

AUDIT

MAGAZINE

VAKBLAD VOOR DE INTERNAL AUDITOR
NUMMER 1 2018 JAARGANG 17

THEMA

Fraude – Ethiek – Integriteit

Kees van Nieuwamerongen,
directeur ILT en AW:

“Ik zou het fijn vinden als de
woningcorporatiesector weer
saai wordt”

*Fraude:
hoe raak
je erin verzeild?*

Samenwerken in het
bestrijden van
corruptie en fraude

IIA Quality Assessment Review

**veel ervaring
veel toegevoegde waarde**



www.fsvriskadvisory.nl

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

Bijdragen kunnen worden gemaald 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@denerlandseassociatie.nl
tel.: 030-2271677

Vormgeving

ViaMare grafisch ontwerp, Marijke Maarleveld

Druk

Senefelder Doetinchem

Advertenties en abonnementen

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

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

Audit Magazine verschijnt vier maal per jaar.

Alle rechten voorbehouden. Behoudens de door de Auteurswet 1912 gestelde uitzonderingen, mag niets uit deze uitgave worden vervoerdigd (waaronder begrepen het opslaan in een geautomatiseerd gegevensbestand) en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van de uitgever. De bij toepassing van art. 16b en 17 Auteurswet 1912 wettelijk verschuldigde vergoedingen wegens fotokopieën, dienen te worden voldaan aan de Stichting Reprorecht, Postbus 3060, 2130 KB Hoofddorp, tel.: 023-7997810. Voor het overnemen van een gedeelte van deze uitgave in bloemlezingen, readers en andere compilatiewerken op grond van art. 16 Auteurswet 1912 dient men zich te wenden tot de stichting Reprorecht, Postbus 3060, 2130 KB Hoofddorp, tel.: 023-7997809. Voor het overnemen van een gedeelte van deze uitgave ten behoeve van commerciële doeleinden dient men zich te wenden tot de uitgever. Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(en) en uitgever geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

Fraude, ethiek en integriteit

Fraude, ethiek en integriteit en zijn thema's die dicht bij elkaar liggen en elkaar soms overlappen. Ethisch handelen en integer handelen hebben een positieve betekenis. Fraude vormt in dit rijtje een uitzondering, want voor het plegen van fraude kun je strafrechtelijk vervolgd worden. Niet-integer of niet-ethisch handelen kunnen we weliswaar niet juist vinden, maar strafbaar is dit handelen niet. Hier komt moraliteit in zicht. Elke dag hebben we allemaal te maken met morele dilemma's. En het kan soms knap lastig zijn om hierin altijd de juiste keuzen te maken.

Is niet-integer en niet-ethisch handelen dan minder schadelijk voor je organisatie? Dat valt te betwijfelen. Niet alleen voor de organisatie als geheel, maar ook het handelen van individuen binnen de organisatie kan verstrekkende gevolgen hebben voor de organisatie als geheel. Social media, zoals Twitter en Facebook worden gebruikt voor 'naming en shaming' als organisaties in onze ogen niet integer handelen. Hierdoor neemt de noodzaak tot het hebben van een juiste moreel kompas binnen de organisatie toe. Maar hoe doe je dat? En waar raakt dit thema de rol van de internal auditor?

Een organisatie kan fraude voorkomen door de AO/IC goed in te richten. Het integer handelen van de medewerkers is moeilijker af te dwingen door het inrichten van een hard control. Een gedragscode of integriteitscode kan een hulpmiddel zijn, maar is een papieren werkelijkheid als de medewerkers er niet naar handelen. Voorbeeldgedrag van bestuurders heeft een veel groter effect. Maar niet alleen bestuurders zijn aan zet. Voorbeeldgedrag, elkaar aanspreken en feedback geven op onjuist handelen is van ons allemaal. Zonder deze soft controls is het toetsen van de AO/IC niets waard.

Wat is de rol van de internal auditor in dit speelveld? Als eerste heeft de internal auditor zich te houden aan de code of ethics. Deze code beschrijft voornamelijk het handelen van de internal auditor zelf. Daarnaast geeft de nieuwe governancecode de internal auditor een belangrijkere rol binnen de organisatie. Dit schept verwachtingen en het hebben van een rechte rug. De internal auditor moet de morele moed hebben om het niet-integer handelen van een organisatie als geheel, bestuurder of ieder individu aan de kaak te stellen. Dit vraagt om competenties als standvastigheid, lef en overtuigingskracht. Als de internal auditor deze rol niet pakt wordt steeds vaker de vraag gesteld: waar was de internal auditor?

Wij wensen u veel leesplezier!

De redactie van *Audit Magazine*



THEMA: Fraude – Ethiek – Integriteit



NFP Photography

“Ik zou het fijn vinden als de woningcorporatiesector weer saai wordt”

Aldus Kees van Nieuwamerongen, directeur Inspectie Leefomgeving en Transport/Autoriteit woningcorporaties. Een interview over de lessons learned en de stappen die de sector heeft gemaakt.

Pag. 6

SIO: een kader voor integere organisaties

Klanten kiezen voor een organisatie die ze vertrouwen. Medewerkers voor een organisatie waar ze trots op kunnen zijn. Kortom, investeren in integriteit loont. Dat kan met SIO, aldus Natascha Rol (MoresMundi). **Pag. 18**

Over fraude: theoretisch kader en casuïstiek

Witwassen, omkoping, fraude: we worden er dagelijks mee geconfronteerd in de media. Marcel Pheijffer over de fraudedriehoek, de frauderisico's en de fraude bij Wells Fargo. **Pag. 10**

Tien tips om veilig te internetten

Hackers, DDoS-aanvallen, ransomware, Russische hackers die probeerden invloed op de Amerikaanse verkiezingen uit te oefenen. Ofwel, hoe internet je zo veilig mogelijk? **Pag. 22**



Fraude: hoe raak je erin verzeild?

Richard Bistrong pleegde jarenlang fraude en moest daarvoor de gevangenis in. Inmiddels adviseert hij organisaties op het gebied van corruptie en compliance. Een interview over het waarom. **Pag. 15**



Is hier sprake van fraude?

Forensisch onderzoeker Inge-Lisa Toxopeus (Hermes Advisory) vertelt wanneer zij wordt ingeschakeld en wat de 'red flags' en de vier fasen van fraudebestrijding zijn. **Pag. 27**



Samenwerken in het bestrijden van corruptie en fraude

Justitie zet steeds meer in op integriteitsbevordering en corruptiebestrijding. De FIOD speelt hierin een belangrijke rol, aldus Claartje van Roosmalen (FIOD). **Pag. 30**

Beïnvloeding om fiscale verplichtingen na te komen

Sjoerd Goslinga, Lisette van der Hel-van Dijk en Maarten Siglé (Belastingdienst) over hoe effectmeting kan worden opgezet binnen de Belastingdienst. **Pag. 34**

Goed integriteitsmanagement loont

Misstanden op het werk. Alain Hoekstra en Arjan Wilbers van het Huis voor Klokkenluiders over de rol van de interne auditor. **Pag. 38**



AVG: techniek of gedrag?

Binnenkort is de Algemene Verordening Gegevensbescherming van kracht. Laszlo Nagy over het 10-stappenplan, techniek, olifantenpaadjes, achterdeuren die openstaan en bewustwording. **Pag. 42**

Werken met cultuur

Wat zijn de ervaringen vanuit het domein veiligheid met cultuur(onderzoek)? Psycholoog Frank Guldenmund en consultant Bas Zandee: de grootste uitdaging voor internal auditors is de (interne) norm los te laten. **Pag. 48**

Doorstoten naar de top: IA Down Under

Waarin onderscheidt Internal Audit van de Commonwealth Bank in Australië zich? Rochelle Degens (AFM) en Age-Jan van der Meer (KoutersVanderMeer) lichten dit toe. **Pag. 52**



Accreditatie RO-opleiding: nu begint het pas

Er was een klein feestje bij de UvA toen de RO-opleiding werd geaccrediteerd. *Audit Magazine* prikte een vorkje taart mee. **Pag. 58**

Rubrieken

- 13** Van het bestuur
- 21** De stelling
- 25** Column Mark van Twist
- 33** Column Hakan Honders
- 46** PAS op de plaats: Gert-Jan Willig
- 51** Boekbespreking
- 56** De overstap
- 60** Verenigingsnieuws
- 61** Nieuws van de universiteiten
- 62** Column Walter Swinkels

Kees van Nieuwamerongen,
directeur ILT en Aw:

*“Ik zou het fijn vinden als
de woningcorporatiesector
weer saai wordt”*

De woningcorporatiesector kwam in de periode voor en tijdens de parlementaire enquête (2012-2014) negatief in de publiciteit. De Vestia-affaire is daarvan het bekendste voorbeeld. Kees van Nieuwamerongen, directeur van Inspectie Leefomgeving en Transport (ILT)/Autoriteit woningcorporaties (Aw), over deze gebeurtenissen, de lessons learned en de stappen die de sector heeft gemaakt.



De corporatiesector werkt in een kwetsbare markt, ofwel 'swimming with sharks'

Wat zijn de belangrijkste uitkomsten van de parlementaire enquête?

"Men oordeelde dat de liberalisatie van corporaties op een aantal onderdelen te ver doorgesloten was. De woningcorporaties moesten weer terug naar hun kerntaak: het huisvesten van kwetsbare bevolkingsgroepen, en weer lokaal ingebed met een belangrijke rol voor de gemeenten.

Corporaties opereren in een kwetsbare markt waar zij over het algemeen niet op waren voorbereid. Mijn collega toezichthouder van Waarborgfonds Sociale Woningbouw (WSW) noemt het 'swimming with sharks'. Het gaat hierbij om 'zwemmen tussen' 1) de financiële sector, 2) de aannemers en 3) de vastgoedondernemers. Je moet als corporatie stevig in je schoenen staan om je staande te houden.

Het intern toezicht van de raad van commissarissen schoot tekort. Dat waren in sommige gevallen te veel erebaantjes geworden en een aantal commissarissen had er ook te veel. Daardoor konden bestuurders dominant worden. Tevens werkte het externe toezicht onvoldoende en hadden de toezichthouders te weinig wettelijke bevoegdheden. Daarnaast had het Centraal Fonds voor Volkshuisvesting (CFV) niet genoeg instrumenten en was het WSW te verweven met de sector. Bovendien waren beide toezichthouders niet voldoende uitgerust voor de toezichtstaak. Ook hadden gemeenten hun vastgoedportefeuille grotendeels afgebouwd en voerden in een aantal situaties de druk op bij de corporaties om bijvoorbeeld te investeren in leefbaarheid en wijkontwikkeling.

Als laatste zijn corporaties niet genoeg kritisch geweest richting corporaties die tekort schoten. Er gold een soort non-interventie terwijl iedereen bijvoorbeeld wist dat uitgebreide derivatenportefeuilles gewoon niet goed konden zijn. Kortom, iedere speler heeft in meer of mindere mate steken laten vallen."

Over...

Kees van Nieuwamerongen studeerde algemene economie in Amsterdam. Hij vervulde verschillende functies op het Directoraat Generaal van de Rijksbegroting op het ministerie van Financiën en was directeur Bestuursondersteuning op het ministerie van VWS. Toezichthoudende ervaring deed hij op als secretaris van het College financieel toezicht op de voormalige Nederlandse Antillen. Sinds november 2015 is hij directeur van de Autoriteit woningcorporaties.

Wat is de ontstaansgeschiedenis van de Autoriteit woningcorporaties?

"De Autoriteit woningcorporaties (Aw) is een samenvoeging van het CFV en een aantal toezichthoudende taken van het ministerie van Binnenlandse Zaken. Begin 2016 is de Aw gestart. De Aw focust zich niet sec op financiële ratio's maar ook op niet-financiële, want de problemen waar de parlementaire enquête de zere vinger op legde, kwamen voort uit een niet-functionerende governance. Problemen werden daarvoor intern niet gesignaleerd of opgelost. Er waren onvoldoende check & balances. De sector was niet aantoonbaar in control. Het primaire doel van de Aw was het herstel en het vertrouwen in de sector terugwinnen en het richt zich daarbij voor een belangrijk deel op governance en integriteit."

Op welke manier houdt de Aw toezicht?

"In de corporatiesector zijn WSW en de Aw de toezichthouders. In zijn algemeenheid is het onderscheid dat WSW de bankfunctie vervult en de Aw de aandeelhoudersfunctie. Een vergelijking met een verdeling in toezicht zoals in de financiële markt (AFM en DNB) is lastig te maken."

Hoe werkt het toezicht met twee toezichthouders?

"We kwamen erachter dat we op een aantal onderdelen beter konden samenwerken. In het toezicht deden we sommige taken dubbel, maar er viel ook een aantal taken tussen wal en schip. Dat leidde tot verschillende zienswijzen, dubbele taken en toenemende lastendruk bij de corporaties. Dit gaat nu al veel beter, doordat we de afgelopen twee jaar intensief gewerkt hebben aan het inrichten van de verschillende toezichtstaken.

We zijn nog meer de samenwerking met elkaar aangegaan en op hoofdlijnen tot de volgende verdeling gekomen:

- Toezicht op de financiële positie. Een belangrijk uitgangspunt is een financieel gezonde corporatie. Zowel WSW als de Aw kijken naar de financiële positie vanuit verschillende toezichtsperspectieven.
- Toezicht op de vastgoedportefeuillestrategie. De vastgoedportefeuillestrategie is een onderbouwing en verdieping van de toekomstvisie en missie op het gebied van wonen, vastgoed en financiën. Dit is een primaire toezichtstaak van WSW.

- Toezicht op de governance van een corporatie. Hoe is een corporatie intern georganiseerd? Dit is een toezichtstaak van de Aw. De uitkomsten van dit toezicht delen we met WSW.”

Dat betekent in de praktijk?

“Een deel van het toezicht van de Aw bestaat uit het houden van inspecties en het uitvoeren van governance audits bij de corporaties. Een inspectie kan aanleiding zijn om diepgaander onderzoek (lees: governance audit) uit te voeren. De Aw heeft de afgelopen twee jaar bij alle 334 corporaties een governanceonderzoek uitgevoerd. Het doel was om een nulmeting uit te voeren om vervolgens te kunnen differentiëren in het toezicht (risicogericht). In een governanceonderzoek beoordeelt de Aw op welke manier de corporatie georganiseerd is. Heeft een corporatie bijvoorbeeld een planning & controlcyclus en op welke manier is een corporatie intern



georganiseerd? Hierbij is het belangrijk dat de corporatie dit daadwerkelijk ook in de praktijk brengt en niet alleen op papier heeft staan.

Bovendien vraagt de Aw twee keer per jaar financiële en niet-financiële informatie op bij corporaties. Op basis van onder andere deze informatie maakt de Aw een risicoanalyse om het toezicht per corporatie te bepalen.

Verder is een belangrijk uitgangspunt van onze bezoeken het ‘goede gesprek’. Dit gesprek gaat over gedrag en cultuur. We voeren gesprekken met het bestuur en de raad van commissarissen (RvC) gezamenlijk en afzonderlijk. In deze gesprekken stellen we kritische en soms ook vervelende vragen en behandelen we casuïstiek. Op deze manier krijgen we ook een beeld van de cultuur van een corporatie.

Daarnaast voeren we stresstesten uit, bijvoorbeeld gericht op de derivatenportefeuille. Deze stresstesten kun je vergelijken met de stresstesten bij de banken. En de Aw toetst alle (her)benoemingen van bestuurders en commissarissen. Hierbij maakt de Aw gebruik van gedragsdeskundigen. Het vrijblijvende karakter van de commissarisfunctie is inmiddels verdwenen. Het toetsen van de commissarissen draagt bij aan het verder professionaliseren van het interne toezicht.”

Hoe ziet de Aw de toegevoegde rol van de internal auditor bij de corporatie?

“Allereerst is er een verschil in omvang van de corporaties. De grootste corporatie heeft 90.000 wooneenheden en de kleinste circa 100. Dit heeft gevolgen voor de manier waarop je als corporatie georganiseerd bent op het gebied van interne beheersing. Een internal auditfunctie (of interne

controlfunctie) maakt hiervan een essentieel onderdeel uit naarmate de omvang van de corporatie groter is. De internal auditfunctie kan bijdragen om het bestuur in control te laten komen. Bovendien is het een instrument van de RvC om zich te laten informeren over de interne beheersing bij de corporatie. De Aw kijkt bij haar toezicht of een internal auditfunctie überhaupt aanwezig is. Het is daarbij belangrijk dat de internal auditfunctie op orde is.”

Welke adviezen hebt u voor de internal auditor?

“Durf de luis in de pels te zijn. Daarvoor sta je opgesteld. Het is belangrijk om kritisch te zijn en op de juiste momenten je rug recht te houden. Het is van belang om het verschil te zien tussen gelijk hebben en gelijk krijgen. De internal auditor heeft de uitdaging om het spel goed te spelen. Hard op de bal, met voldoende

competenties om de boodschap zodanig over te brengen dat verbetering in gang wordt gezet. Anders zet je jezelf buitenspel. Dit geldt overigens ook voor de Aw.”

Wat is de stip op de horizon voor de Aw?

“Ik zou het fijn vinden als de woningcorporatiesector weer saai wordt. Een tijdje terug werd in de kranten weer veel geschreven over een oude fraudezaak bij een corporatie. Dit is een zaak van jaren geleden, maar toch verschijnt de sector dan weer negatief in het nieuws. Er is zoveel ten goede gekeerd de afgelopen jaren, maar dergelijke nieuwsberichten bevestigen de beeldvorming als zou er van alles mis zijn in de sector. De Aw wil een belangrijke bijdrage leveren om het vertrouwen in de sector verder terug te krijgen. De Aw heeft als doel om betrouwbaar en voorspelbaar toezicht te houden. Zij doet dit onder andere door het geven van voorlichting en het zijn van de ‘trusted partner’ van de corporaties en de stakeholders. Maar we zijn ook een ‘ruthless truth teller’, als iets niet klopt treden we ook op. Daar moet de huurder en de belastingbetaler op kunnen vertrouwen. We houden hierbij de aandacht op governance en integriteit bij corporaties. De Aw staat voor wat we zeggen en heeft als doel het belang van de sector en het publiek te behartigen.” <<

Over fraude: theoretisch kader *en* casuïstiek

We hoeven de krant maar open te slaan, naar het journaal te kijken of sociale media te volgen en we komen vele zaken tegen die over fraude, integriteit en ethiek gaan. In dit artikel een theoretisch kader en casuïstiek.

Mijn colleges begin ik steevast met een korte bespreking van de actualiteit. In de week waarin ik deze bijdrage schreef (december 2017) was het ook weer raak. Zo stonden diverse medewerkers van Volkswagen en Renault voor de rechter omdat zij ambtenaren bij de politie en defensie zouden hebben omgekocht. Daarnaast trok de rechtszaak tegen een voormalig directeur van woningcorporatie Laurentius en een architect de aandacht. Laatstgenoemde zou de directeur hebben omgekocht.

Een derde (omkopings)kwestie betreft het beursgenoteerde SBM Offshore. Deze onderneming betaalde via een schikking reeds honderden miljoenen dollars aan de Nederlandse en Amerikaanse justitiële autoriteiten. Vermoedelijk volgt nog een dergelijke schikking met de Braziliaanse autoriteiten. De reden? Het via handelsagenten betalen van steekpenningen teneinde grote opdrachten binnen te slepen.

Witwasbestrijding

Op het gebied van witwasbestrijding bestaan allerhande verplichtingen voor onder meer financiële instellingen, vrije beroepsbeoefenaren en handelaren in goederen van grote waarden (bijvoorbeeld schepen, kunst en antiek). De Amsterdam Trade Bank werd in 2017 geconfronteerd met een doorzoeeking van de FIOD op verdenking van het niet afdoende identificeren van cliënten en het niet naleven van de meldplicht ongebruikelijke transacties conform de Wet

ter voorkoming van witwassen en de financiering van terroristische activiteiten (Wwft). Grootbank ING en Damen Shipyards worden eveneens in verband gebracht met soortgelijke vergrijpen.

In de hoek van de vrije beroepsbeoefenaren werd een Amsterdamse notaris geschorst omdat er geld van de derdenrekening zou zijn verdwenen. Accountant Deloitte is onder het vergrootglas komen te liggen in verband met mogelijke verslaggevingstechnische fraude bij cliënt Steinhoff. Deze Zuid-Afrikaanse meubelgigant zou kampen met een gat in de balans van 6 miljard euro. De door de accountant goedgekeurde jaarrekening over 2016 is inmiddels ondeugdelijk verklaard en de jaarrekening over 2017 kan ook niet worden afgetekend. PwC kreeg van Steinhoff de opdracht tot het uitvoeren van een forensisch onderzoek en de Zuid-Afrikaanse toezichthouder op accountantsorganisaties gaat de rol van Deloitte onderzoeken. Tot slot eindig ik deze – overigens niet-limitatieve – opsomming met een verwijzing naar een aantal artikelen in *Het Financiële Dagblad* over Imtech en fraude met betrekking tot de bouw van een pretpark in Polen.

Kwetsbaar

Ondernemingen, medewerkers, overheden en overheidsinstellingen, burgers maar bijvoorbeeld ook computersystemen en digitale bestanden zijn vatbaar en kwetsbaar voor fraude



en andere integriteitsinbreuken. Onderwerpen die daarom zowel in de preventieve als repressieve zin continue aandacht vereisen. Van en in zowel de publieke als de private sector. En zeker van het controleursgilde en aanverwante beroepsgenoten. Bijvoorbeeld internal auditors en externe accountants, toezichthouders, controllers en compliance officers. Zij dienen kennis te hebben van fraude, de fraudedriehoek en frauderisicofactoren. Voorts is het van belang dat zij kennisnemen van fraudekwesities en methodieken.

Theoretisch kader

Fraude

Bij fraude denkt menigeen aan onderzoeken naar strafbare feiten, uitgevoerd door de politie of de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) onder leiding van de officier van justitie. Strafbare feiten die zijn omschreven in het Wetboek van Strafrecht. In dat wetboek ontbreekt echter het strafbare feit 'fraude' en/of een definitie van dat begrip. Wel vinden we in dat wetboek 'de moeder der fraudedelicten', namelijk: valsheid in geschrifte. En vele andere fraudedelicten zoals: (bedrieglijke) bankbreuk, oplichting en het openbaar maken van een onware jaarrekening.

De fraudedefinitie vinden we wél terug in accountantsregeling. In artikel 26 lid 2 van de Wet toezicht accountantsorganisaties (Wta) is een fraudemeldplicht voor accountants opgenomen en in lid 3 van dat artikel is bepaald dat in een algemene maatregel van bestuur (amvb) 'fraude' wordt gedefinieerd. Het Besluit toezicht accountantsorganisaties (Bta) is de amvb waar het dan om gaat. In artikel 36 Bta treffen we de definitie van fraude aan; daarin staan drie begrippen centraal, te weten: 1) opzet; 2) misleiding; 3) wederrechtelijk voordeel.

Fraudedriehoek

Criminologen bestuderen verschillende criminaliteitsvormen en doen onder meer onderzoek naar daad- en daderkenmerken. Met betrekking tot fraude is binnen dit vakgebied de zogeheten 'fraudedriehoek' ontwikkeld. De drie punten daarvan hebben betrekking op de elementen: 1) *druk* (ook wel: prikkel of stimulans); 2) *gelegenheid*; 3) *rationalisatie* (ook wel: rechtvaardiging). Deze elementen kunnen goed behulpzaam zijn bij het in beeld brengen van frauderisicofactoren die in acht moeten worden genomen bij het inrichten van een organisatie en het uitvoeren van in- en externe controle.

Frauderisicofactoren

Binnen de accountancy zijn diverse controlestandaarden opgesteld. Deze zijn vastgelegd in de 'Nadere Voorschriften Controlestandaarden' (NV COS). Daarbinnen bestaat een specifieke fraudestandaard, te weten NV COS 240. Het betreft een controlestandaard die is opgesteld voor externe accountants die controleopdrachten uitvoeren. Echter, het in NV COS 240 vervatte gedachtegoed is ook goed bruikbaar voor internal auditors. Met name bijlage 1 waarin diverse frauderisicofactoren worden benoemd. Deze worden ingedeeld naar risico's ten aanzien van twee categorieën: 1) frauduleuze financiële verslaggeving (veelal gaat het daarbij om directiefraude); 2) het oneigenlijk toe-eigenen van activa (veelal gaat het daarbij om werknemersfraude). In bijlage 1 van NV COS 240 worden de risico's per categorie ingedeeld conform de elementen uit de fraudedriehoek. Voorbeelden van 'druk of prikkels' betreft het hebben van significante financiële belangen en het kunnen behalen van een bonus. Bij 'gelegenheid' gaat het bijvoorbeeld om inadequate monitoring van de interne beheersingsmaatregelen en ineffectieve systemen voor administratieve verwerking. Een voorbeeld van 'rationalisatie' betreft de houding bij het management om administratieve afwijkingen te rechtvaardigen door te stellen dat deze niet-materieel zijn.

Niet de klant, maar de bonus van medewerkers en het management stonden centraal. Met alle kwalijke gevolgen van dien

Wells Fargo

September 2016 kwam in de Verenigde Staten een fraude bij de bank Wells Fargo naar buiten. Dat was acht jaar na de val van Lehman Brothers. Een val die het begin van een tijdperk kenmerkt waarin de bancaire sector plechtig beloofde de klant (weer) centraal te stellen. Niets bleek echter minder waar bij Wells Fargo. Medewerkers van de bank openden – zonder autorisatie van klanten – bankrekeningen op naam van bestaande klanten. Daarop werden gelden van die klanten overgeboekt om de rekeningen actief te doen lijken. Daarnaast werden credit en debit cards op naam van klanten gezet zonder dat zij dit wisten. Er werden zelfs pincodes voor het gebruik van deze kaarten aangemaakt.

In totaal ging het om meer dan 2 miljoen klanten op een totaal van 40 miljoen klanten die door deze werkwijze van bankmedewerkers werden geraakt. ‘Geraakt’ omdat zij de kosten van de ongeautoriseerde bankrekeningen en cards kregen doorbelast. Velen merkten dat niet eens en konden daardoor niet aan de bel trekken. In totaal hielden meer dan 5300 medewerkers op een totaal van bijna 270.000 medewerkers zich met deze praktijken bezig. Een fraude van ongekende schaal. Maar toch bleef deze lang onder de radar. Ondanks allerhande procedures, complianceregelingen, interne beheersingsmaatregelen en externe controle.

Internal auditors dienen kennis te hebben van fraude, de fraudedriehoek en frauderisicofactoren

De fraude vond plaats omdat medewerkers die de verkoopdoelstellingen niet haalden werden ontslagen. Medewerkers die de doelstellingen wel haalden of zelfs meer dan dat, kregen een forse bonus. Hiermee is zowel de negatieve als de positieve prikkel, ofwel het element ‘druk’, uit de fraudedriehoek gegeven.

