar vanuit een 'betweterige' expert. Toch verschillen de kenmerken weinig (zie *figuur 3*).

Expert: "Luister maar naar mij. Ik weet hoe dit zit; heb het elders al gezien. Daar ging het ook zo. Dus dit gaat hier ook werken. Lijkt me logisch toch? Het lijkt me goed dat ik dit op me neem. Ik hoor althans geen tegengeluiden."
Auditor: "Best practice is dat eerst beleid wordt gemaakt en geformaliseerd. Wij hebben vastgesteld dat dit ontbreekt. We adviseren het management met voorrang aandacht te geven aan een passende beleidsnotitie en deze formeel te accorderen."
Advisor: "Je gaf aan dat je met een knoop in je maag zit. Als dit nu aan de hand zou zijn, wat zou dat dan volgens jou voor de organisatie betekenen? Kan ik je helpen meer inzicht te krijgen in het probleem? Is het voor jou akkoord als we samen naar de mogelijke oorzaken kijken?"

Trusted advisor in de onderzoeksfunctie van internal audit

De IAF-rol voor verschillende stakeholders vereist objectivering van het normenkader, veelal met gebruik van voor certificering bruikbare baselines of good practices. Vanwege de verschillende gezichtspunten van stakeholders stelt de auditor zich autonoom op en maakt zich vooral zorgen over een schijn van afhankelijkheid. De gelijkenissen met Maisters expertrol zijn groot.

Hoe anders is de maatwerkauditrol met de manager als opdrachtgever. Immers, een relevante audit is 'het met onderzoek voldoen aan de kennisbehoefte van de manager' (Bos, De Korte & Otten, 2017). Maisters adviseursrol is het meest herkenbaar wanneer de auditor deze manager adviseert tijdens het opdrachtgeversgesprek (lees: advies aan de voorkant). In een auditor/adviseursrelatie kan de manager ook de behoefte aan nader onderzoek kenbaar maken en kan de auditor/adviseur helpen passende onderzoekers te vinden. Dat kan ook de IAF zijn, mits beschikkend over de benodigde expertise.

De CAE als trusted advisor

Tijdens het IIA-seminar gaf De Korte nader aan wat de rol van de CAE als trusted advisor kan zijn, zonder ook de eigenaar van de onderzoeksuitkomsten te zijn:

- Indien je als CAE verantwoordelijk bent voor een ervaren team dat zelfstandig kwalitatief goede onderzoeken uitvoert, kun je de rapportage en vaktechnische onderbouwingen loslaten. Mits je zorgt voor de randvoorwaarden en het team voldoende van 'het gedoe' afschermt.
- In gesprekken met het bestuur, auditcommittee (AC) en collegamanagers mag het gaan over de business, ontwikkelingen en hoe daarop in te spelen. Men vraagt regelmatig je mening, waarbij je oplet dat duidelijk is wat jouw mening is en wat onderzoeksuitkomsten zijn.
- Zodra onzekerheid managementkeuzen bemoeilijkt, overweeg je de onderzoeksmogelijkheden te duiden. Zonder inhoudelijke bemoeienis, adviseer je over de vraagstelling, scope en optiek van het onderzoek.
- Onderzoeksrelevantie en -urgentie kun je uitstekend uitleggen aan het AC. En als je jaarplan (dat toch al flexibiliteit vraagt) vooral thema's en objecten van onderzoek bevat, is de link daarmee gemakkelijk te leggen.
- De vertrouwensband met de verantwoordelijk manager mag niet direct onder druk staan, omdat 'alles een-op-een' wordt gerapporteerd aan de AC-leden. Er moet ruimte zijn om de eigen opgedane ideeën en acties volgens normale lijnen te communiceren; via het bestuur bij de AC-leden. Vermelding van het onderzoek en daaruit voortvloeiende managementacties, kan voldoende zijn.

Socratisch gesprek als techniek van de trusted advisor
Naar ons idee vind je in Scheins *Process Consultation* en in Quinns *Positive Organizations* leerzame uitwerkingen van de benodigde attitude en technieken voor de trusted advisor. Maister benoemt hierbij het socratische vraaggesprek. Daarin is randvoorwaardelijk wat Wiss de socratische houding noemt en als kern beschouwt voor een goed socratisch gesprek. Hierna schetsen we een breed geaccepteerde visie op socratische gesprekken.

