AUDIT MAGAZINE

VAKBLAD VOOR DE INTERNAL AUDITOR
NUMMER 4 2017 JAARGANG 16

THEMA
Veiligheid

Tjibbe Joustra
Onderzoeksraad voor Veiligheid:

“Veiligheid kun je niet wegorganiseren”

Hoe veilig is onze software?

De achterdeur stond wagenwijd open bij de gemeente Rotterdam

IIA Quality Assessment Review

veel ervaring
veel toegevoegde waarde

FSV
RISK ADVISORY

www.fsvriskadvisory.nl

COLOFON

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

Bijdragen kunnen worden gemaild aan:
auditmagazine@iia.nl

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

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

Burgemeester Stramanweg 102A, 1101 AA Amsterdam
Postbus 22657, 1100 DD Amsterdam
iia@iia.nl, www.iia.nl

Bureauredactie
Ria Harmelink Journalistieke Producties

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

Vormgeving
ViaMare grafisch ontwerp, Marijke Maarleveld

Druk
Senefelder Doetinchem

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

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

Audit Magazine verschijnt vier maal per jaar.

Postbus 1100 3980 DC Bunnik
ISSN: 1570-856X

De vele gezichten van **veiligheid**

Veiligheid. Een woord met een uitsluitend positieve connotatie. Het begrip veiligheid raakt onze bestaanszekerheid. Het is dan ook niet voor niets dat de Amerikaanse psycholoog Maslow dit begrip een prominente plek gaf in zijn bekende hiërarchie van menselijke behoeften. Na primaire fysiologische menselijke behoeften volgt veiligheid.

Veiligheid is ook een begrip dat tegenwoordig veel aandacht heeft van politici en bestuurders. Om dicht bij huis te blijven: na de recente vreselijke gebeurtenissen in diverse Europese steden zijn de burgemeesters en de veiligheidsdiensten meer dan ooit op hun hoede. Regelmatig hebben we ook te maken met 'cyberaanvallen', denk aan de recente ransomeware waardoor diverse bedrijven dagenlang niet naar behoren konden functioneren, en aan DDoS-aanvallen waardoor de websites van onder meer onze banken regelmatig geraakt worden.

Het begrip veiligheid heeft een nieuwe dimensie gekregen, cyber security: alles wat te maken heeft met informatie- en databeveiliging. Zelfs in de wolken speelt veiligheid een belangrijke rol: cloud computing. Veiligheid is een relatief begrip, aangezien niets onder alle omstandigheden volledig zonder gevaar is. Zoals met alle risico's moet ergens een kosten-batenafweging gemaakt worden. 'Kosten' in dit kader hoeven niet alleen geldelijk te zijn. Een voorbeeld. Technisch gesproken kunnen we onze grote treinstations omwille van veiligheid bijna onaantastbaar maken, maar willen we dat onze treinstations bol staan van detectiepoortjes en willen we in lange rijen staan om onze tassen te laten controleren voordat wij in de trein kunnen stappen?

Naast de vaste rubrieken in dit nummer een aantal artikelen waarin het thema veiligheid vanuit verschillende invalshoeken wordt belicht waaronder een interview met de president van de Algemene Rekenkamer, Arno Visser. Is veiligheid een belangrijk thema in de onderzoeken die de Rekenkamer uitvoert? We laten ook de voorzitter van de Onderzoeksraad voor Veiligheid, Tjibbe Joustra aan het woord.Senior auditor Robert Hamburg en auditor Maarten Wisman van de Dienst Justitiële Inrichtingen, vertellen hoe DJI omgaat met fysieke veiligheid van gebouwen waar mensen geacht worden binnen te blijven. Het artikel van Jan Hendrikx handelt over de veiligheid van software. Ook de Piratenpartij komt aan het woord over de afwegingen die wij als samenleving steeds vaker moeten maken tussen burgerrechten versus veiligheid.

Wij wensen u veel leesplezier!

De redactie van *Audit Magazine*

THEMA:Veiligheid

"Veiligheid kun je niet wegorganiseren"

Tjibbe Joustra, voorzitter van de Onderzoeksraad voor Veiligheid, over de onderzoeken, de aanpak, het belang van aandacht voor veiligheid en, uiteraard, de rol van internal auditors hierin. **Pag. 6**

Patiënt- en medewerkerveiligheid bij het LUMC

Harriette Verwij en Petra van de Voorde (LUMC), geven antwoord op de vraag hoe het zit met de patiënt- en medewerkerveiligheid én de veiligheid bij rampen. **Pag. 20**

Hoe veilig is onze software?

Zouden we software durven opeten als het voedsel was?, vraagt Jan Hendrikx zich af. Wat weten we eigenlijk over de veiligheid van de software die we dagelijks gebruiken? **Pag. 12**

"De macht terugbrengen naar de burger"

Burgerrechten en veiligheid kunnen wringen, aldus Matthijs Pontier, woordvoerder van de Piratenpartij. Over transparantie en democratie. **Pag. 24**

De achterdeur stond wagenwijd open bij de gemeente Rotterdam

De gemeente Rotterdam had zelf het idee dat het allemaal best goed op orde was, maar uit het rapport *In onveilige handen* blijkt dat de bescherming van geen kant klopte. Paul Hofstra, directeur van de Rekenkamer Rotterdam, in gesprek met *Audit Magazine*. **Pag.16**

Onderzoek naar veiligheid in de publieke sector

President van de Algemene Rekenkamer Arno Visser vertelt hoe relevant een toegewijd team, protocollen, empathie, rekenkameronderzoeken en cultuur zijn. **Pag. 26**

Openbaar Ministerie: beheerst gezag

Wat is dat eigenlijk: beheerst gezag? En hoe bereikt het OM dat met 254.000 misdrijfzaken en 130.000 overtredingszaken in 2016? Lucas Kroes en Nicole Kuijpers (OM) leggen uit. **Pag. 32**

Veiligheid bij Geldservice Nederland

GSN telt en distribueert voor banken het papieren geld en de bankbiljetten én vult de geldautomaten. Victor de Wolff en Esther Huijser (GSN) vertellen over de veiligheid van waarden en mensen. **Pag. 36**

Komt de digitale Titanic-ramp eraan?

Volgend jaar mei is het zover: dan moet de privacyrichtlijn GDPR geïmplementeerd zijn. Het pad erheen is een helse toer, zegt Brenno de Winter, bekend van het kraken van de OV-chipkaart. **Pag. 40**

Veiligheid binnen DJI: een belangrijk goed

Robert Hamburg en Maarten Wisman van de Dienst Justitiële Inrichtingen (DJI), beschrijven de oorsprong, opzet en uitvoering van de safety, security & housing Audits. **Pag. 43**

Zuurstof in het management control systeem

De roep om meer verantwoordelijkheid neer te leggen bij het lager/decentraal management klinkt steeds luider, aldus Robert Vos (ministerie van Financiën). **Pag. 46**

De 'perfect storm' in de energiemarkt

Jantien Heimel (Vattenfall Group) over de overgang van fossiele naar hernieuwbare energie, windenergie, slimme meters, outsourcing en meer ontwikkelingen in de energiemarkt. **Pag. 52**

Fraude: een uitdaging voor de internal auditfunctie

Noortje de Rooij en Thom Eijken (KPMG Advisory) concludeerden na onderzoek dat auditors moeite hebben met het structureel adresseren van fraude. **Pag. 56**

Rubrieken

Thema Veiligheid
Tekst Bas Zandee MBA MSHE CIA
Raymond Wondergem MSc RO
Beeld David van Dam / De Beeldunie

Tjibbe Joustra, voorzitter van de Onderzoeksraad voor Veiligheid:

"Veiligheid kun je niet wegorganiseren"

Daags na het debat over de missie in Mali en het aftreden van minister Hennis sprak *Audit Magazine* met Tjibbe Joustra, voorzitter van de Onderzoeksraad voor Veiligheid. Het gesprek ging over de onderzoeken en de aanpak van de Onderzoeksraad, het belang van aandacht voor veiligheid en de rol van internal auditors bij veiligheid.

Het is natuurlijk lastig om tegen de hoogste baas te zeggen dat hij het verkeerd ziet, maar het moet wel. Het ultieme doel is veiligheid en geen papieren werkelijkheid

Waarom is er een Onderzoeksraad voor Veiligheid?
"Het is een lange traditie dat er in bepaalde sectoren veiligheidsonderzoeken worden uitgevoerd. De scheepvaart was een van de eerste. Met name de vervoerssectoren hebben al heel lang een vorm van onafhankelijk onderzoek. Deze sectoren zijn de onderliggende pilaren voor de huidige Onderzoeksraad. De aanleiding voor de oprichting was dat er veel ad-hoccommissies waren, zoals bij de vuurwerkramp in Enschede of bij de brand in Volendam. Het idee was om dit samen te brengen in een structureel orgaan en dat is de Onderzoeksraad voor Veiligheid geworden."

Hoe wordt bepaald welke onderzoeken de Onderzoeksraad uitvoert?
"Voor een deel hebben wij verplichte onderzoeken. Dat is ongeveer 40-45% van de onderzoeken, waarvan de grootste brok de luchtvaart en scheepvaart is. Internationale verdragen schrijven voor welke onderzoeken we moeten uitvoeren, de wijze van onderzoek en de rapportagevorm. Daarnaast hebben wij de opdracht om bepaalde voorvallen bij BRZO (Besluit Risico's Zware Ongevallen) bedrijven te onderzoeken. Dit zijn onderzoeken in de petrochemische industrie. Het merendeel van deze verplichte onderzoeken is wat beperkter van opzet, maar leidt soms ook tot een uitgebreid onderzoek. Zoals is gebeurd naar aanleiding van de emissie van ethyleenoxide bij Shell of de veiligheid van het vliegverkeer op en rond de luchthaven Schiphol. De Onderzoeksraad schrijft ook grote en diepgaande rapporten op basis van onderzoeken naar incidenten, zoals het geval was bij het mortierongeval in Mali. Wij willen dan achterhalen hoe dit incident heeft kunnen gebeuren en wat de directe en achterliggende oorzaken zijn.
Belangrijke criteria voor het selecteren van onderwerpen zijn schade (dit kan zowel gaan om financiële schade als om een voorval waarbij slachtoffers zijn gevallen), maar ook om kwesties waarbij er sprake is van maatschappelijke onrust. Een voorbeeld van een dergelijk onderwerp zijn de door gaswinning veroorzaakte aardbevingen in Groningen. Wij bepalen dus zelf wat we onderzoeken. Soms krijgt de Onderzoeksraad een verzoek om een onderzoek te doen van bijvoorbeeld een minister. Dit verzoek kunnen we overigens gemotiveerd afwijzen. De Onderzoeksraad is onafhankelijk en bepaalt zelf de onderzoeksagenda."

Afgelopen dagen gaat het voornamelijk over de veiligheid bij Defensie. Maar kan iets vergelijkbaars ook bij een andere organisatie of bedrijf gebeuren?
"Destijds met het incident bij Chemie-Pack in 2011 zei iedereen 'dat is een klein bedrijf daar kan het gebeuren, zoiets kan in het Rijnmondgebied niet gebeuren'. Vervolgens vond in 2013 het incident bij Odjfell Terminals Rotterdam plaats. Toen was het commentaar dat zulke incidenten niet bij grote en professionele spelers zoals Shell zouden plaatsvinden. In onderzoeken naar Shell in 2013, 2014 en 2016 hebben wij daar echter ook voldoende omissies aangetroffen en zijn we in het laatste onderzoek op zoek gegaan naar de rode draad. Kortom, dit soort incidenten kan overal gebeuren. Zeker in Nederland waar we veel industrie dicht bij dichtbevolkte gebieden hebben, is het belangrijk om goed om te gaan met de veiligheidsrisico's.
Maar veiligheid raakt meer sectoren dan defensie en petrochemie. Onlangs hadden we een discussie over zorginstellingen en brandveiligheid. Iedere organisatie neemt maatregelen op dit gebied, maar niemand denkt dat er echt brand uitbreekt. Als de brand dan wel uitbreekt, staan mensen perplex hoe snel een brand om zich heen grijpt. In 2012 hebben we een brand onderzocht bij de GGZ-instelling Rivierduinen, waarbij drie doden vielen. In het onderzoek hebben we een real-time animatie van vier minuten van de brand gemaakt. Hieruit kwam naar voren dat experts weten hoe een brand ontstaat en zich ontwikkelt, maar dat de medewerkers zich onvoldoende realiseren wat de impact is van een brand die zo snel om zich heen grijpt. Men wordt vaak overvallen door de realiteit.
Mijn advies is, denk vooral niet: dat gaat mij niet gebeuren. Bij BRZO-bedrijven is er vaak wel veel aandacht voor veiligheid. Dit geldt niet altijd voor andere organisaties. In mijn visie ervaart een raad van bestuur veiligheid vaak als een

Over...

Tjibbe Joustra is vanaf 7 februari 2011 voorzitter van de Onderzoeksraad voor Veiligheid. Hij volgde mr. Pieter van Vollenhoven op. Voorheen was Joustra onder meer secretaris-generaal bij het ministerie van Landbouw, Natuur en Voedselveiligheid en nationaal coördinator terrorismebestrijding.

dure kostenpost. Ze zijn pas geïnteresseerd als er iets mis gegaan is. Een oud Engels gezegde luidt: 'Wil je bezuinigen op veiligheid, probeer eens een ongeluk'. Je hoort vaak de uitspraak – 'we moeten aandacht besteden aan veiligheid', maar of dit intrinsiek gemotiveerd is, daar plaats ik grote vraagtekens bij."

We zitten hier de dag na het debat over het onderzoek van het mortierongeval in Mali in de Tweede Kamer. Hoe kijkt u terug op de periode tussen publicatie en het debat van gisteren?

"Defensie doet veel aan veiligheid. Dat is essentieel in de Defensieorganisatie. Alleen, als wij nagaan wat er heeft plaatsgevonden komen we helaas ook tot harde conclusies. In onze onderzoeken leggen we minutieus de stappen in en rond het incident vast. Mensen in het proces denken vaak dat het om geïsoleerde incidenten gaat. En als iemand een

fout maakt of constateert, denken ze: het valt wel mee. Ook omdat anders bijvoorbeeld de uitvoering van een missie in de knel komt. Alleen hebben incidenten zelden één oorzaak. Het incident is vrijwel altijd een cumulatie van allerlei factoren. Daarom is cultuur binnen een organisatie zo belangrijk. Dat is de context van de organisatie waarbinnen het werk gebeurt. Als er een cultuur heerst van 'het is niet helemaal goed, maar we proberen toch de missie zo goed mogelijk te draaien', dan is er vaak sprake van een complex van factoren dat ten grondslag ligt aan het betreffende ongeluk. Dit ongeluk in Mali is geen incident. Veel van deze factoren zijn cultureel bepaald. Het incident is geen toeval, het is een gevolg van verschillende factoren binnen een organisatie die mettertijd samenkomen. Het is alleen de vraag wanneer."

Wat is uw advies voor andere bestuurders voor het waarborgen van veiligheid binnen een organisatie?

"De top van een organisatie heeft een belangrijke voorbeeldfunctie. Als het bestuur bijvoorbeeld pretendeert een 'open' organisatie te zijn, maar een medewerker er bij de eerste kritische melding uit vliegt, vergeet het dan maar. Als het bestuur allerlei ideologische doelstellingen heeft, dan hoort het bestuur daar ook naar te handelen. Dat lijkt heel logisch, maar ik kan garanderen dat dit vaak moeilijker is dan mensen denken. Het bestuur is in belangrijke mate bepalend voor de cultuur. Dus als het bestuur van een organisatie van mening is dat de cultuur verkeerd is, dan zijn zij daar zelf onderdeel van en verantwoordelijk voor. Dat wordt niet altijd onderkend. Het bestuur moet dan zelf ook veranderen.
Verder is het advies om te kijken naar de structuur van je organisatie. Er mag best spanning zitten tussen verschillende functies binnen een bedrijf. Het is wel zaak dat conflicten niet blijven 'hangen'. Een organisatie moet zorgen voor een escalatiemodel. Bij veel organisaties is veiligheid weggeorganiseerd ergens in een stafafdeling. Als een bestuurder vervolgens niets hoort, is het erg verleidelijk om aan te nemen dat het goed gaat. Dit bevordert het wasdom van veiligheid niet. Daarnaast is veiligheid complexer geworden in vergelijking met veertig jaar geleden én is de aandacht en de maatschappelijke betrokkenheid vergroot."

Stel, u bent bestuurder van een commerciële organisatie. Op welke manier zou u veiligheid op de kaart zetten?

"Als eerste onderzoeken op welke manier veiligheid geregeld is. Hierbij is het belangrijk om zowel de veiligheid van de medewerkers als de omwonenden te kunnen waarborgen. Daarnaast heb je ook een commercieel belang. Zoals ik eerder noemde is de maatschappelijke betrokkenheid vergroot en zorgt internet ervoor dat iedereen toegang heeft tot vrijwel alle informatie. Daarnaast bemoeit ook iedereen zich met van alles en nog wat. Een klassiek voorbeeld hiervan is Shell en de Brent Spar. Hieruit heeft Shell belangrijke lessen getrokken. Je moet ervoor zorgen dat een incident bij jou niet gebeurt. Een incident heeft een negatieve invloed op de aandelenkoersen en de afname van je producten. Je kunt dit niet onderschatten. Veiligheid is ook gewoon eigenbelang.
Om hier zicht op te krijgen is vooral het zelf waarnemen door een raad van bestuur belangrijk. Het wegorganiseren in 'harkjes' en het wegdelegeren in de organisatie werkt niet. Zorg ervoor dat je als bestuurder bijvoorbeeld tweewekelijks een half uur overlegt met het hoofd van de afdeling Veiligheid. Zoiets verandert echt de positie van veiligheid binnen een organisatie. Verdiep je ook in het onderwerp door simpelweg de rapporten te lezen en er vragen over te stellen. En als laatste, loop periodiek over de werkvloer. Het is weliswaar een ouderwetse methode, maar het geeft wel inzicht. Een bestuurder moet tijd vrijmaken voor veiligheid.
Daarnaast onderschatten organisaties de verantwoordelijkheid voor veiligheid in de gehele keten. Je hebt als organisatie

Een bestuurder moet tijd vrijmaken voor veiligheid. Periodiek over de werkvloer lopen. Weliswaar een ouderwetse methode, maar het geeft wel inzicht

ook een verantwoordelijkheid in de opdrachtgeversrol naar je toeleveranciers en je onderaannemers. Dit element neemt in onze onderzoeken een steeds prominentere plaats in."

Hoe kijkt u naar internal auditors en interne toezichthouders?
"Het is belangrijk om voelhorens binnen de organisatie te hebben. Als internal auditor moet je alert zijn op het verschil tussen de papieren werkelijkheid en de echte werkelijkheid. We zijn bij organisaties geweest die alle certificaten hadden, maar vervolgens bleek dat er van alles mis was. Dan concludeerden we dat een raad van bestuur in slaap was gesust. Vaak wordt door het bestuur aan de internal auditor alleen gevraagd om de inrichting te beoordelen. Dan is het aan de internal auditor om aan te geven dat het ingerichte systeem niet de werkelijkheid raakt. Het is natuurlijk lastig om tegen de hoogste baas te zeggen dat hij het verkeerd ziet, maar je moet het wel doen. Het ultieme doel is veiligheid en geen papieren werkelijkheid."

Hoe kijkt u terug op de afgelopen dagen?
"Voor ons lag het zwaartepunt niet op de dagen na publicatie van het eindrapport, maar juist de periode daarvoor. De onderzoekswerkzaamheden en het afstemmen van de bevindingen vonden al in een eerder stadium plaats. De grote publiciteit is gekomen na het uitbrengen van het rapport. Het is natuurlijk erg tumultueus verlopen. Gelukkig is de discussie redelijk over het rapport blijven gaan. Wij vinden het altijd jammer als de discussie gaat over het wegsturen van een persoon, in plaats van waar het werkelijk om gaat: de bevindingen van het onderzoek. Met het wegsturen van een persoon los je veiligheidsproblemen niet direct op. Terwijl het doel van de Onderzoeksraad het verbeteren van de veiligheid is. Zelden heb ik zoveel discussie gezien omtrent veiligheid, ik heb het gevoel dat bij dit rapport er voldoende bewustzijn is dat de aanbevelingen opgepakt worden en dat er meer aandacht moet zijn voor veiligheid tijdens nieuwe missies. Het stevige onderzoeksrapport van de Onderzoeksraad heeft hier zeker aan bijgedragen." <<

Van het bestuur

Het jaar 2017 is alweer praktisch voorbij. Een moment om terug te kijken op het afgelopen jaar dat razendsnel voorbij is gegaan. Ook een moment om de plannen voor 2018 te maken en het commitment daarover met elkaar aan te gaan binnen het IIA-bestuur.

Terugkijkend op 2017 is het 20-jarig bestaan een mooie mijlpaal. We hebben het op een aantal momenten gevierd, waarbij het congres (in juni) en het bootfeest (in september) voor meer dan tweehonderd huidige en voormalige vrijwilligers het meest in het oog sprongen. Tijdens dat bootfeest was het prachtig om te zien hoe de verschillende generaties vrijwilligers als het ware in elkaar overgingen, met elkaar hun passie voor Internal Audit delen en zelfs met nieuwe ideeën naar het huidige bestuur kwamen. Oud of jong, lang of kort geleden vrijwilliger, het maakte niet uit; de betrokkenheid met IIA Nederland bleek onverminderd groot.

Terugkijkend naar het jaar 2017 mogen we stellen dat we de meeste speerpunten hebben bereikt. Zo is CAE Services van start gegaan om nieuwe chief audit executives te ondersteunen, is het Internal Audit Ambition Model operationeel geworden, hebben we een zeer succesvol congres achter de rug, zijn er relevante vaktechnische papers uitgebracht en is er een uitgebreid aanbod aan trainingen en andere evenementen. Ook is de website vernieuwd en heeft IIA Nederland haar kantoor uitgebreid om meer 'in house' te kunnen aanbieden.

Voor 2018 zal 'innovatie' het belangrijkste thema vormen. Het bestuur wil actief gaan inspelen op de innovatie in ons vakgebied (robotisering, data-analyse, maar bijvoorbeeld ook de betekenis van het woord 'insight' in de definitie van Internal Audit) en op innovatie in het algemeen (fintechs, blockchain, et cetera). De eerste ideeën zijn tijdens een heidag besproken. De Commissie Professional Practices en de IIA Academy zullen vermoedelijk de eersten zijn die aan het werk gaan om nieuwe inzichten en daaraan gekoppelde trainingen te kunnen aanbieden.

Persoonlijk zal ik in 2018 ook de status van voormalig vrijwilliger aannemen. Na zes jaar volgt een verplicht afscheid van het bestuur. In mei 2018 presenteert het bestuur tijdens de Algemene Leden Vergadering Jantien Heimel (nu vicevoorzitter) als mijn opvolger. Zeer innovatief, aangezien zij de eerste vrouwelijke voorzitter van IIA Nederland zal zijn. Zelf blijf ik overigens wel nog tot juli 2019 actief als lid van de board of directors van IIA Global en als voorzitter van de Global Advocacy Committee.

Audit Magazine heeft voor dit kwartaal het onderwerp Veiligheid gekozen. Ik kan me niet herinneren dat ik er in het verleden over heb kunnen lezen, noch in *Audit Magazine* noch in andere vaktechnische uitingen. Ook innovatief dus! Het is zeker een onderwerp dat in vele sectoren, zoals industrie, transport en bouw, van groot belang is. Ik ben daarom erg benieuwd hoe het de rol van de internal auditfunctie raakt en hoe die daar in de praktijk mee omgaat.

Tot slot mijn dank aan jullie als trouwe lezers. Naast veel leesplezier wens ik jullie ook fijne feestdagen en voor 2018 alvast veel succes, gezondheid en innovatie! Ik zie jullie graag op de nieuwjaarsreceptie in januari 2018.

IIA® Nederland
John Bendermacher is voorzitter van het IIA.

Thema Veiligheid
Tekst Ing. Jan Hendrikx MSc RE CISA CISSP
Beeld 123RF®

Hoe **veilig** is onze software?

Als onze software voedsel was, zouden wij het dan durven opeten? Wat weten wij nu werkelijk over de veiligheid van de software die wij dagelijks binnen onze organisaties gebruiken?

Steeds opnieuw moeten we maar vertrouwen op de goede bedoelingen van een leverancier

We worden steeds afhankelijker van technologie. De opkomst van Internet of Things (IoT), blockchaintechnologie en steeds geavanceerdere apps op onze mobile devices is niet meer te stoppen en de ontwikkelingen gaan razendsnel. De overeenkomst van al deze technologische ontwikkelingen is dat ze gebruikmaken van software. Software vormt de logica die computers en apparaten slim maakt. Het gaat hierbij om computerprogramma's als de apps op onze smartphones tot en met de core applicaties op de servers waar organisaties op steunen.
De steeds verdere integratie van technologie in ons dagelijks leven maakt dat we ook steeds zwaarder steunen op software. Veel van deze software is onzichtbaar voor ons als gebruiker, waardoor we ons vaak onvoldoende bewust zijn van de risico's die het gebruik ervan met zich meebrengt. Dit artikel wil bewustzijn creëren met betrekking tot de beveiligingsrisico's die we als gebruiker lopen bij het gebruik van software.

Totstandkoming van software
Hoe komt veel van de software die we dagelijks gebruiken nu eigenlijk tot stand? Software begint vaak als stukken platte tekst (de zogenaamde broncode, ook wel 'source code' genoemd) op de computer van de ontwikkelaar. Deze stukken tekst bestaan uit een reeks van tekstuele opdrachten, geschreven in een programmeertaal die de uiteindelijke functionaliteit en werking van het computerprogramma bepalen. Als de broncode af is, wordt deze door de programmeur met speciale programmatuur (een 'compiler') omgezet naar een zogenaamde 'executable'. Pas na deze omzetting kan het computerprogramma worden uitgevoerd door een computer.
De eindgebruiker van de software zet een kopie van de executable op zijn computer en kan na het starten van de executable gebruikmaken van de geboden functionaliteit van de software. In de meeste gevallen is het bijzonder lastig om de originele broncode terug te leiden vanuit de executable. Dit komt omdat bij het omzetten van de broncode naar een executable (het compileren) de voor de mens begrijpelijke broncode wordt omgezet naar een reeks machineopdrachten die bedoeld zijn voor de computer.