De fraude kon plaatsvinden omdat de controlestructuren ontoereikend waren. Het management wist niet of wilde niet weten dat er werd gefraudeerd, omdat de effecten die van de negatieve en positieve prikkels uit zouden kunnen gaan niet werden gemonitord en gecontroleerd. Daarmee is ook het element ‘gelegenheid’ uit de fraudedriehoek gegeven. De leiding van Wells Fargo, bij monde van CEO John Stumpf, stelde in een interview in de *Wall Street Journal* dat de fraude volledig de schuld was van de betrokken medewerkers. In hetzelfde interview stelde hij dat er bij Wells Fargo geen prikkel was om slechte dingen te doen, dat het gedrag

van de betrokken medewerkers onacceptabel was en dat de bank geen cent op oneerlijke wijze wilde verdienen. Stumpf werd in een hoorzitting voor de Amerikaanse Senaat echter gegrild door senator Elizabeth Warren. Zij fileerde feilloos de bonuscultuur van Wells Fargo en toonde aan dat het management ‘cross selling’ tot de hoogste kunst had verweven. Het aantal producten per klant moest – aldus Stumpf – groeien tot minimaal 8. Een aantal dat niet was gebaseerd op klantbehoeften. Nee, Stumpf had eens gezegd ‘eight rhymes with great’. Het aantal producten per klant werd bepalend voor het verhaal naar buiten, naar beursanalisten en aandeelhouders. Hoe hoger het aantal producten per klant, hoe hoger de beurskoers. En de variabele beloning van de directie.

Senator Warren noemde het sturen op verkoopdoelstellingen en de bonuscultuur een ‘scam’. Stumpf dacht daar anders over. Hij hanteerde daarvoor tijdens de hoorzitting twee verweren – of beter in termen van het derde punt van de fraudedriehoek: rationalisaties. Ten eerste dat er geen sprake was van een ‘scam’ omdat het niet de bedoeling van de bankleiding was dat medewerkers zouden frauderen. Ten tweede zou er niets ongezonds zijn aan het pushen op verkoopdoelstellingen, want ‘cross selling is a way for deepening the relationship with clients’.

Oog hebben voor frauderisicofactoren

Er gaat geen week, wellicht zelfs geen dag, voorbij of we horen verhalen over fraude. Dus over ‘opzettelijke misleiding met het oogmerk om een wederrechtelijk voordeel te behalen’. Daarom is het van groot belang dat instellingen aandacht besteden aan fraudepreventie en in voorkomende gevallen fraudeonderzoek. Bij fraudepreventie speelt het controleursgilde, waaronder de doelgroep van het *Audit Magazine*, een belangrijke rol. Door oog te hebben voor frauderisicofactoren waarmee hun organisatie te maken heeft.

De fraudedriehoek – met daarin de elementen: druk, gelegenheid en rationalisatie – kan daarbij behulpzaam zijn (evenals bijlage 1 van NV COS 240). De casus Wells Fargo toont aan hoe belangrijk frauderisicofactoren en de fraudedriehoek zijn. In die casus was sprake van het aanzetten tot agressief verkoopgedrag en een ongezonde bonuscultuur. Daarin werden medewerkers opgejaagd, gesanctioneerd en beloond. Maar bovenal was er een gebrek aan adequate procedures, checks & balances en controle. Niet de klant, maar de bonus van medewerkers en het management stonden centraal. Met alle kwalijke gevolgen van dien. <<

Marcel Pheijffer is hoogleraar Accountancy aan de Nyenrode Business Universiteit en hoogleraar Forensische Accountancy aan de Universiteit Leiden.



Van het bestuur

Dit is mijn laatste column voor *Audit Magazine*. Zoals in het vorige nummer al aangegeven, neemt Jantien Heijmel tijdens de ALV op 17 mei 2018 het stokje van mij over. Na ruim zes jaar IIA-bestuur, waarvan ruim twee jaar voorzitterschap, is dat goed. Naast mij neemt ook Winfried Beekmans na zes jaar afscheid. Ik heb er alle vertrouwen in dat het bestuur ook zonder ons gewoon doorgaat, omdat ze de historie en principes achter eerdere besluitvorming goed kennen. En zo niet, dan weten ze Winfried of mij nog wel te vinden. De ALV is bij ABN AMRO en we geven na afloop een afscheidsdrankje weg, dus meld je aan. Gezellig!

Het thema voor dit nummer is wederom heel uitdagend en ik ga hem van a tot z lezen. Niet omdat ik nu meer tijd heb, maar vooral omdat ik iets heb met het thema. Daarbij is het overigens wel goed om een duidelijk onderscheid te maken tussen fraude en integriteit. Minder of niet-integer gedrag valt uiteraard nooit goed te praten, maar is ook lang niet altijd fraude.

Toen ik in 1982 begon als 'Rijksaccountant' bij de Belastingdienst Amsterdam, had je als Rijksaccountant ook opsporingsbevoegdheid. Daarvoor leerden we op de 'dienstopleiding' alles over sfeerovergang; het moment waarop je van een administratief-rechtelijk onderzoek overging naar een strafrechtelijk onderzoek. Heel spannend natuurlijk, zeker als je 21 bent en wel in bent voor wat actie. Eenmaal in de praktijk duurde het nog wel een paar jaar, maar in 1985 was het dan eindelijk zover bij een boekenonderzoek in de seksindustrie. Voordat jullie eventuele 'dirty mind' de kans krijgt: het onderzoek vond uiteraard volledig overdag plaats, hoewel ik mij

nog herinner dat ik samen met een collega achterin de BMW 7-serie van de vuurgevaarlijke bordeeeigenaar zat op weg naar diens villa om het kassaldo te tellen. Dat moest controletechnisch natuurlijk op een zogenaamd 'overvalsmoment', maar het geld was niet op 'kantoor' en dus moesten we met hem mee. Helemaal veilig voelde dat niet, weet ik nog. Toen we later een 'vermoeden van fraude' hadden, hebben we het boekenonderzoek keurig stilgelegd, vooroverleg met de officier van justitie en de FIOD gehad en zijn we daarna doorgeshaard met het strafrechtelijk onderzoek. Een ervaring waar ik nog lang een mooi verhaal door had.

Als internal auditor in de financiële sector ben ik daarna eigenlijk altijd met het onderwerp integriteit bezig geweest. Het belang daarvan nam toe en werd een wezenlijk onderdeel van ons werk. Langzaam kregen we door dat meer regels geen oplossing zouden bieden voor het niet-integer gedrag dat in alle lagen van financiële instellingen werd geobserveerd en later zouden leiden tot een gebrek aan vertrouwen van de klant en tot toename van aandacht voor cultuur en gedrag, ook voor en door de internal auditor.

Natuurlijk ben ik als internal auditor nog tegen fraude aangelopen. Met verdeeld genoegen overigens, omdat de regels rondom persoonsgebonden onderzoek voor registeraccountants inmiddels vrij strak waren geworden. Het recht op transparantie en hoor en wederhoor voor de onderzochte persoon, is natuurlijk goed om een heksenjacht te voorkomen, maar maakt het onderzoek soms erg lastig. In mijn periode als chief audit executive bij SNS REAAL onderzochten we – samen


met de interne compliance & intelligenceafdeling – een fraude die door een tijdelijke property finance restructuringdirecteur werd gepleegd, maar waarbij ook diverse andere externe partijen waren betrokken. Toen het onderzoek – door een lek – uitgebreid de pers haalde en de FIOD zelf onderzoek wilde doen, nam de druk vanuit directie en raad van commissarissen begrijpelijkerwijs behoorlijk toe. Ze wilden worden geïnformeerd, maar we konden en mochten pas mededelingen doen als het onderzoek daaraan toe was. En hoor en wederhoor werd wel erg lastig toen de hoofdpersoon in de cel belandde en ook anderen door de officier van justitie van hun bed werden gelicht. Terugkijkend was dat een zeer leerzame periode, in meerdere opzichten, waarbij het achteraf goed bleek te zijn geweest de vaktechnische voorschriften nauwgezet na te leven.

Mijn advies aan jullie is om altijd te doen wat we in 1985 als Rijksaccountant deden. Zodra je een vermoeden van fraude hebt, en je hebt de tijd ervoor, neem dan een pauze om gedegen te bepalen wat je vervolgstappen moeten zijn. 'Better safe than sorry', ook in het belang van degene die je onderzoekt.

Veel leesgenoegen!



John Bendermacher is
voorzitter van het IIA.



Richard Bistrong pleegde jarenlang fraude. Nadat hij zijn straf in de gevangenis had uitgezeten, besloot hij om zijn ervaring en kennis te gebruiken voor advieswerk op het gebied van corruptie en compliance issues. Een interview over het waarom.

Fraude: hoe raak je erin verzeild?

Waar ging het fout?

“Mijn eerste jaren in het bedrijf waren in de vrijwel risicooloze omgeving van de binnenlandse Amerikaanse markt. Het bedrijf wilde uitbreiden naar de internationale markt en aanzien ik een achtergrond heb in buitenlands beleid, kreeg ik de kans om de internationale verkopen te gaan doen.

Vlak voor ik naar het buitenland zou vertrekken gaf het bedrijf mij een exemplaar van de ‘FCPA’, de Foreign Corrupt Practices Act. Deze moest ik begrijpen. Het was mij duidelijk, ik begreep volledig wat er stond en bedoeld werd.

Terugkijkend naar het moment dat ik voor het eerst de fout in ben gegaan, is dat denk ik een gesprek geweest aan het begin van mijn internationale loopbaan.

Ik was in Zuid-Amerika en ik had een ontmoeting met mijn lokale agent. In de internationale verkopen wordt vaak gebruikgemaakt van een lokale agent/vertegenwoordiger. Je hebt zo iemand nodig om je producten lokaal te kunnen verkopen. Ik had geen enkele indicatie dat deze persoon corrupt was. Je zou hem niet terugvinden in de Panama Papers, hij deed alle dingen die je van een legitieme agent zou verwachten. We praatten over een grote aanbesteding die eraan zat te komen. Terloops deelde hij mij mee dat zijn succes mede kwam omdat hij ‘tol’ betaalde om aanbestedingen te winnen. Ik wist meteen wat hij bedoelde met ‘tol’. Gedurende al die jaren dat ik in de internationale verkoop zat heb ik zoveel verschillende benamingen gehoord om omkoping te beschrijven: ‘tol’, ‘zorgen voor mensen’, ‘mensen blij maken’, ‘zonnestraalbetalingen’, maar het enige woord dat ik nooit gehoord heb om omkoping te beschrijven is: omkopen.

Ik kan mij dit gesprek goed herinneren omdat hij mij niets vroeg. Hij deelde het gewoon mee. En ik dacht: oké, ik weet dat het fout is, maar het is slechts een ‘red flag’ als ik er een red flag van maak. En ik wil deze komende aanbesteding winnen.

De wetenschap van de ‘tol’ en het schudden van mijn hoofd betekende wel dat ik de FCPA overtrad. Als ik mijn bedrijf had gebeld en had beschreven wat er was gebeurd, zou dat een lastig gesprek geweest zijn omdat we vaker met omkoping zouden worden geconfronteerd. Dat zou betekenen dat we onze verkoopstrategie moesten heroverwegen. De vraag is dan of we ons wel in bepaalde markten moesten begeven. De enige vraag echter die ik mezelf stelde was: zouden ze het echt willen weten?”

Zegt dit ook iets over de bonusstructuur van uw bedrijf?

“Het schandaal van Wells Fargo waarbij neprekeningen werden geopend, leidde tot veel aandacht voor de effecten van bonussen. In elk bedrijf is er een natuurlijke spanning tussen de druk van prestatie en de druk van compliance. Daar is ook niets mis mee. De vraag is echter hoe met deze spanning om te gaan. En na te denken over wat er gebeurt als de financiële bonussen op te behalen doelstellingen dermate agressief zijn dat het ertoe kan leiden dat mensen gevaarlijke of verkeerde beslissingen kunnen nemen. Dat is een uitdaging.

Financiële druk kan grote invloed hebben op de beslissingen van mensen. Bonussen geven een duidelijke, onuitgesproken boodschap over het doel van een bedrijf. En de boodschap van een bonus zal geprefereerd worden boven elke papieren boodschap over ethiek en compliance. Idealiter zal er een open discussie met alle functies dienen plaats te vinden over de druk van financiële bonussen, de risico’s daarvan en

hoe daarmee om te gaan. Bonussystemen kun je vergelijken met de bijsluiters van medicijnen. Alles heeft neveneffecten. GlaxoSmithKline heeft haar bonusmodel totaal op de schop gegooid na grote problemen in China. Ik zie nu dat ‘hoe zaken worden gedaan’ een even belangrijk deel uitmaken van een bonussysteem als ‘het bereiken van doelstellingen’. De risico’s van een markt zijn deel gaan uitmaken van een bonussysteem. Dat is een goede ontwikkeling.”

Wat waren uw motieven om ‘tol’ te betalen?

“Mijn motieven waren divers. Een aspect was dat ik totaal niet dacht aan de consequenties van mijn gedrag. Tegenwoordig beschrijft de website van Transparency International de schadelijke langetermijnpact van omkoping. Maar in mooie business class lounges en hotellobby’s zaten de slachtoffers van omkoping niet in mijn hoofd. Ik verkocht militaire benodigdheden die van prima kwaliteit waren. Ik zat niet te prutsen aan kogelwerende vesten. Dus ik dacht: mijn bedrijf behaalt goede verkoopcijfers, ik behaal mijn verkoopdoelstellingen en mijn bonus en de agent is tevreden. En bovendien, in sommige delen van de wereld worden ambtenaren zeer slecht betaald, dus waarom hen niet wat extra betalen zodat ze de eindjes aan elkaar kunnen knopen? Het is een win-winsituatie voor iedereen.

In deze gedachten zit het concept van eigenbelang-altruïsme. Als we denken dat ons eigen onethisch gedrag anderen helpt, zien we dit gedrag als moreel acceptabel. Professor Francesca Gino van Harvard heeft hier interessant onderzoek naar gedaan. Mijn motieven waren dat ik niemand kwaad deed, dat ik mij conformeerde aan lokale normen – dit was blijkbaar de manier waarop zaken lokaal werden gedaan – en ook financiële kant speelde mee: ik had een lucratieve bonusregeling. Ik wilde slagen en dit was de manier om mijn doel te bereiken. En ik werd tien jaar lang als een succesvol persoon gezien omdat mijn slechte gedrag verborgen bleef achter goede prestaties. De markt vertoonde neerwaartse cijfers, maar ik slaagde erin om de verkopen te laten stijgen. Niemand in het bedrijf stelde vragen over mijn prestaties.”

Wat had uw bedrijf anders kunnen doen?

“Allereerst voor alle duidelijkheid: ik ben degene die verantwoordelijk is voor de gepleegde omkoping. De rationalisatie die ik hier beschrijf komt van mij. Het bedrijf valt hierin niets te verwijten. Maar de vraag is inderdaad terecht, wat had mij tegen kunnen houden? Het moment van het gesprek in Zuid-Amerika was te laat. Maar stel je voor dat – voordat ik mijn eerste vlucht nam – iemand van het bedrijf, niet zijnde de juridische-, audit- of compliancepersoon, maar iemand van de business die winstverantwoordelijkheid had,

Over...

Richard Bistrong, CEO, Front-Line Anti-Bribery LLC
www.richardbistrong.com
richardtbistrong@gmail.com

iemand die een stem had in mijn prestatie-evaluatie, mij gewaarschuwd zou hebben voor datgene wat zeker zou gaan gebeuren? Dat ik corruptie zou ervaren. En dat nee zeggen tegen omkoping mij niet voldoende handvatten zou geven. In sommige plaatsen gaat het zover dat nee zeggen als aanvallend beschouwd wordt en je in onveilige situaties kan brengen. Dus het zou een conversatie moeten zijn over hoe ethisch gedrag te operationaliseren, inclusief een gesprek over wie mij kan steunen ter plekke en hoe mij te gedragen om succesvol, veilig en integer te zijn. Het zou een conversatie moeten zijn over scenario's waarin ik geconfronteerd zou kunnen worden met dilemma's. In dit gesprek zou ook de financiële bonus besproken moeten worden. Deze bonus zou geen 'eat what you kill'-prestatie-regeling moeten omvatten, maar gebaseerd moeten zijn op hoe het bedrijf als geheel presteert. Immers, een ethisch duurzaam verkoopmodel vergt in sommige markten meer tijd, dus moet de prestatieregeling hierop aansluiten. Dit zou geen gesprek zijn over ethiek, noch over compliance. Dit zou een gesprek zijn over leiderschap. Ethisch handelen en compliance worden zichtbaar door leiderschap. Niemand zou een dergelijke conversatie vergeten."

Wat zou de rol van Internal Audit kunnen zijn?

"De meeste auditprogramma's zijn gebaseerd op risico's. Bij zo'n aanpak worden veel risico's gemist. Wij kunnen ons druk maken binnen het bedrijf over de risico's die het werken met andere partijen met zich meebrengt en de gevaren voor een multinational. Echter, buiten het bedrijf denken agenten hier niet zo over. Zij achten deze westerse anti-cor-

hun pensioen. Met andere woorden, ze zouden zeer openstaan voor omkoping. Dit laat zien dat het enkele feit van verkiezingen effect heeft op risico's. Het belang van monitoren is cruciaal. Een risicobeoordeling gebaseerd op 'won and done' en 'vet and forget' is onvoldoende.

Auditors kijken naar allerlei data. Maar we vergeten vaak om ons instinct, de beste auditor tool die er is, in te zetten. Auditors zouden beter naar de omstandigheden moeten kijken. Ik kreeg bijvoorbeeld ooit een order onder ogen voor een grote hoeveelheid granaten voor een klein vredelievend Caribisch eiland. Het land had deze granaten niet nodig en de prijs was boven de marktprijs. Ik hoefde geen vragen te stellen om te weten dat hier sprake was van omkoping. En deze order is behandeld door de verkoopadministratie, financiën, debiteurenadministratie, de producten zijn gefabriceerd en verzonden. Niemand zag red flags, maar de hele order zelf was een red flag. Hierdoor vraag je je af of de mensen in verkoopadministratie, fabricage, logistiek, het maakt niet uit waar in de organisatie, zich ambassadeur voelen van ethisch handelen. Zij zien tenslotte veel en kunnen een signaal geven als zij iets niet vertrouwen. Ook Internal Audit heeft een rol om iedereen in de organisatie te betrekken. Integriteit en ethisch handelen is te veel in silo's gegoten."

Ethisch handelen en compliance worden zichtbaar door leiderschap

ruptiemaatregelen irrelevant voor hun maatschappij. Zij zien generositeit en het delen van giften als deel van hun cultuur. Sommigen zullen het zelfs zien als legaal of op zijn minst als tolerabel. Nu komt het auditprobleem. Als agenten een stuk papier gepresenteerd krijgen waarin zij ondertekenen dat zij zich conformeren aan anti-corruptiemaatregelen, zullen zij dit met liefde ondertekenen omdat zij het niet serieus nemen. Immers, als alles wat tussen hen en het zaken kunnen doen met een westerse multinational een stuk papier is, is de keuze duidelijk. Denken dat een contract op papier dit risico kan mitigeren is misleidend, want contracten in deze context hebben geen waarde. Auditors houden zichzelf voor de gek als ze hieraan vasthouden.

Daarnaast wordt te veel waarde gehecht aan de status op een bepaald moment. Veel bedrijven hebben robuuste due-diligenceprocedures. Echter, zodra een derde partij is geaccepteerd, is er te weinig aandacht meer voor wat daarna gebeurt. Een due diligence neemt een foto van gedragingen en activiteiten, maar de wereld verandert voortdurend. Ooit belde een agent mij op. Hij vertelde mij dat er een nieuwe president was gekozen, die een nieuwe minister van Defensie zou aanstellen en deze minister zou weer allemaal nieuwe mensen bij Inkoop aanstellen. De agent vervolgde zijn verhaal dat deze nieuwe mensen goede vrienden van hem waren en dat zij maar enkele jaren te gaan hadden tot

Had een auditor uw omkoping kunnen ontdekken?

"Ik denk niet dat een auditor enige red flags ontdekt zou hebben wat betreft mijn transacties, vanwege de lage commissies en de locaties waar ze plaatsvonden (inclusief New York en Nederland). Maar als je mijn gedrag vanaf een wat hoger niveau zou bekijken, dan zou je een hoop inconsistenties zien, zoals mijn marketingkortingen, marketingvergoedingen, succes fees en commissiestructuur. Alles bij elkaar zou het geen consistente dataset zijn. En dan zou aan mij in ieder geval de vraag gesteld moeten worden hoe ik het klaar speel om zo succesvol te zijn? En dat, zolang er geen goede verklaring is, ik beknot zou worden in mijn autonomie. Maar in de praktijk gebeurde het tegenovergestelde: hoe meer succes ik boekte, hoe meer autonomie ik kreeg."

Ik was verrast dat u ook omkocht in Nederland!

"Ja dat klopt. Vanuit een auditperspectief kun je zeggen dat er hoge-risico- en lage-risicolanden zijn, maar er zijn geen landen zonder risico. De Nederlandse casus was geen andere dan die in andere landen. De Nederlandse intermediair presenteerde mij een mogelijkheid tot omkoping om zo een deal te winnen en ik stemde hiermee in. In dit geval was het een politiefunctionaris van wie ik in ruil voor 15.000 dollar belangrijke informatie kreeg om een aanbeveling te kunnen winnen van het KLPD (Korps Landelijke

We vergeten vaak om ons instinct, de beste auditor tool die er is, in te zetten



Politiediensten). Maar om duidelijk te zijn, niemand dwong mij om de wet te overtreden en bedriegen was een keuze. Het feit dat de intermediair mij deze mogelijkheid voorstelde, maakt mij niet minder medeplichtig of schuldig voor wat ik heb gedaan en hiervoor ben ik veroordeeld. Ik was immers degene die 'ja' zei."

Is het wel verstandig om gebruik te maken van een agent?

"Dat is een terechte vraag waar veel bedrijven mee worstelen. Het aannemen en managen van een globaal verkoopteam is duur. Agenten werken op een succes fee, dus je hebt geen vaste kosten. Maar agenten zijn de achilleshiel van een complianceprogramma. Kijkend naar het Unaoil-schandaal is het geen verrassing dat sommige bedrijven besloten hebben om geen gebruik meer te maken van agenten."

Zouden auditors niet meer betrokken moeten zijn vooraf?

"Er is nu veel discussie gaande of internal auditors meer betrokken moeten zijn bij anti-corruptieprogramma's. In sommige afgelegen delen van de wereld hebben bedrijven wellicht geen lokale compliance officer, maar wel een internal auditfunctie. Daar kan het een goede oplossing zijn dat auditors een meer actieve rol nemen als ambassadeur van ethische normen. Ik denk dat het goed is om de bestaande werknemerspoule te gebruiken in afgelegen regio's en risk en compliance crossfunctioneel te benaderen. Daarnaast kan Internal Audit natuurlijk transacties scannen en reviewen om te voorkomen dat in het bedrijf illegale transacties plaatsvinden."

Kan Internal Audit ook een rol spelen om verkoopprognoses te beoordelen op realiteit?

"Als doelen en bonussen worden besproken, moeten diverse functies betrokken worden, niet alleen de business. Audit hoort daarbij. De business zal focussen op te behalen doelstellingen, maar je hebt ook mensen nodig die dan de vraag stellen hoe de doelstellingen behaald gaan worden. En dan zal vanzelf spanning ontstaan tussen de druk van compliance en de druk van succes. Dit is prima zolang het een gezonde spanning is waar iedereen betrokken is om die spanning te ontrafelen. Immers, spanning is inherent aan een gezonde organisatiestructuur, het gaat er alleen om hoe met de spanning om te gaan."

Geloof u nog in de goedheid van de mens?

"De Wereldbank heeft geschat dat per dag zo'n 100 miljoen dollar omgaat in omkoping. Dat betekent dat er een robuuste vraag is naar omkoping. In veel landen worden ambtenaren onderbetaald, onvoldoende getraind en zijn de regels om zaken te doen niet eenduidig en niet transparant. Zo'n omgeving creëert een dynamiek dat mensen zullen aanbieden om tegen betaling zaken gedaan te krijgen. Maar we gaan zeker een goede kant op. Dat komt ook door schandalen zoals bij Wells Fargo en Volkswagen, waar raden van bestuur

betrokken raken bij ethische onderwerpen en concluderen dat hun reputatie belangrijker is dan de baten van het winnen van een markt. Zeker onder westerse multinationals heerst nu het besef dat omkoping een probleem is. In Brazilië is door het Petrobras-schandaal het hele landschap aan het veranderen, omdat mensen na decennia van straffeloosheid corruptie eenvoudigweg niet meer accepteren. In China wordt binnenlandse corruptie vervolgd, maar gaat internationale corruptie gewoon door. Dus we moeten ook erkennen dat sommige handel gewoon niet gewonnen kan worden door bedrijven die weigeren mee te doen aan omkoping. Maar als bedrijven geduldig zijn, vertrouwen hebben in hun merk en toegewijd zijn aan op lange termijn ethisch en duurzaam zakendoen, dan komt succes vanzelf!"

Een tip om corruptie tegen te gaan?

"Dat is een persoonlijke. Als je ver weg bent in afgelegen gebieden is het makkelijk om los te raken van je familie en vrienden. Probeer dichtbij hen te blijven. Als je worstelt, gestrest bent en dilemma's hebt waar je niet uitkomt, dan is het goed om naar huis te bellen. Luister naar de voor jou vertrouwde stemmen en realiseer je dat je beslissing ook effect heeft op hen. Bel daarna je leidinggevende of de complianceafdeling. Betrek hen in je dilemma en probeer er samen uit te komen. Als je samen probeert te komen tot de beste oplossing, is de kans het grootst dat je de juiste beslissing neemt. Maar dat betekent ook dat je vooraf die relaties gelegd moet hebben zodat je weet dat je met een gerust hart je dilemma kan bespreken. En voor Audit en Compliance is het belangrijk om af en toe een beetje kwetsbaarheid te tonen. Praat met en vraag de mensen in het veld in stabiele tijden naar de risico's waar zij mee te maken hebben. Want als de momenten van stress er zijn, is het belangrijk dat ze weten wie ze kan helpen. Dat is uiteindelijk de baten van een bedrijf, het voelen dat je samen een team bent." <<

SIO: een kader voor integere organisaties

Klanten kiezen steeds meer voor een bedrijf dat ze vertrouwen. Medewerkers willen werken bij een organisatie waar ze trots op zijn. Beleggers geloven dat investeren in betrouwbare, ethische bedrijven veiliger is. Het investeren in integriteit loont dus. Om integriteit binnen een organisatie te verankeren en te managen is het Stimuleringskader Integere Organisaties (SIO) ontwikkeld.

Vertrouwen ontstaat als een organisatie integer handelt. Dit betekent bijvoorbeeld verantwoordelijkheid nemen voor fouten, transparant zijn over de activiteiten, hoogwaardige goederen en diensten leveren, en – in de marktsector – reële waarde teruggeven aan de aandeelhouders. Integriteit wordt van alle organisaties verwacht en integriteitsmanagement helpt om hieraan te voldoen. Integriteitsmanagement is het planmatig bevorderen van de integriteit van een organisatie. Een organisatie is integer wanneer zij eerlijk en betrouwbaar is en wanneer zij zorgvuldig, consistent en uitlegbaar handelt ten aanzien van de rechten en belangen van haar stakeholders.

Stimuleringskader Integere Organisatie (SIO)

Het SIO is in 2010 ontwikkeld door drs. Maarten de Jong (voormalig oprichter/directeur van het Department of Institutional Integrity bij de Wereldbank in Washington), Ronald Jeurissen (hoogleraar Business Ethics op de Nyenrode Business Universiteit) en Bastiaan Odijk (integriteitsexpert met een bedrijfskundige achtergrond). Zij kwamen tot het inzicht dat er geen integriteitsformat bestond waar organisaties aan konden refereren, een kader met alle elementen om te komen tot een integraal integriteitsmanagementsysteem. De krachten werden gebundeld en de kennis werd samengebracht.