Een onderzoek in een gesprek met toestemming voor confrontaties
Socratische gesprekken zijn onderzoekend. Je onderzoekt met iemand waarop gedachten zijn gebaseerd qua aannamen en vooronderstellingen. Met dat inzicht kun je een situatie anders benaderen, met nieuwe kansen op een andere uitkomst, een andere verhouding tussen mensen, of een nieuwe start. Je veronderstelt geen vooraf afgestemde definities. Dit zou het denkproces in de kiem smoren. Juist een verschil in interpretaties is interessant, omdat onderliggende redenen nieuwe inzichten kunnen opleveren.

Vereisten zijn het confronteren en daar toestemming voor krijgen. Zo'n gesprek kan ongemakkelijk worden; de geadviseerde manager moet dit omarmen met de kennis dat alleen dan daadwerkelijk nieuwe of verdiepende inzichten kunnen ontstaan. De manager moet ook voelen dat de adviseur geheel voor hem aan het werk is en dat hij zonder gezichtsverlies het gesprek mag stoppen. De adviseur richt zijn volledige aandacht (zonder eigen gedachten, aannamen en antwoorden) op de manager, zoals Maister beschreef bij 'georiënteerd op de ander'.

Doorvragen en confronteren als essentie
Als trusted advisor blijft de adviseur eerst bij de gebeurtenissen. Daarop gerichte vragen zijn vooral open, omdat die gemakkelijk tot verdieping leiden. En dat is het uiteindelijke doel! Met ongericht doorvragen komen belangrijke elementen naar boven, in een voor de geadviseerde passende volgorde. De adviseur let op taalgebruik: waarom juist die bewoordingen? Tegelijkertijd zal de adviseur het non-verbale en paraverbale waarnemen en hierop doorvragen.

Confrontaties kunnen bestaan uit vragen over mogelijke tegenstellingen: 'Kun je me uitleggen hoe ik a en b moet verhouden?' Daaruit blijkt het onderzoekende karakter, waarin je de meest vanzelfsprekende elementen kritisch bevraagt. Juist die 'domme vragen' zetten aan het denken over wat we 'logisch' vinden. Daarbij is vooralsnog onbelangrijk of dat overeenkomt met je eigen veronderstellingen: je moet eerst écht begrijpen wat wordt gezegd.

De afstand met toetsend onderzoek
Deze techniek staat ver af van het toetsende onderzoek. En om die afstand nog groter te maken: met socratische gesprekken achterhalen we wat we *niet* weten! Ook leren dat je iets *niet* weet, is insight. Het maakt schijnzekerheden confronterend zichtbaar. Het waarschuwt ons voor ondoordacht vertrouwen op best practices en te makkelijke acceptatie van obligate aanbevelingen in een assurancerapport.

Meer toegevoegde waarde voor het management
Zolang je een inhoudelijke bewijsdrang voelt (credibility), sta je ver van de vereisten voor socratische gesprekken. En als de geadviseerde zich nog object van audit voelt (geen intimacy), zijn de randvoorwaarden voor een relatie tussen de trusted advisor en de geadviseerde onvoldoende. Sterker nog, voor wederzijds vertrouwen moet de adviseur opstellen, zijn eigen twijfels laten zien, expliciet maken en ter discussie stellen. Dit is link met Maisters 'nabijheid' als onderdeel van vertrouwen.

Rust en focus voor verdiept inzicht
Het is een compliment van de betrokken manager om als trusted advisor te worden gezien. We komen tot twee aanvullingen op Maister en Chambers. Hoewel in aantal weinig, vereist dit veel van de auditor/advisor (en van de geadviseerde):
- rust en tijd om onzekerheden toe te staan en ongemak te durven uiten;
- focus van de adviseur op alleen de taal, houding en gedachten van de geadviseerde.