Closed en open source
Wanneer we software aanschaffen krijgen we meestal alleen de beschikking over de executable. De broncode blijft vanwege het intellectuele eigendom vaak achter bij de organisatie die de software heeft ontwikkeld. Deze software noemen we daarom 'closed source' software. Dit maakt dat we wel gebruik kunnen maken van de software, maar niet kunnen zien wat de kwaliteit van de oorspronkelijke broncode is. Zo is aan een executable in de meeste gevallen niet te zien of het gaat om professioneel ontwikkelde software van hoge kwaliteit of om software die bijvoorbeeld door een beginnende programmeur in India is geschreven. Vaak weten we daardoor weinig tot niets over de kwaliteit en dus de veiligheid van de software die we gebruiken, terwijl het misschien wel de kroonjuwelen van onze organisaties raakt.
In het geval van 'open source' software kan men wel beschikken over de door de programmeur geschreven broncode. Open source software is in de meeste gevallen afkomstig van hobbyisten of organisaties zonder commerciële drijfveer, waarbij de broncode vaak via internet wordt gedeeld. Iedereen kan deze broncode reviewen en dus zien hoe het programma technisch is gebouwd. Natuurlijk dient men dan wel te beschikken over voldoende technische kennis om de kwaliteit en werking van de broncode te kunnen doorgronden. Open source kan helpen bij het beoordelen van de veiligheid van de software. Een eenmaal gereviewde broncode kan men dan zelf omzetten naar een executable, zodat er zekerheid is over de herkomst van de executable.
Wanneer organisaties eigen software ontwikkelen, kan men beschikken over de broncode en kan gestuurd worden op de kwaliteit en veiligheid ervan. Maar zelf software ontwikkelen is kostbaar en complex en daardoor voor veel organisaties geen optie. Dit verklaart de noodzaak om software van derden te gebruiken.

Fouten
Een eigenschap van software is dat het bijna van nature fouten bevat. Dit blijkt wel uit de hoeveelheid updates die we dagelijks op onze apparaten en computers moeten installeren. Deze updates zijn echt niet alleen maar van cosmetische aard, ze lossen vaak ook beveiligingsfouten op. De kans op fouten in open source software is vergelijkbaar met die in closed source software.
Afhankelijk van onder meer de complexiteit van de software, de gebruikte programmeertaal, de inrichting van de ontwikkelomgeving en de kennis en ervaring van de programmeur, is de kans op fouten groter of kleiner. Fouten zijn soms direct zichtbaar, bijvoorbeeld wanneer deze de werking of functionaliteit nadelig beïnvloeden. In andere gevallen blijven fouten onopgemerkt in de programmatuur zitten. Deze fouten kunnen vroeg of laat ontdekt worden door hackers die bewust op zoek zijn naar deze beveiligingslekken om ze vervolgens te misbruiken.

Risico's
De risico's die we met onveilige software lopen kunnen enorm zijn. Datalekken, datacorruptie, 'malware'-infecties, 'ransomware' en cyberaanvallen door hackers zijn maar een aantal voorbeelden van incidenten die kunnen plaatsvinden. Organisaties denken vaak dat ze geen gevaar lopen als ze hun 'patchmanagement' op orde hebben en software-updates tijdig installeren. Patchmanagement is belangrijk, maar wat als er nog geen update bestaat voor een kritieke kwetsbaarheid in een applicatie of besturingssysteem? In veel gevallen zijn organisaties voor hun software-updates volledig afhankelijk van de leverancier. Het besef dat men hierdoor risico's loopt, ontbreekt vaak.
En wat als er bewust een achterdeur in de software is ingebouwd of andere ongewenste functionaliteiten? De sjoemelsoftware in bepaalde dieselauto's laat zien dat dit werkelijk gebeurt. Maar het kan nog veel verder gaan. Technisch gezien kunnen leveranciers van onze besturingssystemen onze servers, laptops en andere mobile devices massaal onklaar maken met één enkele kwaadaardige update. De kans dat dit gebeurt is echter zeer klein, aangezien dit direct tot een verslechterde reputatie zou leiden. Maar het is een reëel scenario in het geval van 'cyber warfare'. Dat is een van de redenen dat de Amerikaanse overheid geen gebruik wenst te maken van Russische antivirussoftware.
Moeten we leveranciers dwingen om inzage te geven in de broncode van de software die we gebruiken? Zelfs al zouden

Wat als er bewust een achterdeur in de software is ingebouwd?

we de broncode van een closed source product op enig moment mogen inzien, wat zou dat dan voor aanvullende zekerheid over de veiligheid bieden? Het blijft een momentopname en bovendien, hoe weten we dat de gereviewde broncode daadwerkelijk deel uitmaakt van de uiteindelijke executable?
Los daarvan kan iedere update opnieuw kwetsbaarheden introduceren en de werking van het product volledig veranderen. Aan een update is vaak niet te zien wat die precies doet. Steeds opnieuw moeten we maar vertrouwen op de kwaliteit en goede bedoelingen van een leverancier. Bijkomend risico is dat updates vaak met verhoogde rechten moeten worden geïnstalleerd, waardoor ze potentieel ook andere zaken op een systeem kunnen beïnvloeden.

Zonder broncode
Natuurlijk bestaat de mogelijkheid om de executables zelf te testen op onveiligheden, zonder de beschikking te hebben over de broncode. Dit doen hackers immers ook. Vaak wordt dan geprobeerd om extreme of ongebruikelijke situaties te creëren om te zien hoe een programma daarop reageert. Indien een programma dan afwijkend gedrag vertoont, bijvoorbeeld door te crashen, kan dat duiden op een kwetsbaarheid die vervolgens verder onderzocht kan worden. Nadeel van dit soort tests is dat deze vaak veel tijdrovender zijn dan broncodereviews. Het maakt de kans om tekortkomingen tijdig te ontdekken aanzienlijk kleiner.

Security Development Lifecycle
Hoe kunnen we dan wel zekerheid krijgen over de veiligheid van onze software? Men kan de totstandkoming van software in sommige opzichten vergelijken met de bereiding van voedsel. Wanneer voedsel onzorgvuldig wordt bereid, loopt degene die het voedsel opeet een groter risico om ziek te worden. Door de bereiding ervan onder gecontroleerde omstandigheden plaats te laten vinden, kunnen problemen worden voorkomen. Zo is het ook met software. Om de veiligheid van software te beoordelen zal in de 'keuken' gekeken moeten worden.
Een manier om die keuken op orde te krijgen en te houden, is via het inrichten van een 'security development lifecycle' (SDL) proces. Zo'n proces zorgt dat in alle fasen van de ontwikkeling het aspect beveiliging wordt meegenomen en beoordeeld. Inmiddels zijn er al een aantal onafhankelijke partijen die het SDL-proces kunnen reviewen en certificeren, zodat ook leveranciers van software kunnen aantonen dat zij op een verantwoorde manier veilige software maken.

Rol van de auditor
Internal auditors moeten zich vaker de vraag stellen of de organisatie wel op de door haar gebruikte software kan steunen. Dat is lastig, want hoe diep moet je daarbij gaan? Dat hangt helemaal af van waarvoor en op welke wijze de organisatie de software gebruikt en welke informatie deze verwerkt. Vervolgens kan de auditor de vraag stellen of voldoende zekerheid bestaat over de veiligheid van de gebruikte software. Misschien zijn aanvullende zekerheden nodig, zoals certificering of een broncode review. Wordt binnen de eigen organisatie software ontwikkeld, dan kan de auditor zelf het interne ontwikkelproces onderwerpen aan een audit. Als dit niet het geval is, dan zal de auditor zekerheid over de totstandkoming van software moeten vragen aan de leverancier. Gezien het alsmaar toenemende belang van software in combinatie met de steeds strenger wordende regelgeving rondom de privacy, een vraag die we bijna verplicht zijn om te stellen! <<

Jan Hendrikx is ondernemer op het gebied van technische informatiebeveiliging. Hij voert technische beveiligingsonderzoeken uit en adviseert organisaties over de wijze waarop zij hun beveiliging tegen onder meer cybercriminaliteit kunnen optimaliseren.
jan@hendrikx-itc.nl

De lezer over **veiligheid**

Audit Magazine legde de lezer via haar lezerspanel en de website van het IIA vijf stellingen voor over veiligheid. In totaal reageerden 32 lezers.

We hebben redelijk veel vertrouwen in onze IT-auditors. 47% van de respondenten gelooft dat zij op gedegen wijze de informatiebeveiliging van hun organisatie kunnen onderzoeken. Toch twijfelt 28% van de respondenten hieraan en precies een kwart van de respondenten denkt zelfs dat we het onderzoeken van informatiebeveiliging beter kunnen overlaten aan beveiligingsspecialisten.

Zeer eensgezind zijn we het over het feit dat de sociale veiligheid een voor de internal auditor interessant object van onderzoek is. Maar liefst 85% van de respondenten verwierp de stelling dat we met dit onderwerp niets kunnen. Interessant, aangezien sociale veiligheid nog niet binnen alle auditdiensten haar weg naar het auditmeerjarenplan heeft gevonden.

Eveneens eensgezind zijn we over het feit dat fysieke veiligheid een onderwerp is dat niet alleen interessant is voor auditors in de bouw en industrie, maar ook voor auditors die binnen andere branches werkzaam zijn. De eerste groep heeft echter, gegeven de aandacht voor het onderwerp binnen hun branche, de meeste ervaring met het auditen van fysieke veiligheid. Althans, dat mag je toch aannemen. Wellicht kunnen zij hun kennis en ervaringen delen met hun beroepsgenoten?

Een audit naar fysieke veiligheid draait niet voornamelijk om soft controls, zo stelt maar liefst 59% van de respondenten. Toch bestaat er wel degelijk een relatie tussen bijvoorbeeld voorbeeldgedrag van de leiding en fysieke veiligheid op de werkvloer en is ook het bespreekbaar maken van een veiligheidsincident door de manager een (soft) control die we in dit kader zouden moeten toetsen. Wellicht moeten we eens nader verkennen in hoeverre soft controls daadwerkelijk deel uitmaken van een audits naar fysieke veiligheid.

Dat kennisdeling belangrijk is blijkt uit de laatste stelling. Slechts 31% van de respondenten vindt dat zij over voldoende kennis beschikt om veiligheid te kunnen auditen. Hoog tijd dus dat we gaan leren van white hat hackers en sociologen en dat we gaan oefenen met het auditen van fysieke, technische en sociale veiligheid. Voelt u zich geroepen uw kennis over het onderwerp te delen met uw beroepsgenoten, dan bent u bij deze uitgenodigd hierover een artikel te schrijven voor *Audit Magazine*!

Wilt u lid worden van het lezerspanel van *Audit Magazine*? Dat kan! Meld u aan via **auditmagazine@iia.nl**.

één

Informatiebeveiliging is tegenwoordig zo complex dat we het beter aan beveiligingsspecialisten (zoals white hat hackers) kunnen overlaten dan aan IT-auditors

1. Helemaal mee eens	9%
2. Mee eens	16%
3. Neutraal	28%
4. Mee oneens	44%
5. Helemaal mee oneens	3%

twee

Sociale veiligheid (zoals pesten op het werk) is als object van onderzoek voor de internal auditor niet of nauwelijks interessant

1. Helemaal mee eens	0%
2. Mee eens	9%
3. Neutraal	6%
4. Mee oneens	51%
5. Helemaal mee oneens	34%

drie

Fysieke veiligheid is alleen relevant voor auditors in de bouw en industrie

1. Helemaal mee eens	3%
2. Mee eens	3%
3. Neutraal	9%
4. Mee oneens	54%
5. Helemaal mee oneens	31%

vier

Een audit naar fysieke veiligheid draait voornamelijk om soft controls

1. Helemaal mee eens	3%
2. Mee eens	19%
3. Neutraal	19%
4. Mee oneens	47%
5. Helemaal mee oneens	12%

vijf

Van het auditen van veiligheid heb ik zelf onvoldoende kennis

1. Helemaal mee eens	0%
2. Mee eens	28%
3. Neutraal	41%
4. Mee oneens	28%
5. Helemaal mee oneens	3%

Audit Magazine sprak met Paul Hofstra, directeur van de Rekenkamer Rotterdam, over het rapport *In onveilige handen* en de unieke rol van de gemeentelijke rekenkamer.

De **achterdeur** stond **wagenwijd open** bij de gemeente Rotterdam

Thema Veiligheid
Tekst Sander Diks CIA
Drs. Margot Hovestad RO
Beeld 123RF®

Je bent in deze functie je eigen opdrachtgever en hebt geen baas

Hoe wordt een oud-bestuursvoorzitter van het IIA directeur van de Rekenkamer Rotterdam?
"Ik was van 1998 tot 2001 voorzitter van het IIA. Toen ik begon als voorzitter was ik hoofd Operational Audit van de Belastingdienst. Halverwege mijn termijn als voorzitter van het IIA maakte ik de overstap naar Deloitte. Daar werd ik – als niet-RA – partner in de accountantspraktijk. Uiteindelijk ging deze functie schuren met mijn bestuurswerk en besloot ik te stoppen bij het IIA. Na tien jaar externe praktijk wilde ik graag terugkeren in het publieke domein en werd ik in 2009 directeur van de Rekenkamer Rotterdam door gewoon een sollicitatiebrief te sturen toen de functie beschikbaar kwam.
Ik heb destijds gesolliciteerd omdat in deze functie een aantal elementen samenkomen die ik uitdagend en inspirerend vind: onderzoekswerk in een complexe politiek bestuurlijke context. En ook nog eens in Rotterdam, de stad waar ik vandaan kom. Je bent in deze functie bovendien je eigen opdrachtgever en aan geen enkel orgaan verantwoording verschuldigd. Die combinatie is vrij uniek. Je krijgt een bestuurstermijn van zes jaar met mogelijkheid van herbenoeming. Ik zit nu halverwege mijn tweede termijn."

Het thema van dit nummer is 'veiligheid'. De rekenkamer publiceerde begin 2017 het rapport *In onveilige handen*.[1] Wat zijn de belangrijkste conclusies?
"We hebben het onderzoek zelf geïnitieerd en gekeken naar de bescherming van gevoelige digitale informatie zoals bijzondere persoonsgegevens, omdat daar een wettelijke taak van de gemeente ligt. Onze conclusie was dat de bescherming van geen kant klopte aan de daaraan te stellen eisen. De gemeente had zelf het idee dat het allemaal best goed op orde was. Zij heeft vooral gekeken naar het risico van cyberaanvallen van buiten. En dat is inderdaad goed geregeld. Het is ons tijdens het onderzoek dan ook niet gelukt om via internet bij gevoelige informatie te komen.
Helaas stond de achterdeur wel wagenwijd open. Op de fysieke locaties konden onze mensen zo binnenlopen ondanks de poortjes en beveiliging. Vervolgens was het vrij eenvoudig om toegang te krijgen tot gemeentelijke informatiesystemen. De door de rekenkamer ingehuurde hackers hadden binnen een halve dag de hoogste rechten in handen en waren in principe in staat om bruggen open te zetten, verkeerslichten te ontregelen en hadden toegang tot de agenda's van de leden van het college van Burgemeester en Wethouders (college). Hierdoor bestaan er risico's op identiteitsfraude, verstoring van de openbare orde, misbruik van publieke middelen en fysieke onveiligheid van bijvoorbeeld collegeleden. Het merendeel van de conclusies was overigens twee jaar geleden al bekend bij het college, maar er is toen vrijwel niets mee gedaan. Het college heeft daardoor willens en wetens risico's gelopen. Dat vind ik ernstig en neem ik het college behoorlijk kwalijk."

Bent u er achter gekomen waarom het college niets heeft gedaan met de kennis die zij al twee jaar had?
"Twee jaar terug was wellicht de financiële positie meer precair dan nu het geval is. Het was een ingewikkelde tijd met veel reorganisaties en grote tekorten. Informatiebeveiliging had, mede gegeven de financiële beperkingen, niet de prioriteit die het nodig had. Anderzijds had de gemeente het idee dat er weinig problemen waren, omdat de beveiliging tegen aanvallen van buiten goed op orde was.
Misschien was het college ook echt niet op de hoogte van de omvang van het probleem. Twee jaar terug zijn er namelijk geen inlooptesten uitgevoerd zoals wij nu wel hebben gedaan, waardoor ook niet duidelijk werd dat de achterdeur wagenwijd openstond. Gelukkig komt er nu een meerjarig programma Informatiebeveiliging en worden er miljoenen euro's extra per jaar uitgetrokken voor informatiebeveiliging. Dat ligt vast in de voorjaarsnota 2017. Dat is pure winst en dat werd tijd ook."

Het college heeft geprobeerd de publicatie van het rapport tegen te houden. Waarom?
"Ik weet het niet precies. In de eindfase van het onderzoek heb ik de ambtelijke top mondeling geïnformeerd over de uitkomsten en de conclusies die de rekenkamer daaraan zou verbinden. Het bleek dat er geen verschil van mening was over de resultaten van het onderzoek. Ik heb tijdens deze bijeenkomst aangegeven dat het rapport openbaar zou worden gemaakt. Een mededeling waar de gemeente niet mee kon leven, waardoor de rekenkamer in een traject terechtkwam dat er uiteindelijk in resulteerde dat de gemeente dreigde met een kort geding als er zou worden gepubliceerd."

Over...

Paul Hofstra was Inspecteur van Financiën op het ministerie van Financiën, hoofd Operational Audit bij de Belastingdienst en partner bij Deloitte Accountants. Sinds juni 2009 is hij directeur van de Rekenkamer Rotterdam, Barendrecht, Capelle aan den IJssel en Lansingerland. Van 1998 tot 2001 was Hofstra bestuursvoorzitter van het IIA.

Dat is tamelijk uniek. Is dat eerder voorgekomen?
"Het is bij mijn weten nog nooit eerder voorgekomen dat binnen een publieke organisatie het ene bestuursorgaan het andere voor de rechter dreigde te slepen. Als het gaat om publicatie van rekenkamerrapporten is de wet volstrekt helder: een onderzoeksrapport van de rekenkamer wordt openbaar gemaakt tenzij er naar de aard vertrouwelijke informatie in staat. Dat was hier niet het geval. Door het college werd het rapport van meet af aan geframed als een 'handboek voor hackers'. We zouden door publicatie van het rapport kwaadwillende hackers vrij spel geven en de burgers en medewerkers van de gemeente daardoor onnodig in gevaar brengen. Onzin natuurlijk want hackers hebben mijn rapport helemaal niet nodig. Bovendien maakten de technische analyses geen onderdeel uit van het gepubliceerde rapport. Die liggen hier veilig in de kluis."

Had u het gevoel dat het college niet meer terug kon?
"Dat gevoel had ik wel. Als je al begint te roepen dat het rapport een les is in 'hoe hack je de gemeente', dan sla je een duidelijke toon aan. Het blijft gissen, maar het wordt lastig als je eenmaal een dergelijke weg hebt ingeslagen om dan achteraf te zeggen, 'Ach, het valt allemaal wel mee'. Nu het rapport is gepubliceerd, is ook niet gebleken dat er problemen zijn geweest. Het rapport heeft uiteindelijk met het meerjarig programma Informatiebeveiliging een positieve doorwerking gekregen. En overigens niet alleen in Rotterdam."

Toch hebt u een aantal concessies gedaan in het rapport
"Ik heb geen concessies gedaan maar wel een beperkt aantal wijzigingen aangebracht. Naar aanleiding van de dreiging van het kort geding is gekeken of alles wat in het rapport stond ook echt nodig was om de conclusies te onderbouwen. Wij hebben toen bijvoorbeeld de plaatjes die erin stonden verwijderd. Ook is een aantal zinnen iets anders geformuleerd zonder dat dat afbreuk deed aan de conclusies. Het college wilde ook de laatste twee hoofdstukken er helemaal uit hebben. Dat hebben wij niet gedaan. Ik heb namelijk naast de wettelijke bepalingen ook nog te maken met de Professional Standards van het IIA, ik ben RO en CIA. Ik kan daardoor niet zomaar teksten schrappen zonder afbreuk te doen aan de conclusies. Daarnaast sta ik niet toe dat de inhoud van een rapport de uitkomst wordt van een onderhandelingstraject met het college. Dat zou een forse inbreuk betekenen op de positie van de rekenkamer. Ook vind ik dat het afleggen van verantwoording over het gevoerde beleid door het college ten principale met 'open raadsdeuren' moet plaatsvinden, dat wil zeggen, in volle openbaarheid."

Het college heeft willens en wetens risico's gelopen. Dat vind ik ernstig en neem ik het college behoorlijk kwalijk

U geeft aan dat het niet alleen een positieve uitkomst had voor gemeente Rotterdam. Zijn er ook lessen te trekken voor andere organisaties?

"Het belangrijkste is dat het belang van informatiebeveiliging prominenter op de agenda van de gemeente Rotterdam is komen te staan. Informatiebeveiliging is 'Chefsache' geworden.
Wij hebben echter ook veel reacties gekregen van andere organisaties en niet alleen van rekenkamers. Verschillende publieke organisaties hebben gevraagd of zij ons plan van aanpak mogen ontvangen. Ik heb zelfs verzoeken uit België gekregen om het rapport op te sturen. Het heeft daarmee een breed effect gehad. De digitale kwetsbaarheid is natuurlijk ook niet alleen iets van de gemeente Rotterdam maar speelt breed."

In hoeverre werken Concern Audit van de gemeente Rotterdam en de rekenkamer samen?

"Ik heb een keer per kwartaal overleg met het hoofd Concern Audit en dan bespreken wij onze plannen en nemen we kennis van de uitkomsten van elkaars onderzoeken. Dit betekent overigens niet dat ik bepaalde onderwerpen niet oppak omdat Concern Audit hier al onderzoek naar doet. De positie en doelgroep van de rekenkamer wijkt namelijk af van die van Concern Audit. Concern Audit is er ten behoeve van het college. De onafhankelijkheid is daarmee relatief. De rekenkamer is echt onafhankelijk, zowel van de gemeenteraad als van het college. Dat is wettelijk zo geregeld. En omdat onze rapporten per definitie openbaar gemaakt worden, hebben ze een grotere impact en zijn ze vaak ook politiek gevoeliger. We bepalen namelijk zelf onze onderzoeksagenda.
Wij steunen soms wel op informatie van Concern Audit. Ik heb een hoge pet op van de kwaliteit van Concern Audit. Het is een van de weinige organisatieonderdelen waar wij op willen en kunnen steunen. Vanwege de kwaliteit die ze leveren én omdat ze relatief onafhankelijk tot een oordeel komen."

Hoe komt het onderzoeksprogramma van de rekenkamer tot stand?

"We starten met het opstellen van een longlist. Deze komt tot stand door gesprekken met de circa 150 stakeholders van de rekenkamer. Het onderzoeksbureau van de rekenkamer voert onderzoeken uit voor de gemeenten Rotterdam, Barendrecht, Lansingerland en Capelle aan den IJssel. Dat betekent dus gesprekken met vier burgermeesters, alle wethouders, alle fracties in de gemeenteraden, directeuren van ambtelijke diensten en een keur aan maatschappelijke organisaties. Daarnaast voeg ik onderzoeken toe aan de lijst waarvan ik en mijn medewerkers vinden dat deze uitgevoerd dienen te worden.
De longlist wordt vervolgens teruggebracht tot een shortlist van tien tot vijftien onderwerpen per gemeente. De shortlist wordt met behulp van elektronische stemapparatuur in separate sessies geprioriteerd door de betrokken gemeenteraden en de medewerkers van de rekenkamer. Aangezien ik enig lid van de rekenkamer ben en de wet niet toestaat dat er een andere opdrachtgever is dan de directeur van de rekenkamer, geef ik uiteindelijk formeel een klap op het onderzoeksprogramma.
Ook krijg ik gedurende het jaar twee tot drie verzoeken van de gemeenteraad van Rotterdam, waarvoor ik ruimte aanhoud in de toe te wijzen onderzoekscapaciteit. Deze verzoeken worden per motie ingediend. Om gehoor te kunnen geven aan een dergelijk verzoek vind ik het belangrijk dat een comfortabele meerderheid in de gemeenteraad het onderzoek steunt. Ik waak ervoor dat de rekenkamer gebruikt wordt als politiek breekijzer. Omdat ik over mijn eigen onderzoeksagenda ga kan ik verzoeken dus ook weigeren."

Zijn er verschillen tussen internal auditors en onderzoekers van de rekenkamer?

"Niet zozeer in kwaliteit maar wel in expertise. De meeste onderzoeken van de rekenkamer zijn beleidseffectiviteitsonderzoeken. Onze expertise ligt dan ook vooral op dit vlak. De meeste internal auditors houden zich hier niet mee bezig. Een internal auditor is sterk gericht op management control en op onderzoeken met een operational-auditinsteek. Maar als je kijkt naar de onderzoeken die wij verrichten gericht op bedrijfsvoering, dan komt dat redelijk overeen met wat ik gewend was bij een IAF. Ondanks dat ik qua achtergrond en opleiding een heel breed team heb, zit er geen RA en sinds kort ook geen RO meer in mijn team. Dit zou ik graag nog willen veranderen." <<

Noot

1. https://rekenkamer.rotterdam.nl/onderzoeken/in-onveilige-handen/ Barendrecht, Capelle aan den IJssel en Lansingerland.

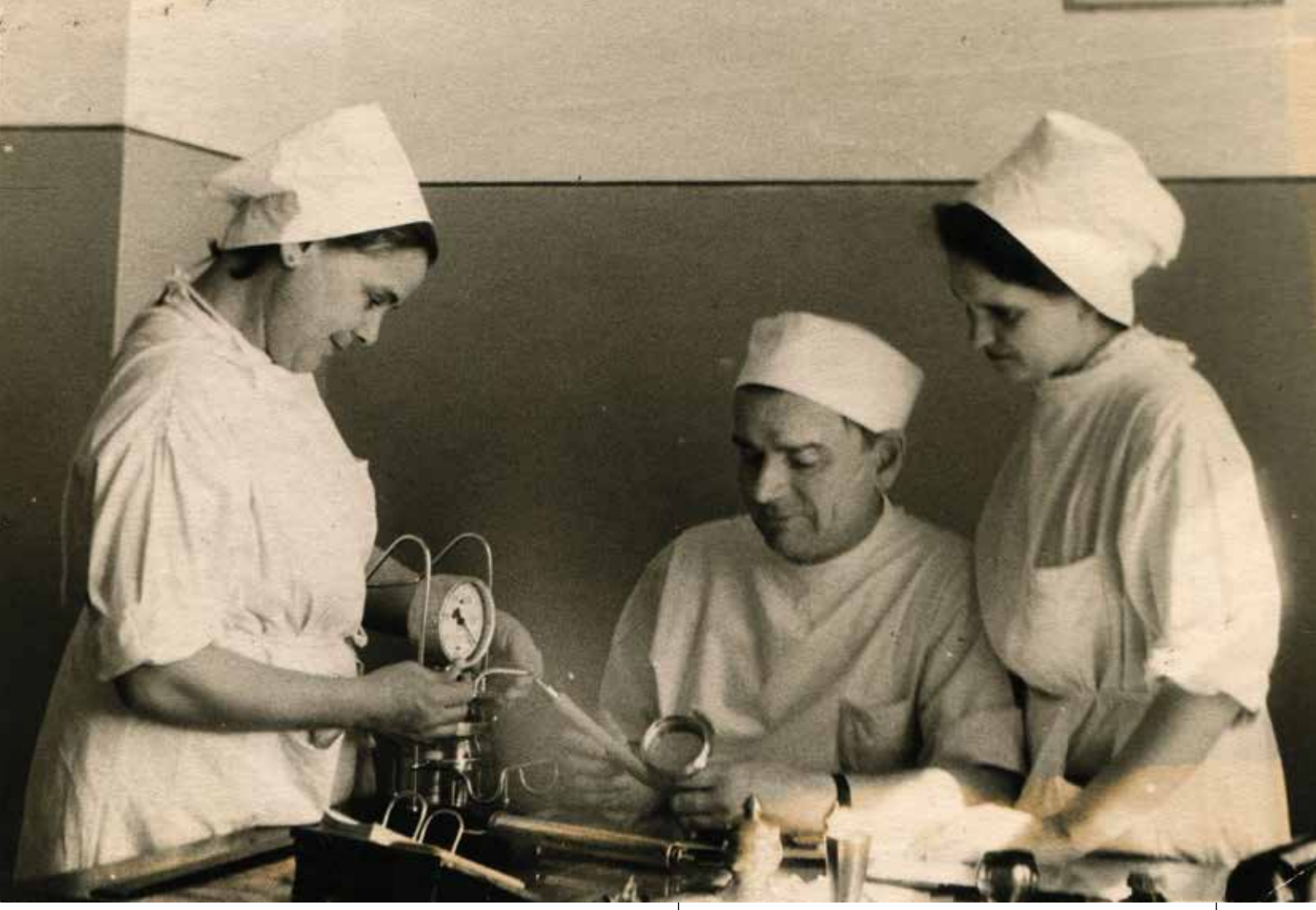
Thema Veiligheid
Tekst Ir. Gezina Atzema RO
Drs. Paul van der Zwan EMIA RO
Beeld 123RF®

Patiënt- en medewerker-*veiligheid* bij het LUMC

Hoe borgt het Leids Universitair Medisch Centrum (LUMC) de veiligheid van patiënten en medewerkers? Met die vraag ging *Audit Magazine* naar Harriette Verwey, cardioloog en voorzitter van de Commissie Interne Audits[1], en Petra van de Voorde, manager Risk en AO/IC. Een boeiend gesprek over patiëntveiligheid, medewerkerveiligheid en veiligheid bij rampen in relatie tot audit.