Het SIO is mede gebaseerd op de 'Ethics Related Actions' van het Amerikaanse National Business Ethics Survey en op de bekende Federal Sentencing Guidelines van de Amerikaanse federale overheid. Tijdens het ontwikkelingsproces haakte ook mr. Arthur Docters van Leeuwen (ex-bestuursvoorzitter AFM) aan. Het normenkader is ondergebracht in de stichting SIO als beheerder en promotor hiervan. Het ministerie van Justitie en Veiligheid zag de potentie van dit kader en heeft dit initiatief gesubsidieerd. Het SIO-normenkader is voor iedere organisatie gratis op te vragen en te gebruiken.¹ Het SIO is een objectief bewijsmiddel om vast te stellen

dat een bedrijf of organisatie een managementsysteem heeft dat de voorwaarden schept om integriteit (beleid) structureel te verankeren in de bedrijfsprocessen. Stakeholderverwachtingen en maatschappelijke eisen zijn in het SIO van doorslaggevende betekenis. De SIO-norm is geïnspireerd op leidende (inter)nationale theoretische en praktische conceptualisering van integriteitsmanagement en daarop gebaseerde richtlijnen. Het beheer van de SIO-norm wordt door een onafhankelijke partij gefaciliteerd.

Het SIO:

- komt tegemoet aan de wens van leidinggevenden om hun organisatie in een verantwoorde en duurzame ontwikkeling te brengen;
- helpt organisaties om praktijken te vermijden die risico's vormen voor het bedrijf of de industrie;
- helpt om deze onverantwoorde praktijken onder de loep te nemen, zodat ze snel kunnen worden beëindigd;
- identificeert potentiële schade aan reputaties en ethische bedreigingen en biedt aanbevelingen om deze bedreigingen te verminderen;
- kan worden toegepast op alle particuliere bedrijven (zowel mkb's als multinationals) en openbare instellingen.

Het verkleinen van de kans op reputatieschade

Een goede combinatie van cultuur- en structurelementen laat een organisatie beter presteren. Het verkleint de kans op reputatieschade. Door zorgvuldig te investeren in mensen, organisatiecultuur en -structuur nemen op den duur ook de kosten voor controles, onderzoeken en eventuele geschillenprocedures af. Het management geeft hierbij de toon aan. Het gedrag, de houding en de woorden van het leidinggevend kader (tone at the top) zijn voor de medewerkers van groot belang.

Ontwikkelingsniveaus en kenmerken

Het SIO onderkent drie ontwikkelingsniveaus:

Niveau 1 – Voorbereiding

Niveau 2 – Bewustwording en cultuur

Niveau 3 – Samenwerking en Integratie

Elk niveau bezit zijn eigen kenmerken. Deze kenmerken zijn onderverdeeld in algemene en stakeholdersmanagement eisen. De kenmerken zijn hieronder in het kort beschreven:

Niveau 1 – Voorbereiding

De organisatie heeft de sterke en zwakke kanten van de integriteitscultuur en -structuur, de stakeholders en betrokken in kaart gebracht. Bovendien heeft de organisatie beleid en strategie ten aanzien van de ontwikkeling naar niveau 2 vastgelegd.

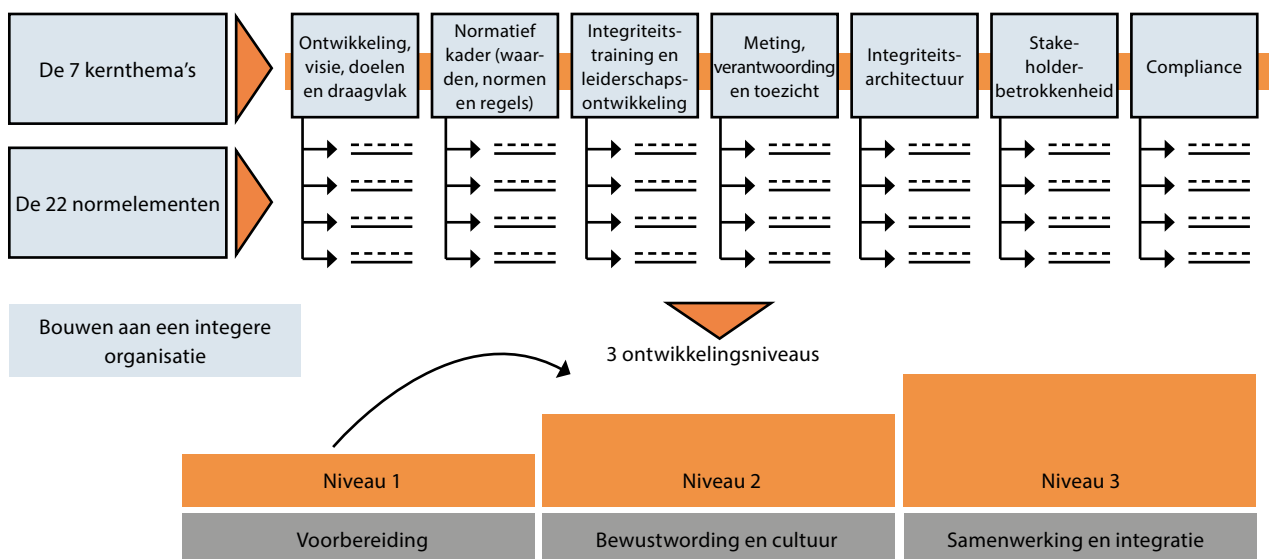
Niveau 2 – Bewustwording en cultuur

De organisatie richt zich op de ontwikkeling van moreel leiderschap in de organisatie en de bewustwording van de medewerkers. De organisatie heeft de stakeholders betrokken en is aantoonbaar bezig met het vastleggen, implementeren en borgen van beleid en normelementen voor het SIO met als doel niveau 3 te bereiken.

Niveau 3 – Samenwerking en Integratie

De organisatie heeft de voor niveau 3 gestelde doelen voor integriteitsmanagement bereikt. Planmatig is vormgegeven aan integere samenwerking met relevante stakeholders. De belangrijkste voorwaarden voor een integere organisatiecultuur zijn gerealiseerd en geborgd. De organisatiecultuur en -structuur is waar nodig zodanig aangepast dat integer gedrag wordt ondersteund en gestimuleerd.

Voor elk van de drie niveaus worden in het SIO zeven kernthema's van integriteitsmanagement onderscheiden. De kernthema's zijn een samenvatting van thema's uit belangrijke publicaties over de integrale managementbenadering van integriteit. De 7 kernthema's van het SIO zijn geoperationaaliseerd in 22 normelementen. Die normelementen dienen als basis voor de omschrijving van concreet meetbare en auditeerbare kenmerken waaraan het integriteitsmanagement zou moeten voldoen. Het SIO kan dus ook als instrument functioneren voor een internal auditfunctie om integriteit binnen een organisatie te onderzoeken. Zie *figuur 1*.



Figuur 1. De zeven kernthema's van het SIO

Door zorgvuldig te investeren in mensen, organisatiecultuur en -structuur nemen de kosten voor controles, onderzoeken en geschillenprocedures af

Toepassingsgebied

De SIO-norm is van toepassing op alle bedrijven en organisaties die zich richten op het systematisch ontwikkelen en borgen van integriteitsbeleid. Desgewenst kan deze ontwikkeling worden gecertificeerd. De SIO-certificatieaudit richt zich op het SIO als managementsysteem. Certificatie van het managementsysteem betekent dat de condities voor integer gedrag van werknemers zijn geoptimaliseerd. Het biedt echter geen garantie dat onethisch of niet-integer gedrag niet meer voorkomt of voor zal komen in het gecertificeerde bedrijf of organisatie. De kans daarop is wel drastisch verminderd.

Ter ondersteuning van organisaties met de implementatie van de SIO-norm, biedt de stichting SIO twee maal per jaar een SIO-leergang aan. Hierin wordt ingegaan op alle aspecten van integriteit binnen het kader

Certificaat

De SIO-certificatienorm is een norm voor een managementsysteem. Specifieker gezegd, een norm voor een integriteitsmanagementsysteem. De cyclus plan-do-check-act staat daarin centraal. De SIO-certificatienorm stelt naast deze uitvoeringscyclus ook eisen aan de resultaten van het integriteitsmanagementsysteem. De organisatie verbindt zich bijvoorbeeld aan de eis tot continue verbetering.

Deze eis gaat verder dan de plan-do-check-act-cyclus. De organisatie heeft een eigen verantwoordelijkheid voor het analyseren van alle relevante integriteitsaspecten. Het maken en uitvoeren van beleid ter voorkoming van integriteitsschendingen en het optimaliseren van de condities voor integer gedrag. Niet alleen de eigen activiteiten dienen in ogenschouw te worden genomen maar ook de samenwerkingsprocessen binnen de keten waarop redelijkerwijs invloed uitgeoefend kan worden.

Op basis van de SIO-certificatienorm kan op de drie ontwikkelingsniveaus een certificaat worden afgegeven, naar gelang het resultaat van de audit. Voor de niveaus 1 en 2 is dit certificaat twee jaar geldig, met als doel de organisatie verder te ontwikkelen en het SIO-certificaat niveau 3 te behalen. Het Integriteitscertificaat op niveau 3 is drie jaar geldig en wordt elke drie jaar opnieuw door een door de Stichting SIO geregistreerde certificatie-instelling vastgesteld of bijgesteld. Het behaalde en vastgestelde niveau wordt op het certificaat vermeld.

Doordat financiële instellingen onder toezicht staan is tevens besloten het kader bij Lloyds Registers neer te leggen om de mogelijkheden tot auditeerbaarheid te bekijken. Lloyds Registers concludeerde dat het normenkader voldeed aan alle eisen van auditeerbaarheid. Hiervoor worden social of behavioral audits gebruikt. Kiest een organisatie voor certificatie, dan biedt dat tevens de mogelijkheid om een andere vorm van toezicht te verwerven door de nationale toezichthoudende autoriteiten. <<

Noot

1. Het volledige overzicht en de uitwerking van de kernthema's en normelementen is kosteloos op te vragen via de website van de stichting SIO. www.stichtingsio.nl

advertentie

nieuwe economie nieuwe perspectieven

Om succesvol te ondernemen moet je wendbaar zijn. Corporate agility, noemen we dat bij BDO. Dat betekent ook: klaar zijn voor de nieuwe privacywetgeving vanaf 25 mei. BDO helpt u hier graag bij met de juiste kennis én mankracht. Zo wordt u niet alleen GDPR compliant, maar creëert u ook meteen nieuwe perspectieven op uw informatiemanagement.

Kijk voor meer informatie op
www.bdo.nl/privacy

BDO

Natascha Rol is oprichter van MoresMundi. Moresmundi adviseert organisaties over de implementatie van het SIO. Daarnaast ondersteunt zij de Stichting SIO in het beheren en promoten van het Stimuleringskader Integere Organisatie.



De IAF moet geen fraudeonderzoek uitvoeren

Arjen van Nes
Zelfstandig interim programmamanager (Nationale Politie, Royal Flora Holland)

Ja Nee

Zou het fraude zijn of misschien een domme fout? Kan ik daar wel antwoord op geven? Moet ik niet eerst nog wat extra vragen stellen? Zal ik dat op de afdeling doen, of alarmeer ik dan iemand? Kan ik ergens anders terecht? Moet ik dan vooraf aangeven dat het vertrouwelijk is? Zouden ze zich daaraan houden? Als het fraude is, zou dan iemand van die andere afdeling ook betrokken kunnen zijn? Zal ik via IT in bestanden gaan kijken? Wat zegt het IPPF er eigenlijk over? En de NBA handreiking 1137? Fraudeonderzoek kan heel snel heel fout gaan: zoek ondersteuning!

Nicolette Verburg-Siebrasse
Internal auditor bij Universiteit Utrecht

Ja Nee

Ik ben tegen deze stelling. Hoewel in de Standards staat dat de auditor geen expert hoeft te zijn op het gebied van fraude, zou dit de auditor er niet van moeten weerhouden zelf fraudeonderzoek te doen. De auditor dient wel bij elk fraudeonderzoek een afweging te maken of de auditor voldoende is geëquipeerd om dit onderzoek zelf uit te kunnen voeren of dat hij hier beter een expert voor in kan huren. Daarnaast dient de auditor een afweging te maken in welke context het fraudeonderzoek plaatsvindt en of er geen sprake is van belangenverstrengeling en/of een groot afbreukrisico voor de IAF.

Serge van Herpen
Internal auditor bij IND

Ja Nee

Ik ben van mening dat een IAF terughoudend moet zijn bij het zelf uitvoeren van onderzoeken die grote directe

persoonlijke/personeelsconsequenties kunnen hebben. In het meest gunstige geval heeft een organisatie een afdeling/-functionaris die gespecialiseerd/verantwoordelijk is voor fraudeonderzoeken en de IAF kan dan zijdelings betrokken zijn. Ontbreekt deze gespecialiseerde afdeling, dan kan de IAF een rol spelen bij het namens het bestuur/directie verstrekken van een externe opdracht tot fraudeonderzoek aan een gespecialiseerd bureau. Zijn er specifieke redenen dat externe inhuur niet mogelijk is en is daarnaast het fraude-risico hoog, dan zou een IAF met de nodig terughoudendheid, waarborgen en voorzichtigheid het onderzoek kunnen uitvoeren.

Brigitte de Vries
Internal auditor bij Staedion

Ja Nee

Bij deze stelling spelen wat mij betreft drie vragen: moet het, kan het en wil ik het?

Moeten: nee. De standaarden schrijven voor dat de mogelijkheid van fraude meegenomen moet worden bij alle onderzoeken en dat de risicobeheersing van frauderisico's periodiek geëvalueerd moet worden.

Kan het: zijn kennis en vaardigheden voor dit soort onderzoeken aanwezig? Naar mijn mening vereist dit soort onderzoek kennis en vaardigheden die niet in de algemene opleiding aan de orde komen.

Wil ik het: wat betekent het voor de IAF en welke invloed heeft deze scope-uitbreiding op hoe de organisatie de IAF beleeft? Gezien de positie en rol is de IAF misschien de meest aangewezen afdeling om dit soort onderzoeken intern te doen. Of, in geval de voornoemde kennis en vaardigheden niet aanwezig zijn, te coördineren. Het gaat tenslotte om een 'lek' in de AO/IC.

Conclusie: wanneer de IAF geen specifieke kennis en vaardigheden bezit in het doen van fraudeonderzoeken, doe ze niet, maar zorg wel dat de IAF betrokken is wanneer deze (extern) worden uitgevoerd.

Tien tips om veilig te internetten

Wapen u tegen digitale bedreigingen! Word geen slachtoffer van hackers, ransomware en cyberspionage, maar internet veilig. Hoe? Door deze tien tips op te volgen.

Het zal je maar gebeuren. Op een ochtend start je, zoals op iedere doordeweekse ochtend, nietsvermoedend je laptop op. Je hebt een drukke dag voor de boeg: voor een belangrijke audit moet een rapportage worden opgeleverd. Eerst maar even koffie halen, terwijl de laptop verder laadt. Je vertrekt voor de korte wandeling naar het koffiezetapparaat. Op het moment dat je even later met een gevulde mok weer achter je laptop kruipt, blijkt dat die helemaal niet is opgestart. In plaats daarvan wordt een vreemd rood scherm weergegeven. Een scherm met een slotje en een klok die aftelt. De boodschap is even helder als zorgwekkend: al je bestanden zijn versleuteld en pas weer raadpleegbaar nadat je hebt betaald. Het angstzweet breekt je uit. Je bent het slachtoffer van ransomware!

Ver-van-mijn-bedshow

Klinkt dit als een ver-van-mijn-bedshow? Toch zijn we in toenemende mate doelwit van cybercriminaliteit. Beroepscriminelen leggen met (Internet of Things) DDoS-aanvallen websites plat of gijzelen met behulp van ransomware, zoals Cryptolocker en WannaCry, kritische data van organisaties voor losgeld. Statelijke actoren krijgen door middel van cyberspionage waardevolle informatie in handen en weten tegenwoordig zelfs door middel van hacking democratische processen te beïnvloeden.

Organisaties lijken zich in toenemende mate bewust van de risico's en voeren maatregelen door. Lang niet alle risico's kunnen echter technisch worden afgevangen. De digitale weerbaarheid van organisaties valt of staat in grote mate met het gedrag van haar medewerkers. Een mooi object van onderzoek voor audit dus. We moeten er daarnaast als auditors natuurlijk ook voor waken dat we zelf slachtoffer worden en daarmee onze organisatie in gevaar brengen. Daarom tien tips om veilig te kunnen internetten.

1 Installeer een virusscanner

Een virusscanner scant de bestanden op uw computer op tekenen van infectie, waarschuwt u wanneer malware wordt aangetroffen en geeft u in sommige gevallen de optie de malware direct te verwijderen of in quarantaine te plaatsen. Verreweg de meeste organisaties dwingen het gebruik van een virusscanner in de zakelijke omgeving af. Het is echter verstandig ook buiten deze omgeving gebruik te maken van een virusscanner. Hierbij is het tevens belangrijk dat u de virusdefinities up-to-date houdt.

2 Activeer uw firewall

Een firewall controleert inkomende en uitgaande pakketten met informatie en blokkeert verdachte pakketten. Organisaties maken doorgaans gebruik van firewalls en ook uw internetserviceprovider dwingt in de meeste gevallen gebruik van een in uw modem geïntegreerde firewall af. Zowel thuis als op uw werk bent u over het algemeen dus goed beschermd. Onderweg bent u echter kwetsbaarder. Firewalls maken vaak deel uit van anti-virus software, maar moeten in sommige gevallen wel separaat worden geactiveerd.

3 Gebruik sterke en unieke wachtwoorden

Het belang van sterke wachtwoorden wordt door veel mensen nog onderschat. Zo kan een wachtwoord dat louter bestaat uit een Engels of Nederlands woord door hackers vaak binnen enkele seconden worden gekraakt. Kijkt u maar eens op <https://howsecuremypassword.net/> (vul hier vanzelfsprekend nooit uw echte wachtwoorden in, u weet nooit wat er met uw invoer gebeurt). Daarnaast weten



cybercriminelen soms de volledige gebruikersbestanden van organisaties te kapen. Zo bleek vorig jaar dat hackers al in 2013 de namen, wachtwoorden en telefoonnummers van alle 3 miljard (!) gebruikers van Yahoo! hadden gestolen. Hackers proberen gestolen wachtwoorden uit op andere diensten, zoals online winkels of betalingssystemen. Dit in de wetenschap dat nog altijd veel mensen hetzelfde wachtwoord gebruiken voor verschillende diensten. Het is dus van groot belang dat u sterke en unieke wachtwoorden gebruikt. Een zogenoemde passwordmanager kan u hierbij helpen, maar het gebruik ervan creëert natuurlijk tegelijkertijd een 'single point of failure'. De keuze is aan u. Wat u ook doet, log in ieder geval nooit in bij een dienst gebruikmakend van een publieke computer, zoals u die aantreft in internetcafés en bibliotheken. Met deze computers kan gerommeld zijn en ze zijn daarom niet te vertrouwen.

4 Activeer two-factor authentication (2FA)

Steeds meer diensten bieden 2FA aan. Hierbij dienen gebruikers twee stappen te doorlopen om in te loggen. De eerste stap is gerelateerd aan iets wat u weet, doorgaans uw gebruikersnaam en wachtwoord. De tweede stap is gerelateerd aan iets wat u hebt of wat u bent. Dit kan bijvoorbeeld een code zijn die u ontvangt op uw smartphone of uw vingerafdruk. 2FA zorgt voor veel meer veiligheid. Activeer 2FA dus daar waar mogelijk.

5 Beheer uw wifinetwerken

Uw computer en smartphone houden voor u een lijst bij van wifinetwerken waar u in het verleden op bent ingelogd. Dat is handig, want zo wordt uw systeem de volgende keer dat

u op een bepaalde plek bent direct weer verbonden met het betreffende netwerk. Hackers weten echter soms op vernuftige wijze gebruik te maken van deze functionaliteit. Zo kunnen zij u verleiden verbinding te maken met hun kwaadaardig netwerk, door dat netwerk een voor u reeds bekende netwerknaam te geven. Hierna kan de hacker iedere beweging die u maakt op internet op de voet volgen. Het is dus zaak om uw wifinetwerken te beheren. Een algemene tip daarbij is dat uw openbare wifinetwerken zo min mogelijk probeert te gebruiken en na gebruik direct weer verwijdert. Maak bovenal nooit verbinding met wifinetwerken die u niet vertrouwt.

6 Maak zoveel mogelijk gebruik van end-to-endencryptie

Bij end-to-endencryptie worden pakketten met informatie versleuteld op het systeem van de verzender en pas ontsleuteld op het systeem van de ontvanger (die hiervoor uiteraard over de geheime sleutel moet beschikken). U herkent het aan het slotje in de adresbalk van uw browser. Een alternatieve wijze om een dergelijke versleutelde verbinding op te zetten is door gebruik te maken van een virtual private network (VPN) dienst. Wanneer u gebruikmaakt van een dergelijke dienst verloopt al uw internetverkeer versleuteld tot aan de server van de VPN-provider, zelfs wanneer u (per ongeluk) met een kwaadaardig wifinetwerk verbonden bent.

7 Blokkeer advertenties

Organisaties verhuren soms een deel van hun website aan advertentienetwerken. Deze advertentienetwerken plaatsen vervolgens op de gehuurde ruimte (maatwerk)advertenties. Hackers proberen via deze advertentienetwerken

advertenties met kwaadaardige codes op allerlei websites geplaatst te krijgen. Dit doen zij bijvoorbeeld door legitiem advertentieruimte in te kopen of door advertentienetwerken te hacken. Wanneer een website een besmette advertentie aan u toont, kan hierdoor op de achtergrond malware op uw systeem worden geïnstalleerd. In 2016 waren gedurende ongeveer een dag de bezoekers van bijna driehonderd Nederlandse websites, waaronder Nu.nl, Buienradar en Marktplaats, het doelwit. Besmette advertenties die via deze sites werden aangeboden, lieten bezoekers ongemerkt verbinding maken met een exploitkit, die vervolgens malware probeerde te installeren gebruikmakend van een aantal bekende kwetsbaarheden in onder meer Internet Explorer en Flash Player. U kunt door gebruik te maken van 'ad blockers' voorkomen dat uw systeem op deze wijze besmet raakt. In Nederland wordt hier steeds meer gebruik van gemaakt. Vanzelfsprekend raakt dit tegelijkertijd de websites die hun inkomsten halen uit het verhuren van advertentieruimte.

helaas niet door iedereen geïnstalleerd, getuige het feit dat WannaCry binnen een dag ruim 230.000 computers in 150 landen wist te besmetten. Het bewijst maar weer eens dat al die waarschuwingen van uw besturingssysteem om te updaten niet voor niets zijn!

10 **Maak back-ups**

We kunnen het niet vaak genoeg zeggen: maak back-ups! Mochten hackers er namelijk toch in slagen uw systeem te compromitteren, dan bent u in ieder geval niet al uw data kwijt. Wij adviseren hierbij de 3-2-1 back-upregel te volgen. Maak drie back-ups van uw data, bewaar die back-ups op twee verschillende soorten gegevensdragers en bewaar één back-up op een externe locatie (of in de cloud).

Zo kan een wachtwoord dat louter bestaat uit een Engels of Nederlands woord door hackers vaak binnen enkele seconden worden gekraakt

8 **Verwijder kwetsbare plug-ins**

Plug-ins als Flash Player, Shockwave Player, Silverlight en Java bevatten vaak veel onbekende (ofwel 'zero day') kwetsbaarheden waar hackers hun voordeel mee kunnen doen. Zo kunnen ze in sommige gevallen uw computer overnemen en toevoegen aan een zogenoemd botnet. Uw computer voert dan in opdracht van de hacker opdrachten uit, zoals het verspreiden van spam of malware, zonder dat u dat zelf merkt. Indien u dergelijke kwetsbare plug-ins niet absoluut nodig heeft, is het beter ze te verwijderen.

9 **Update regelmatig uw software**

Hackers maken ook gebruik van kwetsbaarheden in software. De WannaCry ransomware die vorig jaar zomer uitbrak en meerdere bedrijven hard trof, is daar een sprekend voorbeeld van. WannaCry maakte gebruik van een kwetsbaarheid in het besturingssysteem Windows en heeft in de korte tijd dat het actief was flink weten toe te slaan. Zo werd kritische apparatuur van de National Health Service in Engeland totaal onbruikbaar, vertoonden de schermen langs de perrons van Deutsche Bahn enkel nog het befaamde ransomwarescherm en moesten Nissan en Renault hun productie noodgedwongen tijdelijk stilleggen. Microsoft had drie maanden voorafgaand aan het uitbreken van WannaCry al een security patch beschikbaar gesteld waarmee de betreffende kwetsbaarheid kon worden verholpen. Die was

Helaas kunnen we ook degene die alle tien de tips voor veilig internetten volgen, niet garanderen dat ze nooit slachtoffer zullen worden van cybercriminaliteit. De tips helpen weliswaar, maar bieden nooit absolute zekerheid. Tegelijkertijd geldt dat de toepassing van een combinatie van de besproken maatregelen sterker is dan iedere individuele maatregel op zichzelf. We kunnen slechts ons best doen om ons zo goed mogelijk te wapenen tegen de bedreigingen op het internet. En dat laatste is wel nodig, want een ver-van-uw-bedshow is het inmiddels al lang niet meer! <<

Jan Hendriks 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@hendriks-itc.nl

Björn Walrave is zelfstandig gevestigd organisatieadviseur, docent, trainer en coach en daarnaast redactielid van *Audit Magazine*.
bjorn.walrave@auditability.nl



Voorzichtig zijn? Nooit zonder risico!

Afgelopen zomer verscheen een klein, maar opvallend bericht in de media. De boodschap was dat kinderen in onze tijd steeds vaker onnodig bang en onzeker zijn, omdat de ouders van nu veel te voorzichtig zijn geworden. De fysieke en mentale gezondheid van onze jeugd zou gevaar lopen omdat ouderwets buiten spelen door de beschermende ouders onvoldoende wordt toegestaan. In bomen klimmen, hutten bouwen, slootjespringen, met vloten varen, naar schatten zoeken op geheime plekken: het zit er voor de jeugd van tegenwoordig allemaal niet meer in. Maar, zo werd bezorgd gemeld: kinderen moeten buiten kunnen spelen, zodat ze risico's leren inschatten, zelfredzaam worden en zelfvertrouwen kunnen opbouwen. Ouders begrijpen blijkbaar op zich nog wel dat het goed is voor hun grut, maar zijn toch terughoudend omdat ze bang zijn dan hun kinderen gewond raken én dat anderen in hun omgeving het afkeuren.