Kortom, Maisters trusted advisor is een prachtig concept voor internal auditors die het management meer toegevoegde waarde willen laten ervaren. En in goed overleg met het bestuur, het management én de auditcommissie is het een haalbare aanvulling op het palet aan auditproducten. Althans voor auditors die ook sterk aan zichzelf willen werken en een confrontatie niet uit de weg gaan. <<

Literatuur

- Anderson, U.L. et al, *Internal Auditing: Assurance & Advisory Services, 4th edition*. Internal Audit Foundation, 2017.
- Bos, P., De Korte, R. en J. Otten, 'Management Control Auditing: bijdragen aan doelrealisatie en verbetering', *Auditing.nl*, 2017/2020.
- Korte, R. de, Otten, J. en F. Schuiten, 'Wendbaarheid met internal audit(deel)producten', *Audit Magazine*, 2021.
- Maister, D., Green, C. en R. Galford, *The Trusted Advisor: 20th anniversary edition*, New York: Free Press, 2021.
- Quinn, R.E., *Positive Organization: Breaking Free from Conventiuonal Cultures, Constraints and Beliefs*, Berrett-Koehler Publishers, Inc, 2015.
- Schein, E.H., *Procesadvisering; over de ondersteunde rol van de adviseur en het opbouwen van samenwerking tussen adviseur en cliënt*, Uitgeverij Nieuwerzijds, Amsterdam, 2022.
- Schuiten, F., en R. De Korte, 'Wat is inzicht en wat moet je ermee?', *Audit Magazine*, 2022.
- Wiss, E., *Socrates op sneakers, Praktische gids voor het stellen van goede vragen*, Ambo/Anthos Uitgevers, 2020.

Ron de Korte RA RE RO CIA is partner van ACS Partners. Hij begeleidt hoofden audit risicomanagement en control en hun medewerkers met trainingen counseling en ondersteuning in hun professionalisering.

Manja Knevelbaard MSc is partner van ACS Partners. Ze voert onderzoeken uit naar gedrag en cultuur (behavioural audits) en begeleidt agile audits met multidisciplinaire teams. Ze heeft een achtergrond in managementwetenschappen met een focus op verandermanagement en management control.

Frank Schuiten MA is operational auditor bij de Auditdienst Rijk en daarvoor bij de Europese Rekenkamer. Hij heeft een achtergrond in internationale betrekkingen bestuurskunde en Europese publieke zaken.

Column
Tekst Dr. Michael M. Tophoff

Enkelvoud

Niet alleen noemt elke zichzelf respecterende organisatie zich ‘duurzaam’, zij noemt zich ook ‘inclusief’. Beide begrippen zijn problematisch. Op een eindige planeet is niets duurzaam. Maar wat maakt inclusiviteit problematisch?

De *Dikke Van Dale* omschrijft inclusief als ‘er mede onder gerekend’. Inclusiviteit als een vorm van universalisme is een grote paraplu waaronder iedereen wordt geschaard: ‘wij zijn allemaal mensen’. Inclusiviteit is problematisch omdat hier de verschillen tussen mensen worden verdonkeremaand. Onder de postkolonialistische vlag van één overkoepelende waarheid worden verschillen en identiteiten ontkend: ‘wij zijn allen kinderen Gods’.

Het begrip identiteit viert momenteel hoogtij. Nooit eerder heeft het zoveel plaats ingenomen in het publieke debat. Identiteit is een construct van narratieven over individuen, groepen en naties, gebaseerd op ras, religie, gender of politieke oriëntatie, in welke samenstelling dan ook. Identiteit geeft het gevoel van ‘belonging’, van erbij horen te midden van gelijkgezinden. Identiteit biedt houvast. Identiteit is een toevluchtsoord in een wereld van discriminatie, onderdrukking en agressie. Mijn ‘ik’ wordt tot een ‘wij’, en dat geeft veiligheid en macht. Identiteit wordt dan ook – meer dan ooit – gevierd met vlagvertoon, met demonstraties, met parades waarbij het niet uitmaakt of het hierbij gaat om iemands specifieke seksuele gerichtheid, om huidskleur, om de voetbalclub, om de partij, of om China, de ontwakende reus. Is dit een goed idee?

Dialectisch gezien, veronderstelt elk ik een jij, elk wij een jullie. Ik en jij vertegenwoordigen een exclusieve binariteit, en wel door wederzijdse uitsluiting. Het ik, c.q. het wij, staat voor veiligheid en vertrouwen; het jij en het jullie impliceert anders-zijn, het betekent psychologische afstand. Tegenover mijn ik is de jij een ander, of, anders gezegd, het ik creëert een jij. Hiermee is het fundament gelegd voor elk intermenselijk conflict, tussen individuen, tussen groepen, tussen partijen en tussen volkeren. Elke identiteitsbeweging creëert haar eigen vijand. Inderdaad, identiteit schept veiligheid, maar het is een bedrieglijke veiligheid, want ze houdt het conflict met de ander(en) reeds in.