Wat zijn de ontwikkelingen bij LUMC op het gebied van de interne audit in relatie tot veiligheid?

Harriette Verwey (HV): "Voorheen werd op basis van een auditprogramma een audit uitgevoerd, waarbij met name gesproken werd met leidinggevenden. De audit was gericht op de opzet en het bestaan van de beheersmaatregelen. Interviews met specialisten en verpleegkundigen werden nauwelijks uitgevoerd. De audit werd afgesloten met een verslag, waar geen tot nauwelijks follow-up aan werd gegeven. De audit zelf werd uitgevoerd door teams van eigen mensen, veelal zonder auditopleiding. Je had niet echt diepte-interviews over wat er gebeurde.
Sinds maart 2016 is er echter veel veranderd. Het LUMC werkt nu met het internationaal accreditatieprogramma NIAZ-Qmentum 3.1 (LUMC heeft vier jaar geleden ook een NIAZ-accreditatie gehad). Met het besluit om de NIAZ-eisen na te willen streven is de auditfunctie bij het LUMC verder op de kaart gezet. De afgelopen maanden zijn een zeventigtal interne mensen (artsen, verpleegkundigen en staffunctionarissen) opgeleid tot auditor. Zij voeren in teams zogenaamde tracer audits uit op patiëntveiligheid, veilige werkomstandigheden en apparatuurveiligheid. Naast inhoudelijke auditkennis zijn de collega's ook getraind op interviewtechnieken. Het voornaamste verschil in de uitvoering van de audits zit in de diepgang. Tegenwoordig is het normenkader veel explicieter en wordt – naast een interview met de leidinggevenden – ook gesproken met specialisten en professionals betrokken bij de zorg. Hierbij toetsen we niet alleen de opzet en bestaan, maar ook de uitvoering en het waarom van handelen. Je krijgt dus echt inzicht in de praktijk. De auditrapportage, waarbij expliciet een oordeel wordt gegeven over het wel of niet halen van de norm gaat gepaard met actiepunten en het benoemen van eindverantwoordelijken."



Petra van de Voorde (PvdV): "Daarnaast worden ook op het gebied van risicomanagement op dit moment veel stappen gezet. Het streven is om toe te groeien naar één risicomanagementsysteem, waarbij we meer risicogestuurd gaan werken. Een belangrijk element daarbinnen is het gesprek aan te gaan over risicogestuurd gedrag. Daarbij kan dan bijvoorbeeld besproken worden welke verschillen er tussen afdelingen binnen het ziekenhuis zijn. Het samenwerken tussen afdelingen en het bespreken van risico's en risicogestuurd gedrag willen we de komende jaren nog verder professionaliseren."

U hebt het over tracer audits. Wat moeten we ons daarbij voorstellen?

HV: "Bij een tracer audit wordt het zorgpad (de tracer) van de patiënt gevolgd, waarbij we kijken naar welke procedures er van toepassing waren en naar de deskundigheid (competentieniveau) van de medewerkers. Daarbij mogen de auditors iedereen bevragen. Ze gaan op pad en spreken met medewerkers die bij de zorg van betreffende patiënt(en) betrokken zijn geweest. Het principe geldt: 'tell me, show me'. Dus niet alleen vertellen, maar vooral ook laten zien hoe je werkt!
Om dit mogelijk te maken hebben we veel extra mensen getraind om audits uit te voeren (van dertig naar honderd mensen). Deze auditteams worden intensief begeleid, onder andere met trainingen en gesprekstechnieken. Verder zijn we in gesprek gegaan met de afdelingen om de nieuwe werkwijze toe te lichten en daarmee hun betrokkenheid te vergroten. Wij vragen de afdelingen ook om feedback: hoe hebben zij de audit ervaren? Zo worden beide partijen al doende beter."

Kwaliteitsnorm NIAZ-Qmentum

Het NIAZ maakt gebruik van het internationale accreditatieprogramma Qmentum. Daarbij staat de Q voor kwaliteit, en 'mentum' voor momentum: het is tijd voor kwaliteit. Dit programma is in 2007 ontwikkeld door Accreditation Canada en wordt inmiddels ingevoerd in 27 landen, verspreid over alle werelddelen waar mensen wonen.
Het internationaal accreditatieprogramma NIAZ-Qmentum (KZi 3.1) is het geldende normenkader voor een instelling die een aanvraag voor accreditatie wil indienen op basis van NIAZ-Qmentum.
(Bron: www.niaz.nl)

Hoe ziet de follow-up van dergelijke tracer audits er uit?

HV: "Naar aanleiding van de auditrapportage schrijf ik namens de Commissie Interne Audits een brief naar de afdelingshoofden en teammanagers met de vraag: wat ga je ermee doen en wanneer wordt de Commissie over de verbetermaatregelen geïnformeerd? Het auditrapport gaat ook naar het divisiebestuur en naar de raad van bestuur. Met het eigenaarschap voelen de professionals van de afdelingen zich echt verantwoordelijk om de actiepunten goed op te pakken en dit werkt breed door binnen de organisatie."

Waaraan merkt u dat de draagkracht is vergroot binnen het LUMC?

HV: "Dat merken we aan het gedrag binnen de organisatie. Zo stuurt de Dienst Instrumentele Zaken regelmatig een bericht naar afdelingen dat instrumenten volgens schema nagekeken moeten worden. Voorheen werd er amper

gereageerd, daar waren ook geen directe consequenties aan verbonden. Maar tegenwoordig belt de Dienst Instrumentele Zaken met de afdeling als er niet gereageerd wordt. Vervolgens wordt er binnen de afdeling iemand verantwoordelijk gemaakt voor de servicebeurten van de apparaten. Een verandering aan beide kanten."

Wat zijn de succesfactoren en waar is nog winst te behalen?

PvdV: "We zijn al een hele stap in de goede richting. Wat ik merk is dat de buitenwereld veelal op zoek is naar de bevestiging dat het ziekenhuis alles goed op orde heeft. Hierbij is aantoonbaar in control zijn zeer belangrijk. Met het NIAZ-programma zijn wij intern druk met de professionaliseringsslag. Normen worden expliciet getoetst, verbeterplannen opgesteld en verantwoordelijken in hun rol gezet. De balans tussen de druk van de buitenwereld en de positieve swung binnen het LUMC om te veranderen, lijkt nog wel eens op gespannen voet met elkaar te staan. Hierdoor lijkt de nadruk meer te liggen op aantoonbaarheid in plaats van op de interne bereidheid om de veranderagenda tot een succes te maken."

HV: "Van hoog tot laag is iedereen ervan doordrongen dat het risicobewust handelen en handelen volgens strikte normen noodzakelijk is. Door veel inzicht te geven in wat je doet en uit te leggen waarom normen er zijn en wat het doel is, bereik je veel. Ontegenzeggelijk belangrijk is de zichtbaarheid en steun van de raad van bestuur. Deze is ruimschoots aanwezig, waarmee de raad van bestuur ook echt laat zien waarom de verandering noodzakelijk is en het in belang van de patiënt is.

Ontegenzeggelijk belangrijk is de zichtbaarheid en steun van de RvB. De RvB laat echt zien waarom de verandering noodzakelijk is

In 2018 willen we met audit de stap maken naar het controleren van de follow-up van de verbetermaatregelen. Dan kunnen we toetsen in hoeverre de acties en verbeterplannen hun vruchten hebben afgeworpen en of ook de oorzaken zijn weggenomen." <<

Noten

1. De Commissie Interne Audits gaat over de patiëntgerelateerde audits (patiëntveiligheid, medewerkerveiligheid en instrumentveiligheid) gekoppeld aan de NIAZ/Q Mentum-accreditatie.

Over...

Dr. Harriette Verwey is cardioloog en heeft als aandachtsgebied hartfalen en hartziekten bij vrouwen. Per september 2017 is zij met pensioen. Sinds maart 2016 is zij voorzitter van de commissie Interne Audits van het Leids Universitair Medisch Centrum. Deze taak vervult zij drie jaar.

Drs. Petra van de Voorde RA is manager Risk en AO/IC bij het Leids Universitair Medisch Centrum. Na vijftien jaar werkzaam te zijn geweest bij een groot accountantskantoor trad zij per 1 februari jongstleden in dienst bij het LUMC. Haar belangrijkste opdracht is om in nauwe samenwerking met het Directoraat Kwaliteit en Patiëntveiligheid vorm te geven aan een LUMC-breed integraal risicomanagement.

Rubriek 5 vragen aan de commissaris
Tekst Raymond Wondergem MSc RO
Over Mr. Hans van der Vlist is commissaris bij Woonbron en Parnassia.

Vijf vragen aan...

één

Wat kenmerkt een goede commissaris?

"Het is belangrijk om betrokken te zijn en te blijven bij de organisatie, maar wel met enige afstand. Dit heeft als doel onafhankelijk in je oordeel te blijven. Verder is het goed om je 'oren en ogen' in de organisatie te hebben om niet afhankelijk te zijn van de informatiestroom van de bestuurder. Het gaat erom een open relatie en feeling te hebben met de 'key players' binnen de organisatie, zoals de controller, de or en de managementlaag onder de bestuurder. Daarnaast is het goed om jaarlijks uitgebreid stil te staan bij de strategie van de organisatie. Om niet alleen terug te kijken, maar zeker ook vooruit te kijken. Als laatste is het belangrijk om de werkgeversrol richting de bestuurder serieus in te vullen."

twee

Beschikt u binnen uw commissariaten over een interne auditfunctie? Zo ja, hoe is de relatie tussen de RvC en de IAF?

"De RvC en/of auditcommissie heeft de taak om te zorgen dat de three lines of defense goed georganiseerd zijn. Hierbij gaat het om de inrichting van de auditfunctie en het auditprogramma (de juiste thema's op de planning). Verder kan de RvC via de externe accountant onderwerpen laten onderzoeken. Tevens helpen de verschillende commissies (zoals de auditcommissie) enorm de betrokkenheid van de RvC bij de organisatie te vergroten. Het is een uitdaging voor de RvC om voldoende betrokken te blijven bij de verschillende thema's. Dit doen we door expliciet stil te staan bij de onderwerpen, meer vragen te stellen over de achtergronden van deze onderwerpen en goede notulering. De besluitvorming blijft namelijk een taak van de RvC en niet van de commissies. Die hebben een adviserende en voorbereidende rol richting de RvC."

drie

Is een commissaris vooral een controleur of juist een adviseur?

"Een commissaris staat voor drie rollen opgesteld, namelijk als toezichthouder (controle op de bestuurder), als adviseur van de bestuurder en als werkgever van de bestuurder. Alle drie de rollen zijn even belangrijk."

vier

Wat moet verbeteren aan het toezicht in Nederland? Of, wat moeten de RvC's in Nederland beter doen?

"Dit is een hele brede vraag. Een belangrijk aspect is de samenstelling en de diversiteit van de RvC. Deze diversiteit bestaat uit de verschillende kwaliteiten van de commissarissen, leeftijd, man/vrouw-verhouding, deskundigheden en etnische achtergrond. Bij Woonbron hebben we specifiek gezocht naar een commissaris met een Rotterdamse achtergrond en hebben we de selectie samen met de huurderorganisatie uitgevoerd. Het is lastig om een team van zes personen samen te stellen waarin deze diversiteit terugkomt. De voorzitter heeft een belangrijke rol in het functioneren van de RvC. Hij moet zorgen voor goede verhoudingen (intern en met het bestuur) en elke commissaris voldoende ruimte geven om te kunnen functioneren. Dit stelt hoge eisen aan de voorzitter."

vijf

Hoe ziet u de rol van commissaris zich de komende jaren ontwikkelen?

"We zitten middenin een ontwikkeling. De invulling van de rol van commissaris wordt steeds professioneler. De problemen die ontstaan zijn in de zorg, onderwijs en woningcorporaties hebben gezorgd voor een wake-up call. Dit heeft onder meer geleid tot permanente educatie en de 'fit- en propertest' voor bestuurders en commissarissen. Het belangrijkste doel blijft om met voldoende gezag de bestuurders in het goede spoor te houden."

Thema Veiligheid
Tekst Drs. Nicole Engel-de Groot RA
Beeld 123RF®

Matthijs Pontier, Piratenpartij:

"De **macht** terugbrengen naar de **burger**"

Burgerrechten en veiligheid kunnen wringen. De Piratenpartij wijst op de toenemende macht van de overheid onder het mom van veiligheid. *Audit Magazine* sprak met Matthijs Pontier, woordvoerder van de Piratenpartij.

Waarom kiest u voor de Piratenpartij?
"Ik heb een achtergrond als wetenschapper in technologie en ethiek. De Piratenpartij omarmt techniek maar ziet ook dat het digitale tijdperk leidt tot grote veranderingen. De overheid krijgt veel macht door allerlei data over ons te verzamelen. De kernwaarde van de Piratenpartij is empowerment, het terugbrengen van de macht naar de burger. Wij focussen ons op burgerrechten, transparantie en democratie. Burgerrechten, zoals onze privacy, komt in het geding op het moment dat de overheid onbeperkt data verzamelt en bewaart over burgers. Transparantie gaat over een overheid die onvoldoende transparant is over haar eigen handelen. Democratie gaat over het spreiden van macht. Wij zijn op grond van het subsidiariteitsbeginsel ervoor dat burgers zelf beslissen. Daarnaast zijn technologie en overheid geen gelukkige match. Er zijn talloze voorbeelden waaruit blijkt dat de overheid veel heeft verspild aan ICT-projecten zonder dat dit ergens toe geleid heeft."

Over...
Dr. Matthijs Pontier ontwikkelde aan de Vrije Universiteit Amsterdam emotionele intelligentie en 'moreel besef' voor computers en (zorg)robots. Hij is actief voor de Piratenpartij en stelt zich kandidaat voor de komende gemeenteraadsverkiezingen in Amsterdam.

Veiligheid vereist toch dat de overheid burgers controleert?
"De overheid mag best surveilleren, alleen zie je nu dat zij dat grootschalig doet. Dat is totaal niet efficiënt en heeft te maken met geld. Immers, als onveiligheid blijft bestaan dan ben je verzekerd van budget. Een documentaire over Bill Binney, klokkenluider bij de NSA, maakte dit duidelijk. In plaats van massasurveillance, inbreken op netwerken of internetdiensten en opslag van gegevens van niet-verdachte personen in grote datacentra, kun je veel slimmer en gerichter surveilleren. We maken daarom ook bezwaar tegen de sleepnetmethode van de overheid. Deze methode verzamelt veel data over te veel onschuldige mensen en bovendien wordt dat ook nog eens lang bewaard. Het bestaan van privacy is juist een voorwaarde voor veiligheid vinden wij. Als iemand informatie over jou heeft maakt dat die persoon oppermachtig. Tegenstanders van de sleepwet kunnen hun stem uitbrengen op www.teken.sleepwet.nl.
Daarnaast vinden wij dat de persvrijheid in het geding is. Het afschermen van bronnen bij journalistiek onderzoek is onvoldoende. Dat maakt het onmogelijk dat journalisten bijvoorbeeld onderzoek naar jihadisme kunnen doen."

Waarom is dit erg als je toch niets te verbergen hebt?
"Het probleem is dat je niet van tevoren weet wat er gaat gebeuren met informatie. Geheime diensten kunnen data delen met andere geheime diensten. In andere landen gelden andere normen en waarden en kun je geconfronteerd

worden met informatie over jezelf waarvan je geen idee had dat dit bekend is.
En niet alleen overheden verzamelen allerlei data over burgers, ook bedrijven doen dat steeds meer. Data is goud waard. In politieke campagnes kunnen op grond van data mensen worden gemanipuleerd. Mensen nemen andere beslissingen op basis van de informatie die ze voorgeschoteld hebben gekregen, zonder dat ze zich hier bewust van zijn. Overheden besteden steeds meer diensten uit en er vinden steeds meer publiek-private samenwerkingen plaats. Dit zorgt ervoor dat het voor burgers moeilijker wordt om openheid te krijgen over hun data, omdat onduidelijk is wie welke data waar bewaart."

Geldt die privacy niet voor de overheid en haar ambtenaren?
"Wij vinden dat privacy ophoudt wanneer je andere mensen gaat vertegenwoordigen of handelt namens burgers. Als een ambtenaar onderzoek uitvoert en daarin beleidskeuzen maakt, dan moet transparant worden waarom die ambtenaar die keuzen heeft gemaakt.
Nu weten we niets van wat er gebeurt met de grootschalige data die de overheid over ons verzamelt. Wat de overheid nu doet is bijvoorbeeld op grond van risicoprofielen mensen in de gaten houden. Dat is niet per se erg, maar het moet wel transparant zijn hoe en waarop onderscheiden wordt. Is dat afkomst of religie? Maar ook bijvoorbeeld verzekeraars kunnen op grond van dit soort profielen discrimineren in verzekeringspremie."

Jullie verwelkomen dat auditrapporten over de overheid openbaar worden?
"Ja, dat is tot op zekere hoogte uiteindelijk goed. Maar er wordt krampachtig omgegaan met transparantie. Men kan denken dat transparantie zorgt voor minder openhartigheid of dat het een stok wordt om mee te slaan. Het dilemma speelt dan of transparantie het uiteindelijke doel wel dient. Ik denk dat transparantie per definitie goed is, maar dat er tegelijkertijd een cultuurverandering en een maatschappelijke discussie nodig is over hoe wij omgaan met fouten. Uiteindelijk draait het om vertrouwen. Hetzelfde speelt bij beroepsgroepen als artsen of advocaten. Ook hier geldt dat het normaal moet zijn om transparantie te bieden over hoe een arts of advocaat functioneert. Maar tegelijkertijd is het dan wel noodzakelijk dat mensen met respect met die transparantie omgaan. Dit vereist een maatschappelijke discussie."

In 2016 werd de eerste Piratenpartij opgericht in Zweden. Inmiddels is de Piratenpartij vertegenwoordigd in meer dan zestig landen. In Nederland is de partij verkozen in zowel Amsterdam West als in het waterschap. De partij is opgericht vanuit de noodzaak om prioriteit te geven aan burgerrechten in een digitale maatschappij.

Verwelkomen jullie dan een digitale samenleving?
"Wij zijn enthousiast over de mogelijkheden die de technologie ons biedt. Via internet kun je bijvoorbeeld iedereen betrekken bij de democratie. We vragen iedereen om input te geven op onze programmapunten. Tegelijkertijd zijn er risico's verbonden aan een digitale samenleving. Digitale processen zijn lastig te beveiligen. Hoe weet je dat verkiezingen met stemcomputers juist verlopen zijn? De sleutel om mensen bewust te maken van de risico's van een digitale samenleving zit in onderwijs. Mensen vinden het niet normaal als de overheid hun brieven zou openen en lezen, maar tegelijkertijd heerst onvoldoende besef dat dit met e-mail op een veel grotere schaal gebeurt." <<

Thema Veiligheid
Tekst Naeem Arif EMIA RO
Drs. Nicole Engel-de Groot RA
Beeld NFP Photography
Adobe Stock

Onderzoek naar *veiligheid in* de publieke sector

De Algemene Rekenkamer onderzoekt of de rijksoverheid publiek geld zinnig, zuinig en zorgvuldig uitgeeft. Veiligheid is een belangrijk onderzoeksthema voor de Algemene Rekenkamer. Wij spraken met Arno Visser, president, over de rol van de rekenkamer om de rijkstaken op het gebied van veiligheid tegen het licht te houden.

Waarom is veiligheid een belangrijk onderzoeksobject voor u?
"Wij baseren onze keuze voor onderzoeksthema's op de vraag waar de rijksoverheid risico's loopt en wij dus zoveel mogelijk toegevoegde waarde kunnen leveren. Op veiligheid kunnen wij veel betekenen voor de ontvanger van onze rapporten, het parlement dat de ministers controleert bij de uitvoering van beleid. Het parlement dient hiervoor te beschikken over alle benodigde informatie.
Veiligheid is bij uitstek een terrein waarbij niet alle informatie vrij toegankelijk is. De Algemene Rekenkamer heeft, op grond van haar unieke bevoegdheden, toegang tot alle informatie bij ministeries en uitvoeringsdiensten. Hierdoor kunnen wij vaststellen of ministers het parlement voorzien van alle relevante informatie over Justitie, Defensie en veiligheidsdiensten. Daar kunnen wij toegevoegde waarde leveren. Met het thema veiligheid is bovendien een groot financieel en maatschappelijk belang gediend.
Wij volgen hoe het veiligheidsbeleid van de rijksoverheid, bijvoorbeeld in de strafrechtketen, over een lange periode uitpakt. Bij herhaling komt dit thema terug, om te zien wat de stand van zaken is en hoe acties zijn opgepakt. Onze onderzoeken zijn geen losse flodders."

Wat is de kerntaak van de rekenkamer?
"Wij hebben een wettelijke taak om elk jaar de ontvangsten en uitgaven van de rijksoverheid te controleren, zodat wij de Rijksrekening kunnen goedkeuren. Dat doen wij in het verantwoordingsonderzoek dat op de derde woensdag van mei aan de Tweede Kamer wordt overhandigd. Hierbij geven wij een oordeel over alle departementale jaarrekeningen. Op grond van ons oordeel kan de Tweede Kamer decharge verlenen aan het kabinet. Ons oordeel omvat drie aspecten. Allereerst een oordeel over de rechtmatigheid van uitgaven. Is geld besteed conform de regels en aan het beoogde doel? Het kan zijn dat geld besteed is aan het doel waarvoor het bestemd was, maar de regels omtrent inkoop of aanbesteding niet nageleefd zijn. Andersom kunnen alle uitgaven conform wet- en regelgeving hebben plaatsgevonden maar zijn gelden niet conform de begroting uitgegeven.
Daarnaast beoordelen wij de kwaliteit van de bedrijfsvoering en het financieel beheer. Dit omvat ook de kwaliteit van beleidsinformatie. Beschikt de minister tijdig over de juiste informatie en heeft hij het parlement voldoende geïnformeerd? Een voorbeeld op het gebied van veiligheid: ambtenaren dienen bij indiensttreding gescreend te worden op een bepaald niveau voordat zij toegang krijgen tot gevoelige informatie. Wij hebben geconstateerd dat in een aantal gevallen bij diverse ministeries en diensten al voordat de resultaten van de screening bekend waren, ambtenaren toegang verkregen tot informatie. Dit beoordelen wij als een onvolkomenheid in de bedrijfsvoering.

Over...
Drs. Arno Visser is collegelid sinds januari 2013 en president van de Algemene Rekenkamer sinds oktober 2015. Daarvoor was hij onder meer wethouder van Almere en lid van de Tweede Kamer namens de VVD.

Ten slotte betrekken wij steeds meer de doeltreffendheid van uitgaven en rijksbeleid in ons verantwoordingsonderzoek. Heeft de belastingbetaler waar gekregen voor zijn geld? Dit aspect is relatief nieuw, maar belangrijk. De maatschappij wil meer en meer weten wat er gebeurt met publieke middelen en of beleid effect heeft gehad. Om dit te onderzoeken is het nodig dat er een referentiekader is, heldere doelen zijn geformuleerd en indicatoren zijn vastgesteld op basis waarvan getoetst kan worden."

Wat zijn belangrijke bevindingen op veiligheidsgebied?
"Op het gebied van veiligheid spelen vele belanghebbenden een rol. De politie, brandweer, het Openbaar Ministerie, de rechtspraak, ook de Dienst Justitiële Inrichtingen, en natuurlijk de burgers waar het om gaat. De uitvoeringsorganisaties zijn afhankelijk van elkaar om hun rol optimaal te kunnen vervullen. De keten kan alleen optimaal functioneren als niet alleen de eenheden zelf in control zijn maar ook de keten als geheel. Belangrijke voorwaarde hiervoor is dat gewerkt wordt met uniforme data en indicatoren. Data moet niet alleen uniform zijn, maar ook in systemen over de hele keten gemeten kunnen worden. Op die wijze kan integraal verantwoording worden afgelegd en gestuurd worden. De afgelopen jaren hebben we vastgesteld dat de inrichting van de keten en het werken met een uniforme dataset onvoldoende is. In een tijd met volop bezuinigingen op overheidsorganisaties wringt dat eens te meer.
Het niet optimaal functioneren van de keten is niet alleen een kwestie van systemen. Het heeft ook te maken met cultuur. Binnen de veiligheidsketen bestaat geen cultuur om dingen te bespreken met elkaar. Hierdoor ontstaat een gebrek aan transparantie en inzicht in wat er speelt bij een ander. Het ministerie van Jusititie en Veiligheid heeft dit erkend en een verbeterprogramma opgesteld. In dit programma zijn acties opgenomen waardoor voor ons een referentiekader is geschapen om de voortgang van verbeteringen te toetsen."

Vindt de Algemene Rekenkamer ook iets van zo'n programma?
"De minister van Justitie en Veiligheid is hiervoor verantwoordelijk. Belangrijk is dat wij geen eigenaar worden van een verbeterprogramma. Wij monitoren dat programma intensief, kijken naar de indicatoren en actiepunten en rapporteren hierover als dat van belang is voor de Tweede Kamer, onder andere in het verantwoordingsonderzoek. Wij toetsen of beleid is uitgevoerd zoals het bedoeld is. We doen geen audits voorafgaand aan de implementatie, tenzij de implementatie een dusdanig lang traject is dat het niet zinvol is om pas na de implementatie een audit uit te voeren. Dit was bijvoorbeeld het geval bij de vervanging van de DigiD. Over dit onderwerp hebben we een tussenrapport opgesteld. Het gaat erom dat het kabinet en parlement op basis van onze bevindingen desgewenst kunnen bijsturen. Dit betekent dat we in die gevallen kort op de bal moeten zitten."

