AUDIT magazine

Magazine voor internal en operational auditors

nummer 3 september 2012

thema:

GRC

GRC geïntegreerd en geautomatiseerd: lessons learned GRC 10.0

Three lines of defense: een kwestie van dijkbewaking?

GRC en audit bij Holland Casino: de kracht van de combinatie

Instituut van Internal Auditors Nederland

SVRO Stichting Verenigde Operational Auditors

CRUSHING CUBES IS HUMANLY POSSIBLE

Zet de beste mensen voor jouw organisatie in, of ze zich nu wel of niet aan jouw werktijden houden, bij jou op kantoor werken of zelfs in jouw tijdzone leven. Experis vindt voor jou de beste asset-focused professionals, die verantwoordelijkheid nemen voor jouw project of opdracht, met de grootst mogelijke flexibiliteit en inzetbaarheid. Dit is de denkwijze die organisaties laat groeien en industrieën verandert. Onze Risk professionals zorgen voor een geïntegreerde aanpak van Governance, Risk en Compliance. Zij zetten een mogelijk risico om in een strategische kans. Zo verbetert jouw organisatie haar prestaties en creëert ze duurzaam waarde. Ervaar hoe: **http://www.experis.nl/ras** of neem contact op met Michiel van Gemert, Practice Leader Finance, via michiel.van.gemert@experis.nl of bel 06 270 617 50.

Experis™
Finance
ManpowerGroup

De **auditor** en **GRC**


Laszlo Nagy
voorzitter


Taco Boxem


Jolanda Breedveld


Lisette Eggermont


Nicole Engel


Ton van den Hof


Willem van Loon


Arjan Man

De auditor en governance, risk management en compliance (GRC): wat moeten we hiervan vinden, weten en (in the end, toch altijd) toetsen?

Al in 2010 heeft *Audit Magazine* een themanummer gewijd aan GRC. Omdat dit een regelmatig terugkerend onderwerp is in discussies en werkzaamheden van de auditor, is ook het derde nummer van *Audit Magazine* in 2012 gewijd aan aan dit onderwerp.

Wat kunt u hierover lezen? Een paar zaken lichten we eruit: interessant is te lezen hoe ABN AMRO Bank GRC heeft geïmplementeerd in haar werkwijze. Verder een interview met de voorzitter van de Vereniging van Compliance Officers waarin wij spraken over de vlakken waarop auditors en compliance officers elkaar kunnen vinden. Maar ook een artikel over de lessons learned van de implementatie van SAP GRC tooling: interessant en leerzaam!

Een auditor dient niet in zijn eigen koker te blijven zitten, maar moet zich bewust zijn van de omgeving waarin hij opereert. GRC is een belangrijke component in die omgeving. Het helpt om de visie van anderen te horen over de rol van audit, daarom is het interview met brigadegeneraal Peter Grootendorst over zijn kijk op audit in relatie tot management, zeer lezenswaardig.

Dit is nog maar een tipje van de sluier die we oplichten. GRC is boeiend en dit themanummer zal wellicht leiden tot meer discussie over GRC in de eigen werkomgeving. The story continues…

Ten slotte willen wij Maarten Mennen bedanken die de afgelopen twee jaar de redactie van *Audit Magazine* heeft versterkt. En maken wij gebruik van de gelegenheid om nieuwe belangstellenden voor een plek in de redactie uit te nodigen om zich te melden bij de redactie.

Het thema voor nummer 4 gaat over de crisis in de wereld en de impact op audit. Neem gerust contact op met de redactie als u hierover een artikel wilt schrijven!

Veel leesplezier!

De redactie van *Audit Magazine*

FSV
RISK ADVISORY

info@fsvriskadvisory.nl
www. fsvriskadvisory.nl

Winst is een beloning voor het nemen van risico's

Een goed rendement vraagt dan ook om helder zicht op risico's en om goede maatregelen om risico's te beheersen. Wie dat optimaal in de vingers heeft, neemt een voorsprong op de concurrentie. Dat is waar FSV Risk Advisory elke dag mee bezig is bij een breed scala van organisaties.

We opereren op drie terreinen met een sterke onderlinge verbinding:
- Internal Audit
- Risk Management
- Financial Management

Onze ervaren professionals werken met u samen binnen deze drie 'lines of defence'. Uitgangspunt in onze dienstverlening is het Governance Risk Control model waarin de lines of defence met elkaar verbonden zijn.

Meer weten? Bekijk onze website: **www.fsvriskadvisory.nl**

inhoud

thema GRC

COLOFON *Audit Magazine* wordt uitgebracht namens Het Instituut van Internal Auditors Nederland (IIA Nederland), tevens eigenaar van het magazine, en de Stichting Verenigde Operational Auditors (SVRO). De redactie nodigt lezers uit een bijdrage te leveren aan *Audit Magazine*. Bijdragen kunnen worden gemaild aan: laszlo.nagy@conquaestor.nl **Redactie:** drs. L.Z. Nagy EMIA RO (voorzitter), W.T. Boxem RO EMIA, drs J.F. Breedveld, drs. N.J. Engel-de Groot RA, drs. L. Eggermont RA, A.H.M. van den Hof RO, drs. W.A.J. van Loon RA CIA, drs. J.A. Man CIA **Nieuws van de Opleidingen:** drs J.F. Breedveld en drs. R. Kamstra CIA **Verenigingsnieuws IIA Nederland:** drs. M. Docters van Leeuwen **IIA Nederland:** Postbus 5135, 1410 AC Naarden, tel.: 088-0037100, fax: 088-0037101, e-mail: iia@iia.nl, internet: www.iia.nl **SVRO:** Postbus 5135, 1410 AC Naarden, e-mail: iia@iia.nl, internet: www.iia.nl **Bureauredactie:** R. Harmelink, info@vm-uitgevers.nl **Uitgever:** G. Wymenga **Vormgeving:** M. Maarleveld **Druk:** Senefelder Misset, Doetinchem **Advertenties:** voor informatie over tarieven kunt u terecht bij Bureau IIA Nederland, tel.: 088-0037100, e-mail: iia@iia.nl. **Abonnementen:** IIA Nederland, Postbus 5135, 1410 AC Naarden, tel.: 088-0037100, fax: 088-0037101, e-mail: iia@iia.nl (zie ook de website: www.iia.nl). Abonnementen kosten € 85 per jaar, losse nummers € 25. Leden van IIA ontvangen Audit Magazine uit hoofde van hun lidmaatschap gratis. Abonnementen hebben telkens een looptijd van een jaar en gelden tot wederopzegging tenzij anders overeengekomen. Partijen kunnen ieder schriftelijk opzeggen tegen het einde van de abonnementsperiode, met inachtneming van een opzegtermijn van twee maanden. Audit Magazine verschijnt vier maal per jaar.

ISSN: 1570-856X

VM UITGEVERS

Het is niet moeilijk om in discussies terecht te komen over de definitie van governance-, risk management- en controlprocessen (GRC). ABN AMRO Group Audit realiseerde een praktische GRC-implementatie, gebaseerd op ERM. Zowel GRC als ERM stellen het halen van ondernemingsdoelstellingen centraal.

GRC: een praktische toepassing binnen ABN AMRO Group Audit

E. Ridderbeekx RE
A. van de Burgt RO

Group Audit (GA) is de interne auditorganisatie van ABN AMRO. Er werken zo'n 140 professionals in een innovatieve auditafdeling die onafhankelijk opereert en nadrukkelijk is verbonden met de organisatie. GA's missie is: 'Providing assurance to support ABN AMRO's objectives'. Dit is een bondige opdracht, die op het eerste gezicht weinig verrassends omvat. Bij nadere beschouwing dringt zich echter een aantal vragen op: waarover geven we die assurance en hoe vinden we aansluiting bij de doelstellingen van ABN AMRO?
Als onderdeel van voortdurende kwaliteitsverbetering heeft GA inhoud gegeven aan de uitwerking van dit mission statement. Een centrale plaats wordt daarbij ingenomen door governance-, risk management- en controlprocessen, kortweg GRC.
Op twee niveaus hebben we een inspanning gedaan om het mission statement verder te substantiëren. Ten eerste door een methodologische verfijning en daarnaast door kennisoverdracht en praktische implementatie. Dit artikel gaat in op de wijze waarop dat is gedaan en op het uiteindelijke resultaat.

Aanleiding

De assurance, die GA in haar mission statement belooft, geeft ze over de effectiviteit van governance-, risk management- en controlprocessen binnen de bank. De prominente plek voor GRC is geen toevallige invulling van onze scope. Op de eerste plaats noemt de Code Banken de drie GRC-elementen in de vereiste taakstelling van een bancaire interne auditafdeling. Op de tweede plaats zijn er de IPPF-standaarden: 'The internal audit activity adds value to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control processes'.
Het erkennen van deze voorschriften en standaarden en ze tot uitdrukking brengen in een audit charter is een belangrijke stap. Dat is echter niet voldoende: als een auditafdeling niet in staat is een adequate methodologische en praktische invulling te geven aan het geven van assurance over de effectiviteit van GRC, dan blijft het bij holle frasen en lopen we het risico van een ondoordachte en inconsistente auditfilosofie en -uitvoering. Bovendien vragen interne klanten (het audit committee, de board) en toezichthouders in toenemende mate om een eensluidende en solide invulling van de uitgangspunten en activiteiten van een interne auditafdeling.

> Interne klanten en toezichthouders vragen in toenemende mate om een eensluidende en solide invulling van de uitgangspunten en activiteiten van een interne auditafdeling

Governanceprocessen	Risk managementprocessen	Controlprocessen
Processen, door het management ingericht om de activiteiten van de organisatie richting te geven, te meten en bij te sturen zodat de ondernemingsdoelstellingen worden gehaald	Processen gericht op identificatie, inschatting, monitoring en beheersing van mogelijke gebeurtenissen die van invloed kunnen zijn op het halen van de ondernemingsdoelstellingen	Processen om geïdentificeerde risico's te mitigeren (en kansen te benutten) in overeenstemming met de risk appetite van de organisatie, en die bijdragen aan de waarschijnlijkheid om de ondernemingsdoelstellingen te halen

Tabel 1. Definities

In het kader van een herziening van de Group Audit Manual (GAM) is de invulling van GRC ter hand genomen.

Methodologische verfijning

GRC-processen

Het is niet moeilijk om in discussies terecht te komen over de definitie van GRC. Alleen al de betekenis van de term governance geeft aanleiding tot verschillende inzichten. Group Audit heeft gekozen voor een bruikbare set van definities (zie *tabel 1*).

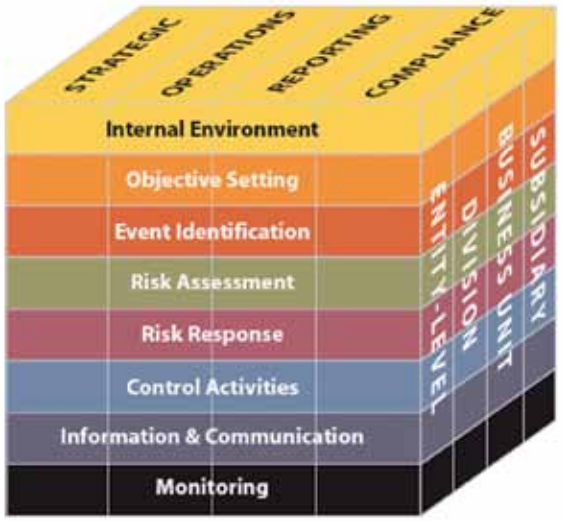
Het element dat in deze drie definities terugkomt is het halen van de ondernemingsdoelstellingen. GRC-processen leveren een vitale bijdrage aan het halen van de organisatiedoelstellingen. Het zijn de processen die het management inricht en stuurt om de onzekerheid, die inherent is aan het nastreven van een strategie en de daarvan afgeleide doelstellingen, te beheersen.
Op deze manier is GRC in het hart van ABN AMRO geplaatst. Assurance over GRC-processen is nu equivalent met assurance over het halen van de doelstellingen. Hiermee bedienen we het audit committee en het bestuur van de bank optimaal en sluiten we aan op hun prioriteiten: het halen van de doelstellingen bepaalt de managementagenda en is in feite hun raison d'être. Het betekent ook dat GA de uitdaging heeft om tijdens de fase van auditplanning objecten te selecteren en te prioriteren in de context van de bankdoelstellingen. Bovendien moet iedere audit qua doelstelling en scoping voortvloeien uit en aansluiten bij de doelstellingen van ABN AMRO. Dat dat van auditors een andere voorbereiding en een gewijzigde mindset vraagt, komt later in dit artikel aan de orde.

Relatie met ERM

Voor de verdere uitwerking van GRC binnen GA zijn de volgende uitgangspunten gehanteerd:

- de realisatie van ABN AMRO-doelstellingen staat centraal;
- de uitwerking van de GRC-methodologie is gebaseerd op een breed geaccepteerd raamwerk;
- GRC wordt ingepast in het enterprise risk managementraamwerk (ERM) dat binnen ABN AMRO aan de basis ligt van risicobeheer.

ERM stelt het management van een organisatie in staat om adequaat met onzekerheid om te gaan, waarbij de realisatie van de ondernemingsdoelstellingen centraal staat. Met de genoemde centrale plaats van de ondernemingsdoelstellingen voor GRC bleek die inpassing een hele logische: zowel GRC als ERM stellen het halen van doelstellingen centraal.



Figuur 1. Enterprise risk managementraamwerk (ERM)

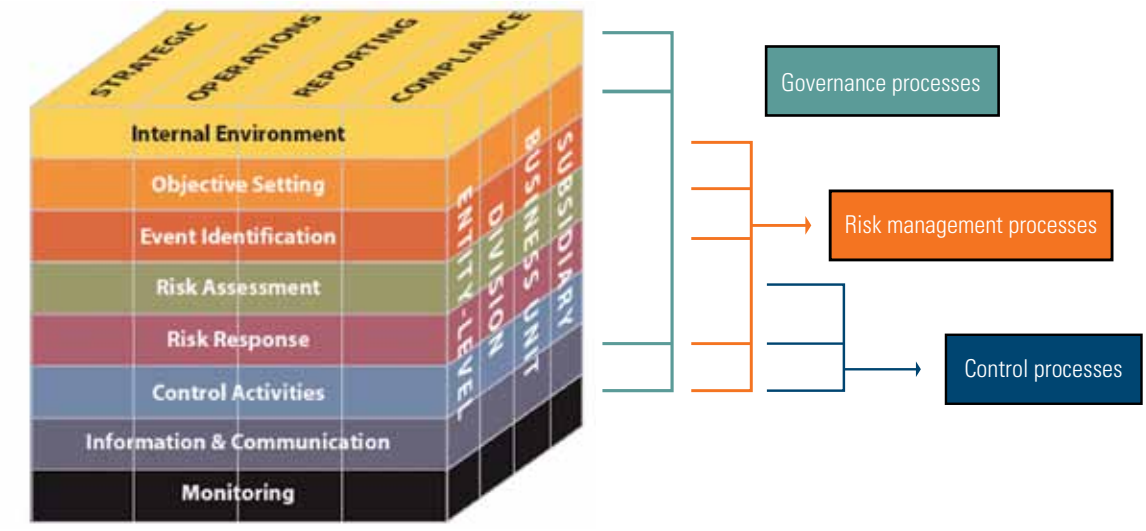
We gaan niet te diep in op ERM, maar brengen wel de bekende ERM-kubus (zie *figuur 1*) in herinnering. De voorkant van de ERM-kubus noemt een achttal componenten die aangeven wat er moet gebeuren om de doelstellingen, die in de bovenkant van de kubus zijn genoemd, te realiseren. Dat deze componenten hun beslag moeten krijgen op alle niveaus van de organisatie is weergegeven in de derde dimensie. In de doelstellingen is onderscheid gemaakt naar strategische doelen, aangevuld met doelstellingen op het gebied van efficiency en effectiviteit (operations), verantwoording (reporting) en compliance.

Het uitgangspunt is geweest dat GRC-processen de praktische implementatie zijn van de ERM-componenten. ERM geeft aan *wat* er moet gebeuren, GRC-processen zijn een invulling van de *manier waarop* dat in de organisatie vorm krijgt. Ter illustratie: een van de componenten van ERM is event identification. Deze stelt dat de organisatie moet zorgen voor mechanismen om relevante gebeurtenissen (die van invloed zijn op het halen van doelstellingen) te identificeren. Het management richt vervolgens een risk managementproces in om dit te effectueren. Het adopteert bijvoorbeeld risk self assessments als instrument en ziet erop toe dat dit organisatiebreed wordt uitgevoerd.

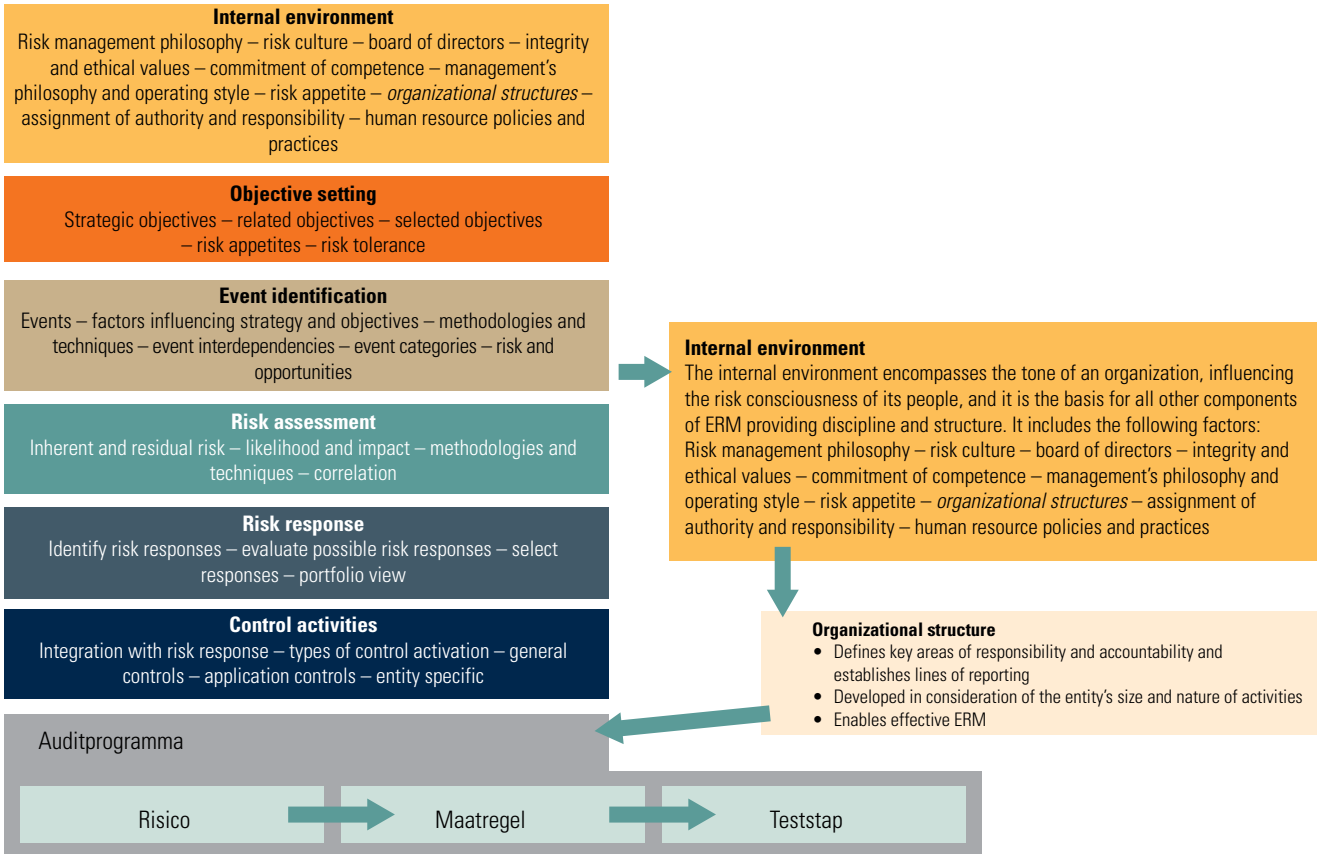
GRC in de auditpraktijk

GRC in audits

Vervolgens lag er de uitdaging om deze uitgangspunten te 'vertalen' naar de dagelijkse auditpraktijk. Dit omvatte onder andere de taak om de GA-auditprogramma's te voorzien van een generieke kern aan auditdoelstellingen en -procedures die op GRC (en dus ook ERM) zouden aansluiten. Allereerst zijn de ERM-componen-



Figuur 2. ERM-raamwerk gerelateerd aan governance-, risk management- en controlprocessen (GRC)



Figuur 3. ERM vertaald naar het audit programma voor Group Audit

ten gerangschikt als 'G', 'R', of 'C'. Daarmee wordt aangegeven of de realisatie van deze componenten door governanceprocessen tot stand wordt gebracht (G), of juist door risk managementprocessen (R) of controlprocessen (C). Soms is de categorisering wat arbitrair, het helpt echter om GRC te operationaliseren (zie *figuur 2*).

Vervolgens is elk van de acht ERM-componenten ontleed in zijn samenstellende factoren en is (per factor) vastgelegd welke:

- risico's ermee gemoeid zijn;
- maatregelen ingericht zouden moeten zijn om het risico te mitigeren;
- teststappen genomen moeten worden om de effectieve werking van die maatregelen vast te stellen.

GA-auditors gebruiken deze generieke sets van risico-maatregel-teststappen vervolgens in elke auditactiviteit, waarbij ze de uitdaging hebben om deze specifieker te maken, rekening houdend met de kenmerken van het auditobject.
In *figuur 3* is deze werkwijze met een voorbeeld geïllustreerd.
Een van de ERM-componenten is internal environment. Deze is gecategoriseerd als governance (G), en omvat meerdere factoren, waarvan organisational structure er een is. ERM noemt wat

er ten aanzien van de organisatiestructuur geregeld moet zijn. Vervolgens is dit vertaald naar een generiek auditprogramma. Als voorbeeld:

- Risico: onvoldoende duidelijkheid in verantwoordelijkheid voor processen.
- Maatregelen: expliciet en in richtlijnen en procedures geformaliseerde verantwoordelijkheden.
- Teststappen: stel vast dat verantwoordelijkheden voor processen ondubbelzinnig zijn vastgelegd en gecommuniceerd en dat betrokkenen op de hoogte zijn.