Niet alleen thuis en in het gezin worden we gemaand voorzichtig te zijn, en geldt dat een dergelijke risicomijdende opstelling allesbehalve zonder risico is. Ook in de context van organisaties en instellingen kan verkramping rondom gevaar verkeerd uitpakken. Denk aan hoe managers en bestuurders zich verhouden tot een fusietraject met een andere instelling, een reorganisatie om de onderneming weer bij de tijd te

krijgen, de invoering van een nieuw ICT-systeem, de vernieuwing van het dienstverleningsconcept of de internationalisering van bedrijfsactiviteiten. Het accepteren van de hiermee gepaard gaande onzekerheid, door het inslaan van nieuwe wegen, het opzoeken van ongemak in de hoop en verwachting dat daar kansen liggen op iets beters, hoort bij goed bestuur en succesvol leiderschap. Als dergelijke risico's steeds uit de weg worden gegaan uit angst voor de mogelijke gevolgen, kan uiteindelijk op de lange termijn de kwetsbaarheid voor een ramp bij de instelling juist toenemen!

Juist voor auditors is dit een spannende kwestie. In de kern draait het in ons beroep immers om zekerheid bieden, risico-inschattingen maken, procedures beoordelen, kijken of alle relevante feiten en omstandigheden wel voldoende scherp in beeld zijn. Toetsend onderzoek kan hierbij makkelijk leiden tot voorzichtigheid, die uiteindelijk resulteert in passiviteit. Control frameworks en normenkaders, toetsingsprotocollen, systemen en processen die bedoeld zijn om de organisatie weerbaar te maken, integer te houden, fraudebestendig te krijgen, pakken dan heel anders uit. Ze zorgen dan voor verkramping, handelingsverlegenheid, duiken en afschuifgedrag.

Veiligheid bieden is van groot belang, maar kan soms zelf juist een bron van

onveiligheid worden voor de organisatie. In een themanummer over integriteit en fraude moet dat besef altijd voorop staan. Voorkomen is beter dan genezen, zo houden we elkaar vaak voor. Maar of dat in de praktijk ook altijd echt zo is, valt nog maar te bezien. Fouten moet je niet altijd willen voorkomen, ook al kosten de leerervaringen die je zo opdoet (veel) geld, tijd en motivatie. Beter is het om fouten te durven maken, ze tijdig te ontdekken om er vervolgens snel van te leren en zo de schade voor de langere termijn te beperken.

Soms kun je beter een beetje ziek worden om snel weerstand op te bouwen tegen een ernstiger besmetting, voor als het er op enig moment echt toe doet. Ook dat weten we natuurlijk allang als we terugdenken aan onze eigen jeugd. Nu alleen nog even puzzelen hoe een auditor dat goed verwerken kan in zijn toetsend onderzoek...

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

Thema Fraude – Ethiek – Integriteit
Tekst Drs. Nicole Engel-de Groot RA
Beeld Adobe Stock



Is hier sprake van *fraude*?

Een forensisch onderzoeker komt in beeld bij een vermoeden van fraude. *Audit Magazine* sprak met Inge-Lisa Toxopeus, forensisch accountant en partner bij Hermes Advisory, voor wie fraudeonderzoek dagelijkse kost is.

Waar houdt u zich zoal mee bezig?

“Ik doe bijzondere onderzoeken en houd mij bezig met het onderzoeken/begroten van vermogensschade. Onder de bijzondere onderzoeken vallen fraudeonderzoeken, onderzoeken naar faillissementsfraude en jaarrekeningfraude. Vooraf is niet altijd zeker of er sprake is van fraude. Daarom noemen wij het bijzonder onderzoek. Bij onderzoek naar vermogensschade moet je denken aan schadebepalingen wanneer de ene onderneming schade heeft berokkend aan een andere onderneming.”

Wat is uw achtergrond?

“Ik ben forensisch accountant, dat wil zeggen dat ik als RA forensische werkzaamheden uitvoer. Niet iedereen in het vakgebied is RA. De niet-RA's in dit vakgebied worden aangeduid met forensisch onderzoeker. Veelal zijn dit voormalige politiemensen en advocaten. Er is veel vraag naar forensisch onderzoek, dus dat maakt het een interessante sector voor advocaten- en accountancykantoren. Er zitten veel juridische aspecten aan dit werk, maar uiteindelijk gaat het er vooral om dat je de administraties begrijpt. Voor het vaststellen van fraude en het winnen van een arbeidsrechtelijke, civielrechtelijke of strafrechtelijke zaak zijn juristen goed toegerust. Echter, voor het vaststellen van de omvang van de schade dien je administratieve kennis te hebben. Bij de Orde van Advocaten en de Juridische Academie geef ik les aan juristen, maar helaas heeft de gemiddelde jurist doorgaans weinig kennis van administratieve processen en boekhouding. Wat mij ook opvalt is dat juristen een casus behandelen vanachter hun bureau. Accountants zijn veel

meer gewend om naar een cliënt te gaan en zelf in de administraties te neuzen. Een groot voordeel om een advocaat het forensisch onderzoek te laten uitvoeren, is dat een advocaat zich kan beroepen op zijn verschoningsrecht. De FIOD zal bij een advocaat niets mogen invorderen. Uiteindelijk geloof ik het meest in de combinatie. Wij werken binnen Hermes altijd met een advocaat.”

Hoe groot schat u het probleem fraude in?

“Ik denk dat fraude nog steeds onderschat wordt. Het is moeilijk er een percentage aan te plakken maar ik durf te stellen dat elke onderneming er wel mee te maken krijgt. Vaak heeft niemand door dat er iets speelt omdat fraude veelal binnenskamers wordt gehouden. Veelvoorkomend is fraude via de crediteurenadministratie. Als voorbeeld ben ik tegengekomen dat iemand binnen de crediteurenadministratie gemachtigd was om

Over...

Inge-Lisa Toxopeus is partner bij Hermes Advisory en als gerechtelijk deskundige gespecialiseerd in het begroten van vermogensschade en bijzonder onderzoek. Daarnaast is zij docent bij het Centrum voor Postdoctoraal Juridisch Onderwijs, de Juridische Academie en de Erasmus School of Accounting & Assurance.

Internal Audit, Risk, Business
& Technology Consulting



HOE REALISEREN
ORGANISATIES TOEGEVOEGDE
WAARDE IN INTERNAL AUDIT,
RISK EN IT?

ZIJ BELLEN ONS!

Protiviti is onafhankelijk,
pragmatisch en internationaal.

Klanten vragen ons bij het combineren
van mensen, kennis en techniek. We zijn
daarin succesvol. Wilt u ook toegevoegde
waarde realiseren?

Neem contact met ons
op via +31 20 3460400
of via contact@protiviti.nl

protiviti.nl

protiviti[®]
Face the Future with Confidence

© 2017 Protiviti Inc. PRO-1117

spoedbetalingen te doen. Als bewijs diende elke betaling door middel van een print getekend te worden door de directeur. De persoon was bovendien niet gemachtigd om crediteuren aan te maken. Echter, wat niemand zich had gerealiseerd was dat ook alle werknemersgegevens opgenomen waren in de crediteurenadministratie. Deze persoon maakte bij elke spoedbetaling ook een bedrag over aan zichzelf. De bankafboekingen werden ook door deze persoon geadmistreerd. Hij benutte tussenrekeningen om boekingen niet te laten opvallen. Op een gegeven moment is de fraude ontdekt doordat een overboeking naar deze persoon niet lukte. Vervolgens belde de bank naar de directeur om te laten weten dat de overboeking niet geslaagd was en daardoor liep de fraudeur tegen de lamp.

Ook aan de inkoopzijde zie ik fraudegevallen. In dat geval is er vaak sprake van samenspanning van een externe en een medewerker. De fraude komt dan neer op het berekenen van te hoge prijzen of het onrechtmatig winnen van orders. Ook komt het voor dat fraude wordt gepleegd via niet-primaire processen. Hiervoor bestaat veelal weinig aandacht zodat een fraudeur ongestoord zijn gang kan gaan. Denk bijvoorbeeld aan het onttrekken van afval dat geld oplevert.”

Op welk moment worden jullie ingeschakeld?

“Dat is het moment dat fraude vermoed wordt. ‘Red flags’ zijn opvallende fluctuaties ten opzichte van vorig jaar of binnen een jaar. Op dat moment moet de organisatie op zoek gaan naar een verklaring. Als dan vermoed wordt dat er meer aan de hand is, is het tijd om een forensisch onderzoek te starten. De fraudedriehoek (druk of verleiding, gelegenheid en rationalisatie) geeft een handvat om het risico van fraude in kaart te brengen. Medewerkers kunnen een risicofactor worden door geldgebrek of relatieproblemen. Als deze mensen op gevoelige posities zitten moet je dat in kaart hebben. Of het kan zijn dat een onredelijke ongelijkheid in een organisatie bestaat of gepercipieerd wordt.

Wij worden ingeschakeld in opdracht van een partij. Het kan zijn dat de partij die de opdracht geeft zelf verdacht is van fraude en ons inschakelt om het tegendeel te bewijzen. We werken weliswaar voor een opdrachtgever, maar voeren ons werk objectief uit. We zorgen zelf dat we toegang krijgen tot de administratie en stellen ons daarin niet afhankelijk op van de opdrachtgever.”

Wat kan Internal Audit wel en niet doen?

“De bestrijding van fraude bestaat uit vier fasen: inventarisatie, preventie, detectie en onderzoek. Inventarisatie en preventie dienen vaste onderdelen op de agenda van Internal Audit te zijn. Op het moment dat er een vermoeden bestaat van fraude kan de forensisch onderzoeker gebruikmaken van Internal Audit om voorwerk in de administratie te laten doen. Oplettendheid is geboden, want je weet niet of en in hoeverre Internal Audit mogelijk betrokken kan zijn bij de fraude.

Een internal auditor dient bij het vermoeden van fraude nooit zelf het gesprek aan te gaan met de verdachte. Bij een interview met een verdachte dienen gedragslijnen voor persoonsgebonden onderzoeken gevolgd te worden. De verdachte dient verteld te worden waar het gesprek over gaat, dat hij niet verplicht is medewerking te verlenen, et cetera.

Een internal auditor RA die deze regels overschrijdt kan tuchtrechtelijk vervolgd worden op grond van overschrijding van de gedrags- en beroepsregels. Daarnaast kan het arbeidsrechtelijke gevolgen hebben wanneer bij ontslag of bij het op non-actief stellen niet de juiste stappen zijn gevolgd.

Het zou ter detectie en preventie van fraude goed zijn als Internal Audit elk jaar een thema pakt, bijvoorbeeld de crediteurenadministratie, en door middel van deelwaarnemingen processen verifieert. Wantrouwend zijn helpt daarbij. Bij mij is het wel een tweede natuur geworden, een beroepsdeformatie. Ik heb pas een huis gekocht en ik vertrouwde de verkopende makelaar simpelweg niet. Ik dacht constant: ah, maar nu naai je me een oor aan. Mijn man had dat totaal niet. Achteraf bleek er niets aan de hand te zijn.”

Hoe verloopt een forensisch onderzoek?

“Een onderzoek start altijd met een goede kennismaking van de kwestie. Daarna stel je vast wie betrokken zijn en wie een betrouwbaar aanspreekpunt hoog in de organisatie kan zijn. Het is belangrijk om binnen IT een betrouwbaar contactpersoon te hebben om bijvoorbeeld toegang tot een mailbox te krijgen. Ook hier dien je er alert op te zijn dat deze persoon niet betrokken is. Vervolgens vindt het onderzoek in de administratie plaats. De verdachte wordt gehoord, gevolgd door een reactie op de bevindingen door de verdachte (de wederhoor). Dit vormt het sluitstuk van het onderzoek.”

Op welk moment moet de verdachte verteld worden dat hij verdacht is?

“Als je start met een onderzoek en je verdenkt iemand moet je dat vertellen. Maar dan loop je het risico dat bewijsmateriaal wordt verdoezeld. Daarom mag je toch al beginnen met een administratief onderzoek, maar dien je goed te onderbouwen waarom je wacht met het informeren van de verdachte. Het mag niet al te lang duren voor je de verdachte informeert.”

Hoe moeilijk is het om juridisch overtuigend bewijs te verkrijgen?

“Dat kan heel lastig zijn. Soms is het zelfs zonder bekentenis van de fraudeur niet haalbaar. Een zaak kan gevoerd worden op drie juridische vlakken waarbij het belang van bewijs varieert. Op het arbeidsrechtelijke vlak hoeft fraude niet per se bewezen te worden. Maar als je snel van iemand af wilt is bewijs van fraude wel fijn. Op het civielrechtelijke vlak dient de omvang van de schade bepaald te worden en is de volle

omvang van de fraude van belang. Tot slot is het op strafrechtelijke vlak vaak zo dat één bewezen strafrechtelijk feit voldoende is om iemand strafrechtelijk te vervolgen. Bij een organisatie die cadeaubonnen uitgifte heb ik geen onomstotelijk bewijs gevonden wie geld heeft onttrokken. De uitgifte van de cadeaubonnen en de verrekening met retailers gingen allemaal contant. De boekhouding was niet bijgewerkt. Meerdere mensen hadden toegang tot de kluis. Er was hierdoor geen bewijs voor een strafrechtelijke en civielrechtelijke zaak, maar er was wel voldoende aan te dragen voor het opzeggen van een arbeidscontract.”

Wat maakt dit werk leuk?

“Mijn achtergrond is extern accountant. Ik vond dit heel saai en ook frustrerend werk, want uiteindelijk wist de organisatie zelf heel goed hoe de processen te beheersen. De toegevoegde waarde van de externe accountant ervaarde ik als klein. Wat ik nu doe geeft wél toegevoegde waarde. Een organisatie heeft een probleem en als forensisch onderzoeker kun je dit probleem oplossen. Dat geeft mij veel voldoening. En het is een creatief proces. Je moet soms echt out of the box denken. Ik was ooit bij een chemisch bedrijf waar een zeer kostbaar element tweemaal gefactureerd en betaald was. Nu was de grote vraag of dit door de externe leverancier was gedaan of door een interne medewerker. De clou zat hem in de vouwlijnen die ontbraken bij een van de twee facturen. Deze was nooit gevouwen en in een envelop gedaan. De conclusie was dat de fraudeur binnen het bedrijf moest zitten.” <<



Samenwerken in het bestrijden van corruptie en fraude

Er gaat geen dag voorbij of we lezen berichten over niet-integer handelen. Justitie zet dan ook steeds meer in op integriteitsbevordering en corruptiebestrijding. De Fiscale Inlichtingen- en Opsporingsdienst (FIOD), de opsporingsdienst van de Belastingdienst, speelt hierin een belangrijke rol.



De FIOD is met 1400 medewerkers gespecialiseerd in het opsporen van financiële en belastingfraude. Oorspronkelijk was de FIOD een tamelijk gesloten organisatie die zich richtte op overzichtelijke belastingfraude en smokkelzaken. Veranderingen in de maatschappij zoals toenemende digitalisering en internationalisering van misdaad, hebben de huidige moraal veranderd. Dit heeft er voor gezorgd dat de FIOD van nu niet alleen meer belast is met het bestrijden van fiscale fraude, maar ook met het bestrijden van georganiseerde criminaliteit op het gebied van witwassen, corruptie en financiële integriteit.

Daarnaast zien we dat het strafrecht is verschoven van 'ultimum remedium' naar 'optimum remedium'. Anders verwoord: daar waar we vroeger kozen voor de inzet van strafrecht als allerlaatste redmiddel (ultimum remedium) kiezen we steeds vaker voor een aanpak die het best bijdraagt aan het oplossen van maatschappelijke problemen (optimum remedium). Deze ontwikkeling is ook in de FIOD-praktijk terug te zien. Zo zien we bijvoorbeeld dat personen die zakelijke diensten hebben verricht voor verdachten, tuchtrechtelijk worden vervolgd. Om in de huidige maatschappij het werk goed te kunnen uitvoeren, zoekt de FIOD de samenwerking met andere opsporingsdiensten en met private partijen zoals banken en accountantskantoren.

Corruptie

Corruptie heeft een sterk ondermijnend effect. Op het moment dat hier niet goed op gehandhaafd wordt, tast dat het vertrouwen in de overheid aan. Het heeft daarnaast een negatief effect op de kwaliteit van publieke dienstverlening, economische ontwikkeling en het ondernemersklimaat. Gelet hierop en gezien het toenemende aantal gevallen van corruptie is vanuit de politiek het signaal afgegeven dat extra aandacht voor preventie en bestrijding van corruptie noodzakelijk is. Het kabinet besliste in 2015 dat vanaf 2016 jaarlijks € 20 miljoen extra wordt geïnvesteerd in de FIOD en het Openbaar Ministerie voor de bestrijding van witwassen en corruptie.

Corruptie kent verschillende verschijningsvormen (zie *figuur 1*). Het verstrekken van opdrachten aan bevriende relaties kan nog relatief onschuldig zijn. Nepotisme en patronage zijn maatschappelijk verwerpelijk maar niet zomaar strafrechtelijk vervolgbaar. Zodra je het hebt over omkoping, verduistering en afpersing kent het strafrecht sancties.

Anti Corruptie Centrum (ACC)

Om corruptie goed te kunnen bestrijden heeft de FIOD in 2016 het Anti Corruptie Centrum (ACC) opgericht. In het ACC bundelt zich de expertise binnen de FIOD op het gebied van corruptiebestrijding. Hiermee kan corruptie beter en sneller gedetecteerd en opgespoord worden. Het ACC heeft onder meer als doel dat het risico op corruptie binnen de directiekamers van Nederlandse bedrijven een serieus onderwerp wordt en blijft. Bewustwording van integer zakendoen moet de norm

zijn in een organisatie omdat corruptie ondermijnend werkt en eerlijke concurrentie verstoort.

In het buitenland zien we de ontwikkeling dat bedrijven zich melden bij het Openbaar Ministerie na het intern constateren dat sprake is van corruptie en fraude. Zowel de VS als de UK hebben een leidraad 'self reporting' ontwikkeld die ondernemingen inzicht geven in wat zij kunnen verwachten zodra zij een melding doen bij het Openbaar Ministerie. In Nederland hebben we weliswaar hierover nog geen regelgeving maar de FIOD adviseert in alle gevallen een proactieve houding van de raad van commissarissen en raad van bestuur zodra intern geconstateerd is dat sprake is of is geweest van corruptie en/of fraude. Proactief betekent vanuit de positie van de FIOD dat melden bij het Openbaar Ministerie van belang is. Het niet melden kan in een later stadium gevolgen hebben voor de onderneming.

Onderzoeken die de FIOD doet naar corruptie kunnen leiden tot strafrechtelijke vervolging of een transactie met het Openbaar Ministerie. Een transactie kan bestaan uit een te betalen geldbedrag in combinatie met een aantal nader overeen te komen maatregelen. In onderzoeken is ook altijd aandacht voor het strafrechtelijk vervolgen van de verantwoordelijke personen. Onderdeel van de transactie is het ontnemen van het wederrechtelijk verkregen voordeel, vaak met een forse boete. In het kader van transparantie wordt een uitgebreid persbericht opgesteld en in de media gebracht. En ten slotte worden maatregelen met de betrokken bedrijven afgesproken om herhaling te voorkomen. Hier ligt ook een belangrijke rol voor externe toezichthouders, internal auditors en compliance medewerkers, bijvoorbeeld in het bewaken van de overeengekomen maatregelen.

In de bestrijding van corruptie werkt de FIOD samen met het Openbaar Ministerie - dat een speciaal thema-team corruptie heeft -, de Belastingdienst en de Rijksrecherche. De Rijksrecherche is verantwoordelijk voor de zaken waar ambtenaren bij betrokken zijn. De FIOD houdt zich bezig met de ondernemingen en ambtenaren in het buitenland. Daarnaast wordt ook de samenwerking gezocht met private partijen en internationale partners.

Melden van fraude bij de FIOD

Vermoedens van fraude kunnen gemeld worden bij het fraudemeldpunt van de FIOD. Waar het specifiek gaat om vermoedens van corruptie of onethisch handelen kan ook rechtstreeks contact opgenomen worden met het Anti Corruptie Centrum (FIOD.ACC@belastingdienst.nl). Het is ook mogelijk een melding te doen bij het Team Criminele Inlichtingen (TCI) van de FIOD. Bijvoorbeeld als een werknemer die kennis heeft van fraude en/of corruptie



Figuur 1. Verschillende verschijningsvormen van corruptie

niet in de positie is om ervoor te zorgen dat de misstand stopt. Het TCI zorgt ervoor dat de identiteit van melders (informanten) is afgeschermd waardoor de veiligheid en de anonimiteit van de melder is gegarandeerd, maar waarbij de informatie wel gebruikt kan worden in een strafrechtelijk onderzoek. Het kan wellicht helpen om dilemma's, waar bijvoorbeeld een internal auditor of compliance medewerker mee geconfronteerd wordt, verkennend te bespreken. Vragen als: 'Zie ik het goed?', 'Waar stopt mijn verantwoordelijkheid?', kunnen zonder verplichtingen vooraf besproken worden. Het inzetten van 'het instrument' TCI is wel aan regels gebonden. Een van de regels is dat het delict waarvoor de informatie wordt binnengehaald 'zware georganiseerde criminaliteit' betreft. Delicten als belastingfraude, corruptie en witwassen vallen hier meestal onder. De informatie die TCI binnenhaalt

verbinding tussen organisaties en opsporing op gebied van veiligheid en integriteit. Bedreigingen kunnen op die manier veranderen in kansen en uiteindelijk waarde toevoegen aan de maatschappij. Dit wordt ook wel het M.O.O.O.I.-concept genoemd (zie *figuur 2*), waarbij partijen vanuit hun eigen perspectief kennis en kunde inbrengen om samen verder te ontwikkelen.

Rol voor internal auditors

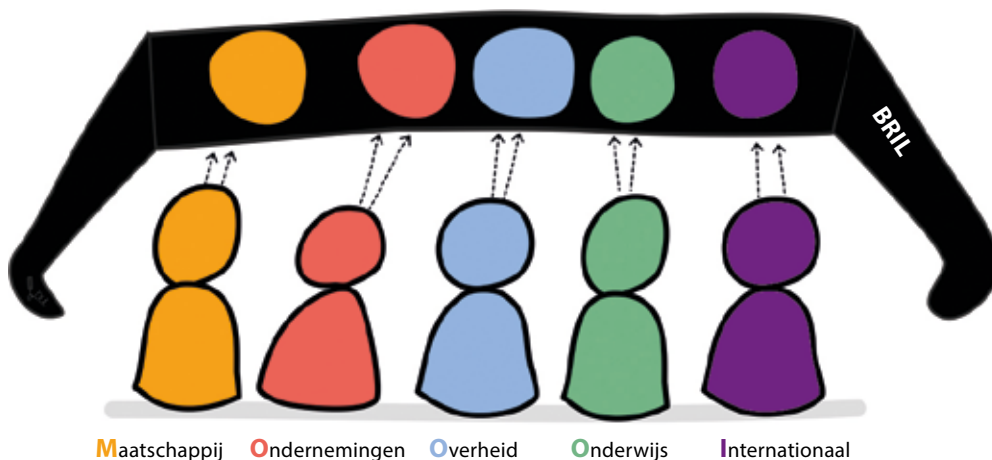
Wat zou de rol van internal auditors en compliance medewerkers kunnen zijn? Hebben internal auditors een onmogelijke taak als zij moeten kiezen tussen het bewaken van de

integriteit of de commerciële belangen van ondernemingen of kan dat samengaan?

De huidige maatschappij is steeds kritischer waar het gaat om integriteit kwes- ties en het eerlijk doen van zaken. Het is dan ook van groot belang dat dit een serieus onderwerp is en blijft in de directiekamers van de Nederlandse bedrijven. Voor internal auditors en compli- ancemedewerkers is het dan de vraag wat hun rol hierin is, alleen 'waarschuwer' of meer? En dan speelt vervolgens de vraag wat prevaleert: business of compliance? In de ideale situatie zouden beiden gelijk op moeten trekken maar in de praktijk lijkt business vaak toch belangrijker te zijn.

Een onderwerp waarbij

de afdeling Compliance en/of Internal Audit een rol zou kunnen spelen, is fusies en overnames. Op 20 december 2017 kopte *Het Financieele Dagblad* op de voorpagina 'Nederlandse concerns gaan in 2018 vol op overnamepad'. Een interessante vraag is of de afdeling Compliance en/of Internal Audit een rol moet spelen bij de aankoop of fusie van nieuwe bedrijfsonderdelen. In de praktijk is de afdeling Merger & Acquisition leidend en vaak zien we dat de afdeling Compliance en/of Internal Audit niet of te laat betrokken wordt bij het aankoopproces waardoor risico's met betrekking tot corruptie niet of niet tijdig onderkend worden. In de ideale situatie trekken de afdelingen Merger & Acquisition en Compliance en/of Internal Audit vanaf het begin samen op. Niet de kortetermijnvisie op het binnenhalen van een bedrijfsonderdeel of onderneming zou moeten prevale- ren maar er zou een gedeelde visie op de aankoop of fusie moeten bestaan waarbij naast het commerciële belang ook beheersing & compliance wordt meegewogen. Voor internal auditors en compliancemedewerkers zijn dit kwesties die wellicht om durf en gerichte keuzen vragen. <<



Figuur 2. Het M.O.O.O.I.-concept

wordt verwerkt in een proces-verbaal. Als de informatie concreet en specifiek is, kan dit aanleiding zijn een strafrechtelijk onderzoek te starten. Ook kan de informatie richting geven aan een lopend strafrechtelijk onderzoek.

Veiligheidsagenda

Nu veiligheid en integriteit steeds meer maatschappelijke thema's zijn, wordt binnen de FIOD getracht met andere partijen op te trekken en daar waar mogelijk samen te werken. Denk hierbij aan het Nederlandse bedrijfsleven en wetenschappelijke instellingen. Gezamenlijk wordt gewerkt aan de zogenoemde 'Veiligheidsagenda'. Door samen te werken en gebruik te maken van elkaars expertise kan dat de opsporing uiteindelijk een voorsprong geven en hiermee waarde creëren voor Nederland. Dit zijn uitdagingen die niet enkel meer het terrein zijn van de overheid en opsporingsdiensten, maar vragen om een actievere betrokkenheid en verantwoordelijkheid van maatschappij, wetenschap en bedrijven. De huidige organisatie en wetgeving zijn nog niet volledig aangesloten op het huidige tijdsbeeld waardoor we minder adequaat kunnen reageren op de moderne georganiseerde criminaliteit die bijvoorbeeld steeds vaker gebruik maakt van complexe internationale bedrijven- en financiële structuren. Dit vraagt om meer flexibiliteit voor internationale samenwerking, samenwerking tussen publieke en private organisaties en betere mogelijkheden om snel informatie te kunnen delen. Wij zien kansen en mogelijkheden in een

Claartje van Roosmalen werkte als stafjurist voor het team Fiscale Fraude van de strafsector van het Gerechtshof 's-Hertogenbosch. Sinds 2014 is zij financieel rechercheur in een opsporingsteam van de FIOD in Utrecht.



Morele moed:

van persoonlijke reflectie tot onderzoeksobject van audit

Een directeur vraagt een audit op verzoek omdat hij tegen een probleem aanloopt. Hij wil graag inzicht in de kern van dit probleem. Je spreekt af direct aan hem te rapporteren. Uit je onderzoek blijken zware bevindingen die mogelijk impact hebben op de continuïteit van de organisatie. Deze bevindingen gaan onder andere over de bestuursstijl en het voorbeeldgedrag van de directeur zelf. Wanneer je je bevindingen terugkoppelt aan de directeur, geeft hij met klem aan dat hij zich niet kan vinden in de uitkomsten van het onderzoek. Hij geeft aan ze naast zich neer te leggen en drukt jou op het hart om ze met niemand anders te delen. Toch ben je van mening dat het bestuur hier weet van zou moeten hebben. Wat doe je?