Hoe bepalen jullie je onderzoeksthema's?
"Het college stelt in een strategisch document met een vijfjaarshorizon vast welke thema's we willen behandelen in onze onderzoeken. Deze thema's kunnen zich richten op belangrijke geldstromen zoals belastingen, andere ontvangsten en ontwikkelingen in de premiesectoren zorg en arbeidsmarkt. Daarnaast selecteren we bepaalde thema's die wij belangrijk achten. Veiligheid is daarvan een voorbeeld. Thema's komen bovendrijven op grond van signalen, onze monitoring of een fingerspitzengefühl. Soms kan het zijn dat we over een lange termijn een tendens in kaart willen brengen. Keuzen worden gemaakt op grond van risico's voor het rijk, de tijdshorizon die verstreken is sinds onze laatste werkzaamheden (lang of juist te recent), het kunnen leveren van toegevoegde waarde vanwege onze bevoegdheden en de politieke relevantie. Dit laatste is een belangrijk criterium want onze onderzoeken dienen maatschappelijk relevant te zijn."

Komt een audit op verzoek van een minister regelmatig voor?
"Een audit op verzoek van een minister of de Kamer komt enkele keren per jaar voor, maar alleen als het inpasbaar is en wij bij uitstek de instantie zijn om het uit te voeren. We bepalen volledig zelf onze onderzoeksagenda. Zo heeft op verzoek van de Tweede Kamer de Algemene Rekenkamer een onderzoek gedaan naar het effect van de subsidie op elektrische en hybride auto's. Het was niet bekend hoeveel subsidie via diverse regelingen verstrekt werd en wat dat opleverde. Wij becijferden dat deze regelingen vrij duur zijn en dat onvoldoende was nagedacht over alternatieven om de verkoop van elektrische auto's te stimuleren. Dat leidde tot aanzienlijke aanpassingen van de fiscale regelingen door de staatssecretaris en de Kamer.
De Algemene Rekenkamer rapporteert feitelijk en doet vaak aanbevelingen. De consequenties voor het beleid worden getrokken door de Tweede Kamer en de betrokken ministers. De minister en het departement en/of de uitvoeringsorganisatie zijn de auditee. Er vindt hoor en wederhoor plaats voordat onze bevindingen gefinaliseerd worden. Wij nodigen de betreffende minister uit per brief te reageren op onze bevindingen, zodat de Kamer meteen over een eerste reactie beschikt. Circa 80% van onze aanbevelingen wordt overgenomen. En we spannen ons in om dit naar 100% te brengen."

Empathie tonen voor de mensen die met hun spreekwoordelijke poten in de modder staan

Welke rol speelt cultuur binnen de overheid en de Algemene Rekenkamer?
"Cultuur is ongekend belangrijk. De Algemene Rekenkamer is geen losstaande entiteit, maar een permanent onderdeel van de feedbackloop voor een betere overheid. Wij dienen een toon aan te slaan waarmee wij begrepen en erkend worden binnen de rijksoverheid. Dat is geen 'betwetertoon', maar empathie tonen voor de mensen die met hun spreekwoordelijke poten in de modder staan. Als we dat niet doen, dan vormen wij zelf de grootste hindernis om tot resultaten te komen, namelijk het creëren van een effectieve interventie. Hier draait het uiteindelijk om.
Met onze werkzaamheden willen we inzicht creëren, leidend tot acties waardoor overheidstaken efficiënter en effectiever worden uitgevoerd. In die zin vind ik, ook vanwege mijn achtergrond als letterkundige, taal heel belangrijk. Er wordt vaak gedacht dat het binnen de Algemene Rekenkamer allemaal draait om rekenen met getallen, maar taal en toon zijn zeker zo belangrijk. Dat wil niet zeggen dat wij hier cultuurexperts in dienst nemen. Cultuur dient in de bagage van alle onderzoekers te zitten. Als cultuur wordt 'weggeorganiseerd' dan wordt het een excuus voor anderen om je er verre van te houden."

Zijn jullie specialisten op de onderzoeksthema's?
"Grote onderwerpen volgen we meerjarig. Dat betekent dat medewerkers gevraagd wordt om zich te verdiepen in een thema of beleidsterrein, zoals zorg of veiligheid. Dit is meer dan vakkennis, want het betekent ook dat je een netwerk opbouwt. Voor veiligheid is het vereist dat we met een toegewijd team werken. Onze mensen worden speciaal gescreend opdat ze toegang krijgen tot vertrouwelijke informatie. Strenge protocollen waarborgen dat alleen zij bij deze informatie kunnen. We zijn hier heel alert op, want we willen te allen tijde voorkomen dat we het vertrouwen beschamen. Wij werken vanuit het feit dat wij toegang hebben tot vertrouwelijke informatie. Dit betekent bijvoorbeeld dat ons onderzoekswerk ook van dienst kan zijn voor de Tweede Kamercommissie voor inlichtingen- en veiligheidsdiensten, ook wel bekend als 'Commissie Stiekem'.
We hebben enerzijds specialismen, anderzijds willen we geen verkokerde organisatie zijn. Dus daar waar het kan werken onderzoekers samen over specialismen heen. We vinden het wel weer gezond als mensen na een periode van circa vijf jaar switchen van specialisme. Wij hebben onlangs onze organisatie gewijzigd. Het is nu voor bepaalde specialismen mogelijk om in hogere schalen werkzaam te zijn of om meer specialisten van buiten tijdelijk in te huren. Dit was nodig om als werkgever te kunnen concurreren met andere organisaties en omdat we bepaalde vakkennis willen hebben en houden, en andere alleen tijdelijk nodig hebben."

Wat is de relatie met de ADR?
"Om te beginnen is het uniek in Nederland dat wij een Auditdienst Rijk hebben. In andere landen maakt een ADR onderdeel uit van de Algemene Rekenkamer. Het verschil tussen de ADR en de Algemene Rekenkamer is dat de ADR rapporteert aan de minister en wij aan het parlement. Wij kunnen gebruikmaken van de rapportages en bevindingen van de ADR als we vinden dat wij hierop kunnen steunen. We zullen dat van geval tot geval beoordelen. We kunnen, zoals onlangs op het onderwerp informatiebeveiliging het geval was, besluiten om gebruik te maken van de ADR-werkzaamheden en vervolgens nog aanvullend onderzoek te doen. We trekken dezelfde lijn voor tolerantie en materialiteitsgrenzen en hanteren dezelfde rechtmatigheidsnormen. De ADR-rapporten zijn tegenwoordig openbaar. Ik vind dat goed, want het zorgt voor een betere dynamiek in de politiek. Waar voorheen plots een minister kon wapperen met een ADR-rapport en dan niemand wist waar het over ging, heeft nu iedereen dezelfde informatie."

Hoe ziet een rekenkameronderzoek eruit?
"Waar voorheen, vóór het digitale tijdperk, onze medewerkers naar het departement toe moesten om informatie uit de kast te halen, hoeft dat vaak niet meer want alles is digitaal beschikbaar. Echter, waar voorheen nog wel eens onverwacht iets uit de kast kon vallen wat een nieuw licht wierp op de zaak, ontvang je tegenwoordig vrijwel altijd wat je vraagt en niet meer. We stimuleren daarom onze onderzoekers om erop uit te gaan en niet alleen achter het bureau te blijven zitten. Het is belangrijk om mensen te ontmoeten en met ze in gesprek te gaan, om de organisatie te leren kennen. We willen ook niet alleen maar een rapport uitbrengen. Het gaat erom dat we een interventie initiëren, dat mensen in beweging komen om dingen anders, beter te gaan doen. We kunnen die interventie teweegbrengen met een onderzoeksrapportage, maar evengoed kan het dat we bijvoorbeeld een congres organiseren met als doel kennis te delen en van elkaar te leren. Onze bijdrage is gericht op verbetering."

Wat moet er gebeuren om Nederland nog veiliger te maken?
"Laat ik voorop stellen dat het in Nederland fijn wonen is, met weinig corruptie en een overheid die de burger serieus neemt. Alle waarborgen zijn aanwezig in dit land om het goed te hebben. Daarmee wil ik niets bagatelliseren, maar wel in een internationaal perspectief plaatsen. Ik was de afgelopen drie jaar voorzitter van de Europese groep van nationale rekenkamers, EUROSAI. In vergelijking met Oost-Europese landen is het hier goed geregeld en wordt serieus en met respect omgegaan met rekenkameronderzoeken. In Nederland is veel te winnen op het gebied van efficiency en effectiviteit. Zie bijvoorbeeld het traject om politiekorpsen te centraliseren. Dat leert dat er nog veel te doen is op dat vlak." <<

Internal Auditors, ga aan de slag met cybersecurity!

Er gaat geen dag voorbij of er wordt in het nieuws gesproken over termen als cybersecurity, cybercriminaliteit, informatiebeveiliging, datalekken en ga zo maar door. Dit is het gevolg van de vergaande digitalisering van onze maatschappij en de kwetsbaarheden die dit met zich meebrengt. Maar wat heeft dit voor gevolgen voor organisaties en welke rol speelt de Internal Auditor hierin?

Door de toenemende digitalisering zijn veel organisaties in grote mate afhankelijk geworden van IT. Wanneer de IT onverhoopt uitvalt, kan dit de volledige organisatie stilleggen met grote financiële schade tot gevolg. Denk bijvoorbeeld aan de wereldwijde cyberaanval die afgelopen zomer voor grote problemen in de Rotterdamse haven heeft gezorgd. Anderzijds heeft de toenemende digitalisering tot gevolg dat organisaties veel persoonsgegevens digitaal verwerken. Ook dit vormt een groot potentieel risico. Wanneer bijvoorbeeld de patiëntgegevens van een ziekenhuis op straat komen te liggen, kan dit tot enorme reputatieschade leiden. Daarnaast komt er vanuit de wet- en regelgeving steeds meer druk op organisaties te liggen. Vanaf mei 2018 dienen organisaties compliant te zijn aan de nieuwe Europese privacyverordening, de Algemene Verordening Gegevensbescherming (AVG). Dit vormt een grote uitdaging voor veel organisaties. Indien organisaties niet aantoonbaar compliant zijn aan de AVG, lopen ze het risico op hoge boetes.

Gezien de huidige ontwikkelingen, speelt anno 2017 cybersecurity een dusdanig belangrijke rol binnen organisaties, dat organisaties er niet meer aan ontkomen om dit onderwerp strategisch in te zetten. Op boardroomniveau dient er voldoende aandacht, kennis en bewustzijn aanwezig te zijn om de juiste strategische beslissingen te kunnen nemen. Hiervoor ligt momenteel een grote uitdaging bij de experts op uitvoerend niveau.

Kloof tussen de Raad van Bestuur en de Information Security Officer

Uit het onderzoek dat Mieke heeft uitgevoerd in het kader van haar afstudeerscriptie, blijkt dat er een belangrijk verschil van inzicht is tussen het strategisch en het uitvoerend niveau binnen organisaties met betrekking tot het onderwerp cybersecurity. Beide niveaus schatten de risico's dus ook anders in. De Raad van Bestuur bekijkt dit onderwerp vanuit de strategie en vanuit de risico-inventarisatie en op basis daarvan is zij tevreden over de aanpak van cyberrisico's. De Information Security Officers vinden daarentegen een gebrek aan kennis, aandacht en bewustzijn op het gebied van cybersecurity bij de board nog altijd een belangrijk knelpunt. De aandacht van de board gaat voornamelijk uit naar het primaire proces en cybersecurity zien ze nog niet als onderdeel van dit proces maar meer als ondersteunend vanuit IT. Dat is juist één van de obstakels.

De experts op uitvoerend niveau kunnen nog zo hard roepen, maar als men het op strategisch niveau niet op de juiste waarde weet te schatten, zal het onderwerp nog steeds niet de aandacht krijgen die het verdient. De ontwikkelingen gaan in sneltreinvaart, maar de Raad van Bestuur ontwikkelt zich niet in hetzelfde tempo mee. Het gevolg hiervan is een beperkte progressie in het treffen van maatregelen die de experts noodzakelijk achten om vooruitgang te boeken bij de beheersing van cyberrisico's.

De Information Security Officer lijkt het alleen niet voor elkaar te krijgen om voldoende draagvlak te creëren bij de Raad van Bestuur op het gebied van cybersecurity. Hier kunnen wij als Internal Auditors toegevoegde waarde bieden!

Aan tafel bij de board of directors

Van ons als Internal Auditors wordt verwacht dat we een onafhankelijk en

Mieke de Lepper:

Mieke de Lepper is Interim Professional bij RSG Finance. Hiervoor is ze 3,5 jaar werkzaam geweest als Internal Auditor en Data Protection Officer bij een ziekenhuis. In deze periode heeft ze, in het kader van haar afstudeerscriptie voor de master Accountancy, onderzoek gedaan naar de wijze waarop invulling wordt gegeven aan de communicatie over de bedreigingen uit hoofde van cybersecurity tussen de Information Security Officer en de Raad van Bestuur binnen de algemene ziekenhuizen in Nederland. Dit onderzoek is in 2016 bekroond met de Nyenrode Essayprijs Accountancy.

Aziz Suhonic:

Aziz Suhonic is Interim IT Audit Professional bij RSG Finance. Met ruim 8 jaar ervaring als IT Auditor heeft hij op het gebied van IT-auditing onder andere de volgende thema's aan de orde zien komen: ITIL, jaarrekeningcontroles (algemene IT beheersmaatregelen), derde partij verklaringen (ISAE3402), Internal Audit ondersteuning, Cybersecurity en Informatiebeveiliging. Hij heeft hierdoor vanuit diverse invalshoeken inzichten verkregen binnen organisaties op deze onderwerpen; op strategisch maar ook op tactisch en operationeel niveau.

objectief beeld geven van de risico's die een organisatie loopt. Dit geldt dus ook voor de cyberrisico's, waarbij breder gekeken moet worden dan alleen naar de IT-afdeling. In hoeverre is een organisatie opgewassen tegen de huidige cyberbedreigingen? En in hoeverre voldoet de organisatie aan de AVG, die over minder dan een half jaar in werking treedt? Als Internal Audit dienen we onze inzichten en risico's rondom cybersecurity bespreekbaar te maken en de leden van de Raad helpen deze te begrijpen en aan te pakken.

Internal Audit bevindt zich in een unieke positie dat zij periodiek mag aanschuiven bij de Raad van Bestuur. Dit is een uitgelezen mogelijkheid om op een laagdrempelig niveau cybersecurity op de agenda te zetten van de board en daarmee het bewustzijn en de kennis bij de leden te verhogen.

Ook het IIA onderschrijft de belangrijke rol die onzes inziens Internal Audit heeft op dit onderwerp. Recentelijk hebben zes Europese Instituten van Internal Auditors, waaronder IIA Nederland, onderzocht wat de 'hot topics' zijn als het gaat om de planning van Internal Audit activiteiten voor 2018 . Hieruit blijkt dat de cyberrisico's hoog op de agenda dienen te staan van iedere Internal Audit afdeling.

Maar hoe krijgt de Internal Auditor nu een goed beeld van de cyberrisico's die een organisatie loopt?

Cybersecurity assessment als instrument

Eén van de mogelijke instrumenten om de cyberrisico's binnen een organisatie inzichtelijk te maken, is een cybersecurity assessment. Met een dergelijk assessment wordt de huidige situatie getoetst. Dit legt de mogelijke risico's bloot ten aanzien van de technologie, de processen en de mens op het gebied van cybersecurity. Het is van belang dat hierbij niet alleen gefocust wordt op de technische kant van cybersecurity maar dat bijvoorbeeld ook aandacht wordt besteed aan de mate van bewustzijn onder de medewerkers inclusief de Raad van Bestuur, waar de verantwoordelijkheden zijn belegd voor cyberrisico's en of cybersecurity structureel op de agenda van de Raad van Bestuur staat.

De volgende componenten dienen onderdeel uit te maken van een cybersecurity assessment:

Van links naar rechts: Ivo van Lierop (algemeen directeur), Mieke de Lepper en Aziz Suhonic

- Organisatie & Governance;
- Gedrag & Cultuur;
- Waardeketen (stakeholders) versus risico's;
- Inzicht in het technologielandschap;
- Wet- & regelgeving;
- Detectie;
- Reactie.

Per component dient vervolgens een goed beeld verkregen te worden van de huidige situatie. Deze informatie kan ingewonnen worden middels het afnemen van enquêtes of interviews met de belanghebbenden. Beperk je bij de selectie van de belanghebbenden niet alleen tot IT-professionals, maar neem hierbij ook de afdelingshoofden van andere organisatieonderdelen en de Raad van Bestuur mee. Zo wordt het assessment ingevuld vanuit verschillende invalshoeken, waaronder het primaire proces, en krijg je een compleet beeld van de organisatie.

De uitkomsten van het cybersecurity assessment vormen vervolgens een mooi uitgangspunt om het gesprek aan te gaan met de Raad van Bestuur. Maak de Raad bewust van het feit dat cybersecurity een belangrijke strategische impact heeft. Anno 2017 is het niet meer voldoende om alleen op uitvoerend niveau een aantal goede experts aan te stellen. Cybersecurity vraagt om een structurele organisatorische inbedding op het hoogste niveau! Werk aan de winkel dus.

Over RSG Governance, Risk & Compliance

RSG G.R.C. is een interim- en adviesbureau op het gebied van Governance, Risk & Compliance. Wij hebben 25 hoopopgeleide professionals in dienst die u kunnen ondersteunen op capaciteits- en kennisvraagstukken binnen Internal Audit, Risk Management en Compliance.
Ook op het gebied van Cyber Security, Data Privacy (GDPR) en aanverwante gebieden als data-analytics bent u bij ons aan het juiste adres.

Wij leveren u snelheid en kwaliteit tegen een interessante prijsstelling. Geïnteresseerd? Neem dan contact met ons op.

RSG Governance,Risk & Compliance

Vestdijk 57a
5611 CA Eindhoven
The Netherlands

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

RSG CORPORATE GOVERNANCE
HUMAN KEY SOLUTIONS

Thema Veiligheid
Tekst Drs. Lucas Kroes RO
Mr. Nicole Kuijpers RO
Beeld 123RF®

Openbaar Ministerie: beheerst gezag

Het Openbaar Ministerie (OM) is de enige bevoegde instantie in Nederland die verdachten van een strafbaar feit voor de rechter kan brengen. Hierbij heeft het OM verregaande bevoegdheden gekregen. Dit artikel geeft inzicht in het OM en specifiek in de organisatie en activiteiten van haar auditfunctie. En hoe invulling wordt gegeven aan continu leren en verbeteren en aan beheerst gezag.

Het OM opereert vanuit de tien arrondissementsparketten, het ressortsparket en drie landelijke onderdelen die samen inhoud geven aan de uitvoering van de strafrechtelijke handhaving van de rechtsorde (zie *figuur 1*). In 2016 behandelde het OM 254.000 misdrijfzaken en 130.000 overtredingszaken. Daarmee is het OM een belangrijke schakel in de strafrechtketen en levert het een grote bijdrage aan een rechtvaardig en veilig Nederland. In de werkzaamheden die het OM uitvoert gaat het naast het vervolgen van verdachten in toenemende mate om de zorg voor bijvoorbeeld slachtoffers en nabestaanden en het leveren van inzet voor het handhaven van de openbare orde en veiligheid. Dit leidt ertoe dat het takenpakket van het OM zich uitbreidt met inzet die vaak buiten het strafrechtelijk kader valt.

Verregaande bevoegdheden

Om criminaliteit effectief te kunnen bestrijden heeft het OM verregaande bevoegdheden gekregen, die diep kunnen ingrijpen in het leven van burgers. Vanzelfsprekend worden daarom hoge eisen gesteld aan de wijze waarop het OM zijn taken uitvoert. De samenleving moet erop kunnen rekenen dat het OM de wet naleeft en kan uitleggen hoe het tot een oordeel is gekomen. Er dient, met andere woorden, sprake te zijn van beheerst gezag. Verschillende incidenten hebben echter ook kwetsbaarheden in het handelen van het OM blootgelegd. Zaken als de moord op voormalig minister Els Borst, de afhandeling van de zaak rond Lucia de B. en, verder in het verleden de Schiedammer parkmoord, hebben laten zien hoe belangrijk de focus op kwaliteit, zorgvuldigheid en professionaliteit zijn en blijven voor het goed functioneren van het OM.

Nieuwe uitdagingen

Ondertussen staat de buitenwereld niet stil en komen er voor het OM steeds nieuwe uitdagingen bij. De aanslagen die plaatsvinden in Europa en de rest van de wereld stellen de Nederlandse overheid voor de vraag hoe daar het best op kan worden gereageerd. Voor het OM is in deze context het belangrijkste vraagstuk hoe het strafrecht hier effectief

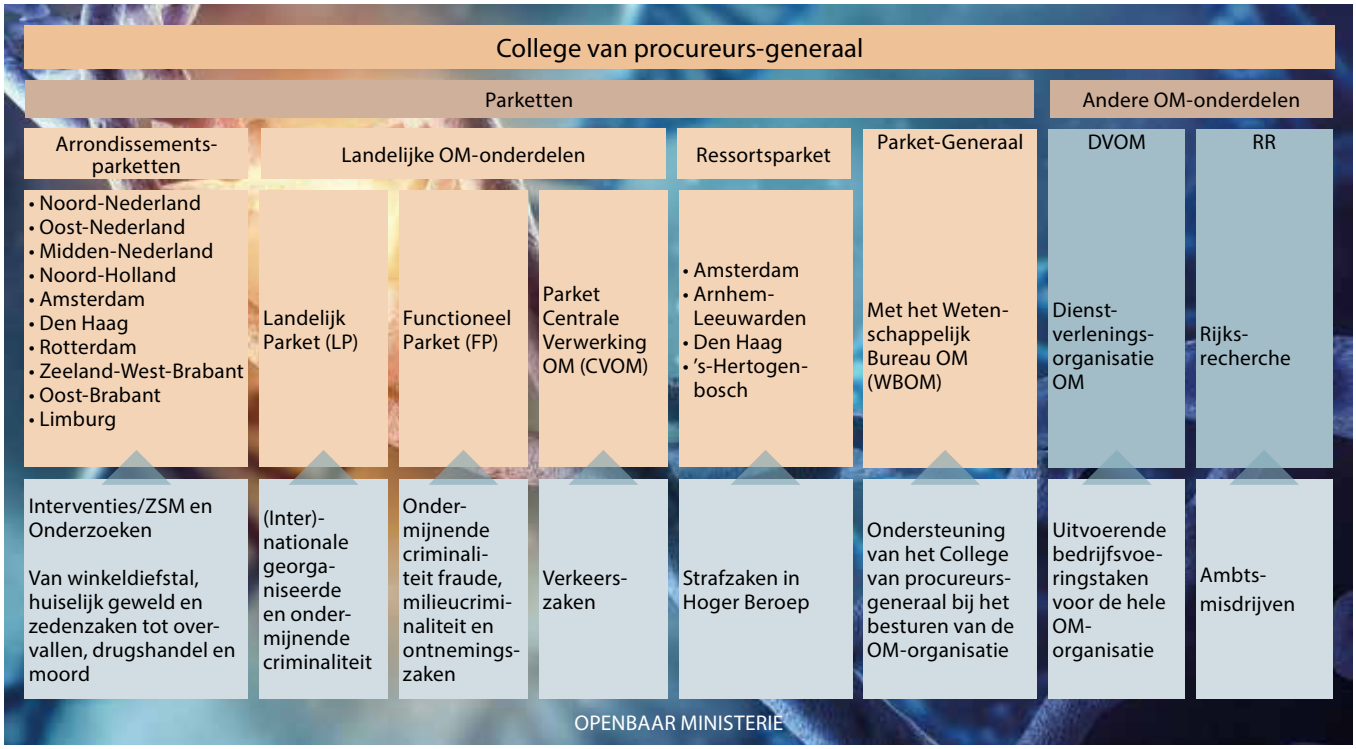
kan worden ingezet. Hoe kan worden voorkomen dat Nederlandse burgers radicaliseren en mogelijk afreizen naar landen als Syrië en Irak om deel te nemen aan de Jihad? Hoe moet worden opgetreden tegen de toenemende mensenhandel en mensensmokkel onder invloed van de groeiende migratiestromen? Voor een effectieve aanpak is internationale samenwerking noodzakelijk en dat stelt nieuwe eisen aan het OM.
Naast deze specifieke aandachtsgebieden geldt in de breedte dat de digitalisering van de samenleving grote impact heeft op de aard van veel criminaliteit. Cybercriminelen kunnen vanaf elke plek ter wereld in een oogwenk duizenden slachtoffers maken, wat in de opsporing en vervolging om een grensoverschrijdende en innovatieve aanpak vraagt. In deze complexe context wordt het gezag van het OM voortdurend aan de orde gesteld en is de beheersing van het grootste belang. Tegen deze achtergrond werkt het OM momenteel planmatig aan het verbeteren van de meest kritische werkprocessen: DNA, OM-strafbeschikking, beslag en executie.[1] De auditfunctie maakt nadrukkelijk onderdeel uit van deze verbeteraanpak.

De auditfunctie van het OM

De interne auditfunctie is een van de instrumenten die het OM beschikbaar heeft om de organisatie scherp te houden, risico's tijdig in beeld te krijgen en het lerend vermogen van de organisatie te bevorderen. De Auditgroep van het OM is centraal gepositioneerd binnen het Parket-Generaal. Dit is het hoofdkantoor van het OM dat samen met het College van procureurs-generaal is gevestigd in Den Haag. Het College van procureurs-generaal bepaalt het landelijke opsporings- en vervolgingsbeleid van het OM en ziet erop toe dat bij de strafrechtelijke handhaving van de rechtsorde sprake is van samenhang, consistentie en kwaliteit.
Analoog aan de organisatiebrede investeringen in professionaliteit en kwaliteit heeft het OM de afgelopen periode geïnvesteerd in de interne auditfunctie. De Auditgroep is uitgebreid en bestaat op dit moment uit twee financial auditors en vier operational auditors. Nu de auditfunctie qua sterkte op orde is gebracht, worden verschillende stappen gezet om Internal Audit binnen het OM kwalitatief naar een hoger plan te tillen. In dit licht is het interessant om er enkele ontwikkelingen uit te lichten: de wijze waarop de Auditgroep wil bijdragen aan het continu leren en verbeteren in de organisatie, de samenhang die wordt beoogd tussen de verschillende auditdisciplines en de beoogde samenwerking met auditfuncties van (justitiële) ketenpartners.

Bijdragen aan continu leren en verbeteren

In de eerste plaats wordt van de Auditgroep verwacht dat zij de klassieke audittaken verricht in termen van 'het



Figuur 1. Organogram Openbaar Ministerie

verschaffen van aanvullende zekerheid over de interne beheersing'. Het auditprogramma bestaat daartoe uit een jaarlijks financial auditprogramma gericht op het financieel beheer en een self assessment AO/IC gericht op de beheersing van het primair proces. Derde onderdeel van het auditprogramma is het uitvoeren van operational audits, waarin vooral maatwerk centraal staat.
Naast de uitvoering van het reguliere auditprogramma wordt nadrukkelijk van de Auditgroep gevraagd dat een bijdrage wordt geleverd aan het continue proces van leren en verbeteren, onder andere in het kader van het 'Programma OM Strafvordering 2020'. Dit programma is gericht op het verbeteren van de hiervoor genoemde meest kritische werkprocessen van het OM. Het programma heeft als doel 'het kwalitatief goed en consistent uitvoeren van de (kritische) strafvorderlijke processen'.[2] Het programma start voor ieder proces met het vaststellen van het strafvorderlijk kader, waarin de wettelijke opdracht voor het OM voor het betreffende proces uiteen wordt gezet.