Impact van GRC

GRC heeft directe invloed op de auditwerkzaamheden in het veld; dat hebben we hiervoor laten zien. GRC heeft een stempel gedrukt op de methodologie van Group Audit en de in eerdere paragrafen beschreven filosofie is consequent toegepast in de herziene GAM. Een niet-limitatieve opsomming van wijzigingen die in het kader van GRC zijn toegepast:

De centrale plaats van ondernemingsdoelstellingen als start- en eindpunt voor auditactiviteiten komt met GRC volledig naar voren

- de centrale plaats van ondernemingsdoelstellingen als start- en eindpunt voor de activiteiten van GA komt volledig naar voren;
- oordelen worden verwoord in 'GRC-terminologie' en spreken zich uit over de betekenis van het auditresultaat in de context van het halen van de bankdoelstellingen. Dit sluit goed aan bij de behoeften en beleving van het management;
- risicoanalyse (als fundamentele peiler onder het auditplanningsproces) houdt duidelijker rekening met de betekenis van auditobjecten in het kader van de doelstellingen van de bank. Dit leidt tot een evenwichtigere en betere selectie van te auditen objecten.

Kennisoverdracht

Het proces zoals in dit artikel is beschreven, is door een GA-taakgroep gecoördineerd. De voorbereidingsfase stond in het teken van inhoudelijke bespiegelingen op GRC en het neerzetten van vaktechnisch verantwoorde en praktisch haalbare wijzigingen die een meerwaarde zouden bieden aan onze klant. Vervolgens is een eendaagse training ontwikkeld om inzicht te geven in de methodologische overwegingen en de praktische implicaties van GRC. In een tijdsbestek van drie maanden volgden alle group auditors van ABN AMRO de training. GRC is momenteel een van pijlers in de werkwijze.

Slotopmerkingen

De voordelen die de GRC-aanpak heeft opgeleverd:

- Startpunt en eindpunt van de audit zijn de doelstellingen van ABN AMRO. De auditproducten en audituitingen sluiten beter aan bij bedrijfsdoelstellingen en (dus) bij hetgeen het management belangrijk vindt.
- Het auditplanningsproces is beter gealinieerd met de ABN AMRO-doelstellingen. De selectie van auditobjecten sluit aan bij de agenda en prioriteiten van het management.
- Auditors hebben een sterkere focus op het belang dat een auditobject voor de bank heeft en stellen andere zaken ter discussie (vooral in het governancedeel).
- Er is een consistente uitwerking van uitgangspunten waaraan GA zich heeft verbonden (IPPF, Code Banken) en die GA in haar eigen mission statement belooft.
- GA-medewerkers worden professioneel uitgedaagd: het auditen van GRC-aspecten vereist andere auditvaardigheden dan de 'traditionele', niet in de laatste plaats omdat in GRC ook het auditen van soft controls is geïncorporeerd.

Er zijn ook nog aandachtspunten. Hoewel de kern van het auditwerk fundamenteel niet is gewijzigd, vereist GRC een andere benadering, waarbij vooral in de voorbereiding van audits de betekenis van het auditobject veel duidelijker in het licht van de ondernemingsdoelstellingen wordt gezien. Dat is niet altijd eenvoudig.

Daarnaast blijkt de omzetting van auditstappen – die in termen van GRC generiek geformuleerd zijn – naar stappen die naadloos aansluiten bij het specifieke auditobject, niet altijd gemakkelijk. De GRC-taakgroep blijft betrokken bij de continue verbetering van de GRC-aanpak.

Ed Ridderbeekx is senior auditmanager bij ABN AMRO Group Audit.
Anton van de Burgt is senior auditor ABN AMRO Group Audit.

GRC geïntegreerd en geautomatiseerd: lessons learned GRC 10.0

Veel organisaties zijn er op een of andere manier mee bezig: het integreren, rationaliseren en/of automatiseren van risicomanagement, interne beheersing, compliance en audit (ofwel governance, risk & compliance – GRC). Het blijkt een voortdurende zoektocht naar het creëren van waarde voor de primaire bedrijfsprocessen. Weinig organisaties weten daarbij GRC tooling op een effectieve en succesvolle manier te integreren in hun interne beheersingsstrategie en organisatie.

Drs. S. Janse
Drs. J. van de Veerdonk

Veel organisaties bevinden zich momenteel in de 'survival modus' en richten zich op het overleven van de economische crisis. Risicomanagement als aandachtsgebied kampt met verschillende uitdagingen:

- organisaties lijken moe van de veelvoud aan risico- en beheersinitiatieven van de afgelopen jaren en de druk op de primaire processen is hoog;
- diverse afdelingen (zoals risicomanagement, interne controle, informatiebeveiliging, compliance en interne audit) staan vaak nog op zichzelf;
- de kloof tussen strategische risico's en operationele beheersmaatregelen blijft lastig te overbruggen;
- risicomanagement is gedaald op de prioriteitenlijst van het topmanagement van veel organisaties;
- bruikbare GRC-rapporten ontbreken.

Hoe kun je dan toch waarde creëren voor de primaire bedrijfsprocessen vanuit risicomanagement en interne beheersing? Door meerdere assurance-initiatieven te integreren, overlap van maatregelen te verwijderen en het internal control framework te versimpelen. Sarbanes Oxley controls kunnen bijvoorbeeld overlappen met maatregelen in het kader van de Wet bescherming persoonsgegevens of met maatregelen voor duurzaamheid, veiligheid & milieu. Operationele controleactiviteiten die vaak op meerdere niveaus binnen een organisatie plaatsvinden, kunnen effectief en centraal worden beheerd.

Meerwaarde kan ook worden verkregen door top-down voor de strategische risico's op operationeel niveau maatregelen te bepalen. Bottom-up moeten de operationele beheersmaatregelen uit het bestaande interne beheersingsraamwerk kunnen worden gekoppeld aan de strategische risico's. Als er geen verband bestaat tussen de bestaande operationele beheersmaatregelen en de risico's op strategisch niveau hebben de beheersmaatregelen mogelijk geen bestaansrecht. *Figuur 1* illustreert een integrale visie op risicomanagement en interne controle.

Figuur 1. Geïntegreerd risicomanagement

Tot slot speelt software een steeds belangrijkere rol bij het integreren en beheren van GRC-processen. SAP GRC biedt de mogelijkheid om de link tussen strategische risico's en operationele beheersmaatregelen expliciet te maken, procesmaatregelen geautomatiseerd te monitoren en de diverse GRC-initiatieven te ondersteunen vanuit één softwarepakket.

SAP GRC-functionaliteit

SAP GRC bestaat uit drie geïntegreerde componenten: 1) risk management 2) process control en 3) access control. In de risk managementmodule kunnen strategische risico's en kansen, die gekoppeld zijn aan de organisatiestrategie en -doelstellingen, worden gedocumenteerd en beheerd. De process controlmodule vormt de basis voor beheer van het internal control framework, onder andere door het documenteren van maatregelen, bijbehorende karakteristieken, testplannen en resultaten van beheersmaatregelen. Daarnaast is het mogelijk om beheersmaatregelen te automatiseren en continu te monitoren. De derde module, access control, helpt organisaties bij het beheren van de SAP-toegangsrechten en het beheersen van veel voorkomende functiescheidingsconflicten. Met SAP GRC kunnen activiteiten efficiënt worden uitgevoerd door middel van workflows en real-timerapportages. Historische testresultaten en bijbehorend bewijsmateriaal kunnen worden bewaard. De sign-off workflows zorgen voor eigenaarschap voor risico's en beheersmaatregelen; managers kunnen pas aftekenen als alle, onder hun verantwoordelijkheid vallende businessunits, dit hebben gedaan. Een belangrijke functionaliteit is het effectief kunnen beheren van meerdere assurance- en verbeterinitiatieven naast elkaar en inzicht te geven in de overlap daartussen. De SAP GRC-modules zijn geïntegreerd met elkaar en de software kan ook worden geïntegreerd met niet-SAP-systemen. De integratie tussen risk management en process control maakt de link tussen strategische risico's en kansen en operationele beheersmaatregelen mogelijk. Maatregelen voor organisatorisch onoplosbare functiescheidingsconflicten, die access control heeft geïdentificeerd, kunnen worden beheerd in process control. *Figuur 2* is een voorbeeld van mogelijke datastromen in relatie tot de functionaliteit van SAP GRC.

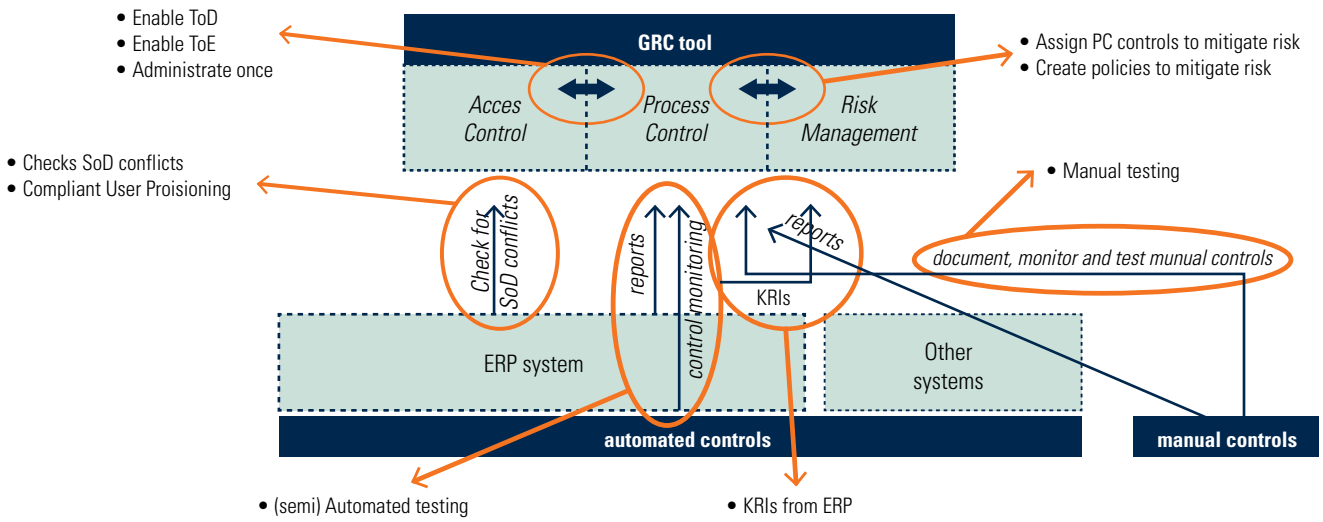
Inzicht in cost of control failures ontbreekt bij veel organisaties

SAP GRC lessons learned

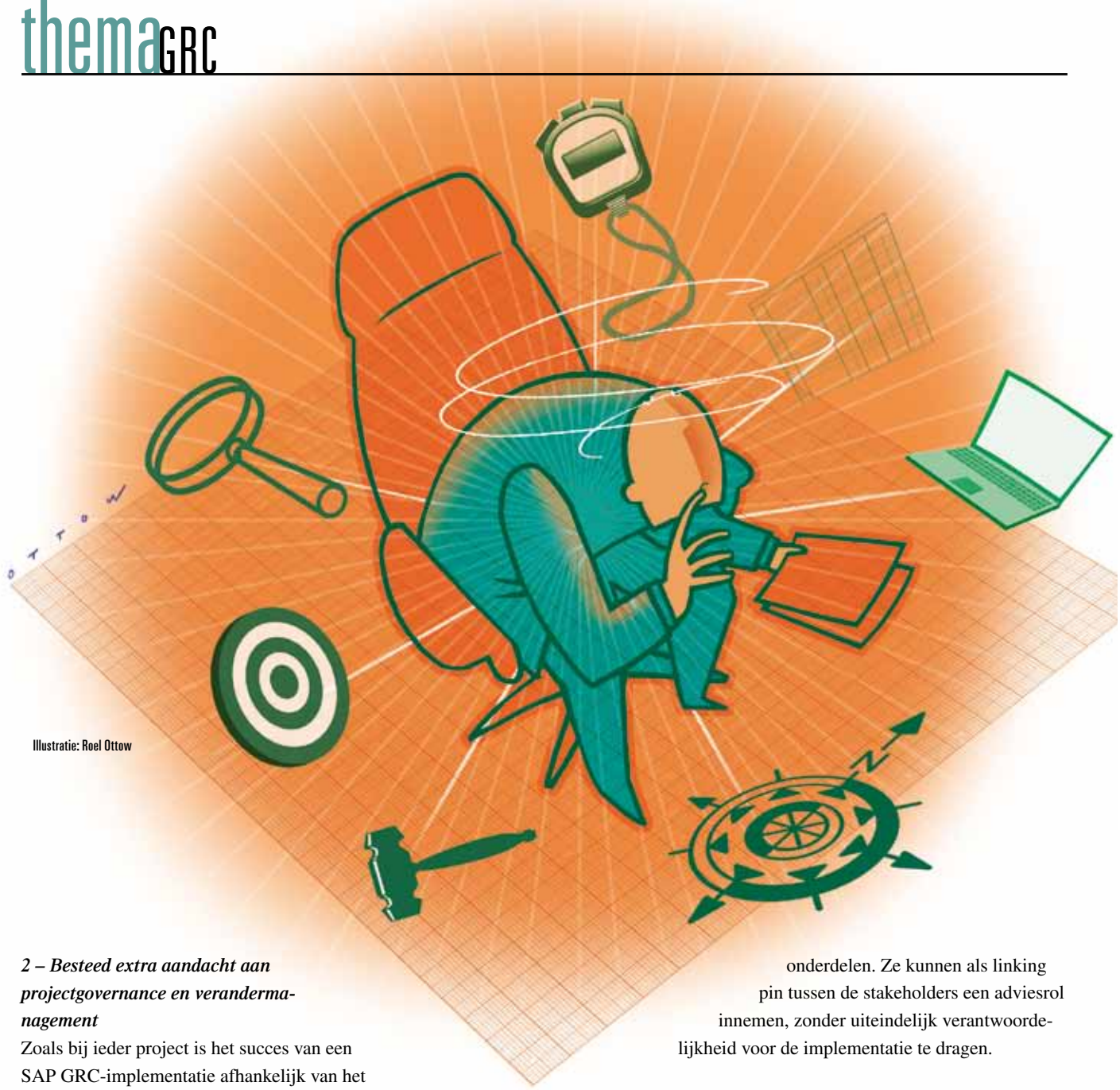
De hierna volgende opsomming van lessons learned is gebaseerd op de ervaringen die we hebben opgedaan tijdens diverse implementaties van SAP GRC en dan specifiek versie 10.0. Als u betrokken raakt bij een SAP GRC-initiatief is het belangrijk stil te staan bij deze activiteiten, waarvan de impact voor elke organisatie verschillend kan zijn. Het belangrijkste is ervoor te zorgen dat een SAP GRC-implementatie goed voorbereid wordt. SAP GRC wordt gezien als het ERP-systeem onder de GRC-softwarepakketten. De verscheidenheid aan stakeholders bij een dergelijk project maakt dat een implementatieproject van SAP GRC veel meer is dan 'de implementatie van een tool'.

1 – Gebruik het wereldwijde netwerk van experts om kennis op te bouwen

Wereldwijd bestaat er inmiddels veel kennis en ervaring over SAP GRC-implementaties. Probeer toegang te krijgen tot het internationale netwerk van kennis en expertise, bijvoorbeeld via gebruikersorganisaties, online fora waarmee nieuwe ontwikkelingen op de voet te volgen zijn. Externe experts bieden vaak de mogelijkheid om cliënten die reeds SAP GRC hebben geïmplementeerd als referentie te benaderen voor het delen van ervaring. Bouw kennis op over SAP GRC-software en de aanpassing daarvan binnen de eigen organisatie of de outsourcing partner.



Figuur 2. Datastromen in SAP GRC



Illustratie: Roel Ottow

2 – Besteed extra aandacht aan projectgovernance en verandermanagement

Zoals bij ieder project is het succes van een SAP GRC-implementatie afhankelijk van het draagvlak ervoor binnen de organisatie. Risicomanagement en interne beheersing zijn complexe specialismen waarover op een heldere manier gecommuniceerd dient te worden naar alle betrokkenen. Bij een SAP GRC-implementatie zijn veel stakeholders betrokken, zoals proceseigenaren, internal/financial controlmanagers, risicomanagers, (IT-)auditors, IT demand management, SAP compentence centremedewerkers, SAP key-users en eventuele outsourcingpartijen. Afhankelijk van de scope van het project, worden ook specialisten van andere compliance-initiatieven betrokken zoals safety, health & environment (SHE) of IT security officers (ISO27000). Ook wil het topmanagement en zelfs het audit committee vaak regelmatig op de hoogte worden gehouden van diverse lopende compliance-initiatieven en het uiteindelijke projectresultaat, dat soms gerelateerd is aan auditbevindingen.

De juiste projectgovernance en aandacht voor communicatie en verandermanagement is essentieel. Auditors kunnen verschillende rollen aannemen in een SAP GRC-implementatieproject. Onze ervaring leert dat nauwe betrokkenheid van auditors heel waardevol kan zijn voor het uiteindelijke projectsucces. Auditors hebben doorgaans veel kennis en ervaring van de verschillende bedrijfsonderdelen. Ze kunnen als linking pin tussen de stakeholders een adviesrol innemen, zonder uiteindelijk verantwoordelijkheid voor de implementatie te dragen.

3 – Maak een uitvoerige businesscase of voer een haalbaarheidsstudie uit

Het is lastig om een gedegen onderbouwde financiële businesscase te maken om GRC-activiteiten verder te integreren en te automatiseren. Hoewel de kosten voor externe en interne audits gemakkelijk zijn te bepalen, ontbreekt vaak een overzicht van de overige cost of control (of zelfs cost of control failures) en de urenbesteding in primaire en controleprocessen. Toch is het belangrijk om – voorafgaand aan een automatiseringsinitiatief – zorgvuldig alle voor- en nadelen af te wegen, de impact uitvoerig te bepalen en zoveel als mogelijk financieel te kwantificeren.

De markt voor GRC-software is volop in beweging en softwareleveranciers zijn drukdoende om functionaliteiten uit te breiden. Plaats een GRC-initiatief in een tijdhorizon van meerdere jaren. Voor organisaties die SAP- of andere ERP-software inzetten ter ondersteuning van hun bedrijfsvoering, is de businesscase doorgaans gemakkelijker te maken. De access controlmodule ondersteunt efficiënt en effectief SAP-gebruikersbeheer. Dit is zonder software een complexe, handmatige en tijdrovende klus. Ook voor grotere bedrijven die vanuit wetgeving verplicht zijn om in control te zijn, is de businesscase sneller gemaakt.

4 – Stel realistische doelen en beperk de initiële scope van het project

Zoals eerder gesteld, wordt SAP GRC gezien als ERP-systeem onder de GRC-softwarepakketten. Een gefaseerde aanpak is bij een dergelijk groot implementatieproject vaak bepalend voor het uiteindelijke projectsucces. Technisch gezien zijn de drie GRC-modules redelijk gemakkelijk te installeren en te configureren, al naar gelang de organisatiebehoeften. Wereldwijd maken vele honderden organisaties al meerdere jaren gebruik van de access controlmodule. De technische implementatie van de process controlmodule is omvangrijker, zeker wanneer van oorsprong handmatige beheersmaatregelen worden geautomatiseerd. Voor elke beheersmaatregel vergt dit een stuk programmering.

Betrokkenheid van auditors is waardevol voor het uiteindelijke projectsucces

De grootste projectuitdagingen zijn met name organisatorisch van aard. Het multi compliance framework van SAP GRC biedt organisaties de mogelijkheid om verschillende beheersinitiatieven centraal te administreren en kent technisch geen beperking van het aantal. Vanuit beheeroogpunt dient de meerwaarde van elk initiatief te worden beoordeeld om het systeem en de rapportages overzichtelijk te houden. Start met een eenvoudige implementatie, bijvoorbeeld voor een bedrijfsonderdeel, en beperk de scope van de eerste implementatie tot datgene waarvoor de software is bedoeld. SAP GRC biedt veel functionaliteit die op diverse manieren is in te zetten. Het ondersteunt bijvoorbeeld naast de invoer van risico's ook de mogelijkheid om kansen te beheren. Laatstgenoemde functionaliteit is echter nog niet op een vergelijkbaar niveau als die voor het beheren van risico's. Dit kan alleen met maatwerkaanpassingen aan de software, wat af te raden is voor software in ontwikkeling.

5 – Laat de SAP GRC-implementatie parallel lopen aan een SAP-onderhoudsproject

Projecten met grote wijzigingen aan het SAP-landschap hebben vaak afhankelijkheden met een GRC-implementatie. Dit verdient aandacht in de projectplanning. Andersom kan de SAP GRC-functionaliteit ook helpen bij het efficiënt en effectief herinrichten van geautomatiseerde en functiescheidende beheersmaatregelen in SAP, bijvoorbeeld in de blueprintfase van een SAP-project.

6 – Maak een mini businesscase per te automatiseren beheersmaatregel

Het automatiseren van beheersmaatregelen in process control is een tijdrovende klus in SAP GRC. Eenmaal ingericht leveren geautomatiseerde beheersmaatregelen veel voordelen op om controls continu te monitoren, maar het is verstandig om van te voren een kosten-batenanalyse te maken. Wanneer een beheersmaatregel rechtstreeks gebruikmaakt van bestaande rapporten in SAP, is de vereiste implementatie-inspanning beperkt. Wanneer meerdere onbekende data-elementen nodig zijn, neemt de tijdsinspanning om de beheersmaatregel te automatiseren toe. Zorg daarom voor duidelijke criteria wanneer een beheersmaatregel in aanmerking komt voor een continuous controlimplementatie.

Ten slotte

SAP heeft met de nieuwe SAP GRC-versie 10.0 de functionaliteit opnieuw uitgebreid en de verschillende modules geïntegreerd in één platform. Met de standaard functionaliteit kunnen organisaties hun assurance en GRC-processen efficiënter en effectiever uitvoeren. Een haalbaarheidsstudie die past in een meerjarenplan is een eerste, voorzichtige stap in de richting van GRC-automatisering. De grootste slag die de meeste organisaties echter op dit moment nog moeten maken is het bepalen van de overlap tussen verschillende assurance-initiatieven en het koppelen van strategische risico's en operationele beheersmaatregelen. Nauwe betrokkenheid van interne auditors bij beide activiteiten kan heel waardevol zijn voor een duurzaam resultaat.

Lessons learned SAP GRC-implementatie

- Gebruik het wereldwijde netwerk van experts om kennis op te bouwen
- Besteed extra aandacht aan project governance en verandermanagement
- Maak een uitvoerige business case of voer een haalbaarheidsstudie uit
- Stel realistische doelen en beperk de initiële scope van het project
- Laat de SAP GRC-implementatie parallel lopen aan een SAP-onderhoudsproject
- Maak een mini businesscase per te automatiseren beheersmaatregel

Figuur 3. Lessons learned SAP GRC-implementatie

Joris van de Veerdonk is senior consultant bij Protiviti – een internationaal onafhankelijk adviesbureau voor business & risk consulting. Hij is afgestudeerd econometrist en heeft een business- en IT-achtergrond. Hij helpt organisaties met het efficiënt en effectief inrichten van processen.