In plaats van een statisch gegeven kunnen we identiteit ook beschouwen als een ontwikkelingspsychologisch proces. Gedurende de puberteit en adolescentie vormt de persoon, in het gunstige geval, zijn eigen identiteit en leert deze te accepteren en misschien zelfs wel te verwelkomen. Huidskleur, seksuele oriëntatie, politieke positie mogen zichtbaar worden, zij kunnen een reden zijn voor trots. Een open en democratische maatschappij maakt een dergelijke ontwikkeling mogelijk.

In een volgende ontwikkelingsfase echter wordt het mogelijk om de valkuilen van de eigen identiteit onder ogen te zien en te begrijpen hoe identiteit de basis is van conflicten. Dan wordt het nodig om de eigen identiteit te transcenderen. De persoon leert niet alleen zijn eigen identiteit, maar daarmee ook de identiteit van de ander los te laten. Pas dan wordt het mogelijk om zichzelf zowel als de ander niet meer waar te nemen als vertegenwoordiger van een clan, maar als persoon, als enkelvoud, als singulariteit. Elk levend wezen op deze planeet verdient het om te worden gerespecteerd als uniek en enkelvoudig. En alle levende wezens op de wereld delen hun singulariteit.

Dan laat de moderne onderneming zich niet langer voorstaan op haar ‘inclusiviteit’ van ‘one size fits all’. Dan leert zij deze specifieke persoon, als enkelvoud, te respecteren en te verwelkomen, in zijn singulariteit.

Dr. Michael M. Tophoff behaalde een MSc in Klinische Psychologie aan de Universiteit van Utrecht, waar hij ook promoveerde. Aan de Vrije Universiteit Amsterdam behaalde hij een Master of Theology and Religion. Hij doceert Personal Skills aan de faculteit voor Economie en Bedrijfskunde aan de UvA (EMIA-EPDA). Hij is research fellow aan de VU.

Deloitte.

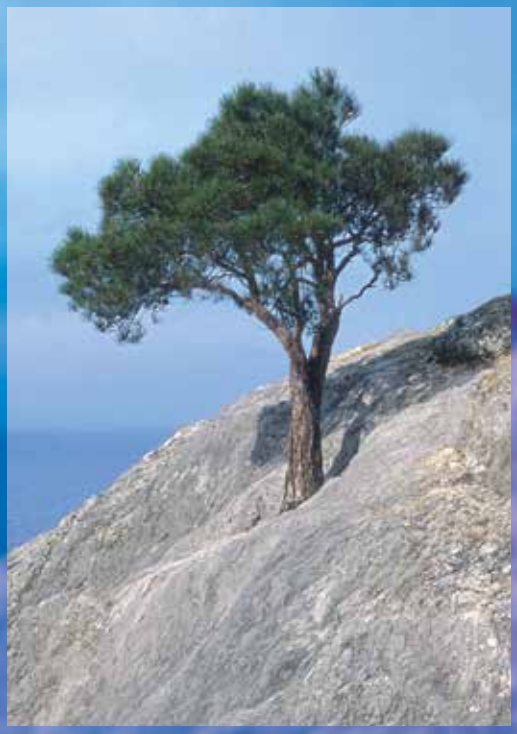
Insights on responsible business

A podcast about organisations building trust, security and resilience to thrive in a new era of uncertainty and stakeholder capitalism.

Tune in to your favourite podcast app or visit
www.deloitte.nl/risk

Is jouw organisatie digitaal weerbaar?

Digitalisering en innovatie leidt tot meer cyberrisico's. Om deze risico's beter in de greep te houden treedt naar verwachting eind 2022 de EU Digital Operational Resilience Act (DORA) in werking. Financiële instellingen krijgen 24 maanden de tijd om aan deze nieuwe regelgeving te voldoen. KPMG ondersteunt internal auditfuncties om hierin voorop te lopen. En tijdig inzicht te geven aan hun organisatie over digitale weerbaarheid en het voldoen aan DORA vereisten.



Meer weten?

Erwin Mol
+31 20 656 7498
mol.erwin@kpmg.nl

Bert Koelewijn
+31 20 656 7635
koelewijn.bert@kpmg.nl

home.kpmg/nl/internalaudit

KPMG