De Auditgroep vervult in het kader van het programma OM Strafvordering 2020 in feite twee rollen. Dit illustreren we aan de hand van de verbeteraanpak die vanuit het programma in gang is gezet rond de OM-strafbeschikking; een straf die het OM zelf kan opleggen (dus zonder tussenkomst van de rechter) voor veel voorkomende strafbare feiten.
Nadat het strafvorderlijk kader voor een proces is vastgesteld voert de Auditgroep samen met de projectleider van het betreffende proces een nulmeting uit, waarmee op ieder parket de kwaliteit van de uitvoering ten opzichte van het strafvorderlijk kader in kaart wordt gebracht. In de nulmeting rond de OM-strafbeschikking is door middel van een steekproef bijvoorbeeld nagegaan of in de geselecteerde dossiers sprake is van een reproduceerbare schuldvaststelling, of de identiteit van de verdachte correct is vastgesteld en of de uitgangspunten ten aanzien van het horen van verdachten worden nageleefd. In de nulmeting zijn verschillende verbeterpunten geïdentificeerd. Ten aanzien van de OM-strafbeschikking bleek bijvoorbeeld dat een meer uniforme registratie nodig is om de reproduceerbaarheid van de schuldvaststelling voldoende te borgen.[3]

De samenleving moet erop kunnen rekenen dat het OM de wet naleeft en kan uitleggen hoe het tot een oordeel is gekomen

In de uitvoering van de nulmeting is ook de 'officierenpool' betrokken. Deze bestaat uit ervaren officieren van justitie die deels zijn vrijgemaakt om bij te dragen aan het programma. Nadat de rapportage over de nulmeting was opgesteld, ondersteunde de officierenpool aansluitend de parketten bij het formuleren en implementeren van verbetermaatregelen. De officierenpool vormt in feite een waarborg dat de lessen die uit de nulmeting zijn getrokken en de benodigde verbeteringen hun beslag krijgen in de dagelijkse praktijk. De Auditgroep heeft geen actieve rol in de uitvoering van de verbeteraanpak, maar komt weer in beeld nadat de verbetermaatregelen geïmplementeerd zijn en het College van procureurs-generaal opdracht geeft om ter afsluiting van de verbeteraanpak een audit uit te voeren.
De audit op de OM-strafbeschikking zal naar verwachting in 2018 plaatsvinden. Momenteel voert de Auditgroep samen met de projectleider OM-strafbeschikking en de officierenpool een (tussentijdse) 1-meting uit, waarin per parket wordt nagegaan in welke mate verbeteringen zijn doorgevoerd in het proces rond de OM-strafbeschikking naar aanleiding van de uitkomsten van de nulmeting.

Samenhang auditdisciplines
De Auditgroep krijgt met regelmaat opmerkingen van de OM-onderdelen over de ervaren 'auditdruk'. Het gaat dan om de frequentie van uitgevoerde audits, de ervaren overlap tussen auditonderwerpen en de planning van de verschillende audits (soms kort na elkaar, soms parallel). Dit heeft onder andere te maken met de verschillen in dynamiek tussen de auditdisciplines. De financial audit kent een strakke jaarlijkse planning die is gekoppeld aan de accountantscontrole op de verantwoording van het financieel beheer aan het departement. De AO/IC is ten dele gekoppeld aan de externe verantwoordingsplicht en volgt daarom dezelfde planningssystematiek. De operational audits hebben een interne functie en zijn daardoor flexibeler in te plannen, al speelt daarbij vaak wel tijdsdruk vanuit de interne opdrachtgever.
Tegen deze achtergrond tracht de Auditgroep meer lijn te brengen in de keuze van auditobjecten, de keuze van onderwerpen en de tijdsplanning. Op die manier moet er meer samenhang komen in het integrale auditprogramma en moet de auditdruk voor de organisatie beter behapbaar worden. Dit brengt tevens met zich mee dat de auditdisciplines meer worden geïntegreerd, wat in eerste instantie vooral zal inhouden dat de auditbevindingen van financial audit, operational audit en AO/IC voor de oordeelsvorming, de selectie van onderwerpen en het bepalen van de focus van een onderzoek (geen dingen dubbel doen) meer onderling worden uitgewisseld en gebruikt. Daarnaast wordt beoogd binnen de Auditgroep meer kennis te delen over methoden en technieken en elkaar te informeren over de 'state of the art' van de eigen auditdiscipline.

Samenwerking met auditfuncties van (justitiële) ketenpartners
Het OM werkt in het primaire proces samen met een groot aantal ketenpartners, in operationele en bestuurlijke zin. De strafrechtketen bestaat naast het OM uit verschillende organisaties die ieder (vaak exclusieve) bevoegdheden hebben

en taken uitvoeren die gezamenlijk moeten bijdragen aan de rechtsorde en de veiligheid. De ketenpartners die het dichtst bij het OM staan zijn de politie en de rechtspraak. De politie staat in feite aan het begin van het operationele proces van het OM. De politie legt processen-verbaal voor aan het OM ter vervolging van opgespoorde verdachten. Voor het OM is van belang dat de kwaliteit van de processen verbaal die de politie aanlevert hoog is, zodat deze zaken goed kunnen worden afgedaan.
De afdoening van een groot deel van de zaken van het OM gebeurt via de rechter. De zaken die het OM bij de rechter ter zitting brengt moeten vervolgens zodanig van kwaliteit zijn dat er een adequate en efficiënte strafrechtsgang kan plaatsvinden. Het is niet moeilijk om te bedenken dat zowel in de dagelijkse gang van zaken 'op de werkvloer' als in de bestuurlijke samenwerking processen niet altijd optimaal verlopen. Met name op de 'koppelvlakken' tussen partners kan nog veel worden verbeterd en dat geldt ook voor de samenwerking met organisaties buiten de strafrechtketen. Onder andere om die reden is in 2016 een nieuwe samenwerking gestart tussen politie, OM en de rechtspraak. De bedoeling van dit traject is gezamenlijk te komen tot een herijking van de maatschappelijke ambitie van de strafrechtketen, door te bepalen waar de strafrechtketen nu staat en waar de partners (gezamenlijk) naartoe willen.
In het kielzog van deze ketenbrede ontwikkeling vindt tegelijkertijd een bezinning plaats op de samenwerking tussen deze partijen op het gebied van bedrijfsvoering en kwaliteit, control en auditing. Politie, OM en de rechtspraak hebben ieder eigen interne auditfuncties en accountants die zorgdragen voor de controle op externe verantwoording over het financieel beheer. Samenwerking tussen auditors van de verschillende organisaties in de strafrechtketen is in het verleden nog maar beperkt van de grond gekomen. Het OM en de rechtspraak hebben de afgelopen jaren al wel samengewerkt in de uitvoering van reviews op de zogenoemde Verkeerstoren.[4]
Tussen OM en politie is al eens samengewerkt op het gebied van auditing, bijvoorbeeld rond de Schiedammer Parkmoord en op dit moment werken de organisaties samen in het kader van het Kwaliteitsplan OM-Politie.[5] In 2017-2018 zal tussen OM en de beide andere partners in de strafrechtketen nader worden verkend hoe de samenwerking op het gebied van auditing verder vorm en inhoud kan krijgen.

Scherp houden

Het OM staat niet stil, bijna dagelijks dienen zich nieuwe maatschappelijke problemen aan waarbij van het OM passende antwoorden worden verwacht. Dat leidt tot een voortdurend veranderende organisatie. Steeds opnieuw moet de vraag worden beantwoord hoe het gezag van het OM, in samenwerking met (keten)partners, nu en in de toekomst beheerst en effectief kan worden ingezet om de veiligheid van de burger te garanderen. Daarbij moet de organisatie steeds zorgvuldig en binnen de wettelijke kaders acteren en bovendien efficiënt en effectief. In deze context stelt de Auditgroep zich tot doel de organisatie scherp te houden en te waken voor beheerst gezag. <<

Commissie Hoekstra

De commissie Hoekstra deed in 2015 onderzoek naar de zaak van Bart van U. en stelde vast dat de afname van DNA van veroordeelden niet naar behoren verliep, dat de uitvoering van gerechtelijke bevelen moet worden aangepast en politie, OM en de geestelijke gezondheidszorg beter moeten omgaan met signalen rond verwarde personen. Bart van U. bracht in januari 2015 zijn zus om het leven en bleek vervolgens ook betrokken bij de moord op oud-minister Borst in 2014. Van U. was in 2012 veroordeeld voor verboden wapenbezit.
Uit het rapport van de commissie Hoekstra bleek dat een bevel tot gevangenneming van Van U. uit 2012 niet was opgevolgd. Ook was na de veroordeling van Van U. in 2012 ten onrechte geen DNA afgenomen, waardoor zijn betrokkenheid bij de moord op oud-minister Borst pas laat, in 2015, aan het licht kwam.
Naar aanleiding van het rapport van de commissie Hoekstra presenteerde het OM in september 2015 het verbeterprogramma 'Maatschappelijke Veiligheid', dat een pakket aan maatregelen omvat, onder andere op het gebied van DNA en de executie van vrijheidsstraffen. In 2016 voerde de Auditgroep een audit uit naar de implementatie van dit verbeterprogramma.

Noten

1. In deze processen gaat het om adequate forensische opsporing (DNA), het correct uitvaardigen van strafbeschikkingen tegen overtredingen en misdrijven waarvoor maximaal zes jaar gevangenisstraf kan worden opgelegd (OM-Strafbeschikking), het op juiste wijze afwikkelen van strafrechtelijk en conservatoir beslag op geld en goederen (Beslag) en de daadwerkelijke tenuitvoerlegging van opgelegde straffen en maatregelen (executie).
2. Het Programma vindt zijn grondslag in het Wetboek van Strafvordering dat op dit moment wordt herzien.
3. Reproduceerbare schuldvaststelling betekent dat alle informatie waarop de uitvaardiging van de OM-strafbeschikking is gebaseerd schriftelijk moet zijn vastgelegd en digitaal raadpleegbaar moet zijn.
4. De verkeerstoren betreft een per arrondissement door OM en ZM gezamenlijk bemand en aangestuurd logistiek bureau gericht op de verbetering van de planning van rechtszittingen.
5. Binnen deze samenwerking worden in iedere regio zaaksbeoordelaars van het OM ingezet om samen met politiecollega's de kwaliteit van de processen-verbaal te verbeteren.

Lucas Kroes is coördinator operational audit en AO/IC audit bij het Openbaar Ministerie.

Nicole Kuijpers RO is operational auditor bij het Openbaar Ministerie.

Thema Veiligheid
Tekst Björn Walrave RO CIA
Drs. Laszlo Nagy EMIA RO
Beeld Adobe Stock

Veiligheid bij Geldservice Nederland

In gesprek met Victor de Wolff, financieel directeur bij Geldservice Nederland (GSN), en Esther Huijser, hoofd Risk, Security en Compliance bij GSN, over de veiligheid van waarden en mensen in een organisatie waar letterlijk veel geld in omgaat.

Over...

Victor de Wolff is financieel directeur bij GSN. Daarvoor was hij 22 jaar in diverse financiële functies werkzaam binnen de divisie Retail van ING Bank. Ook was hij CFO Facility Management van ING.

Esther Huijser werkt als hoofd Risk, Security en Compliance voor GSN. Daarvoor werkte zij als risk manager en compliance officer voor de voorganger van GSN, Altajo. Zij studeerde onder meer internal auditing (RO) aan de Universiteit van Amsterdam.

Wat doet GSN?

Victor de Wolff (VdW): "GSN is in 2011 opgericht door Rabobank, ABN AMRO Bank en ING Bank. Voor deze banken telt en distribueert GSN het papieren geld, de bankbiljetten. Daarnaast zorgt GSN voor het vullen en technisch onderhouden van de geldautomaten van deze banken."

Waarom is GSN opgericht?

VdW: "De filosofie achter de oprichting van GSN is simpel. Door het delen van de infrastructuur voor het chartale geld kunnen de banken veel kosten besparen. We zijn begonnen met de cash centers, waar de geldverwerking plaatsvindt. Je kunt je voorstellen dat de fysieke beveiliging van deze cash centers ontzettend belangrijk en daarmee kostbaar is. Door te optimaliseren hebben we het aantal cash centers de afgelopen jaren kunnen terugbrengen van vijf naar twee. Dat is nodig om in een markt met dalende volumes de kostprijs per handeling op peil te houden.
De banken besparen daarnaast kosten doordat we het vervoer van chartaal geld hebben geoptimaliseerd. Een voorbeeld. Voor GSN verscheen iedere dinsdagochtend op het Leidseplein in Amsterdam om 10.00 uur de waardetransporteur van de Rabobank om diens geldautomaat te vullen, een uurtje later verscheen dan de transporteur van ING Bank ten tonele en nog een paar uur later de transporteur van ABN AMRO Bank. Iedereen voelt wel aan dat dat erg inefficiënt is. Onze waardetransporteurs vullen nu de geldautomaten van meerdere banken. Bovendien doen ze dat op het juiste moment, zodat automaten met zo min mogelijk logistieke bewegingen toch altijd voeding hebben. Die momenten stellen we onder meer vast aan de hand van rekenkundige modellen. Inmiddels hebben we ook het onderhoud van de automaten van de banken overgenomen en op gelijke wijze geoptimaliseerd."

Wat doet GSN aan veiligheid?

Esther Huijser (EH): "De banken hebben met elkaar afgesproken dat ze elkaar niet beconcurreren op veiligheid. Dat klinkt makkelijk, maar je moet er hele goede afspraken met elkaar over maken. We hebben samen met onze partners,

waaronder De Nederlandsche Bank (DNB), het ministerie van Veiligheid en Justitie (V&J) en onze waardetransporteurs G4S en SecurCash, een minimale veiligheidsstandaard bepaald voor de cash centers. Daarnaast hebben we samen met de banken een securitynorm bepaald.
Je kunt je voorstellen dat dit een uitdagend proces is geweest. Immers, iedere stakeholder brengt zijn eigen wensenlijstje mee naar de onderhandelingstafel. Toch zijn we er met elkaar uitgekomen en dat hebben we gedaan door het gesprek te voeren over het 'wat' en niet over het 'hoe'. De stakeholders hebben gezamenlijk bepaald wat zij ten aanzien van veiligheid verwachten. Het was aan GSN om deze verwachtingen binnen budget te realiseren. En dat is gelukt!"
Zowel 'IT- en fysical security' als 'people' maken onderdeel uit van het risk/control-framework van GSN. De waarden, de bankbiljetten, moeten bij GSN veilig zijn en onze mensen moeten bij GSN veilig kunnen werken. Dit gaat hand in hand. We betrekken onze medewerkers actief bij het veiligheidsbeleid. Dat betekent dat zij 24 uur per dag, zeven dagen in de week opvallende zaken kunnen melden. We nemen bij medewerkers actief de gêne weg; je mág iets raar vinden. Gedraagt een collega zich anders dan normaal? Meld het ons! Ben je op het station aangesproken over je werk? Laat het ons weten! We leren onze medewerkers kijken en iets te doen met de dingen die ze zien.
Daarnaast oefenen we iedere maand onze veiligheidsprocedures, zodat onze mensen weten hoe ze moeten handelen in geval van een calamiteit. Breekt er in een cash center brand uit, dan kun je logischerwijs niet zomaar vluchten. Wij trainen onze mensen daarom intensief, zodat ze precies weten hoe ze zichzelf en hun collega's uit een dergelijke situatie kunnen redden. Beide speerpunten, 'security' en 'people', maken ook nadrukkelijk onderdeel uit van de ISAE 3402-verklaring die onze externe accountant en onze waardetransporteurs aan de accountants van de banken verstrekken."

VdW: "We verklaren al snel een incident tot een crisis, aangezien de consequenties van een incident bij ons groot kunnen zijn. We roepen sneller dan menig ander organisatie het crisismanagementteam bij elkaar. Dat doen we niet alleen om aan onze omgeving aan te tonen dat we incidenten serieus nemen, maar ook om met elkaar in de praktijk te oefenen. Erg grote incidenten hebben zich bij GSN gelukkig nog niet voorgedaan. Maar mochten die zich een keer voordoen, dan zijn wij goed voorbereid."

Wat is de rol van de afdeling Risk, Security en Compliance ten aanzien van veiligheid?

EH: "Wij lopen elk jaar de hele risico/control-cyclus af. Zo stellen we jaarlijks samen met de directie de risk appetite van onze organisatie opnieuw vast. Op basis hiervan werken we ons risk/control-framework en de scenarioanalyses bij. Zijn ze nog up-to-date, werken ze nog? Uiteraard hebben we hierbij oog voor nieuwe bedreigingen. Zo gaan de ontwikkelingen ten aanzien van cyber heel hard. De CFO-fraude,

ransomware, noem het maar op. We bepalen hoe we ons hier, uitgaande van onze risk appetite, tegen kunnen weren. Soms vraagt dat om zeer grote investeringen, zeker als je de omvang van onze organisatie in beschouwing neemt. Je ziet dat onze directie daar gezonde beslissingen in neemt, rekening houdend met onze rol in de keten. De nieuwe maatregelen implementeren we, waarbij we zoals gezegd veel aandacht hebben voor het trainen van onze medewerkers. Wat we niet doen is vinken. Je zult ons er niet op betrappen dat we standaardlijstjes nalopen en hierover rapporteren."

Kunt u een voorbeeld geven van bijzondere maatregelen die GSN treft?

EH: "Iets waar we veel ervaring mee hebben is het detecteren en vervolgens frustreren van voorbereidingshandelingen van criminelen. We monitoren hiertoe onze omgeving met camera's. Met behulp van intelligente software kunnen we bijvoorbeeld zien welke voor ons onbekende voertuigen meerdere malen een bezoekje aan ons hebben gebracht. We melden onze waarnemingen van dit afwijkend gedrag bij de Landelijke Eenheid van de politie. Zij volgen deze meldingen vervolgens op. Deze aanpak blijkt zeer succesvol!"

Voeren jullie ook audits uit?

EH: "We hebben geen internal auditfunctie en die gaat er voorlopig ook niet komen. Wel voert mijn afdeling af en toe operational audits uit. Aangezien onze werkzaamheden niet leiden tot extern gerichte verklaringen kan dat prima. Daarnaast laten we externen weleens dergelijke audits uitvoeren. De frisse blik van buitenaf helpt ons namelijk om te bepalen of we nog op de goede weg zijn, of we geen last hebben van tunnelvisie. In dat kader hebben we onlangs nog een uitgebreide IT-assessment laten uitvoeren."

Wie houdt toezicht op GSN?

EH: "Wat heel bijzonder is, is dat er op GSN ten aanzien van veiligheid nauwelijks toezicht bestaat. We zijn namelijk geen bank noch een beveiligingsbedrijf, waarvoor dit toezicht wel wettelijk is geregeld. Anders gezegd, we zijn de grootste geldverwerker van Nederland, maar qua toezicht vallen we overal buiten. Dat betekent dat we ook niet zomaar gebruik kunnen maken van bepaalde privileges, zoals screening van mensen door de politie. Voor dat soort zaken moeten we soms alternatieve oplossingen zoeken. Voor weer andere zaken maken we aparte afspraken. Dat doen we met zowel het ministerie van V&J als met de politie."

VdW: "Wij staan inderdaad niet onder toezicht. Echter, de banken zelf staan natuurlijk wel onder toezicht van DNB, vanwege de chartale distributieovereenkomst. DNB heeft hiervoor een normenkader ontwikkeld, dat door de banken zelf als referentiekader wordt gebruikt bij interne audits. Aangezien de banken een groot deel van de betreffende processen aan ons hebben uitbesteed, vinden die audits ook grotendeels hier plaats. Nu is het niet erg efficiënt als iedere bank haar eigen interne auditteam op ons afstuurt. Daarom hebben we met de banken afgesproken dat een externe partij ons periodiek aan het normenkader van DNB toetst."

Hoe ziet de toekomst van GSN eruit?

VdW: "Contant geld zal altijd blijven bestaan, al is het maar als back-up voor wanneer het elektronische betalingsverkeer volledig uitvalt. De verhouding tussen chartaal en giraal geld gaat wel behoorlijk veranderen. Inmiddels wordt er in Nederland aan de toonbanken al meer betaald met cards dan met cash en die trend zet zich zeker voort. Tegelijkertijd ervaart de consument chartaal geld als een soort openbare nutsvoorziening: het moet er zijn, maar het mag nauwelijks wat kosten. Om het chartale geldverkeer voor de banken betaalbaar te houden, moeten we blijven optimaliseren. De volgende stap in het optimalisatieproces is dat we de geldautomaten van de banken overnemen en een gezamenlijk netwerk van geldautomaten bouwen. In de nieuwe situatie maakt het niet meer uit welke geldautomaat de consument gebruikt. Zij kunnen iedere geldautomaat gebruiken als ware het een automaat van de eigen bank. Hierdoor kan GSN het aantal geldautomaten terugbrengen en tegelijkertijd de dekkingsgraad verhogen. De beschikbaarheid van chartaal geld zal voor de consument dus alleen maar toenemen."

We zijn de grootste geldverwerker van Nederland, maar qua toezicht vallen we overal buiten

EH: "Ook hierbij hebben we nadrukkelijk oog voor veiligheid. We hebben sinds een aantal jaren te maken met het fenomeen plofkraken. Bouwkundig gezien zijn veruit de meeste locaties in Nederland goed. De banken hebben hier altijd veel aandacht voor gehad. Daarnaast zorgen we voor gedegen cameratoezicht, zodat de opsporingsdiensten na een plofkraak zo snel en goed mogelijk hun werk kunnen doen. We plaatsen ook geen nieuwe geldautomaten meer onder of naast woningen om de risico's op letsel van omwonenden bij plofkraken zoveel mogelijk te beperken."

VdW: "Je ziet dat we ook hier weer veel aandacht hebben voor veiligheid. In alle bescheidenheid durf ik te stellen dat we op het gebied van risk en security erg volwassen zijn, ondanks de relatief kleine omvang van onze organisatie. We horen dat ook regelmatig terug van ons audit committee. Veiligheid zit in het DNA van onze organisatie. En daar zijn we best een beetje trots op!" <<

Tekst Dr. Walter Swinkels RO

Veilig thuiskomen!

Kijk je als internal auditor op overkoepelend niveau naar de veiligheid van medewerkers met de gedachte dat iedereen veilig thuis zou moeten komen? Veilig thuiskomen is een uitgangspunt waar niemand het mee oneens kan zijn. De vraag is echter hoe veiligheid, een veilige toestand of situatie kan worden geaudit.

Er zijn verschillende invalshoeken van veiligheid voor een organisatie. De meest bekende betreft de fysieke veiligheid bij gevaarlijke sectoren, zoals bij de gas- en oliesector, de chemische industrie, de bouwsector, et cetera. Ik werk zelf bij een constructiebedrijf waar ik het belang en de nadruk op veiligheid zeer nadrukkelijk terug zie komen. Dit komt tot uiting door expliciete aandacht vanuit de top, strakke procedures, specifieke veiligheidsmedewerkers en een veiligheidscultuur gericht op continue verbetering. In de UK heeft men de duidelijke ambitie vertaald in het credo 'beyond zero', wat zeer inspirerend is.

Een andere invalshoek rondom veiligheid betreft de omgeving waarin een medewerker werkt. Biedt deze omgeving een context waar medewerkers veilig kunnen werken? Dit betekent vertrouwen, openheid, constructieve discussie en een balans tussen de kernwaarden en de daadwerkelijke intrinsieke waarden van medewerkers. Dit betekent ook de veilige omgeving om in actie te kunnen komen bij zien, horen en voelen van zaken die niet passen bij de kernwaarden.

Deze uitspraak staat niet op zichzelf, maar op recente krantenberichten over fraude bij Nederlandse bedrijven. Het gebeurt niet alleen ver weg en in landen die niet goed scoren op de Transparency International list. Niet alleen een bedrijf is verliezer bij fraude, maar ook de fraudeur en diens hele gezin. Zo'n onveilige situatie zou moeten worden voorkomen. Mede omdat het ook kan leiden tot invallen door externe toezichthouders, met alle gevolgen van dien. Denk nog maar even terug aan Royal Imtech.

De hiervoor genoemde onveilige omgeving zou theoretisch voorkomen kunnen worden als die 'onveilige' situaties niet worden geaccepteerd en uit zichzelf zouden moeten worden uitgestoten zoals in de biologie. Dit begint bij sterke kernwaarden, in woord en gedrag. Vanuit de kernwaarden kan een relatie worden gelegd met de strategie, het leiderschap, de remuneratiestructuur en besluitvorming. Tevens is de mate van groepsdruk en 'clan cultuur' een interessant onderdeel van een analyse, want het kan zowel positief (sterke, veilige cultuur) als negatief werken (geen openheid, eigen subgroepsbelang voor algemeen belang, et cetera). De test naar de werkelijke cultuur komt tot uiting in de heldenverhalen. Welke verhalen worden verteld of niet verteld? Een andere maatstaf is het aantal 'speak-up'meldingen? Welke signalen worden hiermee afgegeven? Deze elementen kunnen gemeten worden en de internal auditor kan naar het samenstel van maatregelen en effecten zoeken en deze beoordelen.

Dit is nog het makkelijke deel! Want vervolgens moet je het bespreekbaar maken met het management. Dit vergt een valide en betrouwbare onderbouwing (geen borrelpraat) en overtuiging tijdens de discussie. Lees hiervoor nog even de zes geheimen van het overtuigen van Robert Cialdini.

Voel je je veilig onder de kerstboom? En in je eigen organisatie? Het is binnenkort kerstvakantie, misschien een mooie gelegenheid om hierover na te denken, als medewerker en vanuit de rol van internal auditor. En daarna na te denken over de benodigde actie!

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

Thema Veiligheid
Tekst Brenno de Winter
Beeld 123RF®

Komt de digitale **Titanic**-ramp eraan?

In mei 2018 horen organisaties klaar te zijn met de implementatie van de privacyrichtlijn GDPR (General Data Protection Regulation). Het pad erheen is een helse toer. De regelgeving legt pijnlijk bloot hoe onvolwassen we eigenlijk met data omgaan.

Het kan behoorlijk rommelen in de bestuurskamer. Althans, als men ook maar een beetje door heeft wat de GDPR of de Algemene Verordening Gegevensbescherming betekent. Veel regels rond het beschermen van persoonsgegevens stonden al in de bestaande wetgeving. Eén groot verschil: het woord 'boete' is nu gevallen. De GDPR is een compliancefeestje, omdat niet de autoriteiten moeten aantonen dat een organisatie de zaken op orde heeft. Nee, in de nieuwe situatie moet het bedrijf zelf bewijzen dat het aan de spelregels voldoet.