✉ Contact@protiviti.nl

Suzanne Janse is senior manager bij Protiviti, IT-auditor en heeft een 'Big 4'-achtergrond. Bij Protiviti is zij verantwoordelijk voor de dienstverlening rondom GRC (goverance risk & compliance) tooling en helpt ze organisaties op een effectieve manier hun ERP (project) risico's te beheersen.

✉ Contact@protiviti.nl

Three lines of defense: een kwestie van dijkbewaking?

Three lines of defense (3LoD) is een concept dat ertoe dient om risk management (risk ownership, risk control and risk assurance) effectief en efficiënt in te richten. Daarnaast kan de benadering helpen om taken en verantwoordelijkheden beter af te bakenen en te communiceren.

Drs. H. van Hout RA

Risk management is een 'hot topic' in de financiële wereld en staat sinds de kredietcrisis in verhoogde belangstelling. Bij ABN AMRO is dat niet anders. Risk managementexperts (inclusief consultants en auditors) adviseren steeds vaker om de zogenaamde three lines of defense (3LoD) in te voeren. Diverse grote banken zijn net als ABN AMRO op dit moment doende dit concept in te voeren. Dit is opmerkelijk omdat er nauwelijks een theoretische onderbouwing bestaat. Ook de financiële toezichthouders hebben zich tot nog toe niet formeel uitgelaten over 3LoD. Toch lijkt een verspreiding van 3LoD naar andere (financiële) ondernemingen een kwestie van tijd.

De waker, de slaper en de dromer

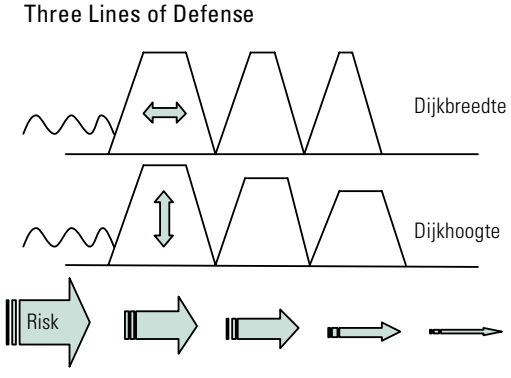
'Dijkbewaking' is een goed passende vertaling voor 3LoD in de Nederlandse context. Immers, in haar strijd tegen het water kent Nederland drie dijken: de waker, de slaper en de dromer. Bij voorkeur neemt de eerste dijk zo veel mogelijk risico weg en is de kans dat alle drie de dijken doorbreken zeer klein. Het volledig uitsluiten van risico is niet mogelijk omdat er altijd een risk returnvraagstuk achter ligt. De investeringen zullen echter aanzienlijk zijn en pas als de risico's groot genoeg zijn zal men bereid zijn meer te investeren.

Dijkhoogte en dijkbreedte

In *figuur 1* zijn de lines of defense vertaald als dijken en het risico als de zee. Eenvoudig gesteld betreffen de keuzen die gemaakt moeten worden de hoogte en breedte van de dijken. De hoogte van dijken betreft dan het aantal verschillende controls en mitigerende acties dat wordt ingebouwd in de verschillende lines of defense.
De breedte zou gelijkgesteld kunnen worden met de frequentie waarmee controls dienen te worden uitgevoerd. De verhouding tussen dijkhoogte en dijkbreedte luistert nauw en voorkomen moet worden dat ze doorbreken. In alle gevallen zal het zo zijn dat de dijken de risico's mitigeren maar waarschijnlijk niet uitsluiten; althans niet tegen aanvaardbare kosten.
In dit kader moet worden opgemerkt dat het materiaal waarmee een dijk gebouwd wordt, de ligging ten opzichte van de zee, de stroming en de ondergrond, eveneens zeer bepalend zijn. Uiteindelijk gaat het om de kwaliteit (voldoet de dijk aan het doel waarvoor deze gebouwd is), hier teruggebracht tot twee dimensies: hoogte en breedte.

Risk management en 3LoD

Niet alleen bij de strijd tegen het water, maar ook bij risk management van banken wordt 3LoD steeds vaker gebruikt. Risk management wordt dan specifiek genoemd als middel tegen vele kwaden, waaronder ook de kredietcrisis.[1] Ging het bij Sarbanes Oxley (SOx) nog om het versterken van controls rondom financiele verslaggeving, bij COSO ERM gaat het al veel meer over een holistische risicobenadering op ondernemingsniveau.



Figuur 1. De three lines of defense

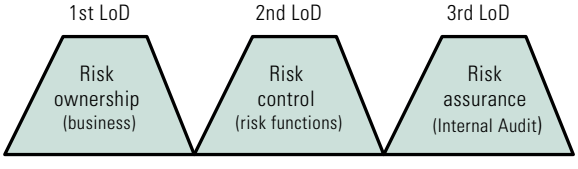
Een voordeel van SOx en COSO ERM-model is natuurlijk dat het ondernemingen stimuleert op een gestructureerde wijze met risk management om te gaan. De 3LoD voegt daaraan toe dat specifiek wordt gemaakt wat met risk management wordt bedoeld en hoe het kan worden toegepast.
Bij 3LoD worden drie verdedigingslinies onderscheiden bij het managen van risico's. De eerste linie wordt dan gevormd door de business of front office (hier ligt het risk ownership). Op basis van risk return besluit men een transactie of contract al dan niet aan te gaan. Bij de tweede linie ligt de nadruk dan veel meer op risk oversight en monitoring. De taken kunnen toebedeeld zijn aan een risk committee of risk managementafdeling (hier samengevat als risk control). De derde linie wordt gevormd door Internal Audit

De Nederlandse versie van de three lines of defense: de waker, de slaper en de dromer

en zal zich richten op het functioneren van de eerste twee verdedigingslijnen door het doen van specifieke onderzoeken gericht op risk assurance (zie *figuur 2*).

Is 3LoD ook effectief?
De effectiviteit moet gezocht worden in de duidelijke afbakening en samenwerking tussen risk ownership, risk monitoring en risk assurance (zijn de dijken sterk en hoog genoeg?). Bij effectiviteit gaat het er dan ook om dat risico's waaraan een organisatie blootstaat worden onderkend en beheerst. Het 3LoD-concept is geen beproefde aanpak, al is het wel zo dat banken als ABN AMRO, Citibank, ING, RBS en UBS dit aan het invoeren zijn dan wel net hebben ingevoerd.
De kritische lezer zal vaststellen dat het merendeel van deze banken niet ongehavend uit de kredietcrisis is gekomen. Des te opvallender is het dat er vanuit de toezichthouders (bijvoorbeeld DNB) officieel nauwelijks aandacht is gegeven aan deze nieuwe risicobenadering. De daadwerkelijke effectiviteitsvraag is dan ook moeilijk te beantwoorden en vraagt om nader onderzoek.

Hoe efficiënt is 3LoD?
Als het gaat om de doelmatigheid moet voorkomen worden dat dubbelslagen ontstaan (zijn de dijken niet te hoog, niet te breed en dus te duur?). De eerste en de tweede lijn moeten niet stel-



Figuur 2. De drie verdedigingslinies

selmatig dezelfde werkzaamheden en controls uitvoeren. Steekproefsgewijs laten vaststellen door de tweede lijn of de eerste lijn zich op een goede manier van haar taken kwijt, is logisch en past bij een monitoringrol. Ook zal het zo moeten zijn dat een goed functionerende eerste lijn leidt tot een 'slankere' en dus goedkopere inrichting van de tweede lijn. Hetzelfde kan gezegd worden over de zwaarte van de derde lijn bij een goed functionerende tweede lijn.
Andersom redenerend zou een slecht functionerende eerste lijn kunnen leiden tot een zwaardere tweede lijn. En een slecht functionerende tweede lijn tot een zwaardere derde lijn. Het probleem dat hierbij ontstaat is in hoeverre controls die ontbreken in de eerste lijn te compenseren zijn in de tweede lijn. In dit verband komt de gedachte op aan 'vervangbare en onvervangbare' controls.[2] Bij het doen van bijvoorbeeld betalingen zal het falen van de eerste lijn heel lastig zijn op te vangen omdat het geld onmiddellijk zal

worden overgeboekt. Het zal dan ook maar beperkt mogelijk zijn falende internal controls in de eerste lijn te compenseren in de tweede of derde lijn.

Waar ligt de verantwoordelijkheid?
Door de eerste lijn gelijk te stellen aan de business en de tweede lijn aan risk control lijkt er duidelijk onderscheid te bestaan tussen beide linies. Bij het nader invullen van 3LoD ontstaan al snel discussies of bepaalde activiteiten of afdelingen onderdeel zijn van de eerste of tweede line of defense. Discussies bij banken spitsen zich veeleer toe op afdelingen als IT, Interne Controle, Finance en Compliance. De activiteiten die de business direct ondersteunen worden dan vaak als eerste lijn gezien en de activiteiten met een meer monitorend karakter als tweede lijn.
Ook is het niet zo dat voor ieder proces er een eerste, tweede en derde lijn moet zijn ingericht. Dat is opnieuw een vraag van kosten en toegevoegde waarde. De derde LoD leidt tot minder discussie en wordt meestal geassocieerd met Internal Audit. Vaak rapporteert de internal audit functie zowel aan het hoogste management alsook via een audit committee aan de raad van commissarissen. Dit laatste betekent overigens niet dat het audit committee ook onderdeel vormt van de derde LoD.

Hoeveel lines of defense zijn er eigenlijk: drie of zes?

Bestaat er een vierde, vijfde of zesde LoD?
De externe accountants en financiële toezichthouders zoals DNB en AFM zullen geregeld beoordelen in hoeverre risk management binnen een bank goed is geregeld. Zij zullen zich in eerste instantie richten op het functioneren van de derde lijn. Zowel de externe accountants als de toezichthouders zullen zich hiertoe niet beperken. In het kader van hun wettelijk vastgestelde taken zullen zij ook kijken naar de eerste en tweede lijn om zich zo een mening te kunnen vormen over het risk management binnen een bank.
De vraag die gesteld kan worden is of de externe accountant en toezichthouder onderdeel zijn van het line of defenseconcept en respectievelijk de vierde en vijfde LoD vormen. Een groot verschil is natuurlijk dat beide groepen geen onderdeel uitmaken van de onderneming.
Tot slot de aandeelhouders, deze staan nog wat verder af van de onderneming maar ook zij kunnen (het bestuur van) de onderneming ter verantwoording roepen. Op deze manier vormen de aandeelhouders de zesde LoD. Het lijkt niet zinvol om deze lijnen toe te voegen aan het 3LoD-model omdat de onderneming hierop geen of weinig invloed heeft. Vanuit de maatschappij gezien ligt dit anders en zal men zeker bij debacles (denk aan Van Der Hoop en DSB) verwachten dat de externe accountant, toezichthouder en aandeelhouder (via de RvC) ook verantwoordelijkheden dragen.

De drie functiescheidingen van de toekomst?
Bij het bespreken van functiescheidingen denkt menigeen al snel aan Starreveld, de controletechnische functiescheiding tussen beheren, bewaren, uitvoeren, registreren en controleren. Het onderscheid tussen risk ownership, risk control en risk assurance is ook een vorm van functiescheiding maar is niet gelijk te stellen aan controletechnische functiescheidingen.
Binnen de first line of defense zullen zowel beherende (bijvoorbeeld kredietverlening), bewarende (bijvoorbeeld geldvoorraad), uitvoerende (bijvoorbeeld verwerken betalingsopdrachten) en registrerende functies (bijvoorbeeld rekening courant administratie) zijn ondergebracht. De derde lijn is daarentegen grotendeels gelijk te stellen aan de controlerende functie, meestal in de vorm van Internal Audit. Binnen de tweede lijn (risk control) kunnen ook diverse soorten functies worden neergelegd: beheer (bijvoorbeeld fiatteren van limietoverschrijdingen), registreren (bijvoorbeeld operationele verliezen), uitvoeren (bijvoorbeeld berekenen kapitaalbeslag) en controleren (bijvoorbeeld inspecties). 3LoD is dus geen vervanging van de traditionele functiescheidingen maar moet eerder gezien worden als een functiescheiding op een hoger, conceptueel niveau.

Eerst praktijkresultaten
Binnen ABN AMRO is het concept van 3LoD niet alleen steeds meer bankbreed bekend, maar wordt het ook actief gebruikt bij het inrichten van processen en het managen van risico's. Met name de vraag waar risk ownership ligt en wie risk monitoring uitvoert schept veel duidelijkheid. Het begrip risk management blijkt in de praktijk namelijk heel verschillend te worden ingevuld (soms wordt risk ownership bedoeld, soms valt risk monitoring daar ook onder en een andere keer weer niet). Door risk ownership en risk monitoring expliciet uit elkaar te trekken wordt veel helderder waar welke verantwoordelijkheden liggen. Dit laatste is voor een financiële instelling als ABN AMRO anno nu natuurlijk essentieel.

Noten
1. *Bringing Back Best Practices in Risk Management Banks, Three Lines of Defense,* Booz&Co (10/2008).
2. Leerboek accountantscontrole 2a (4.2.625).

Huub van Hout is audit director bij Group Audit binnen ABN AMRO Bank. Dit artikel is op persoonlijke titel geschreven. Reacties of vragen naar aanleiding van dit artikel kunnen worden gestuurd naar ✉ vanhout2003@yahoo.com.

De lezer over governance, risk management en compliance

Via de IIA-website zijn wederom stellingen aan de lezer voorgelegd, dit keer over GRC. Zo'n tachtig reacties zijn ontvangen.

Stelling 1

GRC is een ingewikkeld woord voor interne beheersing

	in %
1. Helemaal mee eens	14
2. Mee eens	40
3. Neutraal	4
4. Mee oneens	33
5. Helemaal mee oneens	9

Stelling 2

GRC is het enige effectieve antwoord op de toenemende regeldruk

	in %
1. Helemaal mee eens	5
2. Mee eens	22
3. Neutraal	19
4. Mee oneens	48
5. Helemaal mee oneens	6

Stelling 3

GRC-tools zijn onmisbaar voor de implementatie van GRC

	in %
1. Helemaal mee eens	5
2. Mee eens	33
3. Neutraal	28
4. Mee oneens	26
5. Helemaal mee oneens	8

Stelling 4

Implementatie van GRC kost meer dan het oplevert

	in %
1. Helemaal mee eens	0
2. Mee eens	15
3. Neutraal	17
4. Mee oneens	51
5. Helemaal mee oneens	17

Het begrip GRC is op meerdere manieren uit te leggen. Met de eerste stelling wilden wij weten of auditors GRC als iets nieuws ervaren. Voor de helft van de respondenten is dit niet het geval, zij waren het eens met de stelling 'GRC is een ingewikkeld woord voor interne beheersing'. Een vrij expliciete reactie hierop was de volgende: 'het op orde hebben van je interne beheersing is van alle tijden'. En: 'iedere organisatie doet impliciet of expliciet aan GRC, alleen de invulling, instrumentatie en vorm verschillen'. De overige helft echter was het hiermee niet eens, voor hen geldt dat GRC echt wel iets anders is dan interne beheersing.

Ook wilden wij weten of GRC het enige effectieve antwoord is op de toenemende regeldruk. Een duidelijke meerderheid is het hier niet mee eens. Of dit betekent dat er meer antwoorden mogelijk zijn op de toenemende regeldruk of dat GRC geen effectief antwoord is, wordt uit de reacties niet duidelijk.
Dan de tooling: is dit een noodzakelijkheid om effectief GRC te implementeren of kan GRC ook zonder tooling effectief zijn? De reacties waren verdeeld. Zowel eens als oneens als neutraal kregen veel stemmen.

De laatste stelling leverde wel een duidelijk beeld op. Een overgrote meerderheid van de respondenten vindt dat de implementatie van GRC meer oplevert dan het kost. Uit de reacties kwam echter wel een aantal voorwaarden voor succes van GRC. Zo meldde een respondent dat 'the tone at the top bepalend is voor het succes van GRC'. 'Ook hangt het resultaat van GRC af van hoe je het toepast en of het voldoende is afgestemd op de organisatie', aldus een andere reactie. Verder werd vermeld dat 'heldere communicatie (praktische waarde) en een gefaseerd plan bijdragen aan een omgeving waarin GRC niet langer als een modeterm wordt beschouwd, maar als een aandachtsgebied dat bijdraagt aan de uitvoering van de strategie'.

Dit themanummer over GRC geeft weer voldoende stof tot nadenken. Zonder twijfel zal het volgende themanummer dit ook doen. Wilt u uw mening geven over het komende thema 'Auditing en de crisis' en daarbij kans maken op een boekenpakket? Houd dan de IIA-website in de gaten! Dit keer is de gelukkige winnaar van het boekenpakket **Martin Buitink**.

KPMG
cutting through complexity

IT ADVISORY

IT biedt onbegrensde mogelijkheden. Wat vraagt uw organisatie?

IT staat hoog op elke bestuursagenda. Adviezen zijn er volop en oplossingen lijken grenzeloos. Maar hoe weet u of u de juiste keuzes maakt? KPMG IT Advisory adviseert onafhankelijk en deskundig, maakt risico's beheersbaar en zorgt ervoor dat IT optimaal bijdraagt aan uw business. Nu en in de toekomst.

Meer weten? Bel: (020) 656 8021
kpmg.nl

De compliancefunctie: een toekomstvisie

De compliancefunctie is een essentiële schakel in het risicobeheersingsstelsel van veel organisaties. Samenwerking tussen de audit- en compliancefunctie levert beide functies veel op. Reden voor *Audit Magazine* om Mirjam Bakker, global head Compliance bij AEGON nv en tevens voorzitter van de Vereniging van Compliance Officers, te vragen naar haar visie op de compliancefunctie en de samenwerking met de internal auditor.

Drs. N.J.Engel-de Groot

U bent global head Compliance bij AEGON nv en tevens voorzitter van de Vereniging van Compliance Officers. Wat houden deze werkzaamheden in?

"Wat betreft mijn functie bij AEGON: ik geef leiding aan de complianceorganisatie van AEGON. AEGON is actief in meer dan twintig markten en heeft 47 miljoen klanten wereldwijd. Het domein van compliancemanagement omvat, naast wet- en regelgeving en interne gedragscodes, ook relevante normen en waarden die nog niet zijn verankerd in wet- en regelgeving maar wel van maatschappelijk belang zijn en een impact kunnen hebben op de reputatie van de onderneming. Hoewel ik sturing geef aan de organisatie van compliancemanagement, is iedere medewerker van AEGON, ongeacht de functie, verantwoordelijk voor zijn aandeel in een integere bedrijfsvoering. Persoonlijke accountability in alle gelederen van de organisatie is de kern van een integere bedrijfsvoering. Vandaar dat wij integriteit en ethiek ook verankerd hebben in het *AEGON Global Compliance Charter*. Dit charter omschrijft, naast de rol van de compliancefunctie, de eerstelijn verantwoordelijkheden van management.

AEGON heeft wereldwijd ruim vierhonderd medewerkers die een compliancefunctie vervullen. Het compliancemanagement van de activiteiten in onze drie belangrijkste markten (de Verenigde Staten, Nederland en het Verenigd Koninkrijk) en in opkomende markten (Midden- en Oost-Europa en Azië) rapporteert functioneel aan mij. Hiermee wordt compliance lokaal aangestuurd terwijl er toch een eenduidige lijn naar het hoofdkantoor in Den Haag wordt bewerkstelligd. Materieel betekent dit dat ik gesprekspartner ben van zowel het lokale compliance- en businessmanagement als van de raad van bestuur op AEGON nv-niveau.

Acht jaar geleden ben ik bij AEGON nv gestart als senior legal counsel. Daarvoor ben ik lange tijd werkzaam geweest als bedrijfsjurist bij diverse industriële organisaties. Sinds oktober 2011 ben ik voorzitter van de Vereniging van Compliance Officers (VCO). De VCO heeft binnen de financiële sector leden op diverse niveaus van financiële instellingen. De VCO vertegenwoordigt complianceprofessionals van grote internationaal opererende, alsook van middelgrote en kleine instellingen in Nederland en heeft 425 leden. Wij willen een platform bieden voor de compliancefunctie om kennis te delen en willen een denktank zijn ten behoeve van ontwikkeling van de compliancefunctie. Wij beraden ons op dit moment of we ook een platform zouden kunnen bieden voor compliance officers werkzaam in andere sectoren. De VCO heeft recent een survey gehouden onder haar leden. De uitkomsten van deze survey zullen wij onder meer gebruiken om al dan niet tot deze verbreding over te gaan.

> Een compliance officer moet meer kijken naar de 'menskant' van de onderneming

Wij komen vier keer in het jaar bijeen en tijdens deze ledenvergaderingen komen actuele thema's aan bod. Voor de compliance officer zijn er diverse opleidingen, zoals de postgraduate-opleiding compliance & integriteit management aan de VU Amsterdam of

de leergang certified compliance officer van het NIBE-SVV. Wij worden regelmatig geconsulteerd ten aanzien van de inhoud van opleidingsprogramma's. Wij bieden zelf geen opleidingen, maar zijn wel actief betrokken bij het accreditatiekader van de compliancefunctie dat beheerd wordt door het DSI.[1] Het DSI onderhoudt tevens het bijbehorende register van compliance professionals."

Welke ontwikkelingen onderkent u ten aanzien van het belang van compliance en de rol van de compliance officer?

"De compliance officer bevindt zich traditioneel in de hoek van de wet- en regelgeving. Dat is een vrij enge invulling van de functie. Ik vind dat van de compliance officer verwacht mag worden dat hij zich ook proactief richt op het in kaart brengen van de maatschappelijk relevante ontwikkelingen voor de onderneming. Zeker nu, in een tijd dat er veel druk is op financiële organisaties vanuit de maatschappij. Dit kunnen ontwikkelingen zijn ten aanzien van de belangen van klanten en andere stakeholders die nog niet zijn verankerd in wet- en regelgeving. Hiernaast is ook de vertaling van deze ontwikkelingen naar de implicaties voor de organisatie een belangrijke rol van de compliancefunctie. Dit betekent dat zij als hoeder van de integriteit het businessmanagement moet kunnen adviseren maar deze soms ook als sparringpartner de spiegel moet kunnen voorhouden. Ik zie het als taak van de VCO om deze noodzakelijke aanvulling in de rol van de compliance officer over het voetlicht te brengen."

> Er valt veel te winnen als de second en third lines of defensefuncties hun begripsvorming, doelstellingen en normenkader conceptueel op elkaar afstemmen

Wat maakt een goede compliance officer?