In mijn verschillende rollen als trainer, adviseur en vertrouwenspersoon begeleid ik gesprekken over de professionele grenzen van integriteit. Ik zie daarbij grote verschillen in de frequentie en de tijd die organisaties (bewust) nemen om een goed en gestructureerd gesprek over voorbeelden als hiervoor genoemd te voeren. Hoe het ook zij: als u de behoefte voelt om over dit soort situaties met iemand te sparren buiten uw directe werkomgeving, dan hoop ik dat u iemand hebt die voor u een vertrouwensfunctie kan vervullen. Dat kan een interne of externe vertrouwenspersoon zijn. Iemand die een luisterend oor biedt en helpt in het verkennen van verschillende informele en formele

handelingsmogelijkheden. Die de kluwen aan gedachten en gevoelens met u ontwart, u zuiverder helpt te oordelen of een gevoel van steun biedt om morele moed te tonen bij mogelijk lastige gesprekken. Het kan prettig zijn om te kunnen sparren met iemand die wat verder af staat van de eigen dagelijkse praktijk om tunnelvisie en 'beroepsblindheid' te voorkomen.

Juist u als auditor hebt de belangrijke verantwoordelijkheid om te waken over de grenzen van uw eigen professionele integriteit. Het goed bewaken van die grens kan niet zonder periodieke reflectie en dialoog in het licht van gezamenlijke uitgangspunten, professionele standards en de kernwaarden van de organisatie.

Daarnaast, hoe zit het eigenlijk met de opzet en werking van een interne meldregeling en de functie van vertrouwenspersonen? Wat mij opvalt:

- Dat het soms volstrekt onduidelijk is wie de vertrouwenspersonen zijn, omdat medewerkers hierover niet of nauwelijks zijn geïnformeerd.
- Dat vertrouwenspersonen op het gebied van integriteit niet altijd voldoende zijn opgeleid om hun belangrijke taken en verantwoordelijkheden goed uit te kunnen oefenen.
- Dat het beleid geen helderheid verschaft over vragen als wanneer, waar en hoe medewerkers signalen of meldingen van misstanden kunnen indienen.
- Dat onderzoeken naar misstanden op

een onzorgvuldige manier plaatsvinden en de rechten en plichten van melders, betrokkenen en werkgever tijdens een onderzoek onvoldoende in acht worden genomen.

Werkgevers hebben de wettelijke plicht en verantwoordelijkheid om te zorgen voor een integere en veilige werkomgeving. Dit betekent dat medewerkers zo min mogelijk drempels ervaren om misstanden te melden of dilemma's durven te bespreken. En dat de moed die zij tonen beloofd wordt in plaats van bestraft. Ik hoop dan ook dat audits naar de opzet en werking van het netwerk van vertrouwenspersonen en de interne meldregeling een prominente plek krijgen in de jaarplanning van auditafdelingen.

Terug naar het dilemma aan het begin van deze column: benieuwd naar wat in dit geval zorgvuldig en integer handelen betekent en hoe collega's hier mee om zouden gaan? Ik wens u veel morele moed om deze en andere praktijkvoorbeelden binnen uw eigen omgeving of tijdens een training ethiek en integriteit te bespreken.

Hakan Honders is oprichter van Bureau Indehaeck en trainer en adviseur integriteit, gedrag en cultuur en extern vertrouwenspersoon.

Beïnvloeding om **fiscale verplichtingen** na te komen

Van oudsher zijn belastingdiensten gewend om te sturen op en verantwoording af te leggen over hun 'output'.¹ Daarbij gaat het bijvoorbeeld om aantallen controles, het bedrag aan correcties dat zij naar aanleiding daarvan opleggen, aantallen achterstallige invorderingen en aantallen boetes. De samenleving verwacht van inspecties en toezichthouders en ook van de Belastingdienst echter steeds nadrukkelijker dat ze de effecten van hun handelen zichtbaar maken.²

Niet alleen de output moet in beeld worden gebracht, maar ook de mate waarin de beoogde doelen worden gerealiseerd, ofwel de 'outcome'. De aandacht voor en interesse in het meten van de effecten van het handelen van de Belastingdienst en andere organisaties in de publieke sector neemt dan ook sterk toe.

Het meten van de effectiviteit van de activiteiten van een organisatie is in toenemende mate een verantwoordelijkheid van de interne auditfunctie.³ Deze functie – in het algemeen, maar zeker in publieke organisaties – is namelijk in toenemende mate verantwoordelijk voor het beoordelen van niet-financiële informatie.⁴ Dit betekent dat steeds meer verschillende belanghebbenden verwachtingen blijken te hebben bij de interne auditfunctie. Het inzichtelijk maken van de effectiviteit van de activiteiten van de organisatie door de interne auditfunctie neemt daarmee in belang toe, maar is nog niet zo eenvoudig. Deze bijdrage beschrijft hoe effectmeting kan worden opgezet binnen de context van de Belastingdienst. Dit kan als voor-

beeld dienen voor effectmetingen in andere (publieke) organisaties en kan daarmee ook van belang zijn voor de interne auditfunctie.

Doelen

Waar gaat het om bij het meten van effecten door de Belastingdienst? In de Rijksbegroting staat de algemene doelstelling van de Belastingdienst verwoord: '(...) Doeltreffende en doelmatige uitvoering van [fiscale] wet- en regelgeving zorgt ervoor dat burgers en bedrijven bereid zijn hun wettelijke verplichtingen ten aanzien van de Belastingdienst na te komen (compliance)'.⁵ De Belastingdienst is verantwoordelijk voor de uitvoering van wet- en regelgeving en de essentie zit derhalve in het realiseren van compliance, zijnde de *bereidheid* van burgers en bedrijven om hun wettelijke fiscale verplichtingen na te komen.

Passende dienstverlening, adequaat toezicht en efficiënte massale processen moeten er voor zorgen dat belastingplichtigen



hun fiscale verplichtingen willen en kunnen nakomen, dat naleving zo nodig wordt afgedwongen en dat processen snel en foutloos worden uitgevoerd.⁶ De *Handhavingsstrategie Belastingdienst* beschrijft hoe de Belastingdienst met de inzet van verschillende instrumenten, gegeven de beschikbare capaciteit en middelen, zijn algemene beleidsdoel compliance beoogt te realiseren.⁷

Een lastig vraagstuk ook gezien de teruglopende capaciteit. De Belastingdienst kiest doelbewust welke instrumenten, in welke combinatie en met welke diepgang worden ingezet om in een bepaalde situatie de compliance te ondersteunen of te verbeteren. Voorbeelden van instrumenten zijn de belastingtelefoon, schriftelijke communicatie, tv-spotjes, aangiftebehandeling, boekenonderzoeken, bedrijfsbezoeken, convenanten in het kader van horizontaal toezicht en invorderings- en opsporingsmaatregelen. Bij voorkeur zet de Belastingdienst instrumenten proactief en preventief in, omdat dit effectiever en efficiënter is dan achteraf repressief op te treden.⁸

Om het gedrag van belastingplichtigen effectief te beïnvloeden, is inzicht vereist in de factoren die het gedrag bepalen; de zogenoemde determinanten van compliance. Wetenschappelijk onderzoek leert dat intrinsieke motieven, externe prikkels en de mogelijkheden voor naleving en niet-naleving, compliance bepalen.⁹ De intrinsieke motieven worden ook wel aangeduid met de term belastingmoraal, waaronder persoonlijke en sociale normen worden geschaard.¹⁰ Tot de externe prikkels behoren de (ervaren) pakkans en de mogelijke sanctie bij overtreding van de regel. Met zijn handhavingsactiviteiten beoogt de Belastingdienst de determinanten te beïnvloeden en daarmee de compliance. Via effectmeting kan beoordeeld worden in hoeverre dat lukt. Zie het *kader* voor een voorbeeld.

Opzetten van een effectmeting

Bij effectmeting gaat het om de vraag of en in welke mate inspanningen, activiteiten en interventies van de Belastingdienst ertoe hebben geleid dat het doel dat de Belastingdienst daarmee beoogt (compliance), ook is bereikt. Het gaat derhalve om

Aangiftecampagne

De Belastingdienst voert jaarlijks in maart een aangiftecampagne¹¹ in verband met het tijdig (voor 1 april) doen van de aangifte inkomstenbelasting. Het doel van deze campagne is om de compliance (in de vorm van tijdigheid van aangifte doen) van burgers te verhogen door middel van voorlichting. Aan een dergelijke aangiftecampagne ligt de aanname ten grondslag dat voorlichting de kennis bij belastingplichtigen verhoogt. De tweede aanname is dat deze verhoging van kennis leidt tot een verbetering in compliance. Door effectmeting kan worden getoetst of deze aannames kloppen. In de praktijk vindt het toetsen van het effect van dergelijke communicatie-uitingen niet structureel plaats.

het aantonen of aannemelijk maken van een oorzakelijk of causaal verband tussen de inspanningen van de Belastingdienst en de realisatie van doelen. Het realiseren van een strategisch doel verloopt overigens vaak via de realisatie van allerlei tussendoelen op lagere (tactische of operationele) niveaus. Voor het opzetten van een effectmeting moeten (beoogd) (tussen) doel, inzet van mensen en middelen, uitgevoerde activiteiten, concrete resultaten en de veranderingen in compliance-gedrag van belastingplichtigen met elkaar in verband worden gebracht. Dat kan worden geïllustreerd aan de hand van de zogenoemde effectketen (zie *figuur 1*).

Voor een goede effectmeting is dus noodzakelijk dat het beoogde doel expliciet, concreet en meetbaar is (SMART). Om effecten te kunnen meten moet ook de zogenoemde *beleids-theorie*, dat wil zeggen de veronderstelde relatie tussen de activiteiten en het beoogde doel (de relatie tussen output en outcome), expliciet zijn. En effectonderzoek dient zo te zijn opgezet dat hard, of ten minste aannemelijk, gemaakt kan worden dat de uitgevoerde activiteit het niveau van compliance (of een tussendoel) heeft beïnvloed.

Er zijn verschillende manieren om effectmeting op te zetten.¹² Een onderzoeksdesign met alleen een nameting of met een voor- en nameting levert geen uitspraak op over de causaliteit, omdat niet kan worden uitgesloten dat andere factoren dan de ontplooiende activiteit van invloed zijn op de compliance. Met een experimenteel design, waarbij een groep die de activiteit ondergaat (de experimentele groep) kan worden vergeleken met een (vergelijkbare) groep die de activiteit niet ondergaat (de controlegroep), kunnen wel (causale) uitspraken worden gedaan over het effect van activiteiten en instrumenten. Experimentele onderzoeksdesigns zijn er in allerlei vormen.¹³ Het ideale onderzoeksdesign is de zogenaamde 'randomized controlled trial' of gecontroleerd veldexperiment. De kracht van een dergelijk design zit in de vergelijkbaarheid van de experimentele groep en de controlegroep (door willekeurige toewijzing), waardoor een verschil in compliance tussen beide groepen na de activiteit (nameting) kan worden toegeschreven aan de activiteit (zie *figuur 2*). Met een dergelijk onderzoeksdesign wordt dus uitgesloten dat andere factoren dan de activiteit een verschil tussen de twee groepen hebben veroorzaakt.

In de praktijk is het lang niet altijd mogelijk of gewenst om een volledig gecontroleerd experiment uit te voeren. Het kan

moeilijk of zelfs onmogelijk zijn om een controlegroep te selecteren die volledig vergelijkbaar is met de experimentele groep. Ook kan het zo zijn dat een interventie niet precies gericht kan worden, waardoor ook de controlegroep met de interventie in aanraking kan komen. Ook kunnen tijdsbeslag, kosten, privacyaspecten of geheimhouding een rol spelen voor het wel of niet uitvoeren van een dergelijk experiment. Het is belangrijk om vooraf goed na te denken over de opzet van een onderzoeksdesign. Achteraf kan, wanneer het onderzoeksdesign niet perfect is, in de statistische analyse van de verschillen tussen de experimentele groep en de controlegroep nog een en ander worden gecorrigeerd. Maar een goed effectonderzoek staat of valt met het onderzoeksdesign.

Implementatie

Een uitdaging is om effectmeting op een structurele manier te borgen in de organisatie en onderdeel te maken van de manier van werken. Welp (2012) noemt drie redenen hiervoor: 1) de complexiteit van effectmetingen en de investering in tijd

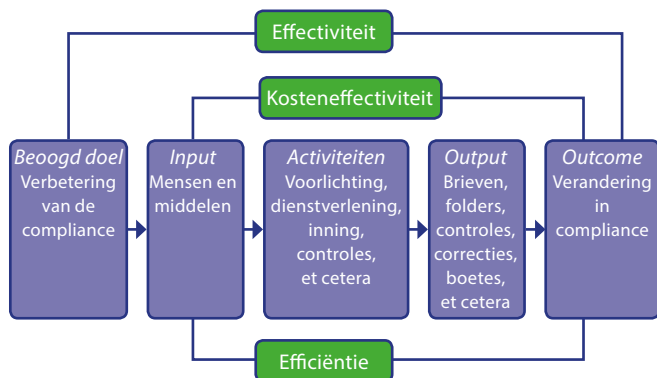
advertentie

De manier waarop, dat maakt het verschil.

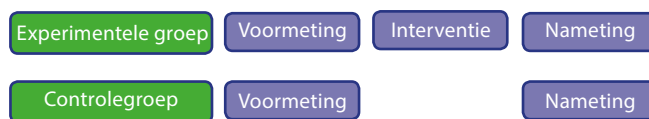
Door onze expertise binnen Internal Audit en een persoonlijke aanpak begeleiden wij met succes audit professionals in hun zoektocht naar een nieuwe uitdaging.



interim - search - advies
www.fellowfield.nl



Figuur 1. Effectketen



Figuur 2. Gecontroleerd veldexperiment

en geld die het uitvoeren ervan met zich meebrengt; (2) toezichthouders die 'risicogericht' werken zijn geneigd direct te willen handelen en zitten minder te wachten op 'langdurig(e)' analyse en onderzoek; (3) de cultuur binnen organisaties is onvoldoende stimulerend voor het uitvoeren van effectmetingen omdat de kans bestaat dat 'slecht nieuws' over prestaties van toezichthouders naar buiten kan komen.¹⁴ Voor effectmeting zijn specifieke kennis en vaardigheden nodig: kennis van methoden en technieken van onderzoek, van (theorieën over) gedragsbeïnvloeding en van het beleid en de werkwijze en werkzaamheden van de Belastingdienst. Het ligt daarom voor de hand om de (eind)verantwoordelijkheid voor effectmeting binnen een organisatie als de Belastingdienst centraal te beleggen bij een beperkte groep mensen die over de benodigde kennis en vaardigheden beschikt. Om effecten te kunnen meten zijn gegevens nodig. Indien mogelijk moeten gegevens gebruikt worden die voorhanden zijn in de organisatie als onderdeel van de 'normale' bedrijfsvoering. Als gegevens ad hoc opgeleverd moeten worden en/of 'apart' bijgehouden moeten worden, levert dit meer en lastig werk op en kan de motivatie en het draagvlak voor effectmeting afnemen. In de praktijk zullen overigens afhankelijk van het soort effectmeting, ook aanvullende gegevens (die niet in de 'bedrijfsvoering' aanwezig zijn) noodzakelijk zijn.

Tot slot

Informatie uit effectmetingen kan gelijktijdig meerdere doelen dienen: de Belastingdienst verantwoordt zich extern conform gemaakte afspraken door het openbaar maken van behaalde resultaten en gebruikt die informatie ook als input voor zijn handhavingsstrategie. Effectmeting kan de Belastingdienst helpen om zijn handhavingsinstrumenten gericht in te zetten teneinde gedrag van burgers en bedrijven inzake de naleving van fiscale regels op de lange termijn structureel te veranderen. Effectmeting is daarmee essentieel voor het leren, sturen en verantwoorden van de inzet van mensen en middelen. De uitgangspunten voor een goede effectmeting – zoals uiteengezet in deze bijdrage – zijn breed toepasbaar, ook buiten de Belastingdienst of zelfs buiten de overheid. In de discussie over de professionele ontwikkeling van de interne auditfunctie in een veranderende wereld komt de vraag naar voren hoe de interne auditfunctie een bijdrage kan leveren aan de effectiviteit van de organisatie. Van interne auditors wordt zodoende in toenemende mate verwacht dat zij ook een bijdrage leveren in het beoordelen van de effectiviteit van bedrijfsprocessen.¹⁵ Een lastig vraagstuk, waar de in deze bijdrage beschreven uitgangspunten mogelijk van pas kunnen komen. <<

Noten

1. OESO, *Co-operative Compliance: A Framework*, p. 75, 2013.
2. WRR, *Toezien op publieke belangen*, Amsterdam University Press, p. 58, 2013.
3. Ngah, J., 'Optimizing internal audit: internal auditors are being continually challenged to improve their effectiveness to better meet growing expectations and workloads', *Internal Auditor*, aug. 2016.
4. Schillemans, T. en M. van Twist, 'Coping with Complexity: Internal Audit and Complex Governance', *Public Performance & Management Review*, 40, p. 257-280, 2016.
5. Hoofdstuk IXb Financiën en Nationale schuld, artikel 1 'Belastingen'.
6. Rijksbegroting, Hoofdstuk IX.
7. De Handhavingsstrategie Belastingdienst is in 2016 op papier uitgewerkt maar vormde ook in de jaren daarvoor de basis voor de handhaving en uitvoering. <https://belastingdienst-in-beeld.nl/wp-content/uploads/2017/02/Handhavingsstrategie-Belastingdienst.pdf>
8. Belastingdienst (2017). Beleidsdoorlichting toezicht en opsporing en massale processen; Belastingdienst (2017). Handhavingsbrief Belastingdienst 2018: Dienstverlening, toezicht en opsporing.
9. Kirchler, E., *The Economic psychology of tax behavior*, Cambridge University Press, 2007.
10. Frey, B., 'The role of deterrence and tax morale in taxation in the European Union', *European Review*, 11, p. 385-406, 2003; Torgler, B., 'Tax morale, rule governed behavior and trust', *Constitutional Political Economy*, 14, p. 119-140, 2003.
11. Hel-Van Dijk, Van der en M. Siglé, 'Effectmeting van horizontaal toezicht bij grote ondernemingen', *Vakblad Tax Assurance*, 1, p. 63, 2013.
12. <http://www.rijksbegroting.nl/beleidsevaluaties/evaluaties-en-beleidsdoorlichtingen/handreiking-beleidsdoorlichtingen/het-meten-van-doeltreffendheid>.
13. Shadish, Cook & Campbell, *Experimental and quasi-experimental designs for generalized causal inference*, Boston, Houghton Mifflin, 2002.
14. Welp, 'Effectiviteit van toezicht: tijd voor responsive evaluation', *Tijdschrift voor Toezicht*, 2, p. 7-22, 2012.
15. Schillemans, T. en M. van Twist, 'Coping with Complexity: Internal Audit and Complex Governance', *Public Performance & Management Review*, 40, p. 257-280, 2016.

Sjoerd Goslinga, Lisette van der Hel-van Dijk en Maarten Siglé werken bij de Belastingdienst. Goslinga is daarnaast verbonden aan de Universiteit Leiden (onderzoeker). Siglé (PhD-student en docent) en Van der Hel (hoogleraar effectiviteit van overheids-toezicht) zijn beiden verbonden aan de Nyenrode Business Universiteit.

Dit artikel is gebaseerd op een artikel dat in uitgebreide vorm eerder is gepubliceerd in het *Tijdschrift voor Toezicht*, 'Het meten van effecten van de handhaving van de Belastingdienst', 2016.

Goed integriteitsmanagement loont

Misstanden op het werk. Je hoopt het nooit tegen te komen, maar hoe ga je ermee om als je ermee te maken krijgt? En welke rol kan de interne auditor vervullen als het gaat om het voorkomen van misstanden? Met deze vragen ging *Audit Magazine* op bezoek bij het Huis voor Klokkeluiders en sprak met Alain Hoekstra, deskundige op het gebied van integriteitsmanagement en met Arjen Wilbers, persvoorlichter en woordvoerder.

Hoe ziet de organisatie van het Huis er uit?

Arjan Wilbers (AW): “Het Huis is een zelfstandig bestuursorgaan en de oprichting daarvan is vastgelegd in de Wet Huis voor klokkenluiders. Het bureau kent een afdeling Advies, een afdeling Onderzoek en een afdeling Kennis & Preventie. De afdeling Advies is er voor werknemers, inclusief ex-werknemers, zzp'ers, uitzendkrachten en vrijwilligers, die

te maken hebben met (mogelijke) misstanden. De afdeling Onderzoek is verantwoordelijk voor onderzoek naar misstanden op zaakniveau. De afdeling Kennis & Preventie richt zich op preventie.”

Wat wordt in dit kader verstaan onder ‘misstanden’?

AW: “Kort gezegd gaat het om werkgerelateerde misstanden waarbij sprake is van een overtreding van wet- en regelgeving of onbehoorlijk handelen/nalaten. Daarnaast zijn er doorgaans meerdere mensen bij betrokken, heeft het een structureel karakter en is er sprake van een inbreuk op het algemeen maatschappelijk belang. Het aanklaarten van misstanden gaat helaas vaak niet goed en resulteert regelmatig in een geschil met de werkgever. Vaak is er een traject van integriteitschendingen aan vooraf gegaan.”

Alain Hoekstra (AH): “Wanneer het een medewerker niet lukt om integriteitschendingen te adresseren dan neemt de impact hiervan op de organisatie toe en worden de negatieve gevolgen geleidelijk ernstiger. De stellingen worden betrokken en de opstelling naar elkaar wordt harder. Er gaat bovendien een katalyserende en besmettelijk effect uit van integriteitsschendingen waardoor je ziet dat het binnen een organisatie van kwaad tot erger gaat. Uiteindelijk kunnen integriteitsschendingen dan uitgroeien tot misstanden. Om dit te voorkomen stimuleren wij werkgevers aandacht te hebben voor (beter) integriteitsmanagement en ondersteunen wij hen hierbij.”



Over...

Drs. Alain Hoekstra werkt bij het Huis voor Klokkeluiders als deskundige op het gebied van ethiek en integriteit. Hij was een van de oprichters van het Bureau Integriteitsbevordering Openbare Sector (BIOS) en is als promovendus verbonden aan de Erasmus Universiteit.



Arjen Wilbers is communicatieadviseur en woordvoerder van het Huis voor Klokkeluiders.

Is er voldoende aandacht bij overheden en bedrijfsleven voor het voorkomen van misstanden?

AW: “De afdeling Kennis & Preventie richt zich op het motiveren en ondersteunen van werkgevers om vorm en inhoud te geven aan integriteitsbevordering/-management. Het gaat dus om de preventieve kant van een goed opgetuigd integriteitsbeleid. De resultaten van het onderzoek *Verkenning Meldprocedures en Integriteitsvoorzieningen* (2017) onder ondernemingsraden laten zien dat preventie aandacht verdient (zie tabel 1).”

AH: “De resultaten van deze Verkenning bieden inzicht in de aanwezigheid van een aantal integriteitsmaatregelen in drie sectoren: de publieke, semipublieke en private sector. Deze maatregelen worden cruciaal geacht voor het bevorderen van een ethische organisatie. Het zijn maatregelen waar werkgevers verantwoordelijk voor zijn en waar werknemers recht op hebben. De Verkenning geeft aan dat integriteitsbeleid onder de maat is, zowel op de ‘harde’ als op de ‘zachte’ maatregelen. Met name de situatie bij de overheid blijkt zorgelijk, zeker gezien het feit dat de Nederlandse overheid al ruim 25 jaar investeert in integriteitsbeleid.”

Wat is nu het belangrijkste als het gaat om een goed integriteitsklimaat?

AW: “Cruciaal is de tone at the top. Dat je als top van de organisatie moreel leiderschap toont en uitstraalt dat het menens is. Dat je serieus werk maakt van integriteit.”

AH: “En dan bij voorkeur vanuit een positieve benadering. Als management heb je namelijk veel te winnen bij een goed integriteitsklimaat. Maak zichtbaar wat de businesscase is, waarom het loont om in integriteitsmanagement en in sociale veiligheid te investeren. Wanneer het integriteitsklimaat goed is zie je veel meer wat er binnen de organisatie speelt, gaat de arbeidsvreugde omhoog, vermindert het ziekteverzuim en word je aantrekkelijker als werkgever. Leiderschap moet je ook herhaaldelijk uitdragen. Het management kan er namelijk ook voor zorgen dat vertrouwenspersonen, integriteitscoördinatoren, et cetera, voldoende budget en ruimte krijgen om de ‘structuurkant’ van integriteitsmanagement op orde te krijgen en om invulling te geven aan de cultuuraspecten.

Wat ik ook belangrijk vind is dat de risico’s en kwetsbare plekken op het gebied van integriteit en ethiek inzichtelijk zijn. Dat dit periodiek in kaart wordt gebracht én dat maatregelen worden getroffen om de zwakke plekken te versterken. Vergelijkbaar met een stresstest bij banken. Het gaat erom of je weerbaarheid goed georganiseerd is om kwetsbaarheid te minimaliseren.”

Naast de afdeling Kennis en Preventie is er de afdeling Advies en de afdeling Onderzoek. Hoe zien adviezen aan mensen die contact opnemen met het Huis er uit.

AW: “Sinds de invoering van de Wet Huis voor klokkenluiders op 1 juli 2016 geldt voor alle organisaties met meer

	Maatregelen	Publiek	Semipubliek	Privaat
C	Open cultuur	50	32	63
U	Intern kritiek	44	32	52
L	Durven melden	32	29	43
T	Angstcultuur	15	17	16
U	Directie communiceert over integriteit	36	40	52
R	Bij misstanden wordt goed gehandhaafd	48	52	55
S	Gedragscode	79	77	85
T	Actualiseren gedragscode	25	46	49
R	Vertrouwenspersoon	92	88	85
U	VP zichtbaar	28	31	30
U	VP vertrouwen	35	51	49
C	Meldprocedure aanwezig	78	87	72
T	Meldprocedure actueel (HvK)	45	58	42
U	Onderzoeksprotocol	57	64	60
U	Organisatie goed voorbereid op melding	44	52	55
U	Integriteitsbeleid	53	38	48
R	Integriteitsfunctionaris	58	44	42

Tabel 1. De aanwezigheid van een aantal integriteitsmaatregelen in drie sectoren (% ja of geheel/gedeeltelijk mee eens (volgens leden van ondernemingsraden). Bron: Verkenning Meldprocedures en Integriteitsvoorzieningen, 2017



GEZOCHT: TALENTVOLLE PROFESSIONALS

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

Voor een bank in de regio Amsterdam zoeken we een:

Internal Auditor financial services (Sr)

Voor een productiebedrijf in de regio Amsterdam zoeken we een:

**IT Auditor (Sr)
Operational Auditor (Sr)
Technical Auditor (Sr)
Manager Internal Audit**

Voor een productiebedrijf in de regio Eindhoven zoeken we een:

**Business Improvement Manager
Internal Control Manager**

Voor meer informatie verwijzen we je graag door naar onze website:

WWW.RSG.NL

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



RSG FINANCE HUMAN KEY SOLUTIONS



ACCOUNTANT? EN NU?

Je bent je carrière gestart binnen de Accountancy en hebt wellicht daarna een aantal jaar bij een grote (internationale) organisatie gewerkt.

En nu wil je verder! Je wilt je werkveld verbreden. Herkenbaar?