Nemen we digitale rampen wel serieus genoeg?
Juist aan dat serieus nemen lijkt het te ontbreken. Als een hack in 2011 het einde van DigiNotar inluidt, blijkt vooral het toezicht te hebben gefaald. Ook de ingehuurde auditor blijkt onvoldoende te hebben geacteerd. De Onderzoeksraad voor Veiligheid trekt na een onderzoek vernietigende conclusies. Velen trekken zich die conclusies aan en ze maken ook de Nederlandse auditors alerter. Maar DigiNotar is niet uniek. Andere hacks – waar ook ter wereld – krijgen niet de aandacht die ze verdienen. In tegendeel, de meeste onderzoeken naar beveiligingsincidenten gaan met schimmigheid gepaard. Zelfs al willen we ervan leren, dan nog gaat het op deze manier niet lukken.

Zwijgen helpt niet
Zes jaar na de hack op DigiNotar blijkt Deloitte gehackt. Het bedrijf staat bekend als prominente speler op het gebied van accountancy, audits en cybersecurity. Uit de mediaberichten wordt duidelijk dat het beheerdersaccount is gekraakt. Dat bleek nog relatief eenvoudig, aangezien 'two-factor authentication' ontbrak. Mogelijk zijn e-mails van klanten met zeer gevoelige informatie door de daders ingezien. Ook lijkt het er sterk op dat met deze hack meer gegevens te benaderen zijn geweest. De organisatie ontdekte het lek – dat ergens in 2016 ontstond – in maart 2017, maar heeft geen idee wie erachter zit: een land, een concurrent, een kind op een zolderkamer of een groep criminelen. Als het lek eind september 2017 naar buiten komt omdat *The Guardian* er lucht van krijgt, is het onderzoek nog bezig. Door het zwijgen is er geen mogelijkheid om lering te trekken en opnieuw worden we er professioneler niet beter van.
De hack op Deloitte is meer een gegeven dan een schok. Wat de zaak opmerkelijk maakt zijn indicaties van basale fouten die naar buiten sijpelen. De zaak roept de vraag op hoe een organisatie kan voldoen aan de toekomstige GDPR. Ook roept het de vraag op wanneer organisaties aansluiting bij de ISO-27001-normering gaan zoeken.[1] We moeten ons afvragen wat er toch aan de hand is in de ICT-industrie wanneer het gaat over informatiebeveiliging. De norm om 10% van alle IT-uitgaven aan beveiliging te besteden wordt in bitter weinig organisaties gehaald. De daden stroken bij veel organisaties niet bij de risicovolle realiteit en een kritische boodschap is iets waarop de boardroom niet zit te wachten.

Digitale rampen gebeuren vaker dan je denkt
Bij ieder incident komt de ernst van het nieuws in eerste instantie hard aan. Een greep uit recente voorbeelden, en het zijn er veel. Neem de honderdduizenden Internet of Things-apparaten die opeens een massale DDoS-aanval uitvoerden op één website; het platleggen van DigiD

waardoor zakendoen met de overheid lastiger werd; cyber attacks op banken waardoor het doen van betalingen met bijvoorbeeld iDeal lastiger werden, KLM dat door de aanvallen het betalen voor bagage moest uitstellen; de meer dan een miljard records die bij Yahoo werden gestolen (en wat lang werd stilgehouden); de zeer gevoelige persoonsgegevens die bij Equifax – over onder andere creditwaardigheid – werden buitgemaakt en wat uiteindelijk leidde tot het aftreden van de CEO; het uitbreken van het Wannacry-virus met gijzelsoftware dat veel organisaties, waaronder ziekenhuizen, industrie en transport, trof; de op Wannacry lijkende uitbraak van gijzelsoftware van Petya of Non-Petya, dat ervoor zorgde dat grote bedrijven maanden digitaal van slag waren. En ga zo maar door. Iedere keer zijn er de 'oeh's en ah's', de media-aandacht en de obligate kamervragen. Veel minder is er het doel om echt door te graven naar de oorzaken en het delen van leereffecten.

Waarom we niet leren van digitale rampen

Een datalek leidt zelden of nooit tot een voor de hand liggend spervuur aan vragen van onderzoekende aard: hoe heeft het daar zover kunnen komen? Had een (internal) auditor de gevaren wel gesignaleerd en, zo ja, waarom is er niet op geacteerd? Loopt mijn organisatie niet precies datzelfde risico? Hoe komt het dat keer op keer dezelfde problematiek zorgt voor dezelfde problemen en niemand iets leert van eerdere fouten? Vragen die kunnen helpen met het op een verantwoorde wijze omgaan met data om zodoende herhaling te voorkomen.
De ernst van de materie lijkt nog niet door te dringen, omdat – zo hoor ik vaak – je data niet kunt 'voelen'. En precies dat argument komt vaak voor bij mensen die te weinig onderzoeken. Neem een zelfrijdende Tesla die concludeert dat een lange vrachtwagen met oplegger uit twee auto's bestaat waar het voertuig nét nog tussen past. De bestuurder overlijdt. Data is niet iets onschuldigs. Bij incidenten is onderzoek geboden, hier kan een internal auditor meerwaarde creëren.

De historische context, de Titanic en de maatregelen

De problematiek is zichtbaar en wordt erkend, maar de risico's dringen nog niet echt door. Dit verschijnsel is niet nieuw. In mijn laatste boek, *Digitale stormvloed*, wijs ik op de stappen die de mensheid moest zetten om volwassen met veiligheid om te gaan. De basis is lang geleden in de zeevaart gelegd. Daar vielen door de loop der eeuwen veel doden, met als dieptepunt de 13e eeuw waar in Mongolië gedurende twee 'goddelijke' stormen meer dan honderdduizend mensen om het leven kwamen bij aanvallen op Japan. Maar ook later, als de stoomboot wordt ingevoerd, neemt het aantal incidenten fors toe. Dit komt onder andere door de hogere snelheid van deze schepen.
Nederland ziet vroeg in dat regelgeving onvermijdelijk is en sluit in 1815 een handelsverdrag met daarin ook afspraken over veiligheid (het Rijnverdrag). Het drukke verkeer en de rivier-engtes maken dat voor de veiligheid noodzakelijk.
In de 19e eeuw loopt een poging om tot wereldwijde regels te komen voor de veiligheid tijdens een zes maanden durende

Stappen in de goede richting als de GDPR – die dwingen over data na te denken – worden gezien als een moetje, gezeur of een hoofdpijndossier

conferentie mis. Vooral de Britten zijn tegen het verdrag. Zij stellen dat de Britse regels volstaan. Die stemming slaat om als in 1912 de SS Titanic na een aanvaring met een ijsberg uiteindelijk in tweeën breekt en zinkt. Vele levens gaan verloren ondanks dat de SS California vlak bij de plaats des onheils vaart. Het gebrek aan uniforme afspraken heeft als gevolg dat de noodsignalen niet goed worden opgepikt. Tijdige hulpverlening blijft uit. Omdat de Titanic zijn eerste tocht maakt en veel hoogwaardigheidsbeklederes aan boord zijn, slaat de ramp in als een bom. Er volgt een luide roep om maatregelen.
In 1914 treedt het SOLAS-verdrag (Safety of Life at Sea) dat een aantal basale zaken rond veiligheid regelt in werking, zoals opleiding, reddingsboten, reddingsvesten, communicatieapparatuur, marifoon, brandblusmiddelen en radarsystemen. Het zijn allemaal zaken die óf de kans op een incident kleiner maken óf juist de gevolgen beperken, mocht er toch een ongeluk optreden. Ook is het verdrag zo vormgegeven dat als inzichten veranderen, nieuwe dreigingen ontstaan of er redenen zijn het verdrag aan te scherpen, dit kan gebeuren zonder een ingewikkeld ratificatieproces. Zo is recentelijk beveiliging onderdeel van SOLAS geworden. De regels zijn toetsbaar en daarom kan een overheid van een verdragsland ingrijpen op alle schepen die niet voldoen. Een Nederlands schip kan zo bijvoorbeeld bij non-compliance in de VS aan de ketting worden gelegd.

Komen tot regelgeving
De manier van denken over risicomanagement bij SOLAS zou eigenlijk hetzelfde moeten zijn als bij informatiebeveiliging. Onderzoek na onderzoek laat zien dat veel digitale rampen dezelfde oorzaken hebben, zoals slecht patchmanagement, zwak wachtwoord- en autorisatiebeheer, slechte compartimentering, gebrekkige detectie van incidenten, niet veilig ontwikkelde software, gebrekkig bewustzijn bij medewerkers met ongelukkig gedrag tot gevolg, en ga zo maar door.
Al deze punten zijn eigenlijk – net als in de zeevaart – hygiëneregels. Voor de meeste zaken hebben we standaarden, waardoor toetsing door bijvoorbeeld een internal auditor prima mogelijk is. Grote incidenten als DigiNotar, KPN, Sony (een aantal malen), Hacking Team, Deloitte, Equifax, lijken allemaal zeer basale oorzaken te kennen. Net als bij het Rijnverdrag loopt ook nu Nederland ten opzichte van veel andere landen voor met eigen ontwikkelde standaarden of het verwerken van de standaarden in concrete toepassingen. Erg nuttig in een 'digitale' zee waar we verbonden zijn met systemen over de hele wereld en er mogelijk slecht beveiligde Internet of Things-apparaten met honderdduizenden tegelijkertijd op de markt komen. Internationaal zijn de geesten echter nog niet rijp voor uniforme regelgeving. Hoewel de ongelukken vaak omvangrijk zijn leiden ze niet tot een brede, fundamentele verandering. Sterker nog, stappen in de goede richting als de GDPR – die dwingen over data na te denken – worden gezien als een moetje, gezeur of slechts als een hoofdpijndossier. Geen klimaat om als internal auditor je lekker bij te voelen. Het ontbreekt daarvoor nog aan die ene Titanic, althans zo lijkt het. Als dat moment aanbreekt hebben wij in Nederland in ieder geval wel een mooie aanzet gegeven met een eigen set aan standaarden, denk aan Grip op Secure Software Development of Grip op Privacy – laat ik het SODADS (Safety of Data at the Digital Sea) noemen. Misschien is dat dan ook het moment dat de sprong wordt gemaakt naar een internationaal framework. Het is mijn overtuiging dat het tijdperk van de internal auditor als onderkenner van dit soort risico's en als adviseur over te treffen maatregelen, echt gaat aanbreken. Het duurt misschien nog even voordat dit ook erkend zal worden in bestuurskamers, hoewel een (digitale) Titanic dit proces zeker zal bespoedigen. <<

Noot
1. ISO 27001 is een ISO-standaard voor informatiebeveiliging.

Brenno de Winter, onder meer bekend van het kraken van de OV-chipkaart, heeft meerdere boeken op zijn naam staan. In zijn meest recente boek *Digitale stormvloed* breekt hij een lans voor een stringentere vorm van beveiliging door een parallel te trekken met de zeevaart.

Thema Veiligheid
Tekst Robbert Hamburg CISA CISSP
Maarten Wisman
Beeld DJI

Veiligheid binnen DJI: *een belangrijk goed*

Na de Schipholbrand in 2005 richtte de Dienst Justitiële Inrichtingen een planmatige controle in die de veiligheid van onder meer de gevangenissen binnen Nederland moet waarborgen. In dit artikel een beschrijving van de oorsprong, opzet en uitvoering van de zogenoemde safety, security & housing (SSH) Audits.

De Dienst Justitiële Inrichtingen (DJI) is verantwoordelijk voor de tenuitvoerlegging van vrijheidsstraffen en vrijheidsbenemende maatregelen die door de rechter zijn opgelegd. Insluiting vindt plaats in verschillende soorten inrichtingen. Er zijn gevangenissen en huizen van bewaring voor volwassenen, die penitentiaire inrichtingen (PI) worden genoemd. Er zijn ook speciale inrichtingen voor jongeren, de rijks justitiële jeugdinrichtingen (RJJI). Voor (tbs-)patiënten zijn er forensische psychiatrische centra (FPC) en voor vreemdelingen maakt DJI gebruik van detentiecentra (DC). Alle doelgroepen samen noemen we justitiabelen.
Momenteel kent DJI 38 locaties verspreid over het land:
- 24 penitentiaire inrichtingen;
- 3 justitiële jeugdinrichtingen;
- 2 forensische psychiatrische centra;
- 3 detentiecentra.

De locaties variëren van hypermoderne inrichtingen (zoals de recent geopende locatie Zaanstad) tot oude, soms historische locaties (zoals de locatie Veenhuizen). Daarnaast koopt DJI in voorkomende gevallen specialistische capaciteit in voor de forensische zorg.

Dagprogramma
Aan alle justitiabelen wordt een dagprogramma aangeboden, dit verschilt per regime. Het programma bestaat uit de zogenaamde 'rechten activiteiten' zoals luchten, maar ook uit andere onderdelen waaronder resocialisatie en het volgen van opleidingen. In dit dagprogramma is DJI verantwoordelijk voor het leveren van een veilige werkomgeving voor haar personeel en een veilige leef-, leer- en werkomgeving voor de verschillende justitiabelen. Veiligheid is hiermee binnen DJI een belangrijk goed. De interne auditafdeling van DJI voert binnen alle inrichtingen periodieke controles uit op het gebied van safety, security en housing (SSH).

De interne auditafdeling van DJI
DJI beschikt over een eigen interne auditafdeling.
Binnen deze afdeling werken tien auditors. De afdeling is

verantwoordelijk voor de derdelijns controles binnen de financiële verantwoording. De auditafdeling werkt hierbij nauw samen met de Audit Dienst Rijk (ADR) die als externe auditdienst de financiële verantwoording controleert en voorziet van een accountantsverklaring. Daarnaast voert de afdeling interne en procesmatige onderzoeken uit in opdracht van het hoger management (vraaggestuurd). Hierbij worden zowel kwalitatieve, als kwantitatieve onderzoeken uitgevoerd.
Ten slotte controleert de interne auditafdeling periodiek en planmatig de veiligheid binnen alle inrichtingen van DJI op de gebieden safety, security en housing op basis van een vast normenkader.

De oorsprong van de SSH Audit
De SSH Audit kent een beladen voorgeschiedenis, namelijk de Schipholbrand van 27 oktober 2005. Deze brand kostte elf gedetineerde uitgeprocedeerde asielzoekers het leven. De Onderzoeksraad Voor Veiligheid voerde destijds een onderzoek naar de brand uit. De conclusies waren hard. Gesteld werd dat DJI steken had laten vallen op het gebied van veiligheid. Er zou te weinig aandacht zijn geschonken aan de brandveiligheid, de bedrijfshulpverleningsorganisatie van DJI was onvoldoende voorbereid en getraind en de samenwerking met de brandweer was onvoldoende.
Naar aanleiding hiervan is binnen DJI de Kerngroep Veiligheid opgericht met als taak de veiligheid binnen de diverse inrichtingen periodiek en planmatig te onderzoeken. Inmiddels is de Kerngroep Veiligheid opgeheven en zijn de genoemde controlewerkzaamheden permanent ondergebracht binnen de interne auditafdeling.

De opzet van de SSH Audit
Een SSH Audit wordt standaard door twee medewerkers van de interne auditafdeling uitgevoerd en duurt drie dagen per inrichting. Elke inrichting wordt om de drie jaar bezocht en gecontroleerd op de gebieden safety, security en housing. Na gemiddeld een half jaar tot een jaar voert de interne auditafdeling een follow-uponderzoek uit en wordt gekeken of, en zo ja, hoe de bevindingen zijn opgepakt.
In bijzondere gevallen, bijvoorbeeld vanwege een calamiteit, kan deze periodiciteit worden aangepast. In de meeste van deze gevallen zal er echter voor worden gekozen om de oorzaak van een specifieke calamiteit te onderzoeken. Indien nodig kan dit vervolgens leiden tot een vraaggestuurd onderzoek waarbij de auditors onderzoeken of betreffende calamiteit een organisatiebreed risico betreft en derhalve dient te leiden tot DJI-brede aanpassingen in beleid, uitvoering of monitoring.

De drie onderdelen
Binnen het onderdeel safety wordt gekeken naar de bedrijfshulpverlening, de brandveiligheid en de arbeidsveiligheid. Het onderdeel security betreft vooral de 'harde' beveiligingskanten van de inrichting. Te denken valt aan de werking en opstelling van detectiepoorten en bagagedoorlichtingsapparatuur om contrabande (zoals wapens en telefoons) buiten de inrichting te houden, de mate van inzet van drugshonden (ter voorkoming van invoer van drugs en voor het controleren op aanwezigheid van drugs), en de uitvoering van diverse controles en inspecties zoals luchtmomenten, toegangscontroles en de celinspecties (waarbij gecontroleerd wordt op eventuele binnen gevoerde contrabande).
Binnen het onderdeel housing wordt gekeken of de inrichting in control is met betrekking tot de staat van het pand en de uitvoering van periodieke inspecties op de aanwezige technische installaties zoals communicatiemiddelen, noodstroomvoorzieningen en camerasystemen. Ook wordt hierbij gecontroleerd of de inrichting in control is op het gebied van legionellabeheer.

De uitvoering van de SSH Audit
Om een oordeel te geven over de mate waarin de inrichting in control is, maken de auditors binnen de uitvoering van de audit gebruik van een drietal bronnen: documentenstudie, interviews en eigen waarneming door middel van een schouw van de gehele inrichting.

Documentenstudie
Binnen de documentenstudie wordt vooraf een vaste set aan documenten opgevraagd. Gedurende de audit bekijken de auditors de opzet van de verschillende controles en werkprocessen. Dit doen zij door het lezen en beoordelen van de opgevraagde dienstinstructies en het beoordelen van de vindbaarheid hiervan voor het uitvoerend personeel. Tevens beoordelen de auditors oefenverslagen met onder meer externe partijen zoals de brandweer en/of de politie en stellen zij vast of de door DJI voorgeschreven planvorming aanwezig is.
Daarnaast wordt binnen de documentenstudie vastgesteld of wettelijk verplichte documenten kunnen worden aangeleverd. Denk hierbij aan zaken als een omgevingsvergunning, een certificaat van de brandmeldcentrale, een dossier dat voldoet aan de Kernenergiewet, maar ook aan de vraag of de vergunningplichtige apparatuur ook daadwerkelijk van een geldige vergunning is voorzien.

Elke inrichting wordt om de drie jaar volledig doorgelicht en gecontroleerd op de gebieden safety, security en housing

Alle rapporten worden aangeboden aan de Inspectie Justitie en Veiligheid

Interviews
Er worden met betrekking tot de onderzoeksgebieden safety, security en housing interviews gehouden met de binnen de inrichting werkzame materiedeskundigen. Voor de interviews wordt een vaste set vragen gehanteerd. Er wordt vooral vastgesteld of de controles en werkprocessen bekend zijn bij de materiedeskundigen alsmede hoe zij borgen dat de inrichting, op hun verantwoordelijkheidsgebied, voldoet aan de wettelijke verplichtingen met betrekking tot bijvoorbeeld de nodige vergunningen.

Schouw
Op de laatste dag van de audit lopen de auditors een uitgebreide ronde door de hele inrichting om zelfstandig vast te stellen hoe de diverse controlewerkzaamheden worden uitgevoerd en of dit plaatsvindt conform de dienstinstructies. De auditors bevragen het uitvoerend personeel naar hun bekendheid met de uitvoering van de controles, de werkprocessen en de vindbaarheid van hun eigen dienstinstructies. Daarnaast bezoeken de auditors enkele willekeurige

cellen waarbij de justitiabelen eveneens worden bevraagd naar bijvoorbeeld de periodiciteit van de uitvoering van cel inspecties.
Voor de oordeelvorming wordt per onderwerp gebruikgemaakt van de uitkomsten van de drie gehanteerde bronnen. Hierbij wordt door middel van bron- en methodetriangulatie een oordeel gevormd over het onderzochte onderdeel.

Rapportage en follow-up
Geconstateerde bevindingen worden gerapporteerd aan zowel de inrichtingsdirecteur als de divisiedirecteur op het hoofdkantoor. Na een half jaar voeren de auditors nog een follow-uponderzoek uit waarbij gericht wordt gecontroleerd of er naar aanleiding van de door de auditors gerapporteerde bevindingen voldoende maatregelen zijn getroffen. Ook de uitkomsten van deze follow-up worden aan de inrichtingsdirecteur en de divisiedirecteur gerapporteerd. De bevindingen die na deze follow-up nog openstaan, worden door de afdeling Business Control opgenomen in de planning & controlgesprekken tussen de divisiedirecteur en de inrichtingsdirecteur.
Ten slotte worden alle rapporten ook aangeboden aan de Inspectie Veiligheid en Justitie. De inspectie bepaalt (mede) op basis van deze rapporten of zij nog aanvullende onderzoeken wil uitvoeren of dat zij steunt op de rapporten van de interne auditafdeling van DJI.

Doorontwikkeling in de toekomst
Momenteel wordt het normenkader, mede omdat interne regelgeving onderhevig is geweest aan mutaties, aangepast. Hierbij wil de interne auditafdeling ook de meerwaarde voor zowel de opdrachtgevers, de verschillende divisiedirecteuren als de veldorganisaties, verder vergroten. Daarnaast ontwikkelt de technologie zich razendsnel waardoor er voor te onderscheppen contrabande andere controlemiddelen worden ingezet (denk bijvoorbeeld aan GSM-speurhonden). De aanpassing van het normenkader wordt uitgevoerd in samenwerking met de materiedeskundigen die werkzaam zijn binnen de verschillende inrichtingen. Zo vergroot de interne auditafdeling zowel de kwaliteit van als het draagvlak voor het nieuwe toetsingskader, en verwacht zij de veiligheid van de verschillende inrichtingen in de toekomst goed te kunnen blijven beoordelen. <<

Robbert Hamburg is senior auditor bij DJI en houdt zich naast de SSH bezig met operational en IT-audits.
r.hamburg@dji.minjus.nl

Maarten Wisman is auditor bij DJI en houdt zich naast de SSH bezig met operational en financial audits.
Maarten.wisman@dji.minjus.nl

Artikel Vaktechniek
Tekst Mr. Robert Vos
Beeld 123RF®

Zuurstof in het management control systeem

Bij de Rijksoverheid klinkt vanuit het topmanagement een steeds luidere roep om meer beleidsruimte voor het decentraal management. Aan de andere kant komen er meer regels die deze ruimte juist beperken. Hoe kan deze paradox in de praktijk hanteerbaar worden gemaakt?

Van zero tolerance naar meer ruimte voor passende oplossingen. Deze ruimte wordt de zuurstof in het systeem genoemd

Het voornemen om meer verantwoordelijkheid te leggen bij het management dateert al uit 2005. In 2015 is opnieuw de wens van een doelmatig en risico- en resultaatgericht controlebestel uitgesproken. Van 'zero tolerance' naar meer ruimte voor passende oplossingen. Deze ruimte wordt de 'zuurstof in het systeem' genoemd. Deze zuurstof moet in het systeem ingebouwd worden, naast de aandacht die er is voor rechtmatigheidsbeheersing, verantwoording en audit op niet-naleving.

Vormgeving regels

Hoe je het wendt of keert, het begint bij de vormgeving van de regels. Met regels is op zich niets mis. Regels bieden houvast en duidelijkheid. Het geeft bijvoorbeeld een gerust gevoel dat er een (verkeers)regel is die iedereen verplicht rechts te rijden. Regelgeving is een middel om een probleem op te lossen of een bepaald doel te bereiken. Maar regels hebben ook een keerzijde:

- regels zijn noodzakelijkerwijs algemeen geformuleerd;
- niet alles is in regels te vangen. Er zijn immers altijd meer situaties dan regels;
- regels kunnen elkaar tegenspreken en de inhoud of de bedoeling van regels is niet altijd helder;
- regels lopen in een dynamische wereld vaak achter op de ontwikkelingen.

Kortom, terughoudendheid met regelgeving is geboden. Regel alleen de essentiële kaders en bepalingen: zaken waarop je zeker moet kunnen rekenen en/of waarvoor uniformiteit geboden is. Dit zijn de *rode* (stringente) regels. In de managementcontrolliteratuur wordt dit type regels ook 'tight controls' genoemd. Hier zal de (centrale) leiding strikt de hand aan moeten houden. Naast deze rode regels dient gebruikgemaakt te worden van regels met een zekere beleidsruimte. Hier zijn afwegingen mogelijk: er is niet eenduidig sprake van 'goed of fout'. Dit zijn de *blauwe* regels. Voor deze categorie geldt: 'comply or explain'. Daarnaast zijn er nog de *groene* regels waaruit geen verplichting voortvloeit. Dit zijn 'informatieve handreikingen' die worden gebruikt voor 'beïnvloeding'. Deze handreikingen moeten echter niet tot regels (normenkader) uitgroeien.

Inbouwen in het management control systeem

Het management control systeem (MSC) moet zorgen voor de verbinding tussen de doelstellingen van de organisatie enerzijds en het gedrag in de praktijk anderzijds en is als zodanig veel breder dan alleen de maatregelen gericht op naleving van regels.[1]

Een deel van de (centrale) regelgeving is voor de organisatie een gegeven dat zo goed mogelijk in de organisatie ingebed moet worden. Deze inbedding dient zoveel mogelijk met behulp van IT-systemen te geschieden: inbouwen onder de 'motorkap', met signalen op het dashboard als zaken niet goed lopen. Daarnaast is de doelcongruentie essentieel: alle medewerkers dienen achter de organisatiedoelstellingen te staan. Het gaat erom dat zij in hun feitelijk gedrag daaraan invulling geven. Hierbij komen allerlei keuzen aan de orde die vaak een professionele afweging vergen. Dit afwegingsproces zal binnen de organisatie in het MCS verankerd moeten zijn, evenals de naleving van regelgeving.

Bij dit 'inbouwen onder de motorkap' (in de IT-systemen) kan gebruikgemaakt worden van (een combinatie van) de hiervoor genoemde indeling in rood, blauw en groen.

- Rood: verboden – In het systeem kun je gewoon niet verder. In geval van de mogelijkheid van ontheffing door degene die daartoe bevoegd is, kun je alleen verder als daarvoor machtiging is ontvangen. Deze ontheffing wordt gelogd en daarover zal verantwoording afgelegd worden door degene die deze machtiging heeft gegeven.
- Blauw: geef toelichting – In het systeem wordt een afwijking ('not comply') gelogd en in een overzicht opgenomen. Degene die deze afwijking heeft ingevoerd, moet deze ook toelichten.
- Groen: slim gebruiken – Het systeem logt de handeling wel, net als de rode en de blauwe handelingen, maar alleen voor datamining, processmining en continuous monitoring.

Een voorbeeld: het nieuwe reisaanvraagsysteem bij de Rijksoverheid. Het IT-systeem kent bandbreedtes waarbinnen medewerkers vrijelijk keuzen kunnen maken (binnen alle 'groene' vluchten die het systeem oppert, mag je zelf kiezen welke je neemt). En er is een 'comply or explain'-deel: wil je een vlucht die duurder is, dan ben je verplicht dit te motiveren in het systeem. De manager moet dit goedkeuren voordat het systeem deze boeking toestaat.

Met behulp van de informatie uit het MCS kan de manager verantwoording afleggen:

- Gaan de zaken goed?
- Is de basis op orde?
- Worden de doelstellingen gerealiseerd?
- Welke risico's worden daarbij gelopen en passen deze (rest) risico's bij de risicobereidheid van de organisatie?

Het gaat om verantwoording op hoofdlijnen, inclusief een overall beeld waar van de regels is afgeweken en waarom. De manager geeft aan op welke punten de organisatie wel en op welke punten minder in control is. Verbetermaatregelen kunnen het beeld complementeren.