"Om te beginnen denk ik dat een compliance officer een meer dan gemiddeld gevoel moet hebben voor het belang van een integere bedrijfsvoering; voor de 'menskant' van de onderneming. Daarbij is het essentieel dat de compliance officer ervan overtuigd is dat een integere bedrijfsvoering leidt tot waardecreatie van de onderneming op lange termijn. Een goede compliance officer moet ook empathisch zijn en in staat zijn om op een positieve manier impact te hebben op zijn management. Dus met enig gezag kunnen optreden als natuurlijk gesprekspartner van het management. Dit alles op basis van een gedegen inhoudelijke kennis van wet- en regelgeving maar ook van risicobeheersingssystemen en analytisch vermogen. Bovendien is ook een goed begrip van de producten en diensten essentieel. Ten slotte let ik er zelf altijd op of compliance officers een helikopterview hebben en goed verbanden kunnen leggen. Verder is, zoals ik al aangaf, een proactieve houding heel belangrijk. De compliance officer is van nature vrij afwachtend en zal eerst kijken naar wat er op hem afkomt om hiervan iets te vinden. Het is juist belangrijk om zelf trends van buiten de organisatie te onderkennen en de impact op de eigen organisatie te onderzoeken.

Dit alles maakt de rol van compliance officer zeer uitdagend maar ook moeilijk. Als 'countervailing power' moet je sterk in je schoenen staan en prioriteiten kunnen stellen. Meebewegen als het kan en je punt maken als het moet. Hierin verschillen de compliance officer en de auditor niet van elkaar. Een goede auditor zal zich goed kunnen kwalificeren als compliance officer. Maar het zou de compliancefunctie verrijken als we ook sociologen, organisatiepsychologen of mensen uit de business weten te inspireren voor een rol als compliance officer. We kijken toch te snel naar mensen met een juridische, risk- of accountancyachtergrond."

Hoe ziet u de relaties met de andere risicobeheersfuncties?

"De compliance officer formuleert namens het management het beleidskader voor compliancemanagement. Daarnaast heeft hij een taak als countervailing power en hoeder van de integriteit. In deze rol acteert de compliancefunctie in de second line of defense samen met andere risicobeheersfuncties zoals operational risk management. De internal auditfunctie bevindt zich in de third line of defense. De compliancefunctie kan een beroep doen op de auditfunctie om een audit uit te voeren op haar werkzaamheden.

Dit is de theorie, de praktijk kan soms wat weerbarstiger zijn. Het functioneren naast en met andere risicobeheersfuncties kan vaak effectiever en efficiënter. Dit geldt voor zowel de samenwerking tussen de compliancefunctie en de andere risicobeheersfuncties die optreden in de second line of defense als voor de samenwerking tussen de compliancefunctie en de auditfunctie. Een goede samenwerking leidt tot synergie. Ik denk dat er veel te winnen is als de second en third lines of defensefuncties hun begripsvorming, doelstellingen en normenkader conceptueel op elkaar afstemmen. Daarnaast is er veel basale kennis uit te wisselen, bijvoorbeeld over soft controls. Natuurlijk kan de business niet

ontbreken in het afstemmen van doelstellingen en de identificatie van soft controls. Helaas zitten de internal audit- en compliancefunctie vaak te weinig met elkaar aan tafel. Het zou goed zijn als compliance- en de auditfunctie dit samen oppakken. Begin maar eens met de soft controls, welke zouden dat moeten zijn en hoe maak je ze meetbaar?"

Wat is volgens u het ideale organisatorische plaatje van de risicobeheersfuncties?

"Ik denk niet dat er één juist governancemodel is. De keuze voor een bepaalde governancestructuur is heel erg afhankelijk van de organisatie. Daarnaast kan de governance er formeel op papier nog zo goed uitzien, als het compliancemanagement in de praktijk geen goede relatie heeft met het businessmanagement dan helpt een rapportagelijn maar beperkt. Bij AEGON rapporteer ik sinds een jaar aan de chief risk officer. Binnen AEGON hebben wij daar bewust voor gekozen om daarmee enterprise risk en compliancemanagement dichter bij elkaar te brengen en elkaars complementaire kwaliteiten te versterken. Waar risk management zich bij financiële instellingen voornamelijk richt op kapitaalrisicomanagement, heeft compliancemanagement vaak meer affiniteit met reputatiemanagement en het proactief beïnvloeden van gedrag en cultuur. Bij kleinere organisaties zie je nog wel eens dat Internal Audit en compliance samen in een functie opgehangen zijn. Dit is wat mij betreft niet aan te bevelen omdat je dan geen onderscheid maakt tussen de second en third line of defense."

Tot slot: wat wordt de toekomst van compliance?

"De compliancefunctie is niet meer weg te denken. We leven in een complexe internationale economische omgeving die continu aan veranderende wet- en regelgeving onderhevig is. Bovendien is anticiperen op maatschappelijke ontwikkelingen van belang voor het bestaansrecht van de onderneming. In zo'n omgeving is een compliancefunctie essentieel. Ik denk daarom dat iedere beursgenoteerde organisatie een compliancefunctie zou moeten hebben. Deze organisaties zijn kwetsbaar; fouten en beeldvorming kunnen een enorme impact hebben op de reputatie. De compliancefunctie zal effectiever zijn in een context waarin de organisatie zelf zich realiseert dat integer ondernemerschap bijdraagt aan duurzame waardecreatie. Veranderprocessen zijn dan gemakkelijk te realiseren. Verwacht niet dat de compliance officer een regelsteller of regelcontroleur is, waar het om gaat is de organisatie in beweging te krijgen en waar nodig de spiegel voor te houden, als gesprekspartner van het management. Uiteindelijk moeten de organisatie en het management zelf deze cultuur van integere bedrijfsvoering omarmen en daar verantwoordelijkheid voor dragen. Zo geldt voor de financiële sector dat zij zich heel goed realiseert dat het centraal stellen van klantbelang elementair is voor haar bestaansrecht. Compliancemanagement heeft een belangrijke rol bij de vertaling van dit principe naar de dagelijkse bedrijfsvoering."

Noot

1. Het DSI verstrekt een persoonsregistratie aan deskundigen binnen de financiële dienstverlening die aan bepaalde eisen voldoen op het gebied van deskundigheid, integriteit en werkervaring.

Nicole Engel-de Groot is redactielid van *Audit Magazine* en werkt bij DNB.

Berichten kunt u mailen naar iia@iia.nl

Personalia

Wie	Uit dienst van	In dienst van
Drs. M.A. van Maarseveen RA CIA	Rabobank	Aegon Nederland
Ing. M.A. van de Wal EMIA RO CIA	Ernst & Young Accountants	Aramco Overseas Company bv
Drs. A. Vermeulen CIA CISA CRISC CISSP	Warnaco bv	Bristol-Myers Squibb
W.M. Landstra RA		Coöperatie Univé
R.F.M. Merkestijn RO	Ministerie van Economische Zaken, Landbouw en Innovatie	Elegas Beheer bv
Drs. I. Veerman RA RO	KPMG	Faber Halbertsma Groep
Drs. I.F.J. Walraven RO	RWS Dienst Zuid-Holland	Gemeente Velsen
Drs. E.F. Van der Burg RO CIA	ING Groep	Hyva
Drs. J. Beens	ABN AMRO Bank nv	ING Groep
H.J. Keyzer RO EMIA CIA	Rijkswaterstaat Noordzee	Inspectie Leefomgeving en Transport
J.J.M. Koenen RA CIA	CZ	KoenenAC&E bv
R. van Tatenhove RA	VION nv	Koninklijke Vopak nv
Drs. M.E. Gielbert RO	Interimpuls Diensten	M-cep Audit & Advies
Drs. M. de Pooter RA CMA CFM CIA	Ernst & Young Accountants LLP	MdP | Management, Consulting
Drs. P. Kool EMIA RO	Ministerie van Verkeer en Waterstaat	Ministerie van Financiën
R. Pijl RO EMIA CIA	Ministerie AD/ OCW	Ministerie van Financiën
Drs. C.G.C. Fadli-Koning EMIA RO	Ministerie van Economische Zaken, Landbouw en Innovatie	Ministerie van Financiën
Drs. A. van Driel - van Trigt RA RO	Ministerie van Economische Zaken, Landbouw en Innovatie	Ministerie van Financiën
Drs. W.P.M. Beekmans MPA	Ministerie van Economische Zaken, Landbouw en Innovatie	Ministerie van Financiën
R.M.M. Damen RA RE	Schering Plough	MSD
Drs. J. van Bruchem EMIA RO	Ministerie van Economische Zaken, Landbouw en Innovatie	Rijksauditdienst
A. van der Waal-Sieminski MSc RA RO	TMF Nederland bv	Robeco
J. van der Hoeven RO	USG People nv	Staatsbosbeheer
B. Runia RA	Demir-Halk Bank nv	Stedin
W.J.F. van Catz CIA	Biomet Europe bv	OctoPlus nv
Drs. P. Hartog	ACS	Sociale Verzekeringsbank (SVB)

De rol van de interne auditor bij ERM als basis voor de rol bij de invoering van GRC

Wanneer de interne auditor wordt betrokken bij de invoering van governance, risk & compliance, zal hij zich een oordeel dienen te vormen over welke rol hij kan accepteren. Kan *The Role of Internal Auditing in Enterprise-wide Risk Management* (The Institute of Internal Auditors, 2004) wellicht helpen bij het maken van deze afweging? Dit artikel levert enkele bruikbare handvatten om deze vraag te beantwoorden.

Drs. E.Blom AA EMIA

De gedragscode van IIA (The Institute of Internal Auditors, 2010) vereist dat de interne auditor onafhankelijk en objectief is. Wanneer de interne auditor bij de invoering van governance, risk & compliance (GRC) een andere dan een assurancerol vervult, zou de interne auditor moeten afwegen of de noodzakelijke onafhankelijkheid en de objectiviteit hierdoor ondermijnd zou kunnen worden. Bij de invoering van enterprise risk management (ERM) dient de interne auditor eenzelfde afweging te maken tussen enerzijds de objectieve auditrol en anderzijds het inbrengen van zijn kennis en ervaring met risk management.
In dit artikel worden aan de hand van de afwegingen in *The Role of Internal Auditing in Enterprise-wide Risk Management* (The Institute of Internal Auditors, 2004) de rollen afgeleid die de interne auditor bij de invoering van GRC zou mogen vervullen.

Aandachtsgebieden bij de invoering van GRC
Om te komen tot 'een geslaagd GRC-project' onderkennen Beugelaar en Van Loon (Beugelaar RE RA, et al., 2010) negen aandachtsgebieden (zie *tabel 1*). In vergelijking met bijvoorbeeld Tarantino (Tarantino, 2008) en Frigo (Frigo, et al., 2009) hanteren Beugelaar et al. een brede benadering van de aandachtsgebieden. Daarom worden deze gehanteerd in het vervolg van dit artikel.

Rollen in een veranderingsproces
Binnen de literatuur worden in hoofdlijnen twee indelingen gebruikt voor de rollen bij een veranderproces: een indeling vanuit het oogpunt van de actoren, de deelnemers aan het veranderingsproces, en een indeling aan de hand van de gehanteerde stijl.
Een indeling op basis van actoren, onder meer op basis van het Office of Government Commerce (PMW11; Office of Government Commerce (OGC), 2006; Office of Government Commerce

1. **Strategie & missie** – Gaat nader in op elementen als aansluiting van bedrijfsdoelstellingen op de risk appetite en het algemene ambitieniveau ten aanzien van risico-integratie. Verder wordt het risicobusinessmodel hier verder vormgegeven alsook de communicatie naar de rest van de organisatie
2. **Charters** – Gaan met name om het nader structureren van functies, rollen, taken, verantwoordelijkheden en inzet van resources en andere hulpmiddelen
3. **Planning** – Behelst de wijze waarop de planning van activiteiten van ieder van de functies plaatsvindt en de mate waarin hier integratie kan plaatsvinden, dan wel een verbeterde samenwerking
4. **Risk & control self assessments** – Gaat nader in op inzet en status van RCSA's binnen de organisatie, zowel voor nieuwe producten, voor review van bestaande processen als voor incidenten
5. **Databases** (voor issues, losses en events) – Betreft met name de kwaliteit van beschikbare gegevens, toegankelijkheid van gegevens en het hebben van een stand-alone of geïntegreerde IT-oplossing
6. **IT** – Gaat nader in op de huidige IT-infrastructuur in termen van platformen, applicaties en overige IT-gerelateerde oplossingen en de gewenste IT-oplossingen, zoals de inzet van GRC-software en het laten draaien van de risico- en controlfuncties op dezelfde server waardoor uitwisseling van data gemakkelijker kan plaatsvinden
7. **Risk & control framework** – Bekijkt met name de aanwezige control frameworks, de overlap en integratie en inzet van GRC-tools
8. **Rapportages** – Betreft vooral de rapportagestructuren, kwaliteit en snelheid van rapportering en beschikbaarheid van juiste, tijdige en volledige informatie om geïnformeerd keuzen te maken en besluiten te nemen
9. **Cultuur & gedrag** – Gaat nader in op de veranderbereidheid binnen ieder van de functies, de cultuur en het gedrag ten aanzien van GRC en de wijze waarop medewerkers met hun verantwoordelijkheden omgaan

Tabel 1. Componenten voor een geslaagd GRC-project, naar Beugelaar en Van Loon, 2010

Sponsor is een senior executive van een bedrijf, verantwoordelijk voor het bereiken van het projectsucces
Voorzitter van stuurgroep is de voorzitter van het lichaam dat verantwoordelijk is voor het programma/project
Lid van stuurgroep is een deelnemer van hetzelfde lichaam
Programmamanager is de direct verantwoordelijke voor de uitvoering van een programma gericht op het realiseren van een strategisch doel. Een programma is een tijdelijk geheel van samenhangende projecten en (organisatorische) activiteiten
Projectmanager is verantwoordelijk voor het goed organiseren en regisseren van het project en communiceert met de opdrachtgever. Tevens stuurt hij het projectteam operationeel aan met betrekking tot de projectwerkzaamheden
Lid van projectteam is een deelnemer aan het project die de resultaten van het project oplevert of ervoor zorgt dat deze door derden wordt opgeleverd. Het team draagt gezamenlijk de verantwoordelijkheid voor de projectresultaten

Tabel 2. Indeling vanuit het oogpunt van de deelnemers aan het veranderingsproces, de formele rollen

Expertrol – In de expertrol verzamelt de adviseur gegevens, lokaliseert en analyseert hij problemen en formuleert hij op grond daarvan oplossingen die door het cliëntsysteem worden geïmplementeerd
Procedurele rol – Hierbij fungeert de adviseur niet alleen als inhoudelijk expert, maar tevens als organisator van het veranderingsproces
Sociaal-emotionele rol – De adviseur begeleidt organisatieleden bij het analyseren en verbeteren van intermenselijke processen en samenwerking in teams
Politieke rol – De adviseur sluit coalities en probeert steun voor het veranderingsproces te verwerven
Initiërende en faciliterende rol – De adviseur brengt mensen bij elkaar om gezamenlijk naar betekenissen in hun werk te zoeken en te experimenteren met nieuwe mogelijkheden

Tabel 3. Indeling aan de hand van de gehanteerde stijl

(OGC)) staat in *tabel 2*. En een indeling op basis van het gedrag van de adviseur, onder meer door (Brouwer, et al., 2009; Caluwé, et al., 2006; Kleijn, et al., 2010) staat in *tabel 3*.

De rol van de interne auditor bij de invoering van GRC

Wanneer de interne auditor een andere rol dan de zuivere assurancerol vervult, dus een van de rollen in tabel 2 en 3, kan de noodzakelijke onafhankelijkheid en de objectiviteit ondermijnd worden. De keuze voor de rol die hij vervult en de wijze waarop de interne auditor die rol vervult, lijkt hierdoor van groot belang om de objectiviteit te behouden. Bij (de invoering van) ERM dient de interne auditor een afweging te maken tussen enerzijds de objectieve assurancerol en anderzijds het inbrengen van zijn kennis en ervaring met risk management. Deze afweging is vergelijkbaar met die voor GRC.

In *The Role of Internal Auditing in Enterprise-wide Risk Management* stelt IIA dat de primaire rol van de interne auditor het verstrekken van objectieve assurance is. Daarnaast geeft IIA aan dat er een aantal rollen is die interne auditors kunnen vervullen wanneer er enkele maatregelen worden getroffen om objectief te blijven, de zogenaamde safeguards. Het IIARF (The Institute of Internal Auditors Research Foundation, 2011) constateert dat deze maatregelen in het algemeen betrekking hebben op het niet nemen van beslissingen en het accepteren van managementrollen. Het IIA identificeert ook enkele rollen die de interne auditor in principe niet mag uitvoeren. Het IIA maakt bij de keuze om een rol te accepteren geen onderscheid naar branche. Of een internal auditafdeling verplicht is vanuit de wet- of regelgeving, maakt voor IIA ook geen verschil in de afweging.
Het IIA deelt de mogelijke rollen bij de invoering van ERM in de volgende drie groepen in:

1. Assurancerollen – deze zijn niet conflicterend met de onafhankelijkheid en objectiviteit van de interne auditor.
2. Rollen met betrekking tot het faciliteren, het coachen, het coördineren, het consolideren van risico rapportages, het ontwikkelen en onderhouden van het ERM-framework – de ondersteuning van de ontwikkeling van ERM en de ontwikkeling van een risicomanagementstrategie ter goedkeuring van het bestuur kan de interne auditor uitvoeren, mits preventieve maatregelen getroffen worden om zijn onafhankelijkheid en objectiviteit te behouden.
3. Rollen die interne auditors niet zouden moeten accepteren – dit betreffen rollen waarbij de risk appetite (de hoeveelheid risico die een RvB acceptabel vindt) wordt bepaald, risicomanagementprocessen worden opgezet, aan het management bevestiging wordt gevraagd dat specifieke risico's worden beheerst, beslissingen worden genomen met betrekking tot risk response, de risk response wordt ingevoerd namens het management of verantwoordelijkheid wordt genomen voor risicomanagement.

Wanneer de interne auditor een andere rol dan de zuivere assurancerol vervult, kan de noodzakelijke onafhankelijkheid en de objectiviteit ondermijnd worden

Maatregelen die getroffen zouden moeten worden voor de rollen in groep 2 zijn de volgende:

- het moet duidelijk zijn dat het management verantwoordelijk is en blijft voor risicomanagement;
- de aard van de verantwoordelijkheden van de interne auditor dient te worden gedocumenteerd in de audit charter en dient

goedgekeurd te worden door het audit committee;
- de interne auditor mag geen enkel risico managen namens het management;
- de interne auditor moet advies verlenen, de besluitvorming van het management ondersteunen en uitdragen, en niet zelf risicomanagementbeslissingen nemen;
- de interne auditor kan geen objectieve zekerheid geven voor het deel van het ERM-framework waarvoor hijzelf verantwoordelijk is. Deze waarborg moet worden geleverd door een andere voldoende gekwalificeerde partij;
- alle werkzaamheden buiten de assurance-activiteiten moeten worden erkend als een consultancyopdracht en de standaarden voor een dergelijke opdracht zullen moeten worden gevolgd.

Bij GRC kan, net als bij ERM, onderscheid worden gemaakt tussen assurancerollen over GRC, consultancyrollen en rollen waarbij managementverantwoordelijkheid wordt genomen. Het verschil tussen GRC en ERM is wel dat ERM een activiteit is in de tweede lijn en dat GRC alle lines of defense omvat, dus ook de eerste en de derde lijn. Managementbeslissingen en -verantwoordelijkheden in de derde lijn zouden onderdeel moeten zijn van de 'normale' interne auditactiviteit en derhalve geen bezwaar mogen zijn voor de noodzakelijke objectiviteit en onafhankelijkheid; het nemen van managementbeslissingen en -verantwoordelijkheden ten behoeve van eerste en tweede lijnsactiviteiten is daarentegen ongewenst om ondermijning van de objectiviteit en onafhankelijkheid te voorkomen. Daarom wordt er in het vervolg van dit artikel van uitgegaan dat de assurancerol over GRC zonder inbreuk op de objectiviteit door de interne auditor kan en dient te worden uitgevoerd.

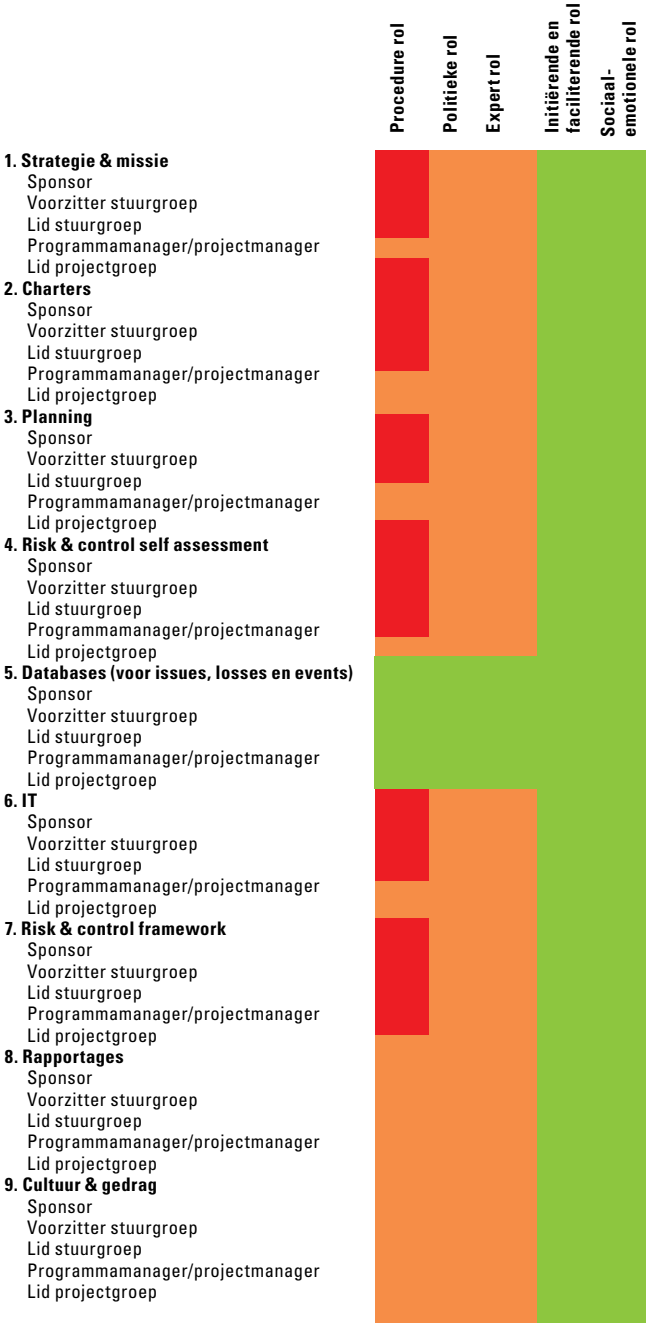
De interne auditor dient te voorkomen dat hij managementbeslissingen of -verantwoordelijkheden op zich neemt

De interne auditor kan consultancyrollen uitvoeren voor zover de beslissingen en de verantwoordelijkheden door het management worden genomen en deze activiteiten in de charter worden opgenomen en goedkeuring krijgen van het audit committee. Ten slotte dient de interne auditor te voorkomen dat hij managementbeslissingen of -verantwoordelijkheden op zich neemt, zoals het bepalen van de risk appetite of verantwoordelijkheid nemen voor de risk response bij risk & control self assessments, zodat de interne auditor objectief en onafhankelijk blijft.