RSG biedt Finance Professionals de kans zich te ontwikkelen. En het goede nieuws is: bij RSG sta jij, onze Finance Professional, centraal!

Ons organisatie-model is erop gericht je te boeien en je aan ons te binden, met een arbeidsvoorwaardenpakket waar je blij van wordt: naast een vast salaris deel je mee in de winst van jouw opdracht! Dat noemen wij het "Flexibel Vennoot Model".

Meer weten? Ga naar onze website: rsg.nl/flexibel-vennoot-model



RSG FINANCE
HUMAN KEY SOLUTIONS

RSG Finance BV

Vestdijk 57a
5611 CA Eindhoven
The Netherlands

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



dan vijftig werknemers de plicht tot het invoeren van een meldprocedure. Werknemers kunnen bij een vermoeden van een misstand al contact met ons opnemen voor advies of ondersteuning. De regie over dit contact en het uiteindelijk wel of niet doen van een melding ligt altijd bij de persoon die contact met ons opneemt. Een melding moet in de regel eerst intern binnen de organisatie worden gedaan. Het is belangrijk dat die melding goed gedaan wordt en daar kunnen de adviseurs van het Huis bij adviseren. Daarna is het belangrijk dat een werkgever goed met de melder en de melding omgaat. Dit is in de praktijk helaas niet altijd het geval. Maar liefst 75% van de klokkenluiders zegt benadeeld te worden door het doen van een interne melding.”

AH: “Overigens is het vaak geen bewuste keuze van mensen om klokkenluider te worden, maar rolt men er gewoon in. Wanneer er na het melden van een misstand niet (adequaat) wordt gereageerd door de werkgever, dan verharden de stellingen zich geleidelijk. En op een gegeven moment ziet men als interne melder van die misstand geen weg meer terug. Een groot aandeel van de mensen die een interne melding doet krijgt daar psychologische klachten door, voortkomend uit een gevoel van onrecht en onmacht. Onze medewerkers van de afdeling Advies kunnen hulp bieden op psychosociaal vlak of kunnen doorverwijzen naar andere deskundigen. Ook niet onbelangrijk is dat collega’s zien wat er met iemand gebeurt die iets gemeld heeft, dat heeft effect op de meldingsbereidheid van die collega’s.”

En tot slot de afdeling Onderzoek?

AW: “Die afdeling doet onder bepaalde voorwaarden onderzoek op verzoek van een klokkenluider. Soms is een onderzoek van het Huis voor Klokkenluiders een ‘last resort’, bijvoorbeeld wanneer het OM of een inspectie nog geen onderzoek hebben verricht. Ons onderzoek kan zich richten op zowel de misstand zelf als op de bejegening van de

Huis voor Klokkenluiders en Wet Huis voor klokkenluiders

Op 1 juli 2016 trad de Wet Huis voor klokkenluiders in werking. De Wet introduceert rechtsbescherming voor klokkenluiders en voorziet in de oprichting van het Huis voor klokkenluiders (het Huis) dat:

- melders van misstanden adviseert,
- onderzoek doet naar maatschappelijke misstanden of naar de behandeling van de klokkenluider,
- voorlichting op het gebied van integriteit geeft aan werkgevers.

melder. Dit kan soms lastig en tijdrovend werk zijn omdat klokkenluiderszaken vaak jaren hebben gespeeld, organisaties niet altijd meer bestaan of betrokkenen er bijvoorbeeld niet meer zijn.”

Welke rol kan een internal auditor spelen als het gaat om preventie van misstanden?

AH: “Internal Audit zou heel goed een onderzoek naar de aanwezige integriteitsmaatregelen, zowel de harde als de zachte, in de eigen organisatie kunnen uitvoeren. Vergelijkbaar met de verkenning op hoofdlijnen zoals wij die hebben uitgevoerd. Met het uitvoeren van een dergelijk onderzoek kan een auditor inzicht verschaffen in het integriteitsmanagement en kunnen op basis van de resultaten maatregelen genomen worden die bijdragen aan het voorkomen van misstanden. En verder zou je er voor kunnen zorgen dat vragen over integriteit standaard worden meegenomen in medewerkertevredenheidsonderzoeken.”

AW: “Als internal auditor kun je overigens best eens bij de afdeling Kennis en Preventie aankloppen voor advies over het opzetten van een dergelijk onderzoek. Bij die afdeling is veel kennis aanwezig die ook voor vertrouwenspersonen, de ondernemingsraad, hrm-afdelingen, bedrijfsartsen en complianceafdelingen van belang kan zijn. En die kennis is ook relevant voor internal auditors bij het ontwerpen van audits op het gebied van ethiek en integriteit.” <<

AVG: techniek of gedrag?

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Organisaties die persoonsgegevens verwerken krijgen dan meer verplichtingen. Meer dan onder de huidige Wet bescherming persoonsgegevens (Wbp) ligt de verantwoordelijkheid bij de organisaties zelf om aan te tonen dat zij voldoen aan de eisen van de wet. Wat zijn de belangrijkste elementen van de AVG en waar ligt de nadruk: op techniek of gedrag?

Al vele jaren moeten organisaties die – al dan niet bijzondere – persoonsgegevens verwerken voldoen aan privacyregels. De huidige Wbp is inmiddels goed bekend in Nederland. Onder deze wet moeten organisaties die persoonsgegevens verwerken (of: ‘bewerken’) zich houden aan een aantal regels, zoals het vastleggen van het doel van de verwerking, het op een adequate wijze beveiligen van persoonsgegevens en het melden van datalekken. De Autoriteit Persoonsgegevens (AP) is verantwoordelijk voor het handhaven van de regels. Waar nodig, kan de AP onderzoek uitvoeren bij organisaties of zelfs een bestuurlijke boete tot 820.000 euro opleggen. Hoewel de Wbp goed bekend is in Nederland, is het maar de vraag in hoeverre organisaties de huidige wet écht serieus nemen.

Met de nieuwe AVG, in Europa bekend als General Data Protection Regulation (GDPR), verandert het een en ander drastisch. Niet alleen wordt het aantal rechten van ‘natuurlijke personen’ flink uitgebreid, ook worden de rechten inhoudelijk versterkt. Hierdoor neemt de impact op organisaties die persoonsgegevens verwerken fors toe. Tot slot gaat het er niet alleen om dát je als organisatie voldoet aan die nieuwe regels, maar dat je dat ook aantoonbaar doet. Dus niet meer impliciet, maar expliciet compliant zijn. En als kers op de taart: als organisaties ernstig en/of verwijtbaar de nieuwe regels aan hun laars lappen, kan de bestuurlijke boete oplopen tot zelfs 20 miljoen euro of 4% van de wereldwijde jaaromzet!

Stappenplan

Inmiddels zijn zowel door de AP als door andere organisaties handreikingen en stappenplannen geïntroduceerd teneinde te helpen aan de AVG te voldoen. De AP heeft eind 2017 het *In 10 stappen voorbereid op de AVG* gepubliceerd, die de belangrijkste stappen beschrijft.

Stap 1 – Bewustwording

Relevante stakeholders, zoals directie en beleidsmakers, moeten bekend zijn met de AVG. Zij moeten bepalen wat de impact ervan is op de organisatie, processen en

Hoe beter de beveiliging hoe sneller mensen geneigd zijn het olifantenpaadje te willen vinden

werkwijzen en welke aanpassingen nodig en wenselijk zijn. Aanpassingen aan organisatie, processen en werkwijzen als gevolg van de AVG kunnen behoorlijke impact hebben, zelfs op het verdienmodel.

Stap 2 – Rechten van betrokkenen

Met de AVG krijgen betrokkenen (natuurlijke personen) niet alleen sterkere, maar ook meer rechten. Versterkte rechten zijn er bijvoorbeeld ten aanzien van inzage, correctie en verwijdering. Een nieuw recht is er ten aanzien van data-portabiliteit, waarbij betrokkenen hun gegevens eenvoudig moeten kunnen opvragen ten behoeve van bijvoorbeeld een overstap naar een andere leverancier.

Stap 3 – Overzicht verwerkingen

Organisaties moeten in een ‘verwerkingenregister’ in kaart brengen welke persoonsgegevens worden verwerkt, met welk

vooraf de privacyrisico's van een gegevensverwerking in kaart gebracht en kunnen vervolgens de juiste maatregelen worden bepaald om de risico's te beperken. Indien er onvoldoende (sterke) beperkende maatregelen zijn, is er de verplichting om vooraf de AP te raadplegen.



doel, waar de gegevens vandaan komen en met wie ze worden gedeeld. Onder de AVG is er een verantwoordingsplicht, dat wil zeggen dat aangetoond moet kunnen worden dat conform de wetgeving wordt gewerkt. Het verwerkingenregister is onderdeel van de verantwoordingsplicht, maar is ook nodig om de privacyprocessen goed uit te kunnen voeren. Bijvoorbeeld bij het opvragen, corrigeren of verwijderen van persoonsgegevens.

Stap 4 – Data protection impact assessment

Als een beoogde gegevensverwerking een hoog privacyrisico met zich meebrengt, is het verplicht om een data protection impact assessment (DPIA) uit te voeren. Daarmee worden

Stap 5 – Privacy by design & privacy by default

Belangrijke uitgangspunten van de AVG zijn privacy by design en privacy by default.

Privacy by design houdt in dat al bij het ontwerpen van producten en diensten de vereisten van de AVG worden toegepast. Bijvoorbeeld een adequate bescherming, het niet meer gegevens verzamelen dan strikt benodigd voor het beoogde doel en niet langer dan benodigd (of wettelijk vereist) bewaren. Niet meer ‘nice to have’ maar ‘need to have’.

Privacy by default houdt in dat technische en organisatorische maatregelen worden genomen om te zorgen dat, als standaard, alléén persoonsgegevens worden geregistreerd en verwerkt die noodzakelijk zijn voor het specifieke doel

van de verwerking. Het bekende standaard ingevulde vinkje bij 'akkoord met algemene voorwaarden' mag dan niet meer, gebruikers moeten zelf ondubbelzinnig akkoord geven.

Stap 6 – Functionaris gegevensbescherming

Bepaalde organisaties zijn verplicht om een formele Functionaris Gegevensbescherming (FG) aan te stellen. Dit geldt in de basis voor overheids- en publieke organisaties, voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen en voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken en waarvoor dit een kernactiviteit is.

Stap 7 – Meldplicht datalekken

Net als onder de Wbp geldt onder de AVG een meldplicht voor datalekken. De AVG stelt wel strengere eisen aan de registratie en documentatie van de datalekken, op basis waarvan de AP moet kunnen controleren of aan de meldplicht is voldaan.

Stap 8 – Bewerkersovereenkomsten / Verwerkersovereenkomsten

Indien (een deel van) de verwerking van persoonsgegevens is uitbesteed aan een derde partij (bewerker, 'verwerker' volgens de AVG), moet beoordeeld worden of deze partij ook op de juiste manier voldoet aan de eisen van de AVG ten

aanzien van persoonsgegevens die zijn 'uitbesteed'. Een en ander dient vastgelegd te zijn in een verwerkersovereenkomst. Uitbesteden betekent dus niet het uitbesteden van de verantwoordelijkheid.

Stap 9 – Leidende toezichthouder

Wanneer een organisatie vestigingen in meerdere EU-lidstaten heeft dan wel de gegevensverwerkingen impact hebben in meerdere lidstaten, bijvoorbeeld een webwinkel die in meerdere landen actief is, hoeft er onder de AVG nog maar met één privacytoezichthouder te worden gewerkt: de leidende toezichthouder. Bepaald moet worden onder welke toezichthouder de organisatie valt.

Stap 10 – Toestemming

Het verzamelen en verwerken van persoonsgegevens mag niet zomaar plaatsvinden. Er moet sprake zijn van een algemeen belang, een gerechtvaardigd belang, een vitaal belang, een overeenkomst, een wettelijke verplichting of toestemming van de betrokkene. De AVG stelt strengere eisen aan toestemming. Aangetoond moet kunnen worden dat geldige toestemming is verkregen om van een betrokkene persoonsgegevens te verwerken. Voorts moet het intrekken

advertentie

www.pwc.nl

PwC Internal Audit. Expect More.

Internal Audit Services

Anoep Singh

Telefoon: +31 (0)6 1261 7579

anoep.singh@pwc.com



pwc

Het belang van cultuur en gedrag voor de interne beheersing van organisaties is evident en heeft in de herziene corporate governance code een stevige verankering gekregen. Van de interne auditor wordt verwacht dat deze de cultuur van de organisatie op waarde kan schatten.

Desondanks hebben interne auditors vaak koudwatervrees om de cultuur te toetsen. Een gemiste kans. Uit onderzoek blijkt immers dat interne auditors bijna vijf keer vaker fraude signaleren dan externe accountants. Wij helpen u graag met het evalueren van de cultuur. Met een multidisciplinair audit team waarin cultuur- en gedragsexperts zijn opgenomen, ondersteunen wij u doelgericht met een aanpak die specifiek is toegesneden op uw organisatie.

Wij wisselen graag met u van gedachten welke cultuur- en gedragsaspecten uw organisatie uniek maken en wat de impact daarvan is op uw interne beheersing.

©2018 PricewaterhouseCoopers B.V. (KvK 3412089) Alle rechten voorbehouden.

van de toestemming net zo makkelijk zijn als het geven van toestemming.

Techniek of gedrag?

Zoals in het 10-stappenplan zichtbaar is, betekent het aantoonbaar voldoen aan de AVG het naleven van een flinke set van formele regels. De vraag is of de primaire oplossingsrichting hiervoor ligt in de techniek. In bijvoorbeeld goede beveiliging of het vragen van expliciete toestemming. Of ligt de primaire oplossingsrichting meer aan kant van de business, de bewustwording en het gedrag van de organisatie? Het antwoord is: het laatste! Het gaat dan met name om zaken als verzameloede, schijnveiligheid en werkbaarheid. Allereerst de ontbrekende verzameloede, we lijken soms wel strandjutters. Alles wat aanspoelt, is van ons en bewaren we. Geen idee of de eigenaar het goed vindt, maar laten we het maar gewoon bewaren en waar nodig gebruiken. 'Doe mij ook een kopietje' of 'doe dat er maar voor de zekerheid bij' zijn hiervan typische voorbeelden. Hiermee verzamelen en bewaren we – soms écht onbewust – enorme hoeveelheden (persoons)gegevens. Van cv's van sollicitanten die we jarenlang bewaren tot kopietjes van een paspoort 'voor het geval dat'. Op dit vlak hebben we allemaal opvoeding nodig: afvragen waarom we die informatie willen of écht nodig hebben. Maar ook of we die gegevens wel mogen hebben. Daarnaast is er de schijn van veiligheid door de veelvuldige focus op informatiebeveiliging. Doordat er zoveel aandacht voor is, denken we (te) snel dat ons niets meer kan gebeuren. 'Het zal best goed beveiligd zijn' denken we dan. Maar aan de achterkant van het schijnbaar veilige fort zit het gezellige achttertuintje waar de medewerkers vertoeven. Medewerkers die zich veilig wanen, 'we hebben immers een virusscanner en een firewall', maar ook medewerkers die graag gemak willen hebben en de onbegrijpelijke of onwerkbare regels graag omzeilen. Hoe beter de beveiliging – en daarmee des te meer sloten op de deur – hoe sneller mensen geneigd zijn toch het olifantenpadje, ook wel de 'work around', te willen vinden. Je kent het wel, het versleten stukje graspad dat naast de mooie en dure slagboom loopt. Of de nooddeur aan de achterkant van het zwaarbeveiligde gebouw die de hele dag open is om makkelijk van en naar het rookhok te kunnen lopen. Dit zijn niet alleen figuurlijk, maar ook letterlijk de achterdeuren waar kwaadwillenden naarstig naar op zoek zijn.

Wat te doen?

Veiligheid en compliance zijn zaken waar we ons allereerst goed bewust van moeten zijn. We moeten het 'waarom' begrijpen. We moeten ons ervan bewust zijn waarom we iets verzamelen en wat we ermee doen. En waarom we het op een bepaalde manier beveiligen. Maar ook waarom de personen in kwestie bepaalde rechten hebben. Bewustwording is ook jezelf afvragen wat je ervan zou vinden als dat jouw – al dan niet bijzondere – persoonsgegevens zouden zijn. De spiegel voorhouden dus.

Tot slot moet het werkbaar zijn. Anders maak je – bewust of onbewust van de regels – 'voor het werkgemak' toch die lokale kopie van de klantgegevens op je privétablet. En ben je onbewust onderweg naar non-compliance. Of naar erger: een datalek.

Soms kunnen we gewoon wat minder opvragen en bewaren om nog steeds prima ons werk te kunnen doen. Waarom

heeft een internetwinkel je volledige geboortedatum nodig? Is een geboortjaar niet genoeg? En waarom moet je je fysieke adres opgeven voor een elektronische nieuwsbrief? Allemaal nice to have!

We moeten dus toe naar een situatie dat we minder gaan opvragen en bewaren. En laat dát nu grote voordelen hebben. Niet alleen kom je met minder verzamelen per definitie dichter bij naleving van de AVG. Maar als je minder bewaart, hoef je ook minder (en soms minder streng) te beveiligen. En je houdt zelfs (opslag)ruimte over! Als je geen smartphone naar het strand meeneemt, kan die ook niet gestolen of nat worden. Easy, toch?

Of toch niet zo easy? De smartphone – overigens ook zo'n prachtige bron van interessante informatie voor kwaadwillenden – vinden we écht onmisbaar. Net als data. Maar is dat

*We moeten ons ervan
bewust zijn waarom we
iets verzamelen en wat
we ermee doen*

zo? Moeten we niet gewoon afkicken van onze verzamelverslaving? We kunnen dat misschien maar beter gelijkmatig doen, anders ondergaan we voordat we het doorhebben de 'cold turkey' van de toezichhouder.

Begin dus met een goede inventarisatie van wat je opslaat en waarom. Ga vervolgens aan de slag met dataminimalisatie, opruimen en keuzen maken dus. Maak tegelijk de organisatie bewust van de eisen van de wet en wat van medewerkers zelf wordt gevraagd. Start dus met weinig techniek en veel gedrag! <<

Laszlo Nagy is hoofdredacteur van *Audit Magazine* en directeur Business Risk Services bij Improven.
Linkedin: <https://www.linkedin.com/in/laszlo-nagy-44735a4/>

Gert-Jan Willig:

“De beperkte omvang dwingt ons optimaal samen te werken met andere afdelingen”

PAS op de plaats is een rubriek waarin auditors van kleine auditdiensten aan het woord komen. Dit keer Gert-Jan Willig, hoofd Internal Audit bij het Havenbedrijf Rotterdam.

Kunt u iets vertellen over de internal auditfunctie (IAF) van het Havenbedrijf Rotterdam?

“Het Havenbedrijf Rotterdam (HbR) is de beheerder en exploitant van het haven industrieel complex in Rotterdam. Dit houdt in dat HbR het gebied exploiteert door het graven van kanalen en het aanleggen van kademuuren en infrastructuur ten behoeve van haar klanten, die zich als huurders vestigen. Daarnaast kent HbR een publieke taak als havenmeester die zorgdraagt voor een veilige en efficiënte afwikkeling van het scheepvaartverkeer.

De IAD van HbR bestaat uit drie vaste medewerkers. De verschillende expertises zijn goed aanwezig in de zin dat zowel de RA-, CIA-, CISA- als RO-achtergrond en ervaring aanwezig zijn. We zijn een kleine afdeling, maar wel goed aangehaakt bij de algemene directie en het management. We proberen onze onderwerpen steeds zo te kiezen dat we zoveel mogelijk toegevoegde waarde kunnen bieden aan zowel het bedrijf, het management als de toezichthouders. In ons auditplan is naast ‘vaste’ onderwerpen ook ruimte ingebouwd om op actuele onderwerpen of verzoeken vanuit de directie in te kunnen springen.”

Welke type onderzoeken voert de IAF uit?

“Dat varieert van het beoordelen van de projectbeheersing en de aanbesteding bij grote projecten tot compliance en advies. We zijn begonnen bij de basis. Dit bestond uit het adviseren bij de opzet van control frameworks en de inrichting van autorisaties in ons kernsysteem SAP. Vervolgens hebben we ons gericht op de onderwerpen compliance en integriteit. Het creëren van een e-learningplatform waarmee onder andere onze bedrijfscode actief onder de aandacht is gebracht, mag je hierbij gerust een succes noemen. Voorts hebben we ons gericht op projecten, zoals de realisatie van het Theemswegtracé, een spoorwegtracé van 4 km met viaducten en fly-overs door de haven. Ook richten we ons op risicomanagement en actuele thema's, zoals het omgaan met terroristische dreiging.”

Voert de IAF ook tweedelijfstaken uit?

“We proberen onafhankelijk en objectief te blijven, maar gelijktijdig zo helder mogelijk te adviseren. We hebben als IAD een ‘consultancy mindset’. Dit kan betekenen dat we

Algemene informatie

Aantal fte organisatie	1164
Aantal fte IAD	3
Rapporteert aan	CEO en auditcommissie

We hebben als IAD een 'consultancy mindset'

het voortouw nemen, zoals bij de ontwikkeling van control frameworks, of voor korte termijn de leiding op ons nemen om een initiatief van de grond te krijgen. We proberen dergelijke onderwerpen vervolgens wel weer spoedig over te dragen aan de (tweede) lijn. In geval we niet meer objectief over een initiatief kunnen oordelen, schakelen we een derde partij in voor een objectief oordeel.

In het kader van de corporate social responsibility (CSR) van HbR geven we samen met de CSR-manager dilemma-training aan de medewerkers in de business. Aan de hand van meer filosofische denkmodellen proberen we dilemma's uit de praktijk te ontleden en de handelwijze op basis van juiste afwegingen te laten plaatsvinden."

is de scrum/agilemethode die binnen IT best practice is geworden. Als auditor word je gedwongen om na te denken over waar de goede aanknopingspunten voor de audit zich bevinden."

Op welke manier vindt kwaliteitsborging plaats?

"Bij de uitvoering van een audit organiseren we meerdere meetings waarin we de doelstelling, de aanpak, de voortgang en de bevindingen bespreken binnen het team en met de auditee. Voor het definitief worden van een auditrapportage zijn dus meerdere iteraties en afstemmingen gangbaar.

Dossiervorming krijgt ook veel aandacht. In het bijzonder daar waar de externe accountant steunt op de werkzaamheden van de IAD wordt teruggevallen op de eigen dossiervorming."

Wat is de ambitie van de IAF op de langere termijn?

"De IAD meer een kweekvijver voor talenten binnen de organisatie te laten zijn. Trainees kunnen dan bijvoorbeeld enige tijd meedraaien om een brede

(verbeter) blik op de organisatie te ontwikkelen. De directie heeft zich inmiddels achter dit idee geschaard. Wat betreft ontwikkeling is recent een van de vaste medewerkers hoofd IAD geworden bij een woningcorporatie. Dat de ervaring opgedaan binnen (de IAD van) HbR daaraan heeft bijgedragen is een mooi compliment. Het betrof een externe stap, in de toekomst zou het mooi zijn als ook intern dergelijke stappen gezet kunnen worden."

Wat is de relatie met de externe accountant?

"Zowel met de voorgaande (EY) als de nieuwe accountant (PwC) is die relatie goed te noemen. We voeren een open dialoog en delen bevindingen. We stemmen goed af hoe we zaken kunnen optimaliseren, zoals bij de audit op het jaarverslag waar de IAD in hoge mate de audit uitvoert en de dossiervorming verzorgt, en PwC vervolgens de eigen verplichte werkzaamheden uitvoert en de verklaring afgeeft."

Met welke uitdagingen krijg je als kleine IAF te maken?

"De ambitie om veel onderwerpen op te pakken versus de capaciteit. De beperkte omvang dwingt ons om optimaal samen te werken met andere afdelingen. We richten ons veel op de procesverbetering en proberen detailwaarnemingen deels te 'outsourcen' naar bijvoorbeeld de afdeling Controlling."

Hoe zorgt u ervoor dat u op de hoogte blijft?

"Als afdeling gaan we jaarlijks naar de IIA-conferentie en we hebben onze PE-verplichting. Round tables en trainingen bezoeken horen er ook bij. Uiteindelijk is HbR een omgeving waarin veel aandacht is voor vernieuwing op gebied van new business, energietransitie en digitalisering. Als IAD moeten we steeds nadenken wat de best practices zijn om daar iets van te kunnen vinden. Mooi voorbeeld



Over...

Gert-Jan Willig is hoofd Internal Audit bij het Havenbedrijf Rotterdam.

Werken *met* cultuur

Cultuur, en in het bijzonder veiligheidscultuur, is binnen het domein van veiligheid inmiddels een vertrouwd concept. Dit concept werd voor het eerst in 1986 gebruikt na de ramp met de nucleaire reactor in Tsjernobyl. Wat zijn de ervaringen vanuit het domein veiligheid met cultuur(onderzoek) en wat is de rol van de internal auditor?

Het begrip cultuur is omgeven door wetenschappelijke discussies over, onder andere, de manier waarop cultuur onderzocht kan worden. Is cultuur meetbaar? Veranderbaar? Dit levert verschillende standpunten op die lijnrecht tegenover elkaar kunnen staan. In de literatuur wordt veel gediscussieerd welk standpunt beter is.

Eén manier om hiermee om te gaan is om deze verschillende standpunten op het gebied van cultuur te benaderen als zienswijzen die je alle verder kunnen helpen met cultuur in de dagelijkse praktijk. Het uitgangspunt is dat de standpunten elkaar niet bijten, maar omdat ze vanuit een ander perspectief geschreven zijn elkaar juist kunnen aanvullen. Ieder standpunt biedt daarmee zijn eigen blik op de werkelijkheid. En daar gaat het tenslotte om, om *werken met* cultuur, in tegenstelling tot *veranderen of beïnvloeden* van cultuur.

Verschillende perspectieven

Zoals eerder genoemd kan cultuur vanuit verschillende perspectieven benaderd worden. Aan de ene kant staat het essentialistisch perspectief. In de wetenschap is essentialisme een opvatting waarbij je veronderstelt dat er iets essentieels, iets fundamenteels, bestaat wat betrekkelijk onveranderlijk is en dat dit essentiële doorwerkt en zich toont in het gedrag van mensen (of de aard van objecten). Het doel van de wetenschap is dan om dit essentiële te achterhalen. Zoiets essentieels kan bijvoorbeeld een bedrijfs-cultuur zijn. De psychologie kent veel essentialistische concepten, bijvoorbeeld intelligentie (met IQ als essentie) of persoonlijkheid (met karakter als essentie). Daarnaast bestaat het contextuele perspectief. Dit perspectief stelt dat mensen met elkaar samenwerken in een bedrijf en op basis daarvan met elkaar gedragspatronen ontwikkelen, waar verder niets essentieels aan is. Die patronen

worden door de context bepaald en hangen bovendien af van de aard van de ontmoeting die plaatsvindt. In deze benadering beïnvloed je op basis van (de kwaliteit van) de interactie het gedrag. De focus ligt hier dus op (de kwaliteit van) de interactie. Het essentiële perspectief en contextuele perspectief zijn twee verschillende perspectieven met ieder een eigen instrumentarium.