De rol van de interne auditor

Voor de leiding van een organisatie is het belangrijk inzicht te hebben in hoeverre het kan steunen op het functioneren van het interne MCS, inclusief een goed gebruik van de beleidsruimte door de medewerkers. De internal auditor kan hierin voorzien door het uitvoeren van een audit waarbij gebruikgemaakt wordt van de negen kritische succesfactoren voor gerechtvaardigd vertrouwen.[2] Hierna volgt een uitwerking van deze negen kritische succesfactoren, toegespitst op het kunnen vertrouwen van de leiding van een organisatie op het interne MCS (realiseren bedrijfsvoeringsdoelstellingen).

1. *Duidelijke afspraken over de beheersing van de bedrijfsvoeringsdoelstellingen (verwachtingen omtrent het MCS)*

Zijn de (beheers)ambities ten aanzien van het realiseren van de (bedrijfsvoerings)doelstellingen en het naleven van de regels geconcretiseerd? Is er een duidelijke hiërarchie of prioritering van regels? Welke ruimte wordt in het MSC op dit punt gegeven en aan wie? Is daar intern, ook richting medewerkers ten aanzien van hun beleidsvrijheid, duidelijkheid over? Hoe doelmatig is een regel wanneer het naleven van een regel meer geld/tijd kost zonder een bijdrage te leveren aan het beoogde doel.

2. *Afspraken/verwachtingen kunnen waarmaken*

De organisatie heeft kennis en kunde om de verwachtingen omtrent de beheersing van de bedrijfsvoeringdoelstellingen en het MCS, ook waar te maken. Dit betreft niet alleen het vorm en inhoud geven aan de interne bedrijfsvoeringsbeleid zelf, maar ook kennis en kunde op het punt van het naleven van de regels en het maken van de juiste afwegingen/keuzen binnen de bedrijfsvoering in een complexe (bestuurlijke) omgeving. Tenslotte is de kennis en kunde met betrekking tot het intern verbinden van beide oriëntaties, te weten regelnaleving versus beleidsafwegingen, belangrijk.

3. *Voldoende gedeeld belang*

Wat betreft de verwachtingen dienen er tussen de leiding en de medewerkers voldoende gedeelde belangen te bestaan om ervan verzekerd te zijn dat er 'samen opgelopen' wordt.

Er bestaat geen absolute zekerheid. Het is belangrijk te investeren in gerechtvaardigd vertrouwen

Binnen de organisatie kunnen er uiteenlopende belangen of verschillen in oriëntatie zijn, kostenafwegingen kunnen bijvoorbeeld voor de leiding voorop staan, voor de medewerkers kan dat een optimale (duurdere) uitvoering van de werkzaamheden zijn. Maar ook: de leiding wil eenduidigheid, medewerkers beleidsruimte. Of andersom: de leiding wil graag ruimte geven, medewerkers willen juist duidelijkheid. In hoeverre slaagt de organisatie erin de verschillen in belangen/oriëntatie intern zoveel mogelijk op een lijn te brengen en te vertalen in het MCS.

4. *Goed gevoel*
Het MCS moet de leiding een goed gevoel geven. Steunen op het MCS betekent durven te vertrouwen op het functioneren van het MCS van de organisatie, ofwel, durven loslaten en de medewerkers waar mogelijk ruimte durven te geven. De leiding moet dit in woord en daad vormgeven en bepaalt hiermee de tone at the top. Dit is een zeer belangrijke en vaak beslissende factor die niet altijd benoemd wordt omdat die als ongrijpbaar gezien wordt.

5. *Doorlopend goede informatie-uitwisseling*
Naast de reguliere interne informatie-uitwisseling zijn tijdige signalen over afwijkende ontwikkelingen/incidenten misschien nog wel belangrijker. Het gaat erom dat deze informatie – al dan niet informeel uitgewisseld – ervoor zorgt dat de leiding, maar ook de medewerkers niet voor verrassingen worden gesteld. Dit betekent intern een open communicatie op ieder moment over de invulling van de (beleids)ruimte, en het bespreken van eventuele spanning tussen doelstellingen en regels. Dit geldt ook voor 'bijna-ongelukken', et cetera.

6. *Zicht op risico's en acceptatie van risico's*
Welk zicht heeft de leiding op het risico dat hun verwachtingen ten aanzien van de interne beheersing door het MCS niet altijd zullen worden waargemaakt en in welke mate zijn zij bereid dit risico te accepteren? Geen enkel MCS zal alle risico's in zijn geheel kunnen mitigeren. Ook in een strikte rule-basedomgeving met veel controle, zullen risico's kunnen optreden: schijnzekerheid, geen verantwoordelijkheid nemen, verminderde alertheid als alles belangrijk is, et cetera. Welke risico's komen naar voren uit de risicoanalyse van de organisatie zelf en het risico management systeem dat onderdeel uitmaakt van het management control systeem? Hoe wordt daarbij door de organisatie omgegaan met deze risico's?

7. *Controle/kritische vragen mogen stellen*
Vertrouwen op het MCS door de leiding moet geen blind vertrouwen zijn. Interne controle en reality checks door de controller en regelmatige doorlichting van het MCS door de auditor moeten vanzelfsprekend zijn. Dit kan ook een vraag om nadere toelichting zijn als er op basis van andere informatie concrete vraagpunten zijn (tegenstrijdige signalen, et cetera). Deze monitoring/controls dienen ervoor om te zorgen dat het vertrouwen van de leiding in het MCS en daarmee ook in het gedrag van de medewerkers voldoende grondslag heeft.

8. *Bespreken van incidenten en daarvan leren*
Er kan en zal in ieder MCS af en toe iets misgaan. Dit is een van de risico's die binnen een bepaalde marge geaccepteerd moet worden. Tegelijkertijd ziet iedereen graag dat het zo min mogelijk voorkomt, vooral bij essentiële regels. Dan gaat het erom dit in openheid intern te bespreken, te analyseren opdat, als onderdeel van het MCS, geleerd kan worden.

9. *Consequenties bij te veel of bewuste inbreuken*
Als er te veel inbreuken zijn (zonder verbetering) of als binnen de organisatie ernstige inbreuken niet worden gemeld, dan is er een grens. Dan is steunen op het MCS door de leiding in die situatie niet (meer) mogelijk. Dan zal de leiding intern aan die veelvuldige en/of ernstige inbreuken consequenties dienen te verbinden (bijvoorbeeld extra intern toezicht, personele consequenties). Eerst zal de basis op orde gebracht dienen te worden, pas daarna zal vertrouwen op het MCS (inclusief beleidsruimte) weer aan de orde kunnen zijn.

Afsluiting
Er bestaat geen absolute zekerheid. Belangrijk is te investeren in gerechtvaardigd vertrouwen met een daarbij behorend loslaten (= risicoacceptatie) binnen bepaalde grenzen. Gerechtvaardigd vertrouwen is sterk afhankelijk van de mate van volwassenheid en professionaliteit van de organisatie. Dat zou voorop moeten staan: het in control zijn van de organisatie met behulp van het management control systeem. Met een gerichte audit hiernaar zoals op hoofdlijnen beschreven in dit artikel, kan de interne auditor hieraan een bijdrage leveren. <<

Noten
1. Definitie: alle formele en informele interne processen, afspraken, procedures en gedragsbeïnvloedende maatregelen (dus hard en soft controls), die een organisatie gebruikt om haar doelen te realiseren.
2. *Vertrouwen geven en in control zijn; gaat dat samen?*, ministerie van Financiën, 2009.

Robert Vos is hoofd Projectbureau audit- en beheersingsvraagstukken bij de directie Begrotingszaken van het ministerie van Financiën. Dit artikel is gebaseerd op de *'Achtergrondverkenning inzake systeemtoezicht, vertrouwen en ruimte voor professionele afwegingen'* en geschreven op persoonlijke titel. r.o.vos@minfin.nl.

Rubriek PAS op de plaats
Tekst Ir. Gezina Atzema RO
Beeld Ipse de Bruggen

Grace Ramkisoen:

"Zelfstandigheid en een flinke dosis creativiteit maken het werk boeiend"

PAS op de plaats is een rubriek waarin auditors van kleine auditdiensten aan het woord komen. Dit keer Grace Ramkisoen, manager Internal Audit bij Ipse de Bruggen.

Algemene informatie	
Aantal fte organisatie	3810
Aantal fte IAD	1
Rapporteert aan	raad van bestuur en auditcommissie/-raad van toezicht

Kunt u iets vertellen over de Internal Auditfunctie (IAF) van Ipse de Bruggen?
"Ipse de Bruggen is een zorginstelling voor mensen met een verstandelijke beperking met vijfduizend medewerkers en tweeduizend vrijwilligers. In de gehandicaptenzorg is het nog niet gebruikelijk om een internal auditfunctie te hebben. De functie is mede op advies van de externe accountant in het leven geroepen.
De IAF binnen Ipse de Bruggen bestaat nu ruim anderhalf jaar. Ik ben in februari 2016 in dienst getreden en heb de IAF van 'scratch' af aan opgezet. Het betreft momenteel nog een solistische functie. Inmiddels wordt wel met de raad van bestuur gesproken over uitbreiding van het aantal fte en het ambitieniveau van de IAF.
Het opzetten van de functie is in het eerste jaar zeer voorspoedig verlopen. Het voordeel van het van scratch af aan opzetten van de IAF is dat je het meteen goed kunt neerzetten. Soms kan het in het begin lastig zijn om bij de auditcommissie aan tafel te komen, maar dit is bij Ipse de Bruggen geen punt van discussie geweest. Vanaf de eerste auditcommissievergadering is besloten dat ik hier standaard aan deelneem."

Welke type onderzoeken voert de IAF uit?
"De IAF voert operational, IT- en financial audits uit. Het zijn geïntegreerde thema-audits waarbij alle aspecten meegenomen worden. Zowel de hard als de soft controls worden onderzocht. In een organisatie die aangeeft van regels naar waarden te gaan, wordt het auditen van soft controls steeds belangrijker. Voorbeelden van enkele uitgevoerde audits zijn audits op Registratie en Declaratie, Borging Kwaliteit Zorg- en Behandelplannen, Zorgverkoop en Informatiebeveiliging. Fraudeonderzoeken zijn niet bij de IAF belegd. Deze worden vooralsnog uitgevoerd door de afdeling Kwaliteit."

Voeren jullie tweedelijnstaken uit?
"De IAF is binnen de organisatie neergezet als een derdelijnsfunctie. Er worden geen tweedelijnstaken uitgevoerd. Wel wordt zorgvuldig afgewogen wat de taken zijn die je wel als derdelijnsfunctie zou mogen uitvoeren. Zo heb ik dit jaar een workshop risicobewustzijn aan managers en controllers gegeven. Je merkt wel dat er soms behoefte is

Creativiteit is de geur van de individuele vrijheid

aan de expertise die je als IAF hebt, zoals op het gebied van risicomanagement of AO/IC. Daarom wordt vaak ook ad hoc om advies gevraagd. Je vervult daarmee als IAF ook de rol van trusted advisor."

Met welke uitdagingen krijgt een kleine IAF te maken?
"Het voldoen aan de IIA Standaarden is een uitdaging voor een kleine IAF, vooral als de IAF uit één persoon bestaat en binnen de organisatie geen enkele andere soortgelijke functie aanwezig is. Het inregelen van een quality assurance and improvement programme is dan lastig. Je moet creatieve oplossingen bedenken en deze soms buiten de muren van de organisatie vinden. Ondanks de beperkte capaciteit die ik als kleine IAF heb, probeer ik wel constant te innoveren.

Zo ben ik bezig om data-analyse meer binnen de organisatie te stimuleren en zorg ik ervoor dat dit ook binnen de audits steeds meer wordt toegepast. Hier zijn al mooie resultaten mee behaald."

Wat haalt u uit de PAS-commissie?
"De PAS-commissie is voor mij nuttig om kennis en ervaringen met deelgenoten te kunnen uitwisselen. Je hebt allen te maken met soortgelijke issues en uitdagingen.
Het is prettig om met vak- en lotgenoten te kunnen sparren over zaken."

Maakt u gebruik van co-sourcing?
"Afhankelijk van het onderwerp en de benodigde capaciteit maak ik gebruik van co-sourcing. Ik huur kennis of capaciteit in. Zo heb ik laatst voor een audit enkele auditors ingehuurd van een Big Four-accountantskantoor. Ik wil voor de audits meer gebruikmaken van process- en datamining en zoek ook hiervoor de samenwerking met externe partijen op."

Hoe zorgt u ervoor dat u op de hoogte blijft?
"Ik kijk regelmatig op de websites van het IIA en NOREA en lees veel artikelen in vakbladen of online. Daarnaast heb ik eens per kwartaal een overleg met managers Internal Audit van andere zorginstellingen. Wij wisselen kennis en ervaring uit en nodigen soms een gastspreker uit. Door het deelnemen aan diverse congressen en symposia blijf ik ook op de hoogte van de meest actuele informatie."

Op welke manier vindt kwaliteitsborging plaats?
"Voor de kwaliteitsborging ben ik een samenwerking aangegaan met een internal auditor van een andere zorginstelling. Wij hebben via onze raden van bestuur geregeld dat wij bij elkaar de dossiers kunnen reviewen. Dit is wat ik graag andere kleine auditafdelingen wil meegeven: kijk voor oplossingen ook buiten de muren van jouw eigen organisatie. Wees creatief."

Wat maakt het werken in een kleine IAF leuk?
"Bij een kleine IAF die nog in de opstartfase zit, is het pionieren datgene wat het werk leuk maakt. Het houden van roadshows, het aftasten wat past bij de organisatie en nog je sporen moeten verdienen binnen de organisatie is uitdagend. Daarnaast maken de grote mate van zelfstandigheid en de flinke dosis creativiteit het werk boeiend."

Wat is de ambitie van de IAF op de langere termijn?
"Een bijdrage leveren aan het op een hoger niveau brengen van de interne beheersing binnen de organisatie. Een zorginstelling met 390 locaties die een transitie doormaakt naar zelforganisatie is qua interne beheersing een enorme uitdaging. De komende jaren is een IAF van een iets grotere omvang nodig. Uiteindelijk wil ik groeien naar een situatie waarbij één auditor voldoende is vanwege de hoge kwaliteit van interne beheersing, risicomanagement en governance."

Over...

Drs. Grace Ramkisoen RE RO CIA CISA is manager Internal Audit bij Ipse de Bruggen en medeoprichter van Success by Culture.

Artikel Energiemarkt
Tekst Mr.drs. Jantien Heimel RA CFE CIA CISA
Beeld Vattenfall, Hansa Blomberg

De 'perfect storm' in de energiemarkt

De afgelopen jaren waren stormachtig voor de grote Europese energiemaatschappijen. Een combinatie van ontwikkelingen zorgde in de energiemarkt voor hoge afwaardering van activa en het onder druk komen te staan van businessmodellen. In dit artikel een aantal ontwikkelingen en effecten hiervan voor Vattenfall en de interne auditfunctie.[1]

De stormachtige ontwikkelingen in de Europese energiesector, door CEO Peter Smink van Vattenfall's 100% dochtermaatschappij, nv Nuon Energy (Nuon), gekscherend de 'perfect storm' genoemd, hebben de laatste decennia de energiemarkt flink veranderd. Langs de lijn van de volgende zes ontwikkelingen worden de effecten voor Vattenfall en de interne auditfunctie (Vattenfall Group Internal Audit) besproken:
1 – Overgang fossiele naar hernieuwbare energie;
2 – Groei in windenergie;
3 – Inpassing energietechnieken en draagvlak van de samenleving;
4 – Flexibele productie, uitrol slimme meters, meer data en privacyaspecten;
5 – Lean operaties en digitalisering;
6 – Outsourcing.

1 – Overgang fossiele naar hernieuwbare energie
De overgang van fossiele brandstoffen naar hernieuwbare energiebronnen is al jaren gaande. Dit wordt onder andere gedreven door de groeiende eisen van klanten en de samenleving ten aanzien van duurzaamheid en het tegengaan van klimaatverandering. De energievoorziening in Nederland wordt duurzamer, mede onder invloed van het Energieakkoord. De eerste oudere kolencentrales zijn gesloten en de productie uit wind en zon neemt toe. Duidelijk is geworden dat veel nodig is om de klimaatverandering tegen te gaan. Een stap hierin is het klimaatakkoord van Parijs, waarmee mondiaal de ambitie is vastgelegd de wereldwijde opwarming tot het jaar 2050 te beperken tot 2° Celsius en te streven naar niet meer dan 1,5° opwarming. Voor Nederland is daarnaast de uitspraak in de Urgenda-rechtszaak relevant. De CO_2-uitstoot moet volgens die uitspraak in 2020 met 25% zijn gedaald ten opzichte van het niveau in 1990. Dit soort ontwikkelingen ten aanzien van emissiereductie zijn van invloed op de prijs van CO_2-emissierechten en daarmee op de marges op traditionele (fossiele) energieproductie.
In Nederland hebben ook de aardbevingen in Groningen grote invloed op de energievoorziening. De minister heeft

besloten de gaswinning in Nederland steeds verder terug te schroeven. Mogelijk besluit de nationale overheid tot gehele afschaffing van gas als warmtebron voor 2050, wat betekent dat in Nederland miljoenen huishoudens en gebouwen een nieuw verwarmingssysteem nodig hebben. Voor Vattenfall biedt dit enerzijds bedreigingen, aangezien een belangrijk deel van de huidige energieopwekking plaatsvindt met gas. Anderzijds biedt dit ook kansen. Vattenfall is via Nuon namelijk leverancier en ontwikkelaar van stadsverwarming en eigenaar van installatiebedrijf Feenstra dat actief is in cv-ketels en warmtepompoplossingen.
Op een energiemaatschappij als Vattenfall is overheidsbeleid op bijvoorbeeld het verplicht sluiten van kolencentrales in Nederland en kerncentrales in Duitsland, van grote invloed. Vattenfall heeft zich ten doel gesteld binnen één generatie vrij van fossiele brandstoffen te produceren. Dat betekent investeren in duurzame energieopwekmethoden als windparken en zonnepanelen en het versneld afstoten van 'oude' activa. Al deze ontwikkelingen raken niet alleen de strategische risico's van de organisatie, maar daarmee ook de specifieke onderzoeksterreinen van de auditfunctie.

2 – Groei in windenergie
Als de Europese lidstaten hun klimaat- en energiebeloften nakomen, kan windenergie volgens de prognoses van de European Wind Energy Association (EWEA) rond 2030 in een kwart van de Europese vraag naar elektriciteit voorzien. In 2020 wil Vattenfall zijn windenergiecapaciteit hebben verdubbeld tot 4 Gigawatt (GW). Dat betekent een totale groei van 400-600 Megawatt (MW) per jaar in bestaande en mogelijk ook nieuwe markten/landen. Deze ambitie kan Vattenfall alleen realiseren als zij voldoende Europese aanbestedingen voor wind op zee wint. Veilingmodellen hebben hier het spel veranderd, biedingsniveaus zijn zelfs tot nul teruggevallen! Dit gebeurde onlangs in Duitsland, wat betekent dat offshore windenergie voor het eerst zonder subsidies zal worden gebouwd.
Group Internal Audit richt zich in de audits op risico's die horen bij het aangaan van deze langetermijnverplichtingen tot miljardeninvesteringen op zee met onbekende toekomstige energieverkoopprijzen. Te denken valt aan projectmanagementaudits, aanbestedingsaudits en audits op het gebied van het aangaan van partnerships en joint ventures. Bij windenergie valt ook te denken aan audits op veiligheidsaspecten. Juist op zee en op hoogte kunnen ongelukken desastreuze gevolgen hebben. Safety is dus een belangrijke 'core value' van Vattenfall waar gerichte sturing vanuit het management voor nodig is. Group Internal Audit onderzoekt

Vattenfall Group Internal Audit

Vattenfall is een van Europa's grootste elektriciteits- en warmteproducenten en -verkopers, 100% eigendom van de Zweedse staat en moedermaatschappij van nv Nuon Energy. De belangrijkste afzetmarkten van Vattenfall zijn Denemarken, Duitsland, Finland, Nederland, het Verenigd Koninkrijk en Zweden. In 2011 had Vattenfall ruim 37.000 medewerkers, momenteel 20.000.
Vattenfall Group Internal Audit, verantwoordelijk voor de auditfunctie binnen de gehele Vattenfall-organisatie (inclusief Nuon), daalde in diezelfde periode van 36 fte naar 25 fte. Waar het team voorheen vooral bestond uit registeraccountants en EDP-auditors, is de achtergrond van de auditors de laatste vijf jaar breder geworden. Het Nederlandse team bestaat nu uit 2 registeraccountants (waarvan 1 ook jurist), 1 ingenieur, 1 econometrist/RE, en 1 econoom.

Vattenfall heeft zich ten doel gesteld binnen één generatie vrij van fossiele brandstoffen te produceren

hoe 'safety management' in de praktijk terugkomt in certificeringen, KPI's, beleid en operationeel op de werkvloer. Zijn er incidentmeldingssystemen, werkt de plan-do-check-act cycle in de praktijk?

3 – Inpassing energietechnieken vergt draagvlak van de samenleving

Sommige vormen van hernieuwbare energie, zoals de plaatsing van windparken op land of voor de kust, leiden tot weerstand. Andere mogelijke bijdragen aan broeikasgasemissiereductie, zoals ondergrondse CO_2-opslag, de inzet van biomassa of kernenergie, wekken ook tegenstand op. Dat laat zien dat voor de energietransitie voldoende draagvlak in de samenleving van groot belang is.

Group Internal Audit kan helpen bij het in kaart brengen of voldoende en effectieve mitigerende maatregelen zijn genomen door het management voor dit soort risico's. Bij weerstand kan lobbyen helpen, maar van belang is dat dit integer gebeurt en zonder dat daar bijvoorbeeld omkoping of corruptie plaatsvindt. Hierbij is van belang dat er voldoende bekendheid gegeven wordt aan de gedragscode. Recent zijn op dat gebied audits uitgevoerd op de onderwerpen 'anti-bribery', 'code of conduct for suppliers' en 'sourcing from countries with increased political risk'. In de praktijk blijkt dat in sommige gevallen niet alleen interne audits maar af en toe ook incidentonderzoeken nodig zijn. Bij Vattenfall is Group Internal Audit verantwoordelijk voor de uitvoering van dergelijke incidentonderzoeken. In elk land is daarvoor tenminste één fraudespecialist binnen de IA-functie, die naast het uitvoeren van reguliere audits ook beschikbaar is om ad-hoc incidentonderzoeken uit te voeren.

4 – Flexibele productie, uitrol slimme meters, meer data en privacyaspecten

Door het toenemende aandeel van de flexibele productie van elektriciteit uit wind en zon wordt het steeds belangrijker om goed te kunnen omgaan met dit wisselende aanbod. Dat verloopt vooralsnog goed: het groeiende aandeel variabele bronnen leidt niet tot een lagere betrouwbaarheid van de elektriciteitslevering. Het opvangen van een wisselend aanbod gebeurt momenteel onder meer door de conventionele productie uit kolen en gas mee te laten bewegen. Andere mogelijkheden zijn het verhogen van de capaciteit van distributienetwerken, het verhogen van transportcapaciteit met het buitenland en de vraag naar elektriciteit mee laten bewegen met het aanbod en opslag van elektriciteit.

Er lopen proefprojecten voor opslag van elektriciteit, bijvoorbeeld in accu's naast windparken, en bij elektrische auto's die ook elektriciteit terug kunnen leveren aan het net. Slimme meters kunnen naast het bieden van inzicht in het energieverbruik, ook een rol spelen in het reageren op actuele energieprijzen. De opgave is om vanuit maatschappelijk perspectief de optimale mix van maatregelen te nemen om de fluctuaties aan te kunnen. Wat hiervoor mogelijk en nodig is wordt op dit moment door de sector onderzocht.

In Nederland worden analoge meters minimaal eens in de drie jaar bij de klant thuis uitgelezen door de netbeheerder. Slimme meters kunnen dagelijks uitgelezen worden door de

netbeheerder: met het verbruik per kwartier voor elektriciteit en uurwaarden voor gasverbruik. Dit mag alleen met de juiste toestemming (mandaat) van de klant. Deze enorme toename aan mogelijke beschikbare data geeft de onderneming opnieuw kansen en risico's. Per 25 mei 2018 geldt binnen de EU de algemene verordening gegevensbescherming (AVG). De AVG zorgt voor versterking en uitbreiding van privacyrechten, meer verantwoordelijkheden voor organisaties en stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.
De ontwikkeling van privacyregels binnen Europa is uitermate relevant voor energiemaatschappijen. Zeker ook de data van de slimme meter en andere klantgegevens moeten goed geborgd worden. Binnen Vattenfall zijn er diverse programma's om medewerkers zich bewust te laten worden van de risico's en hun gedrag daarop te laten aansluiten. Dit vormde voor Group Internal Audit aanleiding om niet alleen audits te gaan uitvoeren op 'Europese privacywetgeving readiness', maar ook om nog eens kritisch te kijken naar de eigen opslag van persoonsgegevens in auditdossiers. Is het nodig om de klantgegevens mee te nemen in de steekproef of kan – of moet – worden volstaan met geanonimiseerde data? Niet alleen de Autoriteit Persoonsgegevens (AP), maar ook de toezichthouder Autoriteit Consument en Markt (ACM) verscherpt het toezicht steeds meer. Mede om die reden staan diverse specifieke compliance audits – afhankelijk van de jaarplannen van de toezichthouders – op de auditagenda.

5 – Lean operaties en digitalisering
Een sterke kosten- en efficiëntiefocus blijft de sleutel om concurrerend te blijven in de huidige energiemarkt. Digitalisering, zoals met de slimme meters, is daarbij een belangrijke factor in de toenemende operationele efficiëntie en flexibiliteit. Efficiënte werking vereist betere gegevens over de toestand van apparaten en meer krachtige en complexe algoritmes voor het omzetten van gegevens in intelligentie en controle. Digitalisering creëert ook nieuwe mogelijkheden voor klantinteractie, en nieuwe oplossingen kunnen meer visueel en begrijpelijker worden gemaakt. Dit resulteert in een steeds competitiever klimaat waar de concurrentie niet alleen uit andere utiliteiten komt, maar ook van andere industrieën zoals IT, internetbedrijven en kleine startende bedrijven. Bij de vele innovaties en initiatieven, zoals Agile, wil Group Internal Audit zoveel mogelijk aanhaken. Verder blijven onderwerpen als autorisatiemanagement en cyberrisico's een belangrijk aandachtspunt voor de interne audits. Daarom werken de IT-auditors steeds meer in combinatie met brede operational auditors.