Welke rol mag de interne auditor vervullen?

Zowel de formele rol als de te hanteren stijl kunnen invloed hebben op de onafhankelijkheid als de objectiviteit van de interne auditor. Daarom zullen deze in combinatie worden beschouwd om inzicht te krijgen in de mate waarin de interne auditor (management)verantwoordelijkheden accepteert en managementbeslissingen neemt in het veranderingsproces. In *tabel 4* worden hiertoe de aandachtsgebieden gecombineerd met de formele rol en de te hanteren stijl. Met groen wordt aangegeven dat deze rol/-stijlcombinatie binnen het betreffende aandachtsgebied zonder meer kan worden vervuld. De kleur oranje wordt gebruikt om aan te geven dat interne auditor de rol/stijlcombinatie kan accepteren, mits de maatregelen worden getroffen zoals beschreven bij ERM groep 2. De kleur rood wordt gebruikt om aan te geven dat een interne auditor de betreffende rol/stijlcombinatie niet zou moeten accepteren.

Bij keuze van de kleur is allereerst beoordeeld of het aandachts-



Tabel 4. Afleiding van de toegestane rollen en de te hanteren stijlen

gebied zelf managementverantwoordelijkheid vereist. Vervolgens is beoordeeld of de combinatie tussen de rol/stijl en het aandachtsgebied leidt tot managementverantwoordelijkheid. Voor de rollen is het stramien gebruikt dat de rollen sponsor en voorzitter van de stuurgroep een grote mate van managementverantwoordelijkheid voor het programma/project hebben. Dit geldt in mindere mate voor een lid van de stuurgroep, de programma- of projectmanager. Voor een lid van het projectteam wordt een beperkte verantwoordelijkheid verondersteld. Voor de stijlen is het stramien gebruikt dat de stijl procedurele rol een grote mate van managementverantwoordelijkheid voor het programma/project heeft. Dit geldt in mindere mate voor de politieke en expertrol. Voor de initiërende en faciliterende rol en de sociaal emotionele rol wordt geen managementverantwoordelijkheid verondersteld.

Op basis van tabel 2 kan worden geconcludeerd dat de rollen sponsor, voorzitter stuurgroep, lid stuurgroep en programma/-projectmanager in combinatie met de procedurele rol/stijl voor de aandachtsgebieden strategie & missie, charters, planning, risk & control self assessments, IT en risk & control framework leiden tot rol/stijlcombinaties die de interne auditor niet zou moeten vervullen. Dit wordt in belangrijke mate verklaard doordat de procedurele rol/stijl een grote mate van managementverantwoordelijkheid met zich meebrengt. Door deze te combineren met rollen die ook een grote mate van managementverantwoordelijkheid vereisen worden rol/stijlcombinaties gevormd die tot ongewenste managementverantwoordelijkheid leiden. Alleen in combinaties met aandachtsgebieden die geen of weinig managementverantwoordelijkheid vereisen – databases, rapportages en cultuur & gedrag – zouden deze rol/stijlcombinaties, met de noodzakelijke safeguards, vervuld kunnen worden door de interne auditor.
De overige combinaties kunnen door de interne auditor worden vervuld, mits voor de oranje gekleurde combinaties, maatregelen worden getroffen zoals vermeld bij groep 2 van ERM.
De rol van de interne auditor bij de invoering van GRC is in een onderzoek getoetst bij 21 bedrijven door middel van een enquête en aanvullend door interviews met drie respondenten. Het model in tabel 4 is ontwikkeld vanuit de theorie en de uitgangspunten daarvan worden onderschreven door de geïnterviewden. Daarnaast blijkt dat 9,68% van de rol/stijlcombinaties zijn geaccepteerd die zij conceptueel niet zouden willen accepteren. Het onderzoek van het IIARF komt tot een vergelijkbare conclusie: 9% van de interne auditors vervult ongewenste rollen bij de invoering van ERM. De omgeving blijkt ervoor te zorgen dat de interne auditor de ongewenste rol/stijlcombinaties in de praktijk toch accepteert.

9% van de interne auditors vervult ongewenste rollen bij de invoering van ERM

Erwin Blom is als manager Internal Audit verantwoordelijk voor Operational & IT Audit bij GlobalCollect. Dit artikel is geschreven op basis van een referaat.
Indien u geïnteresseerd bent in het onderwerp kunt u deze opvragen via ✉ erwin.blom@globalcollect.com.

Concluderend kan worden gesteld dat *The Role of Internal Auditing in Enterprise-wide Risk Management* een handreiking kan geven bij de afweging welke rol de internal auditor, vanuit onafhankelijkheidsoogpunt, kan accepteren bij de invoering van GRC. Maar hoewel IIA daarmee goede kaders aanreikt aan de internal auditor bij de keuze van de juiste rol, blijken deze kaders in de praktijk niet altijd te worden gevolgd. Dit vraagt om nadere guidance door IIA.

The governance challenge

Governance is een actueel onderwerp dat leeft in menig organisatie. Businessmanagers vragen zich steeds vaker af in hoeverre 'de governance' van hun organisatie of divisie verbetering behoeft, teneinde hun beheersing, effectiviteit en business performance te verbeteren. Maar wat is governance eigenlijk en wat zijn de samenstellende componenten hiervan? Hoe moet je als internal auditor omgaan met de governance van een organisatie? Kun je governance auditen en zo ja, waar let je dan op?

Drs. J. Gerkes RA
Drs. A. Man CIA
E. Noorloos RA, RO, AA, EMIA
Drs. H. van der Wijk RA, CIA

Op 14 juni 2012 bracht IIA Nederland een nieuwe publicatie uit, getiteld *The Governance Challenge; a first exploration for auditors*. Hierin wordt een eerste aanzet gegeven voor de beantwoording van de hiervoor genoemde vragen. Zoals de subtitel van de publicatie aangeeft, bevat het geen definitieve antwoorden, maar presenteert het wel een uitvoerige inventarisatie van onderdelen van governance, suggesties voor embedding in de organisatie en voor de rol van Internal Audit. De publicatie gaat tevens gepaard met de uitnodiging om een brede discussie te voeren over governance en hoe de internal auditor hiermee moet omgaan.

Definitie en bouwstenen van governance

Hoewel er internationaal veel geschreven is over governance, corporate governance of organisational governance, is er geen uniforme omschrijving voorhanden. Definities over wat governance is, lopen uiteen van 'a system by which companies are directed and controlled' tot 'legal and factual regulatory framework for managing and supervising a company'. Vaak zijn het containerbegrippen waarbij iedere manager of auditor een ander beeld zal hebben van wat dit concreet inhoudt.

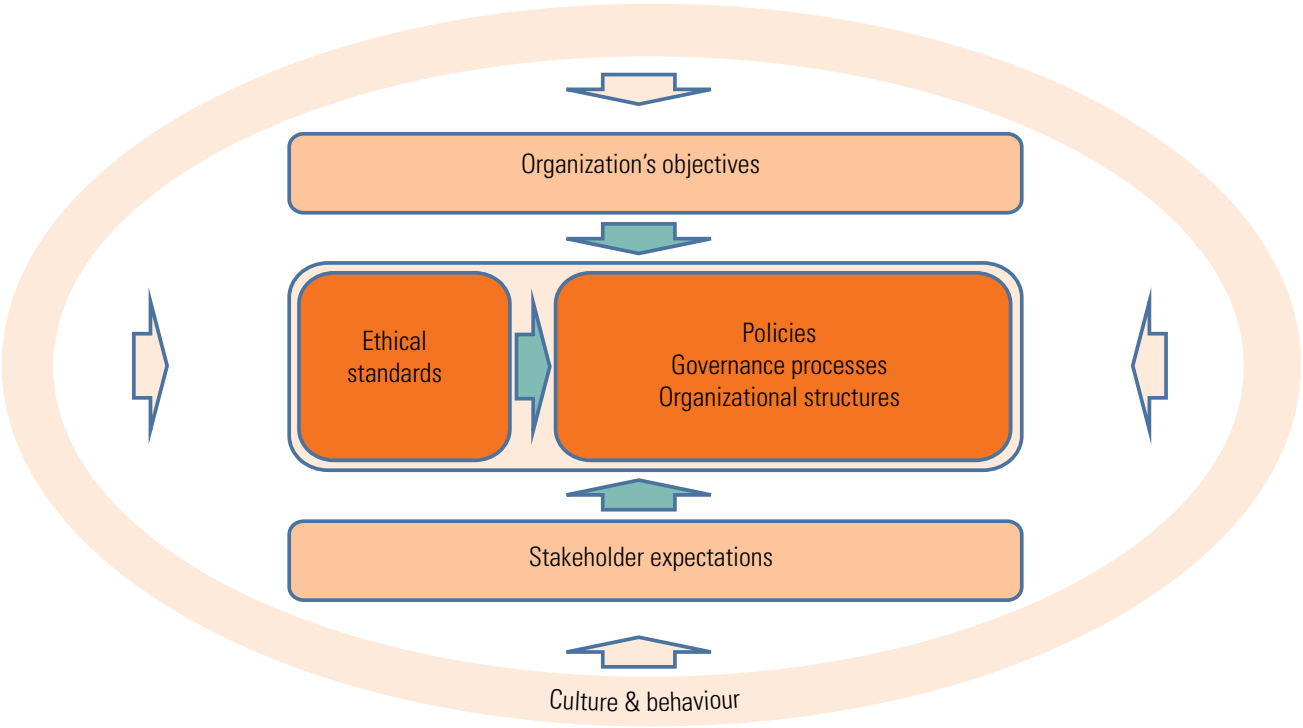
Teneinde de omschrijving en concrete invulling van governance meer te stroomlijnen geeft de publicatie een overzicht van de bouwstenen van governance. *Figuur 1* geeft een schematische weergave van de bouwstenen:

- The organisation's objectives, which provide direction to the organisation, based on its vision and strategy.
- Ethical standards, which give moral guidance to all individuals within the organisation.
- Policies, governance processes and structures, which describe the formal environment and acknowledge the informal environment of the organisation.
- Stakeholder expectations, which provide boundaries and guidance for the organisation.
- Culture and behaviour, which are more informal controls for the governance of the organisation.

De publicatie geeft vervolgens voor elke bouwsteen aan hoe deze concreet binnen een organisatie vormgegeven kan worden. Per bouwsteen zijn enkele kernvragen, voorbeelden en ontwerpprincipes gedefinieerd, alsmede enkele good practices.

De rol van de auditor

Nadat duidelijk is wat onder governance wordt verstaan en hoe dit concreet binnen een organisatie ingevuld kan worden, is de volgende vraag wat dit betekent voor de internal auditor. Kan een internal auditor een audit uitvoeren op de governance van een organisatie en zo ja welke normering gebruikt hij hiervoor? In het hoofdstuk 'How to audit' gaat de publicatie op deze vragen in. Daartoe worden voor elke bouwsteen mogelijke onderzoeksvra-



Figuur 1. Building blocks of governance in an organisation

gen geformuleerd, die de auditor begeleiden in het uitvoeren van zijn onderzoek. Het laatste hoofdstuk presenteert, zonder uitputtend te willen zijn, enkele good practices voor zowel het formaliseren als het auditen van governance.

Het vervolg

Met de publicatie wil IIA een startschot geven aan een brede discussie over het begrip governance en de rol van de internal auditor hierbij. Om deze discussie vorm te geven, wordt in het najaar een round table georganiseerd waarin verschillende belanghebbenden (naast internal auditors bijvoorbeeld risk managers, businessmanagers, bestuursleden, commissarissen) hun mening en visie kunnen geven op dit onderwerp. Op deze wijze zal de first exploration doorgroeien tot een breed gedragen en praktische uitwerking van governance, niet alleen voor internal auditors maar voor een brede groep belanghebbenden.

Inmiddels heeft IIA Nederland de publicatie in het internationale netwerk uitgestuurd. Een eerste reactie van Richard Chambers, President en CEO van IIA Global luidde: "While there is a Dutch perspective embedded in the paper, it does provide a lot of valuable food for thought. I believe it will join the ranks of strong thought/leadership/guidance formulated by other institutes around the world over the years on timely and relevant topics for our profession."

"The Internal Audit activity must assess and make appropriate recommendations for improving the governance process (…)"

Standard 2110 and the related practice advisory 2110-3 on Governance, International Professional Practices Framework (IPPF) – The Institute of Internal Auditors

Jaap Gerkes, Arjan Man, Erick Noorloos en Heiko van der Wijk zijn allen lid van IIA en vormen een werkgroep onder auspiciën van de commissie Vaktechniek van IIA. Jaap Gerkes is werkzaam bij Protiviti, Arjan Man bij PwC, Erick Noorloos bij KPN en Heiko van der Wijk bij KLM. Zij zijn in hun dagelijkse werkzaamheden vanuit verschillende invalshoeken bezig met het concretiseren en toepasbaar maken van (het auditen van) governance.

GRC en audit: organisatorisch strak scheiden of toch combineren? De meningen hierover verschillen. Marieke van de Putte, directeur GRC & Audit, vertelt over haar ervaringen om GRC en audit bij Holland Casino onder een dak te brengen.

GRC en audit bij Holland Casino:

de kracht van de combinatie

Drs. M.K. van de Putte RC

Vijftien jaar lang heb ik advies gegeven op het gebied van risicomanagement in combinatie met het uitvoeren van operational audits. Holland Casino bood mij in 2011 de kans beide aspecten te combineren in de nieuwe functie van directeur GRC & Audit. Deze functie gaf mij de mogelijkheid om de samenhang tussen governance, risk management, compliance en audit te schetsen, qua beheersingssystemen volledig te integreren, alles van 'A tot Z' te ontwerpen en te implementeren en de rol van audit daarin stevig neer te zetten. Ik ben deze uitdaging met veel plezier aangegaan. Holland Casino, met 4231 medewerkers, is in meerdere opzichten een bijzonder bedrijf en interessant voor mijn vakgebied. Er is een grote omloop van (ongeteld) geld. Het is een staatsdeelneming waar herordening van de markt en eventueel privatisering voor de deur staan. Het is een stichting met winstoogmerk, maar heeft daarentegen ook een hele belangrijke rol om gokverslaving tegen te gaan. Holland Casino staat onder toezicht van de ministeries van Veiligheid & Justitie en Financiën en De Nederlandsche Bank en moet als staatsdeelneming voldoen aan de Corporate Governance Code.

Inrichting van de GRC-functie

Bij de inrichting van de GRC-functie hebben wij ervoor gekozen om de auditfunctie zelfstandigheid te geven. Ik ben verantwoordelijk voor de organisatorische aansturing van de gehele GRC-functie, inclusief het functioneren van de medewerkers van Audit. De auditmanager rapporteert direct aan het bestuur en het audit committee zonder mijn inhoudelijke betrokkenheid. De gemeenschappelijke basis vormt het COSO Framework. Audit sluit zich volledig aan bij het (door het GRC-deel) opgestelde risicoprofiel vanuit het idee van risk based auditing.

> Onze afspraken hebben geleid tot een duidelijke scheiding in de advies- en auditwerkzaamheden

Het COSO Framework is een conceptueel kader wat praktisch nader moet worden ingevuld. Wij hebben COSO vorm gegeven in het business control framework. Hierin staat beschreven wat een organisatie zou moeten hebben – van code of conduct tot een goede planning- en controlcyclus. Dit is het uitgangspunt van onze GRC- en auditactiviteiten, omdat dit framework als een kapstok fungeert voor al het beleid en alle procedures. Het blijkt daarnaast een goed middel om gaps ten opzichte van de soll-situatie op te sporen en deze stapsgewijs op te lossen.
Holland Casino is een echte 'doe'-organisatie. Daarom heb ik het eerste jaar met name gekozen voor het oppakken van de gaps, zonder nog het totaalbeeld van het business control framework te schetsen. Een mooie uitdaging was ook het zelf invullen van de governance- en compliancecomponenten met behulp van veel best practices. Zo hebben het Akzo-jaarverslag en het conceptrapport van Integrated Reporting mij erg geholpen in de herziening van de structuur van het jaarverslag, inclusief de risicoparagraaf. Mijn adviesrol daarin werd goed gecombineerd met het opnemen van de door Audit getoetste cijfers in het directieverslag.

Invulling van three lines of defense
Hoe ziet de praktische invulling van de eerste, tweede en derde lijn er nu uit in de praktijk? Hoe is mijn rol ten aanzien van governance en compliance, die organisatorisch niet in mijn afdeling belegd zijn en respectievelijk vallen onder de bestuurssecretaris en de compliance officer? Waar zitten potentiële conflicten en hoe lossen we die op? De oplossing ligt, voor de hand liggend maar waar, in de dialoog en het gezamenlijk oppakken van de werkzaamheden. Het mooie van de combinatie is niet alleen het monitoren of iets werkt, maar ook het kunnen meewerken aan een betere en professionelere organisatie.
Voor mij stond vanaf het begin als een paal boven water dat we de onafhankelijkheid van het auditdeel op mijn afdeling continu moeten bewaken. We hebben duidelijke afspraken gemaakt over deze samenwerking. Volgend jaar staat een audit op het GRC-deel op het programma, waar ik graag aan meewerk.
We merken in de praktijk dat onze afspraken hebben geleid tot een duidelijke scheiding in de advies- en auditwerkzaamheden. De kracht van de combinatie is het continu afstemmen hoe we vanuit de verschillende rollen de organisatie verder kunnen brengen.
Maar ik ben nog niet klaar zodra er een goed business control framework staat en de tweede en derde lijn goed functioneren. In mijn ogen draait alles om ieders rol in waardecreatie van de onderneming. We zetten bijvoorbeeld nu de eerste stappen in de volledige integratie van risicomanagement en performancemanagement in de sturing van de organisatie en de rol van audit daarin.

Marieke van de Putte (1971) is werkzaam bij Holland Casino als directeur GRC & Audit. Hiervoor werkte zij bij PricewaterhouseCoopers en Arthur Andersen. Zij is tevens secretaris van het bestuur van de Vereniging van Registercontrollers.
✉ mvandeputte@holland-casino.nl

Samenwerken wint aan kracht en effectiviteit als je je empathiefactor ontwikkelt. Je richt je dan behalve op de inhoud van de audit ook op de relatie met de klant zelf. Wat leeft in deze persoon en wat in jou en hoe kun je win-win bereiken? Vijf tips voor een verbindende samenwerking.

De empathiefactor in de auditpraktijk

Drs. T.M. Gommans RO
Drs. N. van Ladesteijn

Samenwerken en het voeren van gesprekken doen we elke dag, met collega-auditors, klanten, auditees, opdrachtgevers, managers, et cetera. Binnen de organisatiecontext gaan deze gesprekken meestal over de inhoud: het onderwerp van de audit, de aanpak, de werkwijze, de planning. De laag eronder, de gevoelens en behoeften van onszelf en de ander, laten we meestal buiten beschouwing. Opzijgeschoven als niet ter zake doende. Terwijl het bij 'verbindende' samenwerking juist gaat om de relatie, contact maken en de mens zien achter het auditrapport.

Achterste van de tong

Wat is nu eigenlijk een relatie en contact maken en wat kan je ermee als auditor? Veenbaas (1994) geeft aan dat als je contact maakt, je dat in eerste instantie doet met je intuïtie. Intuïtie is het geheel van ervaringen en gevoelens dat we gebruiken om te bepalen hoe we in de relatie staan. Rosenberg (2011) voegt hieraan toe dat die gevoelens verwijzen naar onze behoeften (of deze wel of niet vervuld zijn) en dat al ons gedrag een manier is om deze behoeften te vervullen. Dit gebeurt vaak onbewust. Zo maak je onbewust de keuze: laat ik wel of niet het achterste van mijn tong zien.

Wil je meer grip krijgen op je keuzeproces? Verlang je naar een effectieve manier van samenwerking waarbij win-win de uitkomst is? En wil je weten hoe je daarop kunt sturen? Hierna volgt een aantal tips hoe je hieraan kunt werken.

1 Verbinden vóór denken en doen

Voordat je aan de slag gaat met de audit zelf is de eerste stap te werken aan de relatie met de klant en/of opdrachtgever.

Organisatieadviseur Marie Miyashiro en schrijver van *The Empathy Factor* noemt dit het toevoegen van de 'derde dimensie' aan 'denken en doen'.

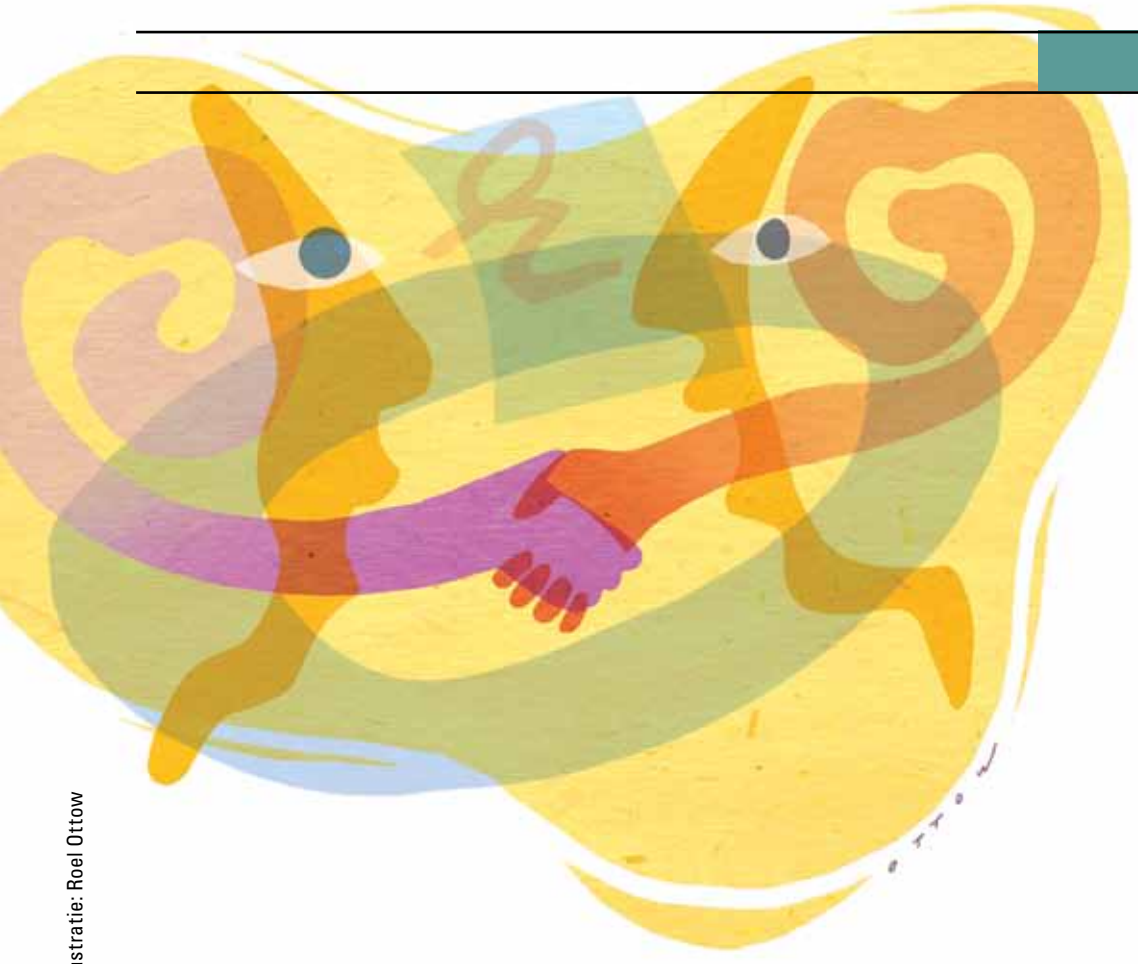
Eerst verbinden voordat we een probleem signaleren en een oplossing bedenken (denken) en deze uitvoeren (doen). Bij verbinden gaat het om de vaardigheid je te verplaatsen in de gevoelens en behoeften van anderen en je in het gesprek hierop te richten. Miyashiro noemt dit het ontwikkelen van je empathiefactor.