Werken met cultuur

Een cultuur ontstaat overal op plekken waar mensen met elkaar samenwerken en waar gecoördineerd handelen noodzakelijk is. Zo ontstaan bepaalde patronen en als deze succesvol blijken te zijn, worden zij steeds herhaald. Zo verandert een gedragspatroon van 'succesvol' naar 'het enig juiste' en dit raakt cultuur. Daarom is een cultuur nooit goed of fout, het is bij voortduring succesvol gebleken, dus 'juist'. *Werken met cultuur* is een bewustwordingsproces, waarmee je inzicht krijgt in gedragspatronen in een organisatie en hoe deze patronen in stand worden gehouden. Als je eenmaal inzicht hebt in deze processen en patronen, geeft dit inzicht in de mogelijkheid om ze te doorbreken of anders aan te pakken.

Hoe maak je werken met cultuur hanteerbaar?

De uitdaging voor het werken met cultuur ligt in het hanteerbaar maken van het begrip. De realiteit is dat medewerkers dagelijks onderdeel zijn van de cultuur. Werken met cultuur is een activiteit die niet alleen is voorbehouden aan experts of wetenschappers. Het doel is om goed gereedschap, informatie en zienswijzen mee te geven aan medewerkers om ze meer bewust met cultuur te leren omgaan. Er zijn op dit moment meerdere instrumenten op de markt die claimen cultuur te kunnen meten. Sommige instrumenten

Het gaat vaak fout als een cultuurmeting een waardeoordeel geeft

gaan zelfs een stap verder en koppelen een waardeoordeel aan een cultuur. Echter, deze instrumenten zijn doorgaans gebaseerd op een aanpak die nooit bedoeld was om een cultuur te 'meten', laat staan te wegen! Deze modellen zijn vervolgens door de cultuurmeters 'gekaapt' en omgezet naar een meetinstrument. Dit is vaak in strijd met het oorspronkelijke doel van de bedenkers van het model. Het kan fout gaan als een cultuurmeting een waardeoordeel geeft. Dit klopt niet, omdat een meting van een cultuur in principe altijd waardevrij is.

Het gevaar van een waardeoordeel is dat mensen dit ervaren als een veroordeling en in het algemeen verzetten mensen zich tegen veroordelingen. Het gevolg is dat er flinke weerstand ontstaat. De gewenste verandering is dan ver weg.

Wat kun je doen om een cultuur in kaart te brengen?

Als internal auditor is het belangrijk om te achterhalen wat de drijfveer is om cultuur binnen de organisatie te onderzoeken. Het verrichten van metingen heeft niet de voorkeur. Het kost vaak veel inspanning en vervolgens heb je als internal auditor slechts alleen een idee van wat de cultuur kan zijn. Dit soort metingen zijn nooit compleet, het is altijd een momentopname. De internal auditor kan wel een leidende rol vervullen in het werken met cultuur. De internal auditor kan dit niet alleen. Het advies is om een werkgroep op te richten met mensen uit de hele organisatie. Deze werkgroep krijgt vervolgens training om patronen waardevrij in kaart te brengen. Om te beginnen kan deze werkgroep met dilemma's als werkmateriaal starten. Denk hierbij aan problemen waar de medewerkers/-deelnemers tegenaan lopen. Laat de werkgroep vervolgens onderzoeken of er iets 'cultureels' onder ligt. Hier kan de internal auditor zijn waarde toevoegen door het inzetten van zijn onderzoekcompetenties.

Met een werkgroep patronen opsporen, ontcijferen en daarna zelf interventies opzetten, is effectiever en waardevoller dan het uitvoeren van metingen. Niet alleen voor de organisatie maar ook voor de werkgroep zelf. Want die zijn samen op ontdekkingsreis om het bedrijf te verbeteren.

Psychologisch veilige omgeving

Cruciaal voor het werken met een werkgroep is een psychologisch veilige omgeving. Met psychologisch veilig wordt

bedoeld dat mensen vrij hun mening kunnen uiten, dat mensen zaken kunnen benoemen en dat zij goed naar elkaar luisteren. Dat is een absolute voorwaarde voordat mensen waardevolle informatie gaan delen en er openheid gaat ontstaan.

De grootste uitdaging voor internal auditors is om de (interne) norm los te laten. Cultuur en het werken met cultuur is substantieel anders dan het geven van assurance. Als internal auditors met cultuur aan de slag willen gaan, moeten ze echt hun normenbril afzetten en leren onbevooroordeeld naar zaken te kijken. Verder vraagt het een andere manier van samenwerken met andere afdelingen binnen de



organisatie en het loslaten van het strikt functioneren in de derde lijn binnen dit onderwerp. Er is namelijk geen rolverdeling tussen de onderzoeker (internal auditor) en de onderzochten (de business). Want gezamenlijk ben je onderdeel van dezelfde cultuur.

Wat is de toegevoegde waarde van werken aan cultuur?

Het is belangrijk om bewijs te verzamelen over de gedragspatronen die je ziet als internal auditor (of werkgroep). In dit proces gebruikt de internal auditor voldoende bronnen om verschillende zijden te belichten. Het advies is om de patronen die met elkaar samenhangen niet als oordeel te

presenteren maar als constatering. Bijvoorbeeld: het valt mij op dat...

Mensen hechten namelijk aan de gedragspatronen die zij in de loop van de tijd ontwikkeld hebben omdat deze succesvol zijn. Ook al zitten er aspecten aan deze patronen die men misschien minder prettig vindt, of aspecten die minder succesvol zijn, mensen zijn vaak sterk gehecht aan deze patronen. Wanneer je als internal auditor deze patronen ter discussie stelt kom je aan hun succesformules. Op dat moment word je, ook als internal auditor, gezien als buitenstaander en creëer je weerstand.

Een werkgroep kan op dat moment helpen om mensen zelf bewust te laten worden van die patronen en dit kan de verandering van binnenuit in gang te zetten. Dat werkt beter dan een verandering die van buitenaf of bovenaf opgelegd wordt. Het is daarbij belangrijk om kritisch te kijken naar de samenstelling en doelstelling van de werkgroep.

Een alternatief bieden

Kortom, aanvankelijk is een gedragspatroon alleen maar een oplossing voor een bepaald probleem. De groep blijft dit herhalen als het patroon succesvol is. Op een gegeven moment krijgen patronen een zekere waarde. Dat wil zeggen, deze patronen zijn zo vaak herhaald, dat zij in de perceptie van de groep de enig juiste zijn. In deze situatie is de eerste stap laten zien dat er ook andere manieren zijn. Het doel is om de groep te verleiden te gaan experimenteren met andere patronen. Op deze manier kan het patroon losgekoppeld

worden van de waarde, er zijn immers nog andere 'juiste' manieren. Het doel is om medewerkers zelf tot het inzicht te laten komen dat een ander, veiliger gedragspatroon dezelfde of nog meer waarde kan hebben. Mensen beseffen vaak niet dat hun gedrag voortkomt uit patronen die over jaren zo gegroeid zijn. Voor succesvolle verandering is het dus noodzakelijk om een alternatief te bieden. <<

Noot

Frank Guldenmund, *Understanding and Exploring Safety Culture*, Uitgeverij BOXPress, 2010.

Frank Guldenmund is psycholoog en al ruim 25 jaar als docent/onderzoeker verbonden aan de sectie veiligheidskunde van de TU Delft. In 2010 promoveerde hij cum laude op het onderwerp veiligheidscultuur.

Bas Zandee is senior consultant Safety, Health, Environment (SHE). Hij richt zich op interim-management, change management, advies en coaching bij het bedrijfsleven en overheden.

advertentie

Audit Manager

Corbulo is het exclusieve carrière en interim management platform dat carrières van financials verbindt met duurzame organisatie doelstellingen. Corbulo is trusted partner in search en interim management van financial talent en executives. Wij werken al meer dan 10 jaar succesvol voor financials en organisaties met ambitie.

Voor diverse opdrachtgevers zoeken wij momenteel talentvolle Audit managers

Functie omschrijving

De primaire focus van de interne audit functie is gericht op de effectiviteit van de (interne controle op) management informatie en financiële rapportages.

Daarnaast ligt de focus op:

- Evaluatie van de kwaliteit en effectiviteit van de interne controle en identificatie van mogelijkheden ter versterking van de interne controle op management- en financiële rapportage processen;
- Evaluatie van de betrouwbaarheid en integriteit van management- en financiële informatie en de mid-delen die worden gebruikt om deze informatie te identificeren, meten, classificeren en rapporteren;
- Evaluatie van interne controle activiteiten op het naleven van relevante interne plannen, richtlijnen en procedures, alsmede wet- en regelgeving welke een belangrijke invloed kan hebben op de financiële positie van de onderneming;
- het uitdragen van 'best practices' en het actief bijdragen aan het verbreden/verdiepen van relevante kennis van de financiële functie binnen de organisatie.

Vereisten

- Certified Internal Auditor/ RO bij voorkeur met een aanvullende post doctorale titel;
- Minimaal 5 tot 10 jaar relevante werkervaring in een complexe en internationale omgeving en / of bij een van de 'big four' organisaties;
- Kennis van informatietechnologie, office systemen, ERP-systemen en data management;
- Kennis van en ervaring met (moderne) audit technieken, risk management, (administratieve) organisatie en (interne) controle.

Meer informatie?

Neem contact op met Feddo Heintz op 070-3197090 of 0646390690 of f.heintz@corbulo.net

Kijk op onze website www.corbulo.net voor de volledige functieomschrijvingen en voor andere mogelijk interessante posities.

Westeinde 4 • 2275 AD Voorburg
Telefoon: 070 - 319 70 90 • www.corbulo.net

Corbulo
dedicated to financials
executive search | talent search | interim management

Management control: innovatie én controle

Management control. Van oudsher ligt de focus op het zodanig beheersen van de organisatie dat de uitkomsten in grote mate voorspelbaar zijn. In toenemende mate is het echter van belang dat organisaties innoveren om succesvol te blijven, of sterker nog, om te overleven. *Een nieuwe visie op management control* is een mooi boek over hoe bestuurders van organisaties kunnen komen tot een toekomstbestendig managementcontrolestelsel, waarbij als een vanzelfsprekendheid de basis op orde is. Een managementcontrolestelsel dat past in een innoverende organisatie. Naast Maurice Franssen en Michelle Arets, delen vijftien andere auteurs hun visie over het vinden van de juiste balans tussen innovatie en controle. Daarbij gelden steeds gezamenlijke uitgangspunten:

1. Een managementcontrolestelsel dient zich gelijktijdig te richten op de beheersing van doelstellingen op de korte én op de lange termijn. Iedere termijn kent een ander niveau van beheersingssysteem.
2. Het managementcontrolestelsel dient in dezelfde mate te innoveren als de organisatie zelf: pas dan ontstaat effectieve beheersing.
3. Er is sprake van een juiste mix tussen analyserend vermogen (instrument, techniek), verandervermogen (menselijk aspect, gedrag) en transformatie (wanneer, proces en snelheid) indien de mensgerichte en instrumentele controls binnen het managementcontrolestelsel in een dynamische en effectieve balans zijn.

In ieder hoofdstuk wordt ingegaan op het door Franssen en Arets gepresenteerde maturiteitsmodel (zie tabel). Een dynamische balans tussen past control, present control én future control zorgt ervoor dat een organisatie de basis op orde heeft én kan innoveren. Bij het hoogste niveau van control bereik je gelijktijdig zowel past, present, als future control. Daarnaast geven de verschillende auteurs hun gedachten weer aan de hand van drie plaatplaten die vooraan in het boek zijn opgenomen. Deze plaatplaten zijn voor de lezer bijzonder handig en maken het mogelijk dat het boek niet in een bepaalde volgorde gelezen hoeft te worden. Ieder hoofdstuk wordt afgesloten met tips en een case waarin de theorie is vertaald naar een vaak herkenbaar praktijkvoorbeeld.

Het boek is overigens niet alleen interessant voor het bestuur van een organisatie, maar ook voor controllers, consultants, auditors en adviseurs die dit bestuur informeren, adviseren en/of zekerheid verschaffen. Er worden namelijk relevante en tijdloze thema's behandeld die aanspreken, zoals risicomanagement, soft controls, leiderschap, strategische gedragsverandering, financiële transformatie en managementinformatie. Verder zet het boek je aan tot reflectie bij vraagstukken over beheersing en sturing van organisaties. Echt een aanrader.



Management Control – Dynamisch balanceren tussen basis op orde en innovatie

Maurice Franssen en Michelle Arets

Vakmedianet

ISBN 9789462760639

€ 31,75

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

Kenmerken	BASIS OP ORDE		INNOVATIE
	Past control	Present control	Future control
Analysierend vermogen	Gericht op het verleden	Gericht op het heden	Gericht op de toekomst
Beheersingsdoelstelling	De dingen goed doen	De goede dingen beter doen	De goede dingen anders doen
Basis op orde versus innovatie	Basis op orde krijgen	Basis is op orde	Basis op orde en innovatie
Verandervermogen	Zo min mogelijk veranderen	Geregeld veranderen	Continu veranderen
Inrichting managementcontrolestelsel	Geïsoleerd managementcontrolestelsel	Gestandaardiseerd managementcontrolestelsel	Geïntegreerd managementcontrolestelsel
Eigenaar managementcontrolestelsel	Een afdeling zoals Finance & Control	Proceseigenaren	Iedereen die actief wil bijdragen aan de realisatie van de doelstellingen
Mix hard en soft controls	Voornamelijk inzet van hard controls	Naast hard controls meer inzet van soft controls	Optimale balans soft en hard controls, waarbij de nadruk ligt op soft controls

Tabel 1. Maturiteitsmodel

Doorstoten naar de top: Internal Audit Down Under

Tegenwoordig moet een organisatie haar toegevoegde waarde voortdurend duidelijk maken aan klanten en overige stakeholders. Dit geldt ook voor Internal Audit. Aan de andere kant van de wereld, in Australië, hecht Commonwealth Bank grote waarde aan de inzichten die Internal Audit creëert voor de rest van de organisatie.

Commonwealth Bank is een Australische internationale financiële instelling die in 1911 door de Australische regering is opgericht om agrarische activiteiten en de creatie van nederzettingen te stimuleren. De bank bedient zowel de particuliere als de zakelijke markt. De bank heeft een notering op de Australische beurs en is de grootste bank op het zuidelijke continent.

Bij Group Audit & Assurance (Internal Audit) werken tweehonderd mensen. De afdeling wordt goed gewaardeerd en een externe quality assessment review riep de afdeling in 2016 uit tot de nummer 1 internal auditafdeling van Australië.¹ De vraag rijst in welke aspecten het onderscheidende vermogen zit, waardoor deze afdeling zo succesvol kan opereren en toegevoegde waarde aan de rest van de organisatie biedt. Dit betreft de volgende aspecten:

- visie & focus;
- strategie & organisatie;
- risicocultuur;
- innovatie.

Visie & focus

Bij zowel de chief audit executive als het MT van Internal Audit staat het leveren van toegevoegde waarde voor alle stakeholders, zowel intern als extern, voorop. Hiertoe zijn zij continu op zoek naar manieren om zichzelf, het team, de afdeling en de organisatie verder te verbeteren. Internal Audit gebruikt hiervoor het Business Model Canvas, dat begint met een stakeholderanalyse (zie *figuur 1*).

Het expliciet maken van de interne en externe stakeholders is uitdagend en complex tegelijkertijd. Wiens belangen staan voorop? Die van de aandeelhouders, de board, de afdelingshoofden of de klanten van de organisatie? Of zijn ze allemaal even belangrijk? Het concretiseren van de relevante stakeholders en hun verwachtingen helpt in het definiëren van de waarde die Internal Audit kan toevoegen.

Internal Audit heeft zich onder andere tot doel gesteld de afdelingshoofden proactief te voorzien van inzichten die voortvloeien uit de werkzaamheden die zij groepsbreed uitvoert. Hiertoe is een tweewekelijks overleg tussen de verschillende subafdelingen van Internal Audit in het leven

geroepen met als doel uitwisseling van lessons learned en identificatie van trends en afdelingsoverstijgende issues. Zo krijgen de afdelingshoofden latente risico's en mogelijkheden voor efficiency- en effectiviteitsverbeteringen aangereikt, die zij kunnen gebruiken voor het beter beheersen en verbeteren van de eigen processen.

Met de uitkomsten van de Business Model Canvas-sessies stelt Internal Audit een driejarenplan op, gericht op kwaliteitsverbetering en innovatie. Dit plan wordt jaarlijks herijkt en vertaald naar een jaarplan met specifieke acties om het businessplan van de afdeling te realiseren.

Strategie & operatie

Kwaliteitsbewaking en de implementatie van alle initiatieven ter vergroting van de toegevoegde waarde, naast het 'gewone' auditwerk, kost tijd. Binnen Internal Audit is een apart strategy & operations team gecreëerd. Het team zorgt voor de methodologie, processen en systemen van Internal Audit, faciliteert het jaarlijkse audit planningsproces & de budgettering en stelt de afdelingsoverstijgende rapportages op voor de senior stakeholders. Daarnaast heeft zij de penvoering over het businessplan van de afdeling en faciliteert zij de uitwerking van de strategische initiatieven. Hierdoor worden de plannen daadwerkelijk geoperationaliseerd en geïmplementeerd.

Strategy & operations gebruikt een capacity development plan om op de langere termijn ervoor te zorgen dat mensen met de juiste achtergrond bij Internal Audit werken. Dit zijn niet alleen auditors, maar ook mensen met een zeer

omvangrijke treasury- of kredietervaring, data-analisten en psychologen.

Het team zorgt ervoor dat de medewerkers en de afdeling als geheel zich blijven ontwikkelen. Hiertoe organiseert zij de benodigde trainingen en uitwisselingen. Dit laatste betreft niet alleen uitwisselingen tussen de auditteams, maar ook uitwisselingen met de business en de tweede lijn. Jaarlijks worden internal auditafdelingen bezocht van buitenlandse instellingen om ideeën op te doen over hoe Internal Audit verder kan worden verbeterd.

Risicocultuur

De wijze waarop gestalte is gegeven aan 'risk culture' auditwerkzaamheden is een voorbeeld van een actie voortvloeiend uit een Business Model Canvas-sessie. Inzicht in de risicocultuur is door Internal Audit jaren geleden geïdentificeerd als een belangrijke aanvulling op het meer traditionele auditwerk. Niet alleen een verhoogde aandacht van toezichthouders voor risicocultuur, maar ook het besef dat cultuur vaak aan de basis van auditbevindingen ligt, heeft geleid tot de ontwikkeling van een specifieke risicocultuur auditmethode.

Voor een juiste aanpak, uitvoering en diepgang van risicocultuur audits, zijn psychologen in dienst van Internal Audit. Deze helpen met het zichtbaar en meetbaar maken van dit onderwerp. Het is een standaard onderdeel van elke audit. Als gevolg hiervan zijn cultuur en knelpunten hierin meer geobjectiveerd en een bespreekbaar thema. Ook wordt gebenchmarkt tussen afdelingen.

Key partners <ul style="list-style-type: none"> - Who are our key partners? - Who are our key suppliers? - Which key resources are we acquiring from our partners? - Which key activities do partners perform? 	Key activities <ul style="list-style-type: none"> - What key activities do our value propositions require? - Our distribution channels? - Customer relationships? - Revenue streams? 	Value propositions <ul style="list-style-type: none"> - What value do we deliver to the customer? - Which one of our customers' problems are we helping to solve? - What bundles of products and services are we offering to each segment? - Which customer needs are we satisfying? - What is the minimum viable product? 	Customer relationships <ul style="list-style-type: none"> - How do we get, keep, and grow customers? - Which customer relationships have we established? - How are they integrated with the rest of our business model? - How costly are they? 	Customer segments <ul style="list-style-type: none"> - For whom are we creating value? - Who are our most important customers? - What are the customer archetypes?
	Key resources <ul style="list-style-type: none"> - What key resources do our value propositions require? - Our distribution channels? - Customer relationships? - Revenue streams? 		Channels <ul style="list-style-type: none"> - Through which channels do our customer segments want to be reached? - How do other companies reach them now? - Which ones work best? - Which ones are most cost-efficient? - Hoe ware we integrating them with customer routines? 	
Cost structure <ul style="list-style-type: none"> - What are the most important costs inherent to our business model? - Which key resources are most expensive? - Which key activities are most expensive? 		Revenue streams <ul style="list-style-type: none"> - For what value are our customers really willing to pay? - For what do they currently pay? - What is the revenue model? - What are the pricing tactics? 		

Figuur 1. Business Model Canvas (Bron: Harvard Business Review, Alexander Osterwalder)

De jeugd heeft de toekomst!

Kies voor het unieke
traineeship van AuditPeople

werving
interim
kennis



AUDIT PEOPLE | ARC PEOPLE
Koninginneweg 4, 1217 KX Hilversum
Telefoon: 085-2733025 E-mail: info@auditpeople.nl

www.auditpeople.nl   

IIA congres 2018

CREATIE EN INNOVATIE



Gijs van Wulfen



Jocelyn Rebbens



Joris Luyendijk



Janne Vereijken



Jan Driessen



Jaya Baloo



Pauline de Wilde



Instituut van
Internal Auditors
Nederland

www.iaa.nl/congres2018

7 en 8 juni 2018

Flint Amersfoort

Kwaliteitsbewaking en de implementatie van alle initiatieven ter vergroting van de toegevoegde waarde naast het 'gewone' auditwerk, kost tijd

Innovatie

Een duidelijk besef is aanwezig dat het implementeren van innovatieve concepten alleen zin heeft wanneer een kwalitatief goede vaktechnische basis staat. De kwaliteit van deze basis krijgt daarom continu aandacht. Dit gebeurt zowel binnen het auditproces zelf alsook op de resultaten van het auditproces. Op periodieke basis worden bijvoorbeeld onderlinge quality assurance reviews van dossiers uitgevoerd en is er een verplichte kwaliteitscontrole van de laatste conceptrapporten door een van de andere MT-leden.

Een van de manieren waarop de kwaliteit van de audits is verhoogd, is het vergaande gebruik van data-analyse. Zo is door de afdeling een dashboard ontwikkeld met meer dan honderd risico-indicatoren, specifiek voor branch audits.² Afhankelijk van het type audit kunnen de relevante indicatoren worden geselecteerd en wordt het veldwerk integraal en toch op efficiëntere uitgevoerd. De planfase van de branch audits is verkort van vele weken naar twee dagen. Dit wordt als positief ervaren door de auditors. Ook de medewerkers en het management van de branches zijn hier over te spreken, omdat zij minder tijd kwijt zijn aan het verzamelen en verstrekken van informatie aan Internal Audit en zij gedetailleerd inzicht in binnen de branch bestaande risico's krijgen.

Het traditionele auditproces zelf gaat op een agilewijze en is daarom omgedoopt tot 'agile auditing'. Het doel van agile auditing is het verbeteren van het auditproces voor de auditee en de auditors en het verhogen van de kwaliteit van de auditbevindingen. Agile auditing komt neer op Afstemmen (met de hoofdletter A). Afstemmen met de auditee, maar ook intern afstemmen binnen de afdeling. Deze interne afstemming betreft dagelijkse zogenaamde '15 minuten huddles', een staande afstemming tussen de leden van het auditteam zodat issues zo snel mogelijk kunnen worden besproken en opgelost. Het betreft ook afstemming met experts en collega's die niet betrokken zijn bij de audit, maar aanpalend werk hebben verricht. Bijvoorbeeld via de verplichte 'mid point review', waarbij een senior auditor die niet bij de audit betrokken is, wordt gevraagd om met een onbevangen en frisse blik naar de aanpak van audit te kijken.

Conclusie

De ervaring bij Commonwealth Bank leert dat het succes van Internal Audit begint met visie en de overtuiging dat Internal Audit van grote toegevoegde waarde kan zijn voor een organisatie bovenop de meer 'klassieke' auditbevindingen uit de individuele rapportages. Vanuit de ambitie om meer te zijn dan controlerende auditors is een pragmatische aanpak nodig om dit te realiseren. Pragmatisch vanuit het oogpunt van de huidige invulling van de taak van Internal Audit en gebaseerd op een helder inzicht in de activiteiten die nodig zijn om hierin veranderingen aan te brengen. Pragmatisch ook vanuit de behoefte van de organisatie: bespreek met de stakeholders deze ambitie en hoe deze kan worden waargemaakt.

De 'heilige huisjes' van Internal Audit worden regelmatig tegen het licht gehouden. Dit heeft tot kleine en grote verbeteringen geleid. Schuw daarom niet om bestaande structuren te wijzigen, zoals de benodigde competenties bij Internal Audit, maar ook de wijze waarop en de frequentie waarmee

met de business wordt gecommuniceerd. En zorg voor een organisatie die de mogelijkheid heeft om te innoveren. Wij begrijpen dat niet alle organisaties een dergelijke, toch wel omvangrijke, afdeling Internal Audit kunnen optuigen als Commonwealth Bank. Toch hopen wij dat wij met het beschrijven van de vier aspecten visie & focus, strategie & organisatie, risicocultuur, innovatie, u hebben kunnen inspireren. Op basis van de beschreven voorbeelden, kan elke internal auditafdeling met kleine interne verbeteringen en grotere auditinnovaties haar toegevoegde waarde voor haar stakeholders verder vergroten. En daarmee doorstoten naar de top! <<

Noten

1. Externe review van de kwaliteit van organisatie, processen en audittechnieken van Internal Audit, conform de kwaliteitsstandaarden van het Chartered Institute of Internal Auditors.
2. In 2016 had Commonwealth Bank 1000 branches verspreid over heel Australië.

Rochelle Degens is senior toezichthouder IT en operationeel risico bij Autoriteit Financiële Markten.

Age-Jan van der Meer is oprichter en mede-eigenaar van KoutersVanderMeer, bureau voor prestatieverbetering op het gebied van IT-beheersing.

Ronald Jansen:

“Met de poten in de klei staan bevalt prima”

In de rubriek De overstap dit keer Ronald Jansen, die na elf jaar KPMG overstapte naar IKEA Group, de grootste franchisenemer van Inter IKEA.

Over IKEA Group

IKEA Group is de grootste franchisenemer van Inter IKEA en beschikt over circa 355 winkels in 29 verschillende landen. Er werken grofweg 149.000 medewerkers, waarvan circa 180 op het hoofdkantoor. Daarnaast heeft het circa 110 miljoen IKEA -familyleden en levert het ongeveer 9500 type producten. In 2017 werd € 36,3 miljard aan omzet gedraaid, resulterend in een netto winst van € 2,5 miljard.

Waarom bent u overgestapt van een Big Four-kantoor naar een retailer?

“Ik heb de overstap hoofdzakelijk gemaakt vanwege de aard van de uitdaging die ik bij IKEA Group aan zou treffen. Ik ben bij IKEA Group binnengehaald om een nieuwe interne auditfunctie op te zetten. Het uit het niets opstarten van een eigen afdeling, waarbij er ook nog eens snel resultaten moesten worden geboekt, is wat mij het meest heeft gedreven om de overstap te maken. Verder kende ik IKEA Group al goed omdat ik in mijn tijd bij KPMG diverse opdrachten voor hen heb gedaan. Dit betroffen opdrachten met name op het gebied risk & compliance. Zo heb ik bij hen bijvoorbeeld een raamwerk voor risk management vormgegeven.”

Wat waren uw eerste indrukken bij uw nieuwe werkgever?