6 – Outsourcing
Binnen Vattenfall is besloten om het potentieel van outsourcing van bepaalde inkoop-, finance en humanresourcebedrijfsprocessen te onderzoeken. Daartoe loopt momenteel een Europees aanbestedingstraject. Het doel is niet alleen kostenbesparing op de lange termijn, maar outsourcen wordt ook gezien als een strategisch managementinstrument om de bedrijfsprocessen aan te sturen en de staffuncties te standaardiseren teneinde de organisatie fit en flexibel voor de toekomst te maken.
Uiteraard heeft de outsourcing van veel staffuncties invloed op de internal controls in de processen. De rol van Group Internal Audit is bijvoorbeeld het formuleren van specifieke auditclausules in outsourcingscontracten en het beoordelen van de opzet van de aangeboden controls door de outsourcingspartners. Zodra de keuze voor de partner is gemaakt en gestart wordt met de implementatie start Group Internal Audit met diverse audits naar de werking van de controls. Nu, maar ook in de toekomst na het outsourcen, werken de auditors van Vattenfall internationaal. Daarbij komt internationaal werken en omgaan met verschillende bedrijfsculturen aan bod. Hoe ga je daar als auditor mee om? Gebruik je dan gemixte teams om zo voldoende aandacht te hebben voor cultuurverschillen? Heeft het invloed op het type aanbeveling dat je geeft? Wat in het ene land werkt, hoeft immers niet per definitie in het andere land effectief te zijn. Tevens heeft de internationalisering geleid tot Engels als voertaal en het investeren in een uniform auditproces met enkel digitale dossiers en een applicatie om zo de kwaliteit over de landen heen te kunnen borgen. Op deze wijze trachten we nu en in de toekomst 'value adding' audits uit te voeren. <<

Klantgegevens moeten goed geborgd worden. Er zijn programma's om medewerkers zich bewust te laten worden van de risico's en hun gedrag daarop te laten aansluiten

Noot
1. Ontleend aan *Energietrends 2016*, een uitgave door ECN, Energie-Nederland en Netbeheer Nederland en het jaarverslag nv Nuon Energy 2016.

Jantien Heimel RA CFE CIA CISA is hoofd Internal Audit Netherlands bij de Vattenfall Group.

Artikel Fraude
Tekst Noortje de Rooij MSc RO
Thom Eijken MSc
Beeld 123RF®

Fraude:
een uitdaging voor de *internal auditfunctie*

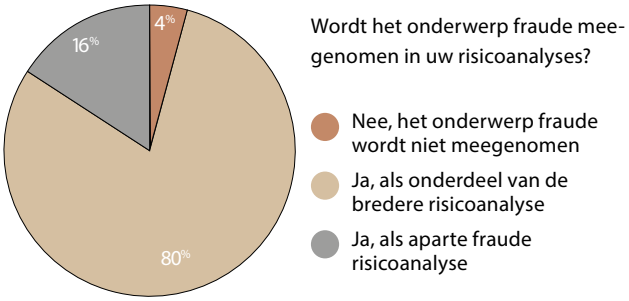
Kwaadwillende medewerkers maken steeds meer gebruik van technologie bij het plegen van fraudes. KPMG onderzocht door middel van vragenlijsten en rondetafelbijeenkomsten in hoeverre internal auditfuncties in staat zijn om fraude te voorkomen, te detecteren en op te volgen. De conclusie: internal auditors hebben moeite met het structureel adresseren van fraude.

Bijna een kwart van de fraudeurs maakt inmiddels gebruik van technologie

Bij bijna twee derde van de interne fraudegevallen spelen slechte interne beheersmaatregelen een rol.[1] Het is in dat opzicht logisch dat de internal auditor een belangrijke rol vervult bij de voorkoming, detectie en opvolging van fraude. De vraag is in hoeverre de internal auditor invulling kan geven aan de aan fraude gerelateerde werkzaamheden, gezien de steeds dynamischere en complexere wereld waarbinnen hij werkzaam is.
In die snel veranderende wereld, waarin het gebruik van technologie bij fraude een steeds grotere rol speelt, is het voor internal auditors uitdagend om de laatste ontwikkelingen op dit terrein bij te houden. Zo blijkt uit een recente vragenlijst van KPMG dat slechts bij 3% van de organisaties waarbij fraude plaatsvond proactieve anti-fraude data-analyse werd toegepast. Dit terwijl inmiddels al bijna een kwart van de fraudeurs gebruik maakt van technologie.
Naast technologie speelt ook de organisatiecultuur een grote rol bij het voorkomen van fraudes. Tijdens de rondetafelbijeenkomsten kwam naar voren dat de internal auditfunctie er zich nog onvoldoende bewust is dat het gebrek aan een goede cultuur op zichzelf ook een groot risico is. Dit artikel gaat over wat de verantwoordelijkheid is van de internal auditor op het gebied van fraude, in hoeverre internal auditors zelf vinden dat zij daar invulling aan geven en hoe zij zich verder kunnen professionaliseren.

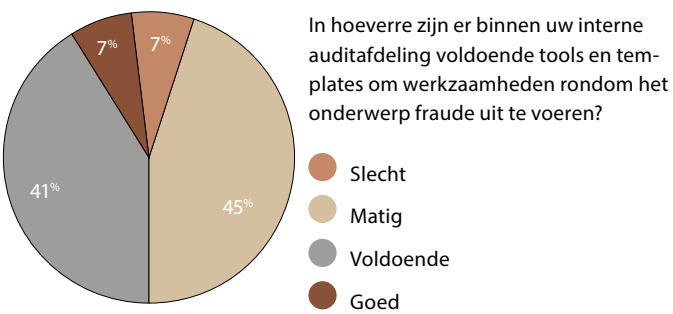
Wat zeggen de IIA Standaarden?
Het IIA heeft de verantwoordelijkheden van de internal auditor ten aanzien van fraude opgenomen in verschillende standaarden. Zo wordt bijvoorbeeld vakbekwaamheid afgebakend: er moet voldoende kennis zijn om frauderisico's te beoordelen, maar er wordt niet verwacht dat de internal auditor de expertise bezit van een persoon wiens voornaamste verantwoordelijkheid het ontdekken en onderzoeken van fraude is. Daarnaast dient een internal auditor bij zijn werkzaamheden rekening te houden met de waarschijnlijkheid van fraude, dient hij regelmatig te evalueren wat de kans is op het bestaan van fraude en hoe de organisatie frauderisico's beheerst. Tot slot dient het hoofd van de internal auditfunctie bij de periodieke rapportage aan het seniormanagement en bestuur ook de frauderisico's te rapporteren.[2]

Internal auditors zijn zoekende
Hoewel de verantwoordelijkheden staan beschreven in de IIA Standaarden ervaart KPMG dat veel organisaties de vertaling naar de praktijk lastig vinden. Daarom organiseerde KPMG verschillende vragenlijsten en rondetafelbijeenkomsten onder 69 internal auditfuncties van financiële instellingen en corporate organisaties, om te inventariseren welke preventieve, detectieve en responsmaatregelen op het gebied van fraude zijn ingericht.
Om fraude te kunnen voorkomen is het van belang inzicht te hebben in frauderisico's. Uit de vragenlijst komt naar voren dat slechts 16% van de ondervraagden een specifieke analyse uitvoert, gericht op het in kaart brengen van frauderisico's (zie *figuur 1*).

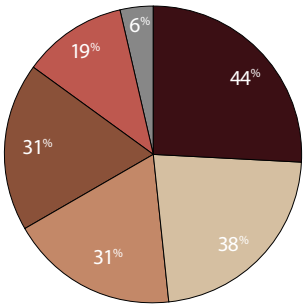


Figuur 1. Fraude en risicoanalyse

Om fraude op structurele wijze te adresseren is een analyse van digitale gegevens een vereiste. Meer dan de helft van de internal auditfuncties geeft aan weinig tools en templates tot zijn beschikking te hebben, waardoor het lastig is fraude structureel inzichtelijk te krijgen (zie *figuur 2*). Naast het gebruik van technologie is het voor een internal auditor van groot belang de juiste vragen te stellen en doortastend te zijn. Dit is een randvoorwaarde om fraudes te kunnen ontdekken. Hierbij is het belangrijk dat ook rekening wordt gehouden met de cultuur in de organisatie en het gedrag van medewerkers. Uit de rondetafelbijeenkomsten komt naar voren dat internal auditors de afgelopen jaren bekend zijn geraakt met het belang van cultuur en gedrag, maar dat zij het nog steeds lastig vinden deze aspecten te auditen dan wel hierover te rapporteren.



Figuur 2. Aanwezigheid tools en templates



Wat is de hoofdreden om geen digitale bronnen mee te nemen in een onderzoek? (Meerdere antwoorden per respondent mogelijk)

- Gebrek aan tooling
- Data privacy
- Complexiteit
- Gebrek aan expertise binnen mijn team
- Kosten
- Tekort aan mankracht

Figuur 3. Meenemen digitale bronnen in een onderzoek

Uit de vragenlijst blijkt dat slechts 25% van de respondenten het afgelopen jaar digitale bronnen heeft betrokken bij het uitvoeren van een fraudeonderzoek. De belangrijkste reden hiervoor is een gebrek aan tooling, gevolgd door gebrek aan kennis over data privacy (zie *figuur 3*). Opvallend is dat veel minder vaak de hoge kosten of het gebrek aan mankracht als reden wordt genoemd. De internal auditor is nog zoekende naar de geschikte tools die hem op structurele wijze kunnen helpen fraudeonderzoeken uit te voeren. De conclusie is derhalve dat internal auditors zich wel bezighouden met de preventie en detectie van en respons op fraude, maar dat dit voornamelijk op ad-hocbasis gebeurt.

Hoe verder te professionaliseren?

Ondanks dat vrijwel alle respondenten van de vragenlijst (98%) aangeven dat er binnen hun internal auditfunctie aandacht is voor het onderwerp fraude, is slechts 14% van mening dat het onderwerp goed belicht is binnen hun functie. Uit de respons op de vragenlijsten en uitkomsten van de rondetafelbijeenkomsten blijkt dat internal auditfuncties zich nog verder kunnen professionaliseren op het gebied van fraude.

Allereerst door fraude actiever te benaderen. Dat kan bijvoorbeeld door het invoeren van een periodieke frauderisicoanalyse. Hiermee worden frauderisicofactoren en frauderisico's structureel inzichtelijk en ontstaat tevens inzicht in hoeverre de frauderisico's zowel preventief als detectief gemitigeerd worden.

Hoe sterk interne beheersmaatregelen ook zijn ingeregeld, het voorkomen van fraude valt of staat met het hebben van een gewenste cultuur. Fraude ontstaat namelijk vaak doordat interne beheersmaatregelen worden omzeild. Een internal auditor moet daarom ook rekening houden met de naleving van de normen en de beleving van de waarden binnen de organisatie. In hoeverre is er een open cultuur, spreekt men elkaar aan op ongewenst gedrag en is er het juiste voorbeeldgedrag vanuit het management? Dit zijn elementen die de internal auditor daadwerkelijk periodiek kan meten.

Bovenal is de digitale fraudeur bezig met een opmars die niet meer te stoppen is. Het is noodzakelijk dat de internal auditor digitale bronnen en data-analyse gaat benutten bij het bepalen van frauderisico's en het detecteren en afhandelen van incidenten. De laatste jaren is er veel software ontwikkeld die toegankelijk is zowel qua prijs als gebruik. Het is essentieel voor de internal auditfunctie dat de internal auditor meegaat in dergelijke technologische ontwikkelingen.

Internal auditfunctie en fraude: het is van nature geen vanzelfsprekende match. Toch kan de internal auditor een belangrijke rol spelen bij de preventie en detectie van en respons op fraude. We zien dat periodieke frauderisicoanalyses en aandacht voor cultuur en digitalisering bijdragen aan een sterkere positie van de internal auditor inzake fraude. <<

Internal auditors houden zich wel bezig met de preventie en detectie van en respons op fraude

Noten

1. KPMG International, *Global profiles of de fraudster. Technology enables and weak controls fuel the fraud*, 2016.
2. IIA, *International standards for the professional practice of internal auditing, Standards*, 2017.

Noortje de Rooij is manager bij KPMG Advisory en ondersteunt internal auditfuncties bij fraudepreventie, detectie en respons.
derooij.noortje@kpmg.nl

Thom Eijken is senior manager bij KPMG Advisory en ondersteunt organisaties bij het detecteren van fraude aan de hand van digitale gegevens.
eijken.thom@kpmg.nl

Vertrouwen en data

'In God we trust – all others must bring data'. Dat is het motto van dit zeer leesbare en leuke boek van rechtspsycholoog Merckelbach. Getriggerd door een vijfsterrenrecensie in *de Volkskrant* en altijd geïnteresseerd in onze psyche en de gevolgen van ons meestal beperkte oordelen, heb ik het boek aangeschaft en ik kan iedereen aanraden dat ook te doen. Maar ja, dan moet ik daar wel bewijs voor leveren natuurlijk. Want alleen op basis van een uitspraak in een recensie koop je geen boek.

Merckelbach toont, met een stortvloed aan voorbeelden aan dat intuïtie echt gevaarlijk kan zijn, veel schade kan opleveren. Hij doet dat door voorbeelden uit de praktijk te belichten. De moordenaar van de familie uit Naarden die doodleuk in hun huis was ingetrokken en zelfs de politie om de tuin leidde door heel aardig te doen. Heel beleefd had hij hen verteld dat de bewoners naar Spanje waren gegaan en hij zolang op het huis paste. Peter R. de Vries ontmaskerde hem door vragen te blijven stellen en onmogelijkheden aan te tonen. Door dus niet te geloven, maar door feiten te checken. Ongelooflijk veel rechtszaken passeren de revue. Onderzoeken die fout zijn uitgevoerd of gewoon niet, we geloven het wel, het is toch duidelijk.

De auteur stelt op pagina 91 dat politie en justitie zich nogal wispelturig opstellen. Is er veel media-aandacht dan worden aangiftes kritiekloos geaccepteerd, zijn er gerechtelijke dwalingen aangetoond dan worden aangiften superkritisch bejegend. Het risico van het eerste is dat er gemakkelijk gedwaald wordt (de aangifte blijkt onjuist of onterecht) en van het tweede dat zaken over het hoofd gezien worden (de aangifte toont aan dat het fout zit maar wordt niet geloofd).

Ook de andere kant van het verhaal wordt steeds kritisch behandeld. Zo toont hij bij een casus aan dat een patiënt van dokter Jansen (de dokter uit Enschede die mensen onterecht diagnosticeerde met verregaande dementie en andere dodelijke ziekten) bijna onmogelijk te overtuigen was van het feit dat ze geen dementie had. Twee jaar en zeer zorgvuldige behandeling door een andere arts waren nodig om haar geloof (en de angsten als gevolg van die verkeerde diagnose) in haar eigen dementie te laten afnemen. Blijkbaar willen we zelf ook graag witte jassen geloven.

Het boek is uitstekend, snel en deskundig geschreven. Uitstekend omdat Merckelbach bij ieder voorbeeld en iedere casus beide kanten van de medaille laat zien. Logisch dat men eerst dit dacht, maar dat het eigenlijk anders zit. Snel, omdat het goed doorleest, een prettige verteltrant heeft. En deskundig omdat uit alle zaken blijkt dat hij als psycholoog zijn zaken goed kent. Hij heeft de data op orde en komt overtuigend met bewijs.

Lees het boek, het zal ook u helpen om kritisch te staan tegenover uw eigen intuïtie! Steeds op zoek te gaan naar overtuigende data. Om zo met vertrouwen keuzen te kunnen maken!

Intuïtie maakt meer kapot dan je lief is
Harald Merckelbach
Prometheus
ISBN 9789044634396
€ 19,99

Renze J. Klamer, Agile coach, Bijenco
www.bijenco.nl
klamer@bijenco.nl

VERENIGINGSNIEUWS

Audit Magazine als app

Audit Magazine heeft een eigen app. Afgelopen maanden hebben we besteed aan het prettig leesbaar maken van het magazine voor telefoon en tablet. Je vindt de app in de Play Store en App Store. Ook is het blad via www.auditmagazine.nl te lezen, zowel in leesweergave als in bladerweergave.
http://bit.ly/2gYBmT1 http://apple.co/2z7draH

Uitgegeven Certificaten Kwaliteitstoetsing

De interne auditafdelingen van de volgende organisaties ontvingen de afgelopen tijd een Certificaat Kwaliteitstoetsing: Alliander, ASML, Deloitte Nederland, InHolland.

Vaktechnische publicaties

26-10-2017 – Global Perspectives and Insights: Artificial Intelligence
03-10-2017 – Een goede bestuurder en toezichthouder verdient een goede internal auditfunctie
22-09-2017 – Risk in Focus: hot topics for internal audit 2018
14-09-2017 – Engagement Planning: Establishing Objectives and Scope
Meer publicaties: http://bit.ly/2gQUluS

IIA feliciteert de geslaagden

Nieuwe CIA's: Arjan Brouwer, Martin van Duyse, Vincent Jorna, Edward Roozenburg, Ana Maria van der Maarl
Nieuwe CFSA: Nicole Huijbrechts
Nieuwe CRMA: Jasper Jacobus Casteleijn, Andries Held

Rectificatie: In nummer 3 van *Audit Magazine* is per abuis bij Nieuwe CIA's, de naam Andries Held vermeld. Dit is onjuist, hij is sinds 2002 CIA en nu geslaagd voor het examen CRMA.

Save the date: 8 maart Internationale Vrouwendag

Op 8 maart 2018 is het Internationale Vrouwendag. Voor het IIA een uitgelezen moment om aandacht te besteden aan de vrouwelijke auditors. Slechts een op de vier auditors is vrouw, terwijl de inbreng van een vrouw vaak een groot verschil maakt in de mannenwereld. We trakteren onze vrouwelijke leden op een inhoudelijk sterk programma met topvrouwen als sprekers, die binnen en buiten het internal auditvakgebied werkzaam zijn. Meer informatie volgt.

Commissarissen Symposium

Het Commissarissen Symposium in oktober 2017 stond in het teken van de herziene Corporate Govenance Code waarin onder andere de aandacht uitgaat naar cultuur en gedrag. Vier sprekers deelden hun visie en best practices over dit thema. Vervolgens gingen de aanwezigen in breakoutsessies aan de slag met stellingen die daarna in het Lagerhuisdebat door voorstanders fel werden verdedigd en vervolgens door tegenstanders weer omver werden geblazen.
Het verslag: http://bit.ly/2yYXscI

PAS-conferentie

Op 2 november 2017 werd voor de vijfde keer de PAS-conferentie gehouden. De ruim honderd aanwezigen konden luisteren naar Paul Hofstra van de Rekenkamer Rotterdam die sprak over het rapport *In onveilige handen*. Roel van Rijsewijk vertelde op geanimeerde wijze hoe je cybersecurity als kans kunt zien en na een interactieve sessie over kwaliteitstoetsing door Arnoud Daan, ging men in kleinere groepen aan de slag in diverse breakoutsessies.
http://bit.ly/2zz534D

RO Masterclass

Op 23 en 24 november 2017 vond de RO Masterclass plaats. Een groots evenement met interessante sprekers dat altijd op veel belangstelling mag rekenen. Het thema van dit jaar was Vakmanschap. Een thema dat zich goed leende voor een breed scala aan onderwerpen, zoals agile auditing, risk management en gamification.
Zie de IIA-website voor een terugblik op deze masterclass.
http://bit.ly/2A6USSk

Kopjaar IT-Auditing & Advisory (RE) in trek bij RO's

Bij ESAA is dit collegejaar wederom een enthousiaste groep studenten begonnen aan het kopjaar van de post-masteropleiding IT-Auditing & Advisory. In deze groep zijn naast RA's ook behoorlijk wat RO's die hun kennis van het IT-vakgebied willen vergroten.Speciaal voor degenen die al een R-opleiding hebben gevolgd heeft ESAA het kopjaar ontwikkeld. Kopjaarstudenten krijgen diverse vrijstellingen en kunnen in één jaar de opleiding doorlopen. Bij ESAA is het ook mogelijk om de beide opleidingen (RO en RE) af te ronden met een gecombineerde afstudeeropdracht.

Waardevolle inbreng
Omdat de rol van IT in organisaties is gegroeid en de risico's navenant willen deze studenten hun kennis in IT-Auditing verdiepen. Daarnaast is er ook de wens om hun vaardigheden te vergroten en operational audit en IT-audit nader aan elkaar te verbinden.
Prof.dr. Egon Berghout, wetenschappelijk directeur van de ITAA opleiding: "Door moderne technologie worden bedrijfsprocessen steeds moeilijker te doorgronden en te beheersen. Dat vraagt om grondige IT-kennis om belangrijke en minder belangrijke zaken van elkaar te kunnen scheiden. En dan komt de kennis uit de ITAA-opleiding opeens geweldig van pas. Onze ervaring met de RO-studenten is dat zij een waardevolle inbreng hebben door hun brede kijk op (IT-)problemen. De combinatie met studenten met andere vooropleidingen levert een goede mix van invalshoeken, kennis en ervaring."

ESAA is verhuisd op de Campus

In verband met renovatie van het gebouw waarin ESAA de afgelopen jaren was gehuisvest, verhuisde ESAA de afgelopen zomer op de campus naar het Van der Goot gebouw. Bezoekadres: M5-20.

Universiteit van Amsterdam

Amsterdam Business School

Actualiteiten

Op vrijdag 15 september jl. hebben zeven EIAP- en zeven AITAP-studenten hun bul behaald op de Amsterdam Business School.

V.l.n.r.: Marlies van Uhm | Dennis Wolthuis | Anoep Singh | Abdes Allach | Martijn Broenink | Hassan Khosravi | Judith Berendsen | Arjan Kieneker | Abderrafik Asseban | Maarten Slotema | Irfaan Santoe | Wouter Ensing | Wilma Bakker.

Verrijking EIAP-opleiding met twee vakken

Qua curriculum kunnen we melden dat we binnen de regels van de Opleidings- en Examenregeling (OER) van de Universiteit van Amsterdam de EIAP-opleiding hebben verrijkt met de vakken Data Science en Soft Controls/Behavioural Auditing. Aan beide vakken werd al gefragmenteerd aandacht gegeven, maar we hebben nu een verdere verdieping aangebracht door deze vakken een meer prominente plek te geven in het programma. Zo worden de huidige studenten opgeleid en klaargestoomd voor de internal auditor en internal auditfunctie van de toekomst!

Nieuw Academisch collegejaar

Het Academisch collegejaar is weer volop van start gegaan en we kunnen het goede nieuws delen dat elf EIAP-, vijf reguliere AITAP- en negentien fast track AITAP-studenten zijn gestart in het gezamenlijke eerste jaar.

Rubriek **Column**
Tekst **Drs. Willem van Loon RA CIA**

Het dilemma van **veiligheid**

De laatste tijd houdt de vraag: wat betekent veiligheid?, mij steeds vaker bezig. Als we het over IT-security hebben is het meestal wel duidelijk, daar lopen we als (IT-)auditor maar al te vaak tegenaan. Dan zijn er legio protocollen en beperkende maatregelen. Datzelfde geldt voor kermisattracties en de luchtvaart. Alles is erop gericht dat niets misgaat, er geen data lekt en geen doden vallen. Maar wat nu als ik mijn wachtwoord vergeet en de helpdesk onbereikbaar is door een telefoonstoring? Of als die kermisattractie opeens tot stilstand komt door langdurige stroomuitval? Dan krijgt het automatisch zekeren van alle stoeltjes opeens een heel andere dimensie.

Waar de een juist veiligheid zoekt in het zekeren, zetten van kaders en zorgen dat er niets buiten de lijntjes wordt gekrabbeld, vindt de ander deze juist in het creëren van bewegingsruimte om te kunnen ontsnappen aan restricties en ongewenste situaties. Wat voor de een veilig voelt, leidt bij de ander juist tot angst. Voor de een is een open en losse omgeving veilig, terwijl de ander juist vastigheid en geslotenheid opzoekt. En wat voelt veilig voor jou?

Gevangen en afgeschermd	of	vrij en toegankelijk
Oud en verleden	of	heden en de toekomst
Licht en donker	of	zwaar en licht
Prince2	of	Agile
Delen	of	juist voor jezelf houden…

Waar het vroeger vaak zo klaar was als een klontje, ligt tegenwoordig het antwoord veelal besloten in de tegenstelling. Ook als we het hebben over iets ogenschijnlijk evidents als vuurwapenbezit. Toen ik kind was mocht een plastic pistooltje niet tot mijn speelgoedarsenaal behoren. In het volwassen leven zijn de meningen stevig verdeeld over wat nu veilig is en niet. Het hebben van een wapen creëert wellicht een gevoel van veiligheid en jezelf kunnen verdedigen. De afwezigheid ervan biedt anderen overtuigend het gevoel van veiligheid omdat er niet geschoten zal worden. En autorijden? Ook daar lijkt helder wat veilig is, maar hoe zit het met zelf rijden of zelfrijdend? Daar is het waarschijnlijk een kwestie van wachten opdat het beeld over wat veilig is behoorlijk gaat schuiven.

Spannender wordt het als we kijken naar wat veiligheid persoonlijk met je doet. Als je ooit een nare ervaring hebt gehad, zoek je eerder het licht op, waar iemand anders zich juist veilig voelt als hij zich even in het donker kan verschuilen. Prince2 biedt houvast door structuur waar Agile die juist biedt door flexibiliteit. En wat betekent veiligheid voor jou in relatie tot de ander? Als ik, als auditor, wil weten of strategieën, processen en doelen voldoende in control zijn, dan is het zaak te begrijpen wat voor de ander als veilig aanvoelt. Daar is dus niet een eenduidig antwoord op te geven. Zo kan ik nog wel even doorgaan, maar dan zou ik buiten de 'veilige' kaders van deze column komen.

Zelf heb ik de afgelopen drie jaren de veiligheid opgezocht door mijn gedachten, in de vorm van geschreven columns aan jullie, de lezers, toe te vertrouwen. Dit in de wetenschap dat het misschien veiliger is om over deze gedachten in discussie te gaan en ze met andere invalshoeken te verrijken. Wellicht wordt dat mijn volgende uitdaging. Na veertien columns, draag ik graag het stokje over aan de volgende columnist.

Willem van Loon is als docent en examinator verbonden aan het Executive Internal Audit Program van de Universiteit van Amsterdam. Daarnaast is hij bestuurslid van IIA NL en vol enthousiasme actief op het gebied van governance, risk management en Internal Audit.

Is risk still risky when your people see it coming?

EY believes that an organization's internal controls are only as good as the Risk Culture: the behavior of all employees within the organization that influences risks and outcomes.

Our approach to internal controls enables you to engage your employees in changes, stimulate a culture that promotes desired behavior and encourages employees to act with integrity. For more information please contact Will Weerts (will.weerts@nl.ey.com, +316 52 46 59 34).

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

EY
Building a better working world

Co-sourcing

Flexibiliteit in resources en toegang tot actuele kennis

In de huidige complexe wereld is het voor organisaties bijna niet meer mogelijk om op alle inhoudelijke terreinen over voldoende kennis en ervaring te beschikken om zelf internal audit-werkzaamheden uit te voeren. Daarnaast zijn er veel kosten gemoeid met het op peil houden van het juiste kennis- en opleidingsniveau.

Dit vraagt om een flexibele schil rondom uw internal audit-functie. Voor de nodige flexibiliteit in resources, maar ook voor toegang tot actuele kennis die kan worden ingezet om de organisatie naar een hoger niveau te brengen en competenties verder te ontwikkelen.

KPMG helpt uw organisatie verder. Op het gebied van IT- en cyberrisico's, data analyse, soft controls, contract compliance, integrated reporting tot risk based strategies.

Contact

Bart van Loon
T: +31 (0)20 656 7796
E: vanloon.bart@kpmg.nl

kpmg.nl