Bij 'verbinden' gaat het in de gesprekken met de opdrachtgever en auditee over de inhoud: wat is de onderzoeksvraag en wat is de aanpak? Je zoekt op inhoudsniveau verbinding. En je maakt verbinding op mensniveau, waarbij het gaat over gevoelens, waarden en behoeften, over de mens achter de inhoud. Zo'n gesprek gaat bijvoorbeeld over de frustratie van de auditee over de hoeveelheid werk die een audit kost en over de angst afgerekend te worden op het rapport, ondanks goede intenties. Of het gaat over de bezorgdheid van de auditor een fundamentele bijdrage te kunnen leveren aan de organisatie en de angst dat het rapport in de bureaula verdwijnt.

Dus besteed naast de audit zelf expliciet aandacht aan de onderlaag met vragen als: Ben je bang voor…? Wil je kunnen vertrouwen dat…? Ben je bezorgd dat...? Heb je behoefte aan…?

2 Snoeien in je communicatie

Om een volle emmer nog meer te kunnen vullen moet er eerst wat uit. Zo gaat dat ook met mensen als ze ergens vol van zijn. De emoties (blij, bedroefd, boos, bang) lopen soms zo hoog op dat je niet meer kunt luisteren naar de ander. Bij samenwerken is



Illustratie: Roel Ottow

het van belang naar de gevoelens van je gesprekspartner te kunnen luisteren zodat er weer ruimte ontstaat voor de ander.
Stel, je hebt een gesprek met de directeur van de divisie waar je een audit hebt uitgevoerd. Het conceptrapport wordt besproken. Je merkt het al meteen bij binnenkomst, 'de spanning hangt in de lucht'. De ontvangst is kort en afgemeten, je krijgt dit keer geen koffie aangeboden en de controller zit ook bij het gesprek. Je gesprekspartner valt meteen maar met de deur in huis: 'Ik heb nog nooit zo'n waardeloos rapport gelezen!' Daar zit je dan en wat doe je dan? De verleiding is groot over te gaan tot zelfverdediging of de tegenaanval. Immers, je bent ervan overtuigd dat je je werk wel goed hebt gedaan en dat nu eens gezegd moest worden hoe het er werkelijk aan toe gaat. De meest gebruikelijke manieren om dan te reageren zijn:

- *Corrigeren/beleren*: 'Ik denk dat u het niet helemaal heeft begrepen, in de bijlage staat helemaal uitgeschreven hoe wij aan onze bevindingen zijn gekomen en....'
- *Ondervragen*: 'Kunt u precies aangegeven waar u het niet mee eens bent en wat er dan staat dat niet goed is?'
- *Overtreffen*: 'Het valt nog best mee, er gaan ook wel dingen goed.'
- *Terugtrekken/uitleggen*: 'Ik had ook eigenlijk eerst mondeling nog wat punten met u af willen stemmen, alleen was daar geen tijd voor en.....'

Grote kans dat de haren van je gesprekspartner overeind gaan staan en hij zich terugtrekt in zijn eigen loopgraaf. Daarom is onze tip te snoeien in die vormen van communicatie. Bedenk dat dit niets over jou persoonlijk en het rapport zelf zegt, maar over wat het oproept bij de ander. Verder geldt dat jij niet verantwoordelijk bent voor de gevoelens van de ander en de wijze waarop iemand zich uit. Haal even diep adem en tel tot tien. Geef jezelf in stilte erkenning wat het met jou doet, zodat jij ook weer ruimte krijgt in je hoofd. Dit is nog niet het moment om erkenning van de ander te vragen.

3 De ander horen

Wat kun je dan wel doen om je punt te maken? De sleutel is eerst empatisch te luisteren naar wat de gesprekspartner, in dit geval de directeur, daadwerkelijk heeft te vertellen. Met luisteren bedoelen we dan: horen wat bij iemand speelt, verbinden met wat er leeft/is bij de ander, proberen met volle aandacht bij diegene te zijn zodat de ander de ruimte krijgt te vertellen wat er leeft. Want wat zit er achter de woorden: 'Dit rapport is waardeloos'? Zo blijkt het er regelmatig niet om te gaan of iets klopt, maar om wat het rapport teweeg kan brengen in de organisatie. Luister als auditor dan naar iemands gevoelens en (on)vervulde behoeften. Je kunt bijvoorbeeld vragen: 'Bent u geschrokken van wat er in het rapport staat omdat u graag meer erkenning wilt waaraan het team allemaal wel bijdraagt?' Zorg tijdens het gesprek voor stiltes. Stiltes geven de gelegenheid om na te denken, te voelen wat is en te reageren.

4 Emoties benutten

We krijgen nogal eens terug dat mensen oordelen hebben over het praten over gevoelens op het werk: 'Kost veel te veel tijd', 'Is voor softies', en: 'Doe dat maar thuis'. Tegelijkertijd: wat bereik je als je – dat wat is (frustratie, teleurstelling) – onbespreekbaar laat? Vroeg of laat komt het probleem toch boven tafel of leidt het tot spanningen in de relatie, met alle gevolgen van dien. Een schat aan informatie blijft liggen: weten wat er speelt bij jezelf en de ander geeft namelijk inzicht in de situatie en helpt de audit zo af te ronden dat de audit daadwerkelijk toegevoegde waarde levert aan de organisatie.
Emoties (ook wel 'onderbuik' of 'intuïtie' genoemd) zijn een waardevolle graadmeter welke behoeften wel of niet vervuld zijn en leveren de energie op die nodig is om deze behoeften te vervullen. Het zichtbare resultaat is het gedrag. Het gedrag benoemen en woorden geven aan het onderbuikgevoel of intuïtie helpt jezelf en de ander om wat speelt bespreekbaar te maken en gedrag te veranderen. De manier om gedrag te veranderen is emoties te benutten en ze te benoemen.

Stel, in het hiervoor genoemde voorbeeld probeert de directeur zijn emoties te beheersen (ofwel negeren/onderdrukken) en hij gaat het rapport bespreken. De hete aardappel blijft liggen. Je kunt dit doorbreken door het gesprek aan te gaan over wat er leeft bij de directeur. Het gedrag van de directeur, boos, kan zo omslaan in gezamenlijk toewerken naar een audit met aanbevelingen die daadwerkelijk opgepakt worden.

In onze maatschappij leren we weinig om woorden te geven aan gevoelens en behoeften

Overigens kun je ook emoties benutten als het goed gaat en de resultaten van de audit positief zijn. Zeg bijvoorbeeld eens: 'Bent u trots op uw team dat ze zich zo inzetten om de klanten aan de balie optimaal te bedienen?' Dit levert vaak hele leuke reacties op!

5 Synergie creëren

Als je met inleving hebt geluisterd (waarbij gevoelens en behoeften helder zijn geworden), weet je wat bij de ander speelt. Minstens zo belangrijk is dat je ook luistert naar jezelf. Wat is belangrijk voor jou? Als auditor heb je je eigen professionaliteit en is erkenning hiervan waarschijnlijk belangrijk. Je hebt rondgelopen binnen de divisie en bent op basis van gedegen onderzoek tot de conclusies gekomen. De vraag die je jezelf stelt is wat je behoeften zijn achter je gevoelens. Zo wil je wellicht risico's zichtbaar maken die de organisatie loopt en respect en erkenning voor het werk dat je geleverd hebt.
En als jouw behoeften en die van de ander helder zijn, ga je zoeken naar hoe je het kunt oplossen. Waar zit de win-win voor beiden? Vaak zijn er veel meer oplossingen dan in eerste instantie gedacht. Vraag de directeur hoe hij het opgelost wil zien. Wat moet wel en niet schriftelijk gerapporteerd worden? Moet jij rapporteren of kunnen jullie bijvoorbeeld gezamenlijk het rapport opstellen voor de raad van bestuur. Hoe kun je ervoor zorgen dat de punten die jij gesignaleerd hebt worden meegenomen en de directeur de ruimte krijgt zijn eigen verhaal en oplossingen in te brengen? Dit is het moment om te zoeken naar het gezamenlijke belang en de synergie. En niets is zo prettig als iets doen waar je zelf achter kunt staan.
Een voorbeeld uit de praktijk is dat bij een audit de auditee gelijk met het auditrapport een verbeterplan presenteerde. Hiermee kon hij aan de directie laten zien dat hij de uitkomsten van het rapport serieus nam en echt bereid was de verbeterpunten op te pakken. Vervolgens gaf de directie bij de presentatie meteen de opdracht aan de auditor na drie maanden te beoordelen hoe het ervoor stond. Winst voor iedereen!

Pionieren: gewoon doen!

De manier om uit te vinden of iets werkt is het in de praktijk te gaan doen. De afgelopen jaren zijn wij zelf ook zo aan de slag gegaan. We hebben eerst tijdens een training geleerd hoe je gevoelens en behoeften (h)erkent en er woorden aan geeft. Daarna brachten we het geleerde in de praktijk. Wat een energie geeft het als het je lukt je empathiefactor in te zetten! Het heeft ons best wat maanden gekost. Bij het je eigen maken helpt het als je criticaster even op de gang blijft staan. Geef ruimte aan je eigen gevoelens en behoeften in zo'n geval en zet je empathiefactor in voor jezelf.
Ten slotte, in onze maatschappij leren we weinig om woorden te geven aan gevoelens en behoeften. Het vraagt oefening je gevoelens te kunnen herkennen en te benoemen en de onderliggende behoeften te achterhalen. Hiervoor zijn gelukkig op internet diverse sites te vinden die een overzicht geven van gevoelens en behoeften. In de literatuurlijst staan boekverwijzingen. En ook bij dit verwoorden geldt: oefening baart kunst!

Literatuur

- Miyashiro, M.R., *The Empathy Factor - Your competitive advantage for personal, team and business succes*, PuddleDancer Press, 2011, Nederlandse vertaling, zomer 2012.
- Rosenberg, M.B., *Geweldloze communicatie – Ontwapenend, doeltreffend en verbindend*, Lemniscaat, 2011.
- Brink, J.W. van den en M. van Os, *Opdrachtgever gezocht*, Academic Service, 2010.
- Veenbaas, W. en P. Weisfelt, *Hoe raak ik je aan?*, Phoenixopleidingen, 1994.

Theresia Gommans (l) is sinds 2010 zelfstandig organisatieadviseur op het gebied van auditing, bedrijfsvoering en verandermanagement. Hiervoor was zij onder andere auditmanager bij de interne auditdienst van de gemeente Rotterdam.
www.theresiagommans.com

Nicole van Ladesteijn is communicatietrainer en eigenaar van CommunicatieWijs. Zij is gespecialiseerd in verbindende communicatie en begeleidt mensen en organisaties bij een meer effectieve communicatie en samenwerking.
www.communicatiewijs.nl

Internal auditors luisteren niet[1]

A. Molenkamp RO

A. Molenkamp RO

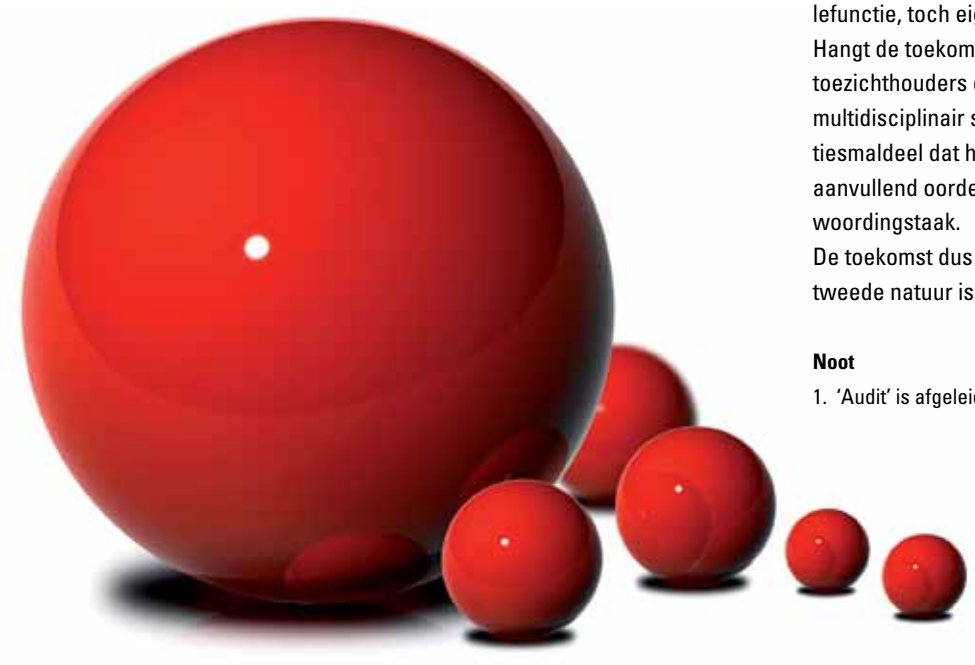
Toezichthouders en bestuurders maken, als paarlen voor de zwijnen, onophoudelijk duidelijk welke verwachtingen men van Internal Audit heeft. Voorbeelden te over: "Liever fit for purpose dan fully in control" (Lock), "De aandacht voor interne beheersing mag niet verslappen" (Koster), "Welk probleem wil men eigenlijk oplossen door een rijksauditdienst in het leven te roepen?" (Jacques Wallage), "Naast de excellente accountantsafdeling beschik ik over twee organisatiemedewerkers die me echt vertellen wat er speelt" (CFO multinational), "De externe accountant moet wegblijven bij de internal auditor" (Dieleman), "Internal Audit is voor een commissaris een belangrijke steunpilaar en informatiekanaal" (Holsboer), "Rol, taak en verantwoordelijkheid van een IAF is maatwerk" (Pheiffer), "Laat je regelzucht los auditor en besef dat je de doerak van de organisatie bent" (Streppel), "De internal auditfunctie gedraagt zich als een verlengstuk van de externe accountant" (Rekenkamer Rotterdam).
Het heeft er alle schijn van dat auditors in groepsverband, bijvoorbeeld tijdens seminars en binnen centrale auditafdelingen, deze signalen niet kunnen of willen opvangen en vooral onderling communiceren over hoe verschillend men elkaar toch ervaart.

"Operational audits waardevoller dan cijfercontrole" (Smits)
Dat was de betekenisvolle uitspraak van Hans Smits, CEO van het Havenbedrijf, tijdens een seminar over publieke verantwoording (juni 2012). De bij dat seminar in grote getale aanwezige overheidsauditors gingen na het vertrek van Smits spoorslags over tot de orde van de dag. Het voortzetten dus van de uit de vorige eeuw stammende strijd over het verschil tussen Financial en Internal Audit. En natuurlijk de domeindiscussie tussen externe controle-instanties zoals de Algemene Rekenkamer, de externe accountant en het ministerie van Financiën.

"Internal Audit is een wezenlijk onderdeel van de checks en balances binnen mijn departement" (Demmink)
De secretaris-generaal van een departement maakte tijdens het congres over verantwoording (september 2011) duidelijk dat de departementsleiding daartoe dankbaar gebruikmaakt van een aantal interne feedbackfuncties. Het aanwezige auditpotentieel liet zich daardoor niet van de (eigen)wijs brengen; het ministerie van Financiën gaat onverdroten voort met haar pogingen, al sedert 2008, tot het inrichten van een megacentrale auditdienst.

86% van de commissarissen vindt dat regionale banken moeten beschikken over een intern audit charter
Uit een enquête (juni 2012) onder deze commissarissen blijkt dat de internal auditfunctie cruciaal is voor het kunnen uitoefenen van haar taak. De auditors van de centrale auditdienst zijn kennelijk doof voor dit geluid en acteren alsof deze functie exclusief door hen wordt uitgeoefend. Dit dus in schril contrast met de enquêteresultaten waaruit blijkt dat deze centrale auditfunctie als (zeer gewaardeerde) externe accountant wordt geafficheerd.

De toekomst aan de managementkundige auditor?
Het heeft er alle schijn van dat de overwegend financieel geschoolde auditors van de grote centrale auditafdelingen weliswaar vanuit een machtige positie opereren, maar desondanks niet geheel beantwoorden aan het door toezichthouders en bestuurders geschetste profiel. Bestuurders hebben naast de noodzaak tot *controle*, behoefte aan feedback over *control*. In de praktijk blijkt dan ook dat bestuurders, in weerwil van een centrale controlefunctie, toch eigen auditgroepjes instellen.
Hangt de toekomst van de auditprofessie dan toch af van de door toezichthouders en bestuurders gewenste, op maat gesneden, multidisciplinair samengestelde Small Audit Shop? Een organisatiesmaldeel dat het resultaatverantwoordelijke management met aanvullend oordeel en advies bijstaat in haar sturende en verantwoordingstaak.
De toekomst dus aan de SAS-auditor voor wie luisteren *wel* een tweede natuur is…



Noot

1. 'Audit' is afgeleid van het Latijnse adire, dat luisteren betekent.

www.pwc.nl

Een transparant auditproces

Internal Audit Matters

Petra de Groot
Adviseur Internal Audit

pwc

Het audit management systeem dat ik bij mijn klant heb geïmplementeerd, helpt bij het plannen en uitvoeren van de audits. Doordat alle gegevens overzichtelijk worden samengebracht, kan de internal audit afdeling gemakkelijker en beter werken.

Met zo'n transparant systeem kan mijn klant dus echt aan de slag.

Wil je meer weten over onze dienstverlening, kijk dan op www.pwc.com/nl/ias of neem contact met mij op via +31 (0)88 792 6983.

IIA-YP en ESAA event: oordeels(ver)vorming, auditor ken uzelf!

Het is maandagmiddag 25 juni 2012 als IIA Young Professionals en de Erasmus School of Accounting & Assurance gezamenlijk de bijeenkomst 'Oordeels (ver)vorming: auditor ken uzelf!' organiseren. Kan het zo zijn dat de oordeelsvorming van deze groep professionals feilbaar en aan vervorming onderhevig is?

E.A.P. Mol MSc

De sprekers Edwin Hummel en Lucienne Saraber deden in 2009 onderzoek naar de beïnvloeding van psychologische aspecten op het oordeel van de auditor. Aanleiding voor dit onderzoek was dat tunnelvisie bij professionals in bijvoorbeeld de rechtspraak aan het licht kwam, maar dat er maar weinig psychologisch ingestoken onderzoek was gedaan binnen de beroepsgroep van internal auditors. De verwachtingen vanuit de beroepsregels, met woorden als onbevooroordeeld en objectief, lijken niet overeen te komen met wat bekend is over de oordeelsvorming in het menselijk brein.

Hoe werkt ons brein?
Er is veel onderzoek gedaan naar de werking van ons brein en onderzoekers komen veelal uit op een onderverdeling tussen een intuïtief en analytisch systeem. Het intuïtieve systeem kan snel schakelen, werkt onbewust en oordeelt aan de hand van associaties. Het analytische systeem is daarentegen in staat om bewust, expliciet, gecontroleerd maar wel langzamer, tot een op regels gebaseerd oordeel te komen. Opvallend is dat experts zoals ervaren auditors ongeveer 80% van hun beslissingen nemen op basis van het intuïtieve systeem. Maar dit systeem kent belangrijke denkfouten die niet altijd gecorrigeerd worden door het analytische systeem.

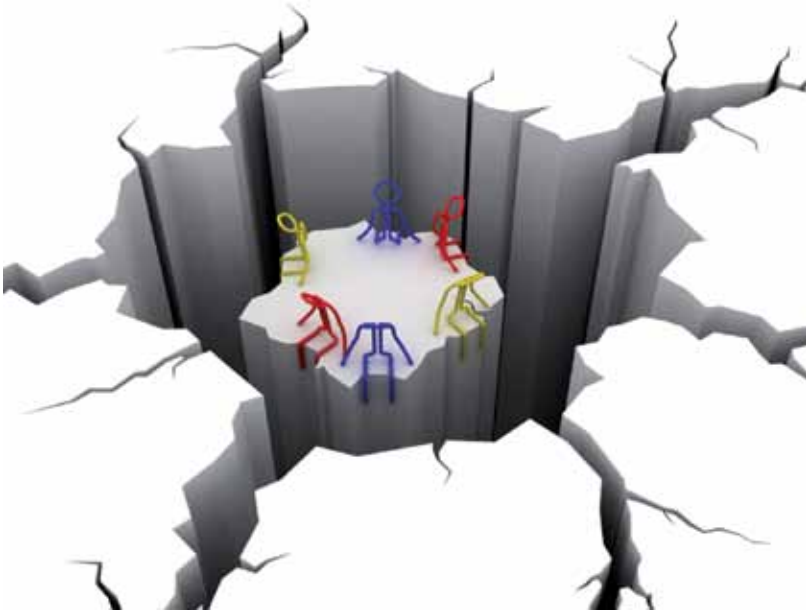
Mogelijke valkuilen bij een audit
We bekijken een viertal bekende systematische denkfouten en de invloed daarvan op het uitvoeren van audits.

Eerste indruk
Het onderzoek toont aan dat (de eerste) indruk van de auditee de oordeelsvorming van auditors beïnvloedt. Auditors die te maken hadden met een onzekere of slordige auditee beoordeelden hetzelfde object van onderzoek een stuk minder goed dan auditors die te maken hadden met een zekere of geordende auditee.

Tunnelvisie
Een gebrek aan tijd kan leiden tot aandachtsvernauwing waardoor bepaalde onderdelen minder aandacht krijgen. Ook is het menselijk brein geneigd om te zoeken naar informatie die een eerder vermoeden bevestigt. Dit maakt het uitstellen van oordeelsvorming van groot belang.