“Wat mij vooral opviel is hoe open de medewerkers staan ten opzichte van nieuwe collega's. Zowel op persoonlijk vlak als op het gebied van inzichten en ideeën die je als nieuwkomer meebrengt. Bij IKEA staan ze open voor een nieuw geluid. Dit sluit ook aan bij een van de core values van IKEA: 'togetherness'. Ofwel, door samen te werken en gebruik te maken van elkaars ideeën en krachten kunnen we het onmogelijke mogelijk maken. Deze mentaliteit is helemaal vervlochten met het dagelijks werk, het zit als het ware tussen de oren. Wat ook opviel is dat er weinig hiërarchisch wordt gewerkt en de medewerkers veel ruimte krijgen voor nieuwe initiatieven. In die zin wordt er ook nauwelijks gebruikgemaakt van strakke procesbeschrijvingen, procedures en key controls. Het werk wordt veel meer in samenspraak tot stand gebracht. Dit gaat op een respectvolle manier waarbij iedereen de ruimte krijgt om ideeën en inzichten te delen. Door met elkaar in gesprek te gaan en elkaar feedback te geven ontstaan nieuwe ideeën en manieren om die te bereiken. Dit proces van het samen bespreken en beargumenteren wordt het 'washing proces' genoemd.”

Wat zijn opmerkelijke verschillen tussen beide organisaties?

“De verschillen zijn het grootst op het gebied van de bedrijfscultuur. Bij IKEA is er sprake van een intensieve beleving van de bedrijfscultuur en de bijbehorende waarden. Dit is niet te vergelijken met de situatie binnen KPMG. Bij IKEA



gelden de waarden als vertrekpunt van de organisatie en deze komen in elke vergadering en bijeenkomst terug. In de cultuur wordt veel waarde gehecht aan de onderlinge relaties, ook op persoonlijk vlak. Dit geldt zowel verticaal als horizontaal. Medewerkers zitten goed in hun vel en blijven ook relatief lang in dienst. Vanochtend werd bijvoorbeeld afscheid genomen van een collega die ruim 32 jaar voor IKEA heeft gewerkt. Ik was onder de indruk van de wijze waarop afscheid werd genomen, met veel persoonlijke anekdotes en warme woorden. In die zin is er echt sprake van een IKEA-family. Het is fijn om in deze omgeving te vertoeven. Er is sprake van een groepsmentaliteit en je merkt dat je met elkaar onderdeel bent van een groter geheel. In die zin zijn er wel raakvlakken met mijn eerste baan bij Defensie: die saamhorigheid, het voelt wel een beetje als toen.”

Hoe ziet de nieuwe interne auditafdeling eruit?

“Die bestaat uit vier personen. Wij hebben gekozen voor een model waarbinnen hoofdzakelijk met co-sourcing wordt gewerkt. Zelf bereiden wij audits voor tot en met de scoping. Vervolgens zetten wij onze opdracht uit in de markt en vragen wij externe dienstverleners hun ideeën en aanpak aan ons te presenteren. Dit werkt heel goed.

Ten behoeve van de planning van de activiteiten werkt de interne auditafdeling met een (globaal) jaarplan. De global risk assessment geldt als een van de belangrijkste vertrekpunten. Uit deze assessment volgen de onzekerheden en zwakke plekken waar de organisatie zich mee geconfronteerd ziet. Daarnaast komen onderwerpen tot stand op basis van gesprekken met onder meer de business leaders van IKEA Group. Dit zijn informele besprekingen, soms letterlijk ‘met de benen op tafel’.

Verder heeft het decentrale karakter met beperkte hiërarchische sturing consequenties voor de wijze waarop audits worden uitgevoerd. Er wordt binnen het bedrijf veel teruggevallen op de values van IKEA en er wordt veel aan mensen en managers overgelaten. Soft controls zijn hier met de paplepel ingegoten door de grondlegger Ingvar Kamprad. Ook wordt er veel waarde gehecht aan afstemming en overleg. Dit maakt het voor een interne auditafdeling relevanter om de diverse stakeholders vroegtijdig bij de opzet van audits te

betrekken en hen continu te informeren. Resultaten worden in een workshop setting besproken. Door voor die benadering te kiezen ontstaat een meer actieve houding bij alle stakeholders; deze aanpak wordt als erg positief ervaren.”

Keert u ooit nog terug naar een extern adviesbureau?

“Ik ben nu circa een jaar in dienst bij deze bijzondere werkgever en ik zie mijzelf niet terugkeren naar een extern adviesbureau. Voorlopig is dit echt genieten. De uitdaging was om mijn eigen afdeling op te zetten. Daar had ik vooraf een duidelijk beeld van hoe dat zou moeten: klein opstarten en daarna bijsturen en uitbouwen. Nu de basis is gerealiseerd en ik de organisatie heb laten zien wat Internal Audit voor het bedrijf kan betekenen, is het mij duidelijk geworden dat de aanpak ‘spot on’ was. Ik geniet nu van het doorontwikkelen van de afdeling en het zelf ‘met de poten in de klei staan’ bevalt mij prima. Dat is echt fantastisch!”

Wat wilt u mensen meegeven die een overstap overwegen?

“Je weet natuurlijk nooit 100% zeker waar je terecht gaat komen. Maar als je een dergelijke overstap wilt maken, zorg er dan voor dat je vooraf zoveel als mogelijk een compleet beeld krijgt van hoe het er bij je toekomstige werkgever aan toe gaat. Spreek met mensen die er al werken, kijk goed wat de strategie van het bedrijf is en hoe het bedrijf zijn doelen wil bereiken. Vorm je vooraf een goed beeld. Maak niet zomaar een keuze maar zorg ervoor dat je zicht krijgt op hoe een organisatie functioneert, maak daar echt werk van!”



Over...

Ronald Jansen is CAE bij IKEA Group. Daarvoor werkte hij onder meer bij Defensie, PwC en KPMG. Tevens is hij voorzitter van het bestuur van de SVRO en bestuurslid binnen het IIA.

Accreditatie RO-opleiding: nu begint het pas

Bij de RO-opleiding van de UvA was er begin januari een klein feestje. De opleiding is namelijk recent geaccrediteerd door de NVAO. Afgestudeerden dragen voortaan de titel Master of Science. *Audit Magazine* prikte een vorkje taart mee.

Velen hebben afgelopen jaren bijgedragen aan dit succes. Present waren naast de huidige opleidingsdirecteur Edo Roos Lindgreen, zijn voorganger Bob van Kuijk, associate programmadirecteur Huck Chuah en programmamanager Sook Reker. Ook enkele leden van de Programme Board van de opleiding waren aanwezig: John Bendermacher, Paul Scholte, Vincent Moolenaar en Gerben Everts. Het gezelschap reflecteerde op de afgelopen periode en op de plannen voor de toekomst.

Waarom is deze accreditatie belangrijk?

Edo Roos Lindgreen (ERL): “Deze accreditatie is zowel belangrijk voor de beroepsgroep als voor de universiteit. De universiteit voert de lijn dat elke opleiding geaccrediteerd moet zijn en dus moet leiden naar een academische titel. Studenten investeren twee jaar in een opleiding en willen daar iets tastbaars aan overhouden. Een mastertitel telt, geeft toegevoegde waarde. Het geeft aan dat een wetenschappelijke studie van hoge kwaliteit is volbracht. Dit geldt in de eerste plaats voor studenten die nog geen mastertitel voeren maar evenzo voor studenten voor wie deze opleiding resulteert in een dubbele mastertitel.”

John Bendermacher (JB): “Het IIA is hier enorm bij gebaat. Als je het beroep wil professionaliseren, hoort daar een topclassopleiding bij. De opleiding was natuurlijk altijd al goed, maar met deze accreditatie wordt die kwaliteit nadrukkelijk erkend.”

Gerben Everts (GE): “Het sluit aan bij de ambitie van de vakgroep om de ontwikkeling van het vakgebied een wetenschappelijke basis te geven. Er bestaat een maatschappelijke

behoefte aan goed opgeleide auditors en daar hoort een goed fundament onder.”

JB: “IIA Global rekent deze opleiding, evenals de opleiding aan de Erasmus, tot de internationale top. Wij zijn ‘s werelds eerste RO-opleiding met deze accreditatie.”

Bob van Kuijk (BvK): “We zijn een centre of excellence en dit brengt ook een plicht met zich mee om internationaal die rol waar te maken. Er komen verzoeken uit de hele wereld van studenten om hier te studeren, onderzoek te doen, verzoeken voor tijdelijke detacheringen en samenwerkingen. Dit is prima, maar tegelijk geldt dat het niet onze primaire doelstelling is om ons internationaal te profileren.”

Wat ging aan deze accreditatie vooraf?

ERL: “Bloed, zweet en tranen.”

BvK: “Vanaf 2013 zijn we al bezig om ons voor te bereiden op de accreditatie. Dit lijkt een hele lange tijd, maar die heb je ook nodig om kritisch de onderwijsprocessen inhoudelijk te beoordelen, te kijken hoe je kunt stroomlijnen en ook de docenten in dit proces mee te nemen. We hebben eerder in 2010 een accreditatieverzoek gedaan. Toen is dat niet gelukt. We hebben natuurlijk vooral gewerkt aan de pijnpunten die toen naar voren kwamen. Een van die punten was het scriptieproces. De visitatiecommissie beoordeelde in deze ronde een aantal scriptiedossiers inhoudelijk en gaf ons terug dat deze scripties met vlag en wimpel de toets der kritiek kunnen doorstaan. De beroepsgroep zal daarvan kunnen profiteren want de scripties bieden een goede basis om op voort te bouwen in wetenschappelijke vervolgonderzoeken.”

ERL: “Het scriptieproces laat een heel duidelijke verbetering

V.l.n.r. staand: Huck Chuah, John Bendermacher, Gerben Everts. V.l.n.r. zittend: Edo Roos Lindgreen, Vincent Molenaar, Sook Reker, Paul Scholte, Bob van Kuijk.



zien, maar je hebt meer gerealiseerd Bob. Je hebt gezorgd voor meer gepromoveerde docenten, meer wetenschappelijke literatuur, meer research-based onderwijs.”

JB: “En dat alles met behoud van het praktisch nut. Bij de vorige accreditatie kregen we vragen over het wetenschappelijke gehalte van de opleiding. Nu kregen we vragen over de praktische toevoeging. Dat betekent dat je die shift heel duidelijk gemaakt hebt.”

BvK: “Helaas zijn er niet veel docenten die theorie aan praktijk kunnen koppelen en ook kunnen lesgeven op het internal auditvlak. Lezers die een docentschap overwegen zijn dan ook zeer welkom.”

Was het op enig moment spannend of accreditatie zou gaan lukken?

GE: “Vanuit de programme board hebben we tijdens onze vergaderingen steeds de vinger aan de pols gehouden. We zijn intern binnen de universiteit getoetst door hoogleraren en docenten en uiteraard is dan spannend wat de uitkomst is.”

BvK: “Dit is geen proces om over een nacht ijs te gaan. Regelmatig hebben we onszelf de vraag gesteld of het niveau afdoende is.”

ERL: “Ik moet zeggen vanaf het moment dat ik het stokje overnam van Bob, 1 juli 2017, heb ik nooit enige spanning gevoeld. Tegelijk was het toen min of meer duidelijk dat we zouden slagen.”

GE: “We hebben ook op safe gespeeld, eerst zeker weten dat de boel op aarde is en dan pas accreditatie aanvragen. En als iets niet goed was werd dat punt eerst opgepakt voor we verdergingen.”

Paul Scholte (PS): “Op 1 juli 2016 was het dossier feitelijk afgerond. Maar toen hebben we een rustpauze ingelast om een aantal zaken nog de revue te laten passeren. En het was ook spannend omdat niet alleen deze opleiding beoordeeld wordt, maar ook de relevante universitaire processen. Dat betekent ook dat de universiteit als zodanig moest voldoen.”

Hoe verloopt zo'n accreditatieproces?

ERL: “Kortweg start je met een nulmeting, doe je een gap-analyse, stel je een verbeterprogramma op dat je uitvoert en monitort en schrijf je tot slot een informatiedossier. Dit laatste beschrijft de hele opleiding conform het toetsingskader van de accreditatieorganisatie, de NVAO. De afdeling Academische Zaken van het college van bestuur van de UvA beoordeelt dit dossier. Een commissie van de NVAO komt vervolgens visiteren. Dat gebeurt een dag lang waarin ze dossiers bekijken, interviews doen met de programmaleiding, de programme board, het bestuur, de examencommissie, werkgevers, docenten, studenten en oud-studenten. Dit resulteert in een rapport met een aanbeveling van de visitatiecommissie aan de NVAO. Dat was in ons geval een aanbeveling tot accreditatie.”

BvK: “Het was voor ons nuttig dat we als opleiding hebben meegedraaid in allerlei business-schoolaccreditatieprocessen van de universiteit. Dit was ook leerzaam. Uiteraard hebben we ook al eerder het proces tot accreditatie van de beroepsgroep, de SVRO-accreditatie, ervaren.”

Kunnen jullie nu op je lauweren rusten?

ERL: “Nee hoor, nu begint het pas. De komende periode gaan we de opleiding sterker maken en vernieuwen. Niet alleen door meer research-based onderwijs te bieden, maar ook op inhoudelijk vlak. Het IIA heeft twee onderwerpen aangedragen die belangrijk zijn voor de beroepsgroep. Wij gaan die twee onderwerpen, gedrag en cultuur en data science, al het komende studiejaar inbedden in de opleiding. En daarnaast gaan we kijken hoe we beter de instroom van hbo'ers kunnen faciliteren waarbij tegelijkertijd het hoge niveau van de opleiding wordt vastgehouden. Tot slot hoop ik dat we meer tijd en energie kunnen stoppen in onderzoek. We willen op het gebied van data science een PhD-student aantrekken om research te laten doen. Er is hiervoor financiering beschikbaar.”

Waar zijn jullie vooral trots op?

JB: “Ik denk dat we vooral trots mogen zijn op Bob en Huck. Zij hebben persoonlijk commitment getoond en het lef gehad om hier 100% voor te gaan.”

ERL: “Ik ben trots op onze studenten die tijdens de visitatiegesprekken een ontzettend positieve indruk hebben achtergelaten bij de commissie.”

PS: “Het proces is echt lonend gebleken, want het zoemt al rond dat studenten een Master of Science willen halen bij onze RO-opleiding.”

ERL: “We meten het verkeer op onze website en zien dat dit nu toeneemt. Ook is het aantal mensen op voorlichtingsdagen een stuk hoger dan voorgaande jaren. We verwachten meer studenten aan te nemen. Tegelijkertijd kunnen we niet meer studenten aannemen dan passen in de collegezaal. Dus mocht je een opleiding tot Executive Master of Science in Internal Auditing aan de UvA overwegen, schrijf je dan snel in!” <<



IIA Congres 2018: Creatie & Innovatie

(Inter)nationale topsprekers, innovatieve inzichten binnen het vakgebied van Internal Audit, kennismaken en netwerken met maar liefst zevenhonderd vakgenoten. Dát is in een notendop wat het IIA Congres 2018 met het thema 'Creatie & Innovatie' te bieden heeft. Waarom je er bij moet zijn? Ga naar www.iaa.nl/congres2018 voor alle informatie!

Internationale Vrouwendag

Op Internationale Vrouwendag op 8 maart jl. hield IIA Nederland een ontbijtsessie voor vrouwelijke internal auditors. Slechts een op de vier internal auditors is vrouw. Hoe activeren we meer vrouwen om dit beroep te kiezen? Sprekers Amba Zeggen, Suzanne Janse, Wilma Bakker en Mildred Hofkes deelden hun worstelingen én successen met als doel: hoe kun jij als vrouw extra toegevoegde waarde leveren op de werkvloer?

IIA feliciteert de geslaagden

Nieuwe CRMA: Mehul Chandra
Nieuw CIA: Elke Geerdink, Pascal de Bock, Arjan Kieneker

IAF bij beursfondsen

Vorig jaar werd de *Internal Audit Monitor 2017* uitgevoerd waaruit bleek dat kleinere beursfondsen zelden over een IAF beschikken. Op 16 januari 2018 werd tijdens een seminar bij Nyenrode het onderzoeksrapport door John Bendermacher uitgereikt aan Jaap van Manen (aftredend voorzitter Monitoring Commissie Corporate Governance Code). Commissarissen, internal auditors en andere stakeholders gingen vervolgens met elkaar in gesprek over het belang en de toegevoegde waarde van een IAF bij Nederlandse beursfondsen.

<http://bit.ly/2DMsAh7>



Audit Magazine op de mat? Ja/Nee

Via je persoonlijke profielpagina op de website van IIA Nederland kun je vanaf dit jaar zelf aangeven welke magazines en nieuwsbrieven je wilt ontvangen. In het streven papier te besparen, hebben we voor alle leden de functie automatisch op opt-out gezet. Ga naar 'Ledenprofiel' op de pagina 'Ledenservice' en klik op de knop 'Privégegevens bewerken'. Lees hier meer: <http://bit.ly/2DMBP1m>



Internal auditor gevaarlijk beroep

Medio januari 2018 presenteerden IIA Nederland en Nyenrode Business Universiteit het onderzoeksrapport *Morele moed en internal auditors*. In het rapport wordt een groot aantal handvatten gegeven om met 'gevaarlijke' situaties om te gaan, bijvoorbeeld door het stellen van een kritische vraag of door een bestuurder te wijzen op de kernwaarden van zijn of haar organisatie. <http://bit.ly/2EFi9AA>

ALV december 2017

Tijdens de ALV afgelopen december droeg voorzitter John Bendermacher drie bestuursleden voor herbenoeming voor en besprak hij de strategie 2016-2020. Penningmeester Jantien Heimeel lichtte de conceptbegroting voor 2018 toe en meldde dat de contributie in 2018 ongewijzigd blijft. Alle stukken zijn terug te vinden op de pagina Ledenservice. De volgende ALV is in mei 2018.

Vaktechnische publicaties

- 16-01-2018 – Internal Audit Monitor
- 09-01-2018 – Auditing Liquidity Risk
- 08-01-2018 – Gamification voor Internal Audit
- 27-12-2017 – Reporting Misconduct
- 14-12-2017 – Whistleblowing Frameworks
- 21-11-2017 – Assessing Fraud Risks
- 21-11-2017 – Internal Audit and External Audit

Meer publicaties: <http://bit.ly/2gQUluS>

Diploma-uitreiking

Eind november 2017 was er weer een gezamenlijke diploma-uitreiking van de post-masteropleidingen Internal Auditing & Advisory en IT-Auditing & Advisory. De studenten kregen hun diploma uit handen van Mark van Twist, Jan Pasmooij en Jolanda Breedveld. Namens de studenten bedankte Evelien van Domselaar-Jansen de opleidingen voor hun onderwijs en ondersteuning en blikte ze terug op de opleiding IAA met een compilatie van collegesheets.

De IAA-studenten die hun slotexamen hebben afgelegd in de periode juli-november 2017 zijn:

Hans Bank Invloeden van externe toezichtscriteria op de interne organisatie van IAF's van banken | Bina Bissembhar Het leervermogen van de internal auditor in de bankensector, bezien vanuit zijn leerstijl en omgang met informatie-overload | Monica Boom-van der Meer Combinatie controlling en auditing | Evelien van Domselaar-Jansen Analyse van de risicohouding van medewerkers in de 1e, 2e en 3e line of defense van de Rabobank | Erwin Engels en Bas de Weijer De IAD, manusje van alles | Ewout van Geuns Strategisch coöperatief. Een 'good practice' strategievormingsproces voor tuinbouwcoöperaties | Pauline Kamps Risicomanagement bij woningcorporaties anno 2017 | Wim Salij Internal Auditing & Performance Excellence | Vincent Westerweel Security Regie Management (discussiedocument)



**Save the date:
viering 25-jarig bestaan
29 juni 2018**

In 1993 zijn we gestart met de opleiding Internal/Operational Auditing aan de Erasmus Universiteit Rotterdam. Dit jaar bestaat de opleiding, die inmiddels Internal Auditing & Advisory heet, 25 jaar. We willen dit graag met onze alumni, docenten en studenten vieren. Vrijdagmiddag 29 juni 2018 organiseren we een symposium met als dagvoorzitter prof.dr. Mark van Twist. Meer informatie volgt op onze website en via de mail.



 UNIVERSITEIT VAN AMSTERDAM

Amsterdam Business School

Actualiteiten

Het Academisch collegejaar is alweer bijna halverwege. Met plezier zien we het aantal aanmeldingen voor de Executive MSc in Internal Audit (EMIA) flink toenemen, zie ook pagina 58 van dit nummer. Daarnaast is de herziene Corporate Governance Code nu alweer een jaar van kracht, wat een versterkend effect heeft op de interesse in de opleiding.

Onmisbaar onderdeel

Nu de internal auditfunctie (IAF) definitief haar plek heeft veroverd en een onmisbaar onderdeel is geworden van good governance, moeten we het ook als beroepsgroep van internal auditors 'waarmaken', het in ons gestelde vertrouwen niet schaden en ervoor zorgdragen dat de kwaliteitsfundamenten van een IAF goed geborgd worden. Naast de IIA-kwaliteitstoetsing, is het opleidingsniveau van de internal auditor een van de kwaliteitsfundamenten. De EMIA en/of RO-titel kan een wezenlijke bijdrage leveren aan de kwaliteitsverwachting.

Algemene informatie

Het Executive MSc in Internal Auditing aan de Universiteit van Amsterdam is de opleiding tot register operational auditor (RO), en een parttime programma voor ambitieuze internal auditors. Het is de eerste master of science (MSc) titel voor Internal Audit in de wereld. Een prestatie waar we als Nederland trots op mogen zijn!

Interesse

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

Integriteit en ethische *uitdaging* in de **toekomst**

Hebben we het vraagstuk van integriteit en ethiek richting de toekomst wel goed in het vizier? Zien we wel de 'early warning signals' van verandering?

Laten we starten met het onderdeel van integriteit dat niet verandert, namelijk dat mensen een neiging hebben om te liegen. Er bestaat zelfs een spreekwoord voor: 'een leugentje om bestwil'. Dit is al een eerste discussiepunt, wanneer is het oké en wanneer niet? Daarnaast hebben veel mensen de neiging om normafwijkend gedrag te vertonen. Bekende voorbeelden zijn het niet juist declareren van zaken bij de verzekering, het illegaal downloaden van muziek of films via internet, te hard rijden of te weinig belasting betalen of... vul maar een eigen voorbeeld in. Zoekt de internal auditor naar voor het bedrijf van toepassing zijnde (normafwijkende) signalen binnen de organisatie? En naar de effectiviteit van ingezette mechanismen om afwijkend gedrag te corrigeren of voorkomen?

De wereld staat niet stil, dus er wordt vanuit verschillende instanties gekeken naar mogelijkheden om 'voorspellende' analyses uit te voeren om signalen van normafwijkend gedrag te identificeren. Ik las recent een interessant boek van Martijn en Tokmetzis over privacy. Daarin stond dat de Belastingdienst ons allen al een risicoprofiel heeft gegeven in relatie tot potentiële fraude. Dit voelt surreëel aan, maar is al werkelijkheid. In de tussentijd zijn Google, Facebook, datahandelaars, maar ook overheidsinstanties ons aan het 'profilen'. Ze koppelen big data aan elkaar en weten daardoor meer van ons dan we zelf weten en beïnvloeden ons daar ook mee via advertenties en aanbiedingen. Is dat wel integer en ethisch? Zijn we ons bewust van de ethische risico's van deze ontwikkeling? En wat gebeurt er op dit gebied binnen uw eigen organisatie?

Misschien goed om nog eens te kijken naar de film *Minority report* waarin het draait om het onderdeel 'pre-crime', met als doel toekomstige moordenaars te arresteren voor ze een moord plegen. Maar het is niet onomstotelijk te bewijzen dat de gearresteerden ook daadwerkelijk schuldig zijn, aangezien ze worden veroordeeld voor een misdaad die niet begaan is. De filmtitel wordt verklaard doordat de afwijkende data door het proces wordt uitgefilterd, wat meteen de integriteit van het proces en de keuze blootlegt. Is hetgeen in de film wordt gedaan ethisch? En hoe kan dit worden vertaald naar de huidige praktijk? Het is deels al werkelijkheid: zie het eerdere voorbeeld van de Belastingdienst met betrekking tot 'profiling' van potentiële fraudeurs.

In de organisatie waar ik werk zijn we ook veel bezig met data, sensoren en het koppelen van data. We zijn nog niet zo datagedreven als Google, Facebook of de Belastingdienst. Zouden zij trouwens niet op korte termijn een chief ethics officer moeten aanstellen als uitdager van de technologiemenen? Bent u als internal auditor al getriggerd om na te gaan welke data-ontwikkelingen binnen uw organisatie aan de gang zijn en welke 'profiling' al gebeurt of ontwikkeld wordt? Het lijkt mij goed daar eens met een ethische bril naar te kijken en daar vragen over te stellen. Ook lijkt het mij integer dit ethische vraagstuk bespreekbaar te maken! Ik heb het al op mijn agenda gezet als een van de aandachtspunten in 2018.

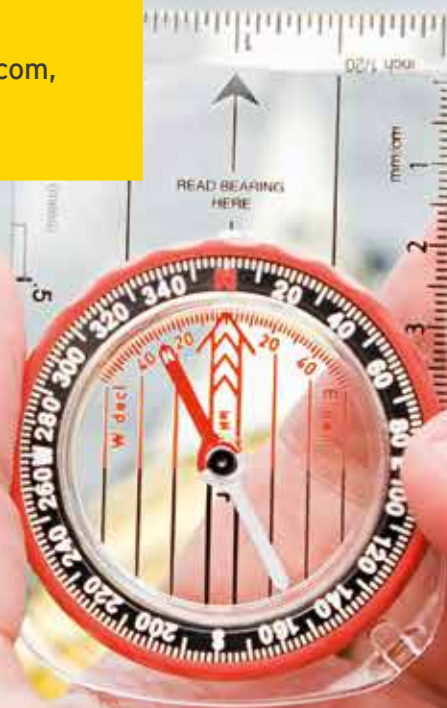
Walter Swinkels is group director Governance Risk Compliance bij Royal BAM. Hij is tevens verbonden aan het Executive Internal Audit Program van de Universiteit van Amsterdam.



Internal audit en gedrag binnen uw organisatie

Van tone at the top tot de werkvloer: gedrag en cultuur zijn sterk bepalend voor het realiseren van uw doelstellingen. Maar hoe vertaalt u uw visie en missie naar gedrag? En net zo belangrijk, hoe zorgt u ervoor dat uw organisatie de gewenste cultuur en het gewenste gedrag omarmt? Welke rol kan uw internal audit functie hierbij vervullen?

Wij vertellen u er graag meer over. Uw contactpersonen bij EY zijn Daniël Smidts (daniel.smidts@nl.ey.com, +316 29 08 40 22) of Birgit Stein (birgit.stein@nl.ey.com, +316 29 08 40 01)





25 jaar KPMG Forensic & Internal Audit

25 jaar geleden startte KPMG met forensische dienstverlening in Nederland. Met die ervaring én gebruikmakend van de nieuwste technologie helpen we internal auditfuncties met het opsporen van fraude. Zo bundelen 'jong en oud' hun krachten en staan we internal auditors bij in de essentiële rol die zij vervullen.

Together Smarter, Together Forward.

Wil je meer weten over de ontwikkeling van forensische risico's? Kijk op smarttech.kpmg.nl



Bart Van Loon
(020) 656 7796
vanloon.bart@kpmg.nl

Thom Eijken
(020) 656 8348
eijken.thom@kpmg.nl