Volgordelijkheid
De volgorde waarop informatie tot ons komt heeft een effect op de oordeelsvorming. Het blijkt dat informatie die in het begin of juist aan het eind van het onderzoek tot ons komt van grotere invloed is. Interessant is dat een ervaren auditor minder gevoelig is voor deze valkuil.

Invloed van anderen
Er zijn tal van voordelen van het werken in een groep maar anderen beïnvloeden de oordeelsvorming van een auditor. De neiging tot conformiteit in een groep, de weging van de mening van anderen en ook gemakzucht, maken dat de auditor tot een ander oordeel kan komen.



De sprekers op de bijeenkomst: Edwin Hummel (l) en Lucienne Saraber.

Oplossingsrichtingen

Deze valkuilen zijn onder meer te voorkomen door te werken in gemêleerde groepen en tijd te nemen om bewust over een oordeel na te denken. Het is ook goed om regelmatig van auditobject te wisselen om zo met een frisse blik naar een proces te kunnen kijken. Organiseer tegenspraak binnen en buiten het auditteam. Dat leidt tot bewustwording met betrekking tot het maken van keuzen, en vragen van een relatieve buitenstaander leggen bepaalde valkuilen bloot.

Conclusie

Internal auditors zijn mensen en moeten zich bewust zijn van systematische denkfouten en de invloed van psychologische factoren op hun oordeelsvorming. Stel je als auditor daarom open voor andere mogelijkheden en ga op zoek naar tegenbewijs. Manage verwachtingen door eerlijk te zijn over je beperkingen en leer je eigen valkuilen kennen en herkennen.

Erwin Mol is adviseur bij KPMG binnen de afdeling Internal Audit, Risk and Compliance Services. Hij adviseert klanten op het gebied van Internal Audit, risicomanagement en internal control.

Ton Amende (54), internal auditor bij Yarden, heeft een bijzondere loopbaan binnen de uitvaartbranche. Na 32 jaar gewerkt te hebben in diverse functies in de boekhouding, de business en de IT, is Ton sinds zes maanden werkzaam als internal auditor. Bevestigt deze overstap de trend naar 'internal audit nieuwe stijl'; de ontwikkeling dat meer mensen uit de operatie actief worden binnen de internal auditfunctie? We vroegen het Ton.

Drs. J.A. Man CIA
Drs. L. Eggermont RA

Wie ben je en waarom zit je hier?
"Ik werkte als hoofd Algemene Zaken en als operationeel manager in diverse kleinere bedrijfsonderdelen bij Yarden. Na de laatste grote fusie, zo'n zes jaar geleden, werkte ik als regiomanager in de buurt van Zwolle. Bij de regioclustering vorig jaar zijn regio's gecombineerd. Daarom is voor een aantal regiomanagers, waaronder ik, op basis van competenties beoordeeld wat een goede vervolgstap zou kunnen zijn. De internal auditorpositie binnen Yarden was op dat moment net vrijgekomen, omdat mijn voorganger met pensioen was gegaan. Yarden hecht er bijzondere waarde aan om mensen en kennis binnen de organisatie te houden. Ik ben daarom specifiek gevraagd voor deze functie vanwege mijn kennis van de processen en de mensen. Zo ben ik op deze plek terechtgekomen."

Hoe reageerde je omgeving op je overstap?
"Iedereen reageerde heel positief, ze vinden me er geknipt voor. Vooral oud-collega's vinden dat." Op onze vraag of hij dan ook een tikkeltje eigenwijs is, volgt een bevestigende glimlach...

Wat vind je leuk aan dit beroep? Wat is je het meest opgevallen als internal auditor ten opzichte van je vorige functies?
"Ik zit nu op een plek waar ik de organisatie echt vooruit kan helpen, dat is ook mijn grootste drijfveer. Wat mij een heel warm gevoel geeft is dat mensen me zelfs uitnodigen, ik ben altijd welkom. De openheid valt me op. Dat komt, denk ik, omdat mensen weten wie ik ben. Het helpt dat je operationeel ervaren bent."

Wat kenmerkt jou als auditor en op welke manier probeer je de organisatie verder te helpen?
"Ik ben geen politieagent, maar wel iemand die zich houdt aan de regels en die integriteit hoog in het vaandel heeft. Mensen waarderen mij vanwege mijn kennis en ik kan uitleggen waarom iets moet veranderen. Juist ter zake kundig zijn is belangrijk bij de acceptatie van kritische bevindingen. Omdat ik de operationele kennis bezit, is het ook gemakkelijk om het over te dragen."

Maar je vroegere betrokkenheid bij de operationele gang van zaken kan ook je onafhankelijkheid beïnvloeden. Hoe ga je hiermee om?
"Succesvol zijn in het bewaren van afstand ligt in mijn persoonlijkheid. Ik ben eigenwijs en integer handelen staat voor mij altijd voorop. Tijdens mijn sollicitatie hebben de directie en ik dit uitgebreid besproken, want het niet onafhankelijk (kunnen) functioneren werd natuurlijk wel gezien als een potentieel risico."

Wat vind je van de IA-wereld? Wat is lastig?
"Ik werk alleen, onder directe aansturing van de CEO, ik mis dus wel eens sparringpartners binnen de organisatie. Ik heb contact gezocht met internal auditors in de branche. Dit contact is tot nu toe positief geweest. Ook ben ik lid geworden van IIA en ben ik van plan om relevante bijeenkomsten bij te wonen. Daarnaast ga ik een opleiding voor internal auditing volgen. In eerste instantie leek de internal auditwereld een vrij besloten club. Een van de redenen daarvoor is dat IIA zich met name op haar leden lijkt te richten, veel materiaal op de website is bijvoorbeeld alleen voor leden toegankelijk. Maar in de praktijk valt dat mee."

Heb je nog een opdracht meegekregen van de directie en het audit committee?
"Houd het effectief en de communicatie eenvoudig."

Tot slot de clichés: je betaalt met een uitvaartverzekering zestien keer je uitvaart, koffie en cake is het meest populair…
"Alleen de koffie en cake is waar. Al het andere is een misvatting."

Drs. Peter Grootendorst RO (1958) is werkzaam bij het ministerie van Defensie in de rang van brigadegeneraal bij het roemruchte Korps Mariniers. Zijn huidige functie is controller bij de Commandant der Strijdkrachten (CDS). De eerste twintig jaar van zijn militaire loopbaan vervulde Grootendorst diverse lijn- en staffuncties bij het Korps Mariniers. Daarna is hij (naar eigen zeggen) per abuis in het vakgebied Control & Audit terecht gekomen, waar hij nu alweer dertien jaar in diverse functies actief is. Grootendorst studeerde bedrijfskunde en volgde zowel de post-hbo-opleiding Operational Auditing (Haagse Hogeschool) als de RO-opleiding (Erasmus Universiteit).

Brigadegeneraal Peter Grootendorst

over auditing binnen Defensie

A. Molenkamp RO
N. Arif RO EMIA

Kunt u een korte schets geven van internal auditing binnen Defensie in de laatste vijftien jaar?

Verbijzonderde interne controle en accountantscontrole

"Internal Audit binnen Defensie vertoont een grote overeenkomst met de rijksbrede ontwikkelingen en we voeren dezelfde discussies als bij de beroepsverenigingen. Ongeveer vijftien jaar geleden beschikte Defensie nog over een omvangrijke certificerende Accountantsdienst (DEFAC). Deze dienst hield zich voornamelijk bezig met de uitvoering van wettelijke controletaken. Daarnaast voerden de krijgsmachtdelen (Marine, Landmacht, Luchtmacht en Marechaussee) lijncontroles uit binnen de financiële processen. Dat gebeurde door afdelingen Verbijzonderde Interne Controle (VIC) die deel uitmaakten van de controllerorganisatie en voor de commandanten werkten."

In de reeks interviews met 'spelers die ertoe doen' in het veld van Control & Audit is dit de tweede aflevering. Na de wetenschapper Marcel Pheijffer nu de controller Peter Grootendorst. Als we naar de bijzondere carrière en huidige positie van Grootendorst kijken mag hij gerekend worden tot de Top-10 van RO's die binnen de overheid en het bedrijfsleven een vooraanstaande positie bekleden.

Internal auditing

"Ongeveer twaalf jaar geleden werden binnen Defensie geleidelijk zelfstandige internal auditfuncties ingevoerd. Het lijnmanagement binnen Defensie had behoefte aan meer informatie over de bedrijfsvoering en vooral ook aan meer zekerheid over de kwaliteit van de (kritische) bedrijfsprocessen. Binnen de krijgsmachtdelen werden voor het uitvoeren van audits BEAU-afdelingen opgericht (BEAU = BeleidsEvaluatie en Audits). Auditonderwerpen werden geselecteerd aan de hand van een onderzoeksprogramma dat was gebaseerd op een systeem van risicoanalyse. De onderzoeksresultaten werden direct aan de commandanten uitgebracht. Terugkijkend kunnen we stellen dat deze BEAU-afdelingen een goede aanzet waren tot een zuivere internal auditfunctie. De BEAU's werkten volledig onafhankelijk van de certificerende accountantsdienst. Het doel was vooral het verhogen van de kwaliteit van de audits door het ontwikkelen van handboeken, auditjaarplannen en een gedragscode. Veel internal auditors zijn toen opgeleid aan de Haagse Hogeschool, de Erasmus Universiteit Rotterdam en de Universiteit van Amsterdam.

Ook de Defensie Accountantsdienst maakte in deze tijd een ontwikkeling door. De DEFAC werd omgedoopt tot Audit Dienst Defensie (ADD) en ging naast de wettelijke taak ook operational audits en IT-audits uitvoeren. Vanzelfsprekend was er in die tijd soms sprake van wrijving en grensconflicten. Er ontstond enige na-ijver tussen de naar een internal auditdienst omgezette centrale accountantsdienst en de decentrale internal auditafdelingen die een professionaliseringsslag doormaakten."

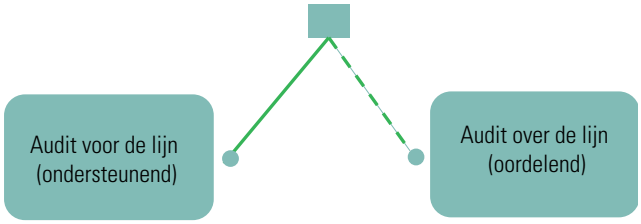
Met de komst van de afdelingen Onderzoeken Interne Beheersing (OIB's) was er binnen Defensie voor het eerst sprake van een volwaardige internal auditfunctie

Professionalisering

"Omstreeks 2005 vond de doorontwikkeling plaats van de decentrale internal auditfunctie door het samenvoegen van de afdelingen BEAU met de VIC-groepen. Dit resulteerde in afdelingen Onderzoeken Interne Beheersing (OIB). In deze OIB's werden alle onderzoeken voor de commandanten van de defensieonderdelen samengebracht. Deze afdelingen OIB ontwikkelden zich voorspoedig tot professionele units die veelal werden geleid door een RA, een RO of een RE. Het niveau van de OIB's en de bruikbaarheid van de uitkomsten werden dusdanig goed ontvangen dat de OIB-onderzoeken een vast onderdeel gingen uitmaken van de manier waarop commandanten hun bedrijfsvoering verbeterden en beheersten. De feedback betrof compliance-informatie, oordelen over de beheersing van processen en conclusies over de realisatie van gestelde doelen. Binnen Defensie was er voor het eerst sprake van een volwaardige internal auditfunctie.
De ADD concentreerde zich in eerste instantie op haar wettelijke taak, maar voerde daarnaast voor de departementale top (SG) ook IT- en operational audits uit. De samenwerking en afbakening tussen de decentrale OIB's en de ADD werd in deze periode geoptimaliseerd. OIB werkte zowel voor decentrale commandanten als voor de ADD en de secretaris-generaal."

Afbouw

"De huidige ontwikkeling laat de ontmanteling zien van de eertijds succesvolle OIB en luidt daarmee het einde in van een fraaie zelfstandige interne auditfunctie. De kwaliteit van de OIB en de onderzoeken die werden uitgevoerd hadden zich zo goed ontwikkeld dat zowel de Auditdienst Defensie (wettelijke taak) als de Algemene Rekenkamer (RJV) van de onderzoeksresultaten gebruikmaakten. Steeds vaker werden onderzoeksprogrammeringen, onderzoeksmethoden en normenkaders van OIB en ADD



Figuur 1. De slinger van audit

op elkaar afgestemd. Kortom, de OIB's gingen qua vaktechniek, instelling en werkwijze steeds meer op de ADD lijken en bij de bezuinigingsronde in 2010 werd dan ook besloten de OIB's en de ADD samen te voegen. Daarna werd de gecombineerde OIB/ADD-capaciteit gehalveerd en wordt deze in maart 2013 bij de Auditdienst Rijk (ADR) ondergebracht.
Gelukkig blijft er bij de controller van Defensie nog een kleine onderzoekscapaciteit achter waarmee nog beperkt procesgericht onderzoek kan worden uitgevoerd. Deze in omvang beperkte capaciteit zal hopelijk op termijn weer kunnen uitgroeien tot nieuwe volwaardige internal auditfuncties."

Voor of over het management

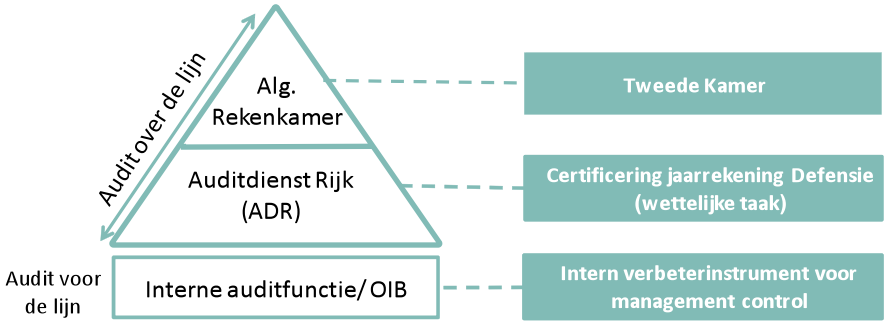
"Vanuit de optiek van het lijnmanagement zijn er twee vormen van auditing (zie *figuur 1*) te onderkennen. 'Voor de lijn', waarbij audit primair een verbeterinstrument van het management is en 'over de lijn', waarbij het auditinstrument voor toezichthouders is. Door de jaren heen zien we een slingerbeweging. Eind vorige eeuw lag het accent vooral op de certificerende en oordelende accountant. Daarna verschoof het accent naar ondersteunende vormen van audit met als hoogtepunt de instelling van OIB's in 2005. Nu, met de oprichting van de ADR, gaat de slinger weer de andere richting op. Mijn opvatting is dat een IAF het karakter hoort te hebben van audit voor de lijn en ik vertrouw erop dat de slinger in de toekomst weer de juiste richting zal weten te vinden."

Hoe hebt u deze ontwikkelingen ervaren?

"Wat ik, terugkijkend, jammer vind is dat er vaak sprake was van een zekere spanning en concurrentie tussen de interne auditfunctie en de departementale accountantsdienst. Dit werd nog versterkt door de discussie die tegelijkertijd plaatsvond tussen de toenmalige VRO en het NIVRA over de plaats en impact van operational auditing. Met wat meer samenwerking zouden de interne auditor en de departementale accountant al in een vroeg stadium veel toegevoegde waarde gehad kunnen hebben. Beide functies (accountant en Internal Audit) hebben een vergelijkbare ontwikkeling doorgemaakt naar een bredere taakuitvoering. Binnen Defensie zijn de ADD en de interne auditfunctie uiteindelijk weer naar elkaar toegegroeid. Een ontwikkeling die ook plaatsvond tussen de (voormalige) beroepsverenigingen IIA en VRO. Gelukkig hebben we nu één Nederlandse beroepsorganisatie voor internal auditors."

Hoe kijkt u aan tegen de vorming van de ADR, waarbij alle auditvormen bij Financiën worden gecentraliseerd?

"Hoewel betrokkenen benadrukken dat de nieuw gevormde ADR een multidisciplinaire internal auditfunctie is, verwacht ik dat het 'gewoon' een certificerende accountantsdienst gaat worden. Immers, het certificeren van de departementale jaarrekeningen is een wettelijke taak. De ervaring van de afgelopen jaren leert dat de niet verplichte operational audits, die gericht zijn op het verbeteren van de bedrijfsvoering, vanwege 'andere prioriteiten' onvoldoende uit de verf komen. Ik zie geen reden om aan te nemen waarom dit nu anders zal zijn. En als er een operational audit wordt uitgevoerd staat elke gevonden omissie in het systeem van interne beheersing ook in het financial auditrapport. Het draagvlak voor operational audits wordt hierdoor uitgehold. De uitkomsten uit een op verbetering gerichte audit voor het management worden gebruikt voor een auditrapport dat over het management oordeelt. Het interne verbeterinstrument wordt opeens een extern afrekeninstrument. De betreffende lijnmanager zal zich in het vervolg niet meer kwetsbaar opstellen en dus zullen 'de kasten en laden' de volgende keer letterlijk en figuurlijk dicht blijven. De hiaten in de interne beheersing komen dan onvoldoende aan het licht en dus lijdt het leervermogen van de organisatie hieronder. *Figuur 2* geeft mijn visie op de gelaagdheid van de rollen en verantwoordelijkheid in de nieuwe situatie.
Ik ben geen voorstander van de ADR als eindsituatie. Wel is het een praktische stap in de goede richting om de weerstand tegen veranderingen zoals die zich bij de departementen voordoen, te neutraliseren. De huidige DAD's zullen eindelijk serieus werk gaan maken van het op een moderne en efficiënte wijze uitvoeren van de verplichte controles, inclusief alle vormen van audits op verzoek. Van de kant van de opdrachtgever zal het in het begin niet veel uitmaken, maar bij de uitvoeringsfase zal meer systeemgericht en meer multidisciplinair worden gewerkt. De vorming van de Auditdienst Rijk (ADR) voorziet wel in de mogelijkheid om de discussies met de Algemene Rekenkamer (ARK), over afbakening van taken en verantwoordelijkheden, beter en slagvaardiger te gaan voeren."



Figuur 2. De centralisatie van de departementale auditdiensten

Wie is nu eigenlijk de externe accountant van Defensie?

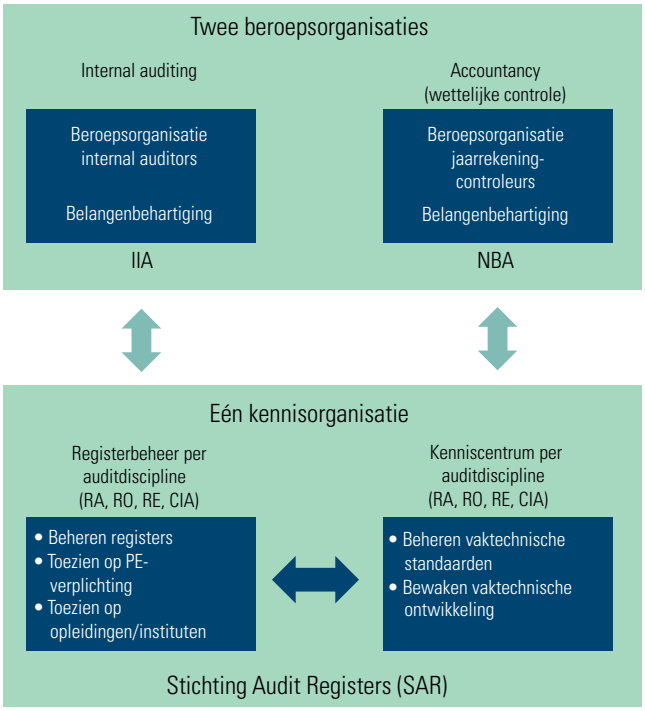
"Deze discussie loopt al heel lang en kan, wat mij betreft, snel worden beëindigd. Op dit moment, maar ook in de nieuwe situatie met de ADR, blijft er sprake van overlap, van ondoelmatigheid en van hinken op verschillende gedachten. De meest doelmatige inrichting is dat de Algemene Rekenkamer (ARK) optreedt als externe accountant van de departementen. Het is de ARK die als enige instantie zekerheid geeft bij de jaarrekening/het jaarverslag ten behoeve van de Tweede Kamer. De handtekening van de president van de ARK volstaat hierbij en deze hoeft niet te vallen onder de accountantsregels die gelden voor civiele accountantsverklaringen. De ARK moet voor deze taak wel worden ingericht. Een andere mogelijkheid is dat de ARK een deel van de werkzaamheden uitbesteedt aan private accountantskantoren. De ADR wordt dan een controlelaag zonder toegevoegde waarde, terwijl er ook geen opdrachtgever is. Dat betekent dat de ADR zou kunnen worden opgeheven. De

Het interne verbeterinstrument wordt opeens een extern afrekeninstrument

vrijvallende ADR-onderzoekscapaciteit kan voor een deel richting ARK gaan en deels kan deze terugvloeien naar de departementen. De leiding van de departementen, in casu de secretarissen-generaal beschikken dan weer over een volwaardige en zuivere internal auditfunctie. Op deze wijze is elke overlap verdwenen en wordt Rijksbreed een aanzienlijke besparing gerealiseerd."

Tot slot nog: de beroepsorganisatie

"De universiteiten en hogescholen leveren mensen af die ook zeer bruikbaar zijn bij andere functies in het bedrijfsleven en bij de overheid. Dat geldt vooral voor functies op het gebied van compliance en risk management. In die functies is veel kennis en ervaring nodig op het gebied van procesinrichting, procesbeheersing, risicoanalyse en onderzoeksplanning. De beroepsverenigingen stellen nu allerlei eisen aan hun leden die gericht zijn op het zuiver functioneren als auditor; terwijl deze leden ook werkzaam kunnen zijn als controller of als consultant.
De oplossing is mijns inziens een splitsing naar enerzijds een kennisorganisatie voor iedereen die ooit in een auditdiscipline is opgeleid en zijn vakkennis wil onderhouden en anderzijds zuivere beroepsorganisaties. Voor een individuele auditor houdt dit in dat hij na het afstuderen blijvend lid is van een kennisorganisatie. Zodra hij als auditor gaat werken zal hij bovendien voor een beroepsorganisatie moeten kiezen (zie *figuur 3*)."



Figuur 3. Het onderscheid tussen kennis- en beroepsorganisaties

Arie Molenkamp is organisatieadviseur, auteur en opleider. Hij is verbonden aan de Amsterdam Business School ten behoeve van de Executive Master of Internal Auditing (EMIA) en het Research Center for Internal Audit Excellence (RCIAE).
✉ consulting@molenkamp.biz

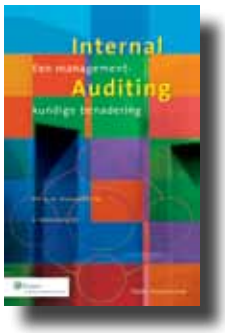
Naeem Arif is zelfstandig audit consultant. Hij adviseert en ondersteunt organisaties op het gebied van internal auditing en risk management. Daarnaast treedt hij op als opleider/docent, onder andere aan Nyenrode Business Universiteit.
✉ naeem.arif@xs4all.nl

Rien ne va plus. Achter de schermen bij Holland Casino

Marco Rosman • Bertram + de Leeuw • ISBN 9789461560834 • € 17,95

In dit boek beschrijft Marco Rosman hoe het staatsbedrijf Holland Casino een gemankeerd beleid voert met betrekking tot het voorkomen en tegengaan van gokverslaving. Kreeft en flessen whisky worden ingezet om gasten maar te laten gokken. Je kunt dood neervallen bij de roulettetafel, waarna andere gokkers direct je plaats innemen. Het boek biedt een kijkje achter de schermen: fraudes, feestjes, kansspelverslaving, witwaspraktijken, omgangsvormen, machtsspelletjes en rechtszaken.

Internal Auditing: ook voor toezichthouders, bestuurders en controllers.



A.J.G. Driessen en A. Molenkamp • Kluwer, vijfde herziene druk 2012 • ISBN 9789013108484 • € 82,50

Binnenkort verschijnt de geheel herziene vijfde druk van het standaardwerk *Internal Auditing*, een managementkundige benadering. Driessen en Molenkamp zijn erin geslaagd om op basis van onderzoek, advieservaringen en literatuurrecherche het theoretisch en praktisch fundament onder de strategische positie van internal auditing verder te versterken.

De economische en financiële malaise heeft het bewustzijn ten aanzien van organisatierisico's en het informeren van bestuurders over deze risico's vergroot. De waarde van de internal auditfunctie voor commissarissen en bestuurders is optimaal wanneer de functie wordt ingericht en gepositioneerd conform de criteria en scenario's zoals die zijn beschreven. De raad van bestuur ontvangt dan objectieve en onafhankelijke oordelen en adviezen over de wijze waarop met de strategische doelen en risico's wordt omgegaan.

Om de functie van internal audit nog specifieker te duiden zijn twee nieuwe hoofdstukken toegevoegd. Een apart hoofdstuk gaat in op auditvormen als financial auditing, operational auditing en forensic auditing. Een ander hoofdstuk behandelt public auditing; de betekenis van audit voor het publieke domein.

De invalshoek van het boek, het managementkundige standpunt, is onmiskenbaar leidend gebleven. Internal auditing staat immers hoog op de agenda bij toezichthouders, commissarissen en raden van bestuur, zodra er gesproken wordt over governance, risicomanagement en compliance. De functie wordt nadrukkelijk geafficheerd als waarborg dat risico's adequaat worden gemanaged, dat wordt voldaan aan wet- en regelgeving en dat de beheersmaatregelen goed zijn ingericht en zodanig functioneren dat met meer zekerheid de strategie van de onderneming kan worden gerealiseerd.

Einde van de privacy

Adjiedj Bakas • Scriptum • ISBN 9789055948581 • € 22,50

Internet is voor Nederlanders een eerste levensbehoefte geworden. Trendwatcher Adjiedj Bakas maakte een rondgang in de veiligheids-, marketing-, hr- en IT-industrie en schreef een prikkelend boek over de toekomstige rol van internet en privacy in ondernemerschap en consumentengedrag in 'de Eeuw van de Burger'. Een aantal toekomstvoorspellingen van Bakas op een rij:

- De 400 miljoen Europeanen hebben samen al 50 miljard sporen op internet achtergelaten. Het koppelen van al die verschillende data via algoritmen en 'business analytics' wordt een megatrend
- Webwinkelen wordt maatwerk, passend bij de persoon en het aankoopgedrag.
- De beveiliging van internet wordt een enorme groeimarkt. Internet security is de branche van de toekomst en cyberwar wordt een nieuwe kerntaak van het leger en Defensie.
- Naast gratis internet komt er betaald internet en burgers slaan hun digitale identiteit in de 'cloud' op.
- Liefde, vriendschap, seks en intimiteit starten vaker op internet, dat uitgroeit tot 'interslet'. Met een elektronische contactlens, waarop teksten worden geprojecteerd, kun je straks teksten lezen terwijl je met iemand staat te praten.
- Hoe belangrijker ons leven 'online' wordt, hoe belangrijker ook ons leven 'offline' wordt. We gaan elkaar vaker fysiek ontmoeten.

MicroData

Peter W.M. van Nederpelt EMEA EMIA RO • ISBN 9781471006371 MicroData • € 15

Het management wil iets met kwaliteit of risico's doen, maar weet niet waar te beginnen. Het moet liefst niet te ingewikkeld zijn en ook niet te veel tijd kosten, maar het moet wel hout snijden. Ook wil het management graag klein beginnen en er later eventueel meer aan doen. Het Object-oriented Quality and Risk Management (OQRM)-model dat in dit boek wordt beschreven, wil in deze behoefte voorzien. Het doel van het boek is om managers in staat te stellen dit model in de organisatie toe te passen. Het OQRM-model is generiek van opzet en kan in elke organisatie, op elk niveau, op elke schaal en op elk gebied worden toegepast en helpt om op een systematische manier maatregelen vast te stellen om een aandachtsgebied in control te houden of te krijgen. Het model integreert kwaliteits- en risicomanagement en voorziet bovendien in de behoefte aan maatwerk.

Three Lines of Defense

L. Brandts PhD*

De vijand kon van alle kanten komen: uit de valleien, onverwacht uit de bergen, via de rivier, of toch gewoon over de weg. Een verstandige koning in de Middeleeuwen trok daarom verdedigingslinies op die hem konden beschermen tegen alle mogelijke aanvallen: wachters aan de buitenkant op de aarden wallen, bewapende soldaten op de stadsmuren en een linie van goed getrainde elitesoldaten direct rondom de koning.

Verdedigingslinies in een onderneming

Op een soortgelijke manier is het risicomanagement van moderne ondernemingen georganiseerd. De medewerkers en managers vormen de eerste line of defense. Deze weerspiegelt de moderne variant van de wacht op de aarden wal. De soldaten op de stadsmuren zijn de verschillende risicomanagement- en complianceafdelingen en de elitesoldaten zijn de interne auditors die rechtstreeks aan de CEO rapporteren.

De koningen in de Middeleeuwen hadden een aantal zaken goed op orde. De koning wist precies van welke kant de risico's kwamen en had zijn adviseurs in alle linies opgesteld. De soldaten op de aarden wal waren goed bewapend en waren bekend met de risico's. De soldaten op de stadsmuren werkten goed samen en alleen een zeer gecoördineerde en langdurige aanval kon hen deren. De elitesoldaten zorgden voor het overzicht en rapporteerden over de actuele situatie aan de koning. Iedereen wist zijn plek in de verdediging en begreep de gevolgen als hij verzaakte.

De tegenwoordige opsplitsing in verantwoordelijkheden binnen ondernemingen is uitstekend en zorgt uiteraard voor de juiste focus. Het proces van de audit moet de belangrijkste focus zijn en niet de auditafdeling op zich. Gebrek aan samenwerking zal het risico-overzicht in de weg staan. Het probleem dat dan kan optreden is dat alle soldaten hun ogen gericht houden op de weg en dat de eerste de beste aanval uit de vallei tot problemen leidt.

Internal Audit kan helpen om 'de koning' het overzicht en de balans te laten houden. Laten we bij wijze van voorbeeld COSO ERM volgen en uitgaan van vier hoofdcategorieën van risico's: strategie, operationeel, reporting en compliance. Velen op de aarden wallen en de stadsmuren (de eerste en tweede line of defense) focussen op reporting en compliancerisico's. Operationele risico's en met name strategische risico's, zijn lastiger te monitoren. Hetgeen helaas niet wil zeggen dat ze daarom minder belangrijk zijn.
Doorgaans zal het strategische risico zelfs niet optimaal zijn afgedekt. Internal Audit zal dit wellicht onderkennen, maar zal zich toch vaak gedwongen voelen om te blijven focussen op de compliance en reporting risico's. Het is alsof er continu vijandige elementen over de weg komen en dat de elitesoldaten telkens moeten assisteren om deze tegen te houden. Terwijl ze in hun ooghoeken ook vijandige troepen zien aankomen over de bergen. Door de soldaten in de frontlinie beter te bewapenen kunnen de elitetroepen doen waar ze voor bedoeld zijn: zich concentreren op de meer complexe groep van risico's.

In hedendaagse risicotermen kan 'beter bewapenen' op verschillende manieren plaatsvinden. Een manier is de meest voorkomende risico's zoveel mogelijk weg te automatiseren, zodat ook deze soldaten kunnen focussen op belangrijkere zaken. Continuous monitoringtechnieken zijn de belangrijkste moderne wapens voor de frontsoldaat (de business). Hierdoor worden risico's verlaagd en wordt het werk van de business eenvoudiger en prettiger. Internal Audit kan vertrouwen op de continuous monitoringresultaten en hoeft dus minder zelf te doen op dit gebied. Internal Audit kan zich vervolgens meer richten op de strategische risico's.

In elk geval moeten de drie lines of defense als één defensiesysteem worden bekeken. Uiteraard met inachtneming van de onafhankelijkheid van Internal Audit. Ook de koning in de Middeleeuwen had dat goed begrepen. Hij organiseerde zijn defensie vanuit de gedachte dat vertrouwen prima is, maar controle beter. Wellicht dat we niet zo ver hoeven te gaan dat een auditor elke dag de lunch van de CEO voorproeft, maar wellicht kunnen we toch nog wel een paar andere lessen leren van de Middeleeuwen.

* Luc Brandts is CTO & Founder BWise
www.bwise.com/blog

Round table ‘Auditen van social controls’

Op 27 juni jl. vond er een round table plaats rondom het thema ‘Auditen van social controls’. Deze round table is door de commissie Vaktechniek van IIA georganiseerd in vervolg op het boekje *Auditen social controls, handvatten voor het meten van Entity level social controls.*

Drs. W.A.J. van Loon RA CIA

Het boekje is vorig jaar uitgebracht door IIA en beschrijft vele modellen die auditors kunnen gebruiken bij het beoordelen van social controls. Hard nodig, want, zoals de voorzitter van IIA in zijn voorwoord schreef, de groep internal auditors die over social controls spreekt is nog altijd groter dan de groep die daadwerkelijk social controls expliciet onderdeel laat zijn van audits.

Met zo’n zeventien personen was de round table druk bezocht. Niet alleen internal auditors, maar ook vertegenwoordigers uit de lijn, controlling, accountancy en toezichthouders waren aanwezig. Het onderwerp heeft duidelijk aan belang en belangstelling gewonnen. Hoewel succesvolle toepassingen in de praktijk al hebben laten zien dat het auditen van social controls geen rocket science is, moet er nog wel iets gebeuren om een groter draagvlak te creëren. Niet alleen bij (het management van) de organisatie, maar ook bij auditors zelf.

Primaire vraag

Na een korte introductie van Peter Hartog namens de commissie Vaktechniek van IIA, lag al snel de primaire vraag op tafel: hoe krijg je het auditen van social controls nu geïmplementeerd en geaccepteerd richting de organisatie? Deelvragen die daar uit voortkwamen waren snel gevonden:

- Hoe verkrijgen we acceptatie bij het management?
- Hoe verkrijgen we acceptatie bij de auditors?
- Welke kennis en kunde is nodig c.q. moet worden vergroot?

Succesvol in de praktijk

Hoe het auditen van social controls in de praktijk succesvol kan zijn werd door twee presentaties duidelijk. Johan Buitenga van Corporate Audit Services (CAS) bij ING (tevens gastheer voor deze round table) vertelde dat het auditen van social controls een weg is van rustig beginnen, gradueel uitrollen en leren van ervaringen. Het daadwerkelijk doorvragen naar de root causes van bevindingen vereist een enigszins modelmatige aanpak die zo dicht mogelijk blijft bij wat de auditor normaal al doet. Het is vooral nodig dat de auditor leert om dat wat hij vaak al denkt en aanvoelt te vertalen naar concrete observaties. Hij wordt daarin ondersteund door handvatten om binnen de ruimte te opereren die het concept van bijvoorbeeld ‘deugdelijke grondslag’ biedt. Daarnaast is een stevig uitgesproken commitment van het hoogste management voor het betrekken van social controls in audits een belangrijke steun.

Adriaan Bouwdewijn vervolgde met de aanpak van de Accountantsdienst van UWV en legde de nadruk vooral op lef en overtuiging. Het door de auditor opzoeken van de dialoog met de auditee en durven doorvragen zijn cruciaal voor succes.

Terughoudendheid

Ook al is er in het begin terughoudendheid tegenover het auditen van social controls, als er eenmaal mee begonnen is zijn de erva-

ringen van zowel de auditee als auditor vrijwel altijd positief. Het auditen van social controls betreft in essentie aandacht voor waarden, houding en gedrag van human capital. De terughoudendheid van auditors is terug te voeren op onwennigheid, een andere rolinvulling en het gebruik van andere (interview- en analyse)technieken dan in assurance audits. Bij het auditen van social controls moet de auditor dieper willen kijken. Controlsystemen en -maatregelen 'doen het niet als vanzelf goed'. Het is de menselijke factor – gerichtheid, houding en gedrag van personen – die bepaalt of systemen in handelen worden vertaald en maatregelen naar hun intentie worden geëffectueerd. Voor een adequaat onderzoek heeft de auditor zich, naast op opzet, bestaan en werking, te verdiepen in de effectiviteit van sturing op houding en gedrag. Auditors en auditees zijn een dergelijk onderzoekskader niet gewend. 'Stimuleren' in lef en op 'out of his comfortzone' handelen door de auditor is nodig. Daarnaast is een adequaat verwachtingenmanagement richting het management en de auditees een succesbepalende factor.

Ervaringen delen

Na deze presentaties is verder doorgesproken aan de hand van enkele stellingen, gekoppeld aan de drie deelvragen die in het begin van dit artikel staan vermeld. Met de nodige levendigheid zijn de diverse ervaringen gedeeld. Veel discussiepunten zijn naar voren gekomen over het werkelijke onderscheid tussen hard en soft controls, maar ook over de argumenten om het management mee te krijgen. Suggesties als 'de buren doen het ook' en het gradueel toepassen van de social controls in audits zijn gedeeld.
Algemeen werd het idee gedeeld dat Internal Audit uiteindelijk de vraag moet *krijgen* van het management om uitspraken te doen over de werking van social controls. Wat de tweede deelvraag betreft ging de discussie met name over de rol die auditors moeten spelen en de geleidelijke invoering van social controls in de auditwerkprogramma's. Ook de samenwerking met compliance en hrm werd besproken.
En de verdere conclusies? Die zullen op de IIA-website terug te vinden zijn. En dan zal ook de verdere discussie gevoerd worden, want de dicussie over en de toepassing van het auditen van social controls stopt niet met deze round table.

Internal Audit moet uiteindelijk de vraag krijgen van het management om uitspraken te doen over de werking van social controls

Op de website van IIA (zie www.iia.nl) wordt een meer uitgebreid verslag van deze round table geplaatst, inclusief de presentaties en conclusies (tips & tricks) op de drie genoemde deelvragen.

Willem van Loon is redactielid van *Audit Magazine* en werkt als hoofd Internal Audit bij Triodos.

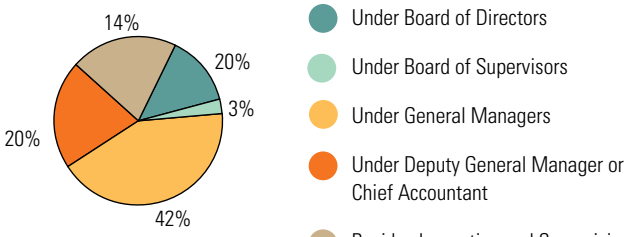
Internal auditing in China

Dit artikel is een korte weergave van een onderzoek naar internal auditing in China. Het cijfermateriaal geeft een mooie aanvulling op het CBOK-onderzoek naar het functioneren in een groot aantal andere landen. Internal auditing in China blijkt nog in opkomst. Maar zoals op vele andere terreinen gaat de ontwikkeling snel.

Z. Wenxiu
G.J. van der Pijl
S. Xian

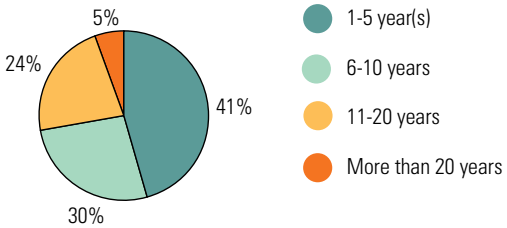
In 2006 werd het grootste onderzoek ooit naar de stand van het internal auditingberoep over de wereld uitgevoerd: het CBOK-onderzoek. Het bracht gedetailleerde en gestandaardiseerde informatie over ontwikkelingen in het interne auditberoep per land naar voren. Dat onderzoek is niet in China uitgevoerd. Maar in 2008 kwamen de resultaten van een groot onderzoek onder publieke en private ondernemingen in China beschikbaar. Nou ja, beschikbaar? De resultaten werden alleen in het Chinees gepubliceerd.
Het recente bezoek van de Chinese onderzoekster Wenxiu Zhang aan de Erasmus Universiteit Rotterdam maakt het mogelijk een samenvatting van de resultaten nu ook in het Nederlands te presenteren. Het behoeft geen betoog dat de ontwikkeling van het vak in het grootste en economisch gezien snelst groeiende land van de wereld ook voor ons van belang is. Economische samenwerking tussen bedrijven uit Nederland en China maakt het immers wenselijk dat er wederzijds begrip is van de werking van elkaars interne controlestelsel.

Onderzoeksuitkomsten
In totaal namen 1024 ondernemingen aan het onderzoek deel. Iets meer dan de helft daarvan was volledig in handen van de overheid. 83% van de aan het onderzoek deelnemende ondernemingen beschikt over een internal auditactiviteit, ruim 75% daarvan is opgezet als een afzonderlijke auditafdeling. Bij de andere organisaties is de interne auditfunctie ondergebracht bij andere afdelingen, zoals bijvoorbeeld de afdeling Financiën.
Interessant is ook dat 20% van de onderzochte auditafdelingen rapporteert aan de raad van bestuur en slechts 3% aan de raad van commissarissen (zie *figuur 1*). De rest (ruim 62%) rapporteert aan lagere managementniveaus. Dit heeft mede te maken met het feit dat auditfuncties in andere afdelingen zijn ondergebracht.



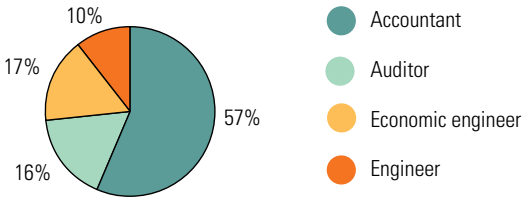
Figuur 1. Niveau van rapportage

Uit het onderzoek blijkt dat het opleidingsniveau van internal auditors veelal lager ligt dan in Nederland. Slechts een zeer klein percentage heeft een opleidingsniveau boven bachelor. Daarbij komt dat interne auditors in China niet veel training ontvangen. Ruim 90% heeft slechts twee of minder malen per jaar enige vorm van training. Zoals *figuur 2* laat zien is de gemiddelde ervaring van auditors in China vrij kort. Dit is niet verwonderlijk als men zich realiseert dat de internal auditfunctie in China pas sinds 1983 voorkomt. Daarnaast is er veel job rotation.



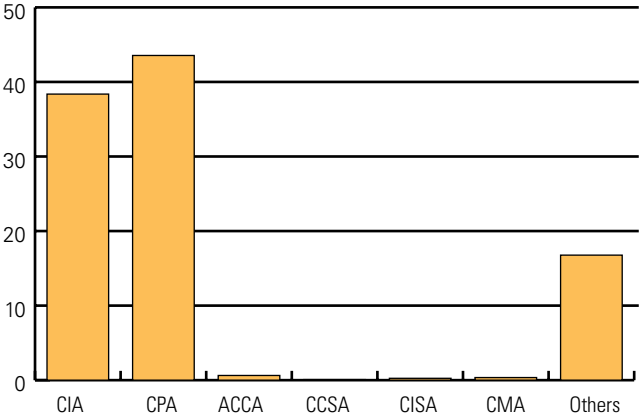
Figuur 2. Aantal jaren ervaring

Ruim de helft van de medewerkers van de internal auditafdelingen heeft een professionele titel in accounting (hiermee wordt de financiële administratie bedoeld), slechts 16% voert de professionele titel van auditor (zie *figuur 3*).



Figuur 3. Gevoerde professionele titel

Ruim 80 % van de respondenten heeft een CIA- of CPA-titel (zie *figuur 4*).



Figuur 4. Titels

Tabel 1 geeft een inzicht in de bezigheden van interne auditors in China. Financiële audits voeren duidelijk de boventoon, zeker als deze samen worden genomen met internal control assessments en subsequent audits. Maar ook voor performance, ofwel operational audits, is flink wat aandacht. De categorie economic responsibility audit is een specifiek Chinese vorm van Internal Audit. Het gaat daarbij om het beoordelen van het functioneren van (door de overheid aangestelde) bestuurders van overheidsorganen en bedrijven. Het is een typische activiteit voor interne auditdiensten in een communistisch land en, zoals blijkt, in China een belangrijke auditactiviteit. Daarnaast komen IT-audits, milieumanagementaudits en fraudepreventie en onderzoek regelmatig voor.

No.	Content	Never	Few	Ordinary	Often	Must
1	Financial audit	0%	0%	6%	43%	51%
2	Performance audit	3%	17%	35%	33%	12%
3	Economic responsibility audit	2%	5%	7%	37%	49%
4	IT audit	14%	28%	38%	13%	7%
5	Internal control assessment	6%	19%	42%	21%	12%
6	Fraud prevention and investigation	14%	28%	41%	12%	5%
7	Environment management audit	26%	34%	26%	11%	3%
8	Strategic audit	28%	36%	28%	7%	1%
9	Subsequent audit	6%	29%	33%	23%	9%

Tabel 1. Aard van de werkzaamheden

Het is interessant om te kijken naar de kennis en vaardigheden van internal auditors in China. *Tabel 2* en *3* geven daarvan een beeld. Duidelijk is dat de meeste ervaring ligt op het terrein van financieel management en interne controle en daarnaast ook de ervaring op het gebied van (deze specifieke terreinen van) Internal Audit en de beroepsstandaarden groot is. Internal Audit blijkt zich dus nog sterk te concentreren op het gebied van financial audit. Veel ervaring op het gebied van risk management ontbreekt nog. Daarnaast is redelijk veel kennis aanwezig over aan financiële zaken verwante wetgeving.

Option of issue	Unfamiliar	General understanding	Very familiar
Corporate Governance	24%	66%	10%
Science of Organizational Behavior	18%	72%	10%
Corporate Strategy	26%	68%	6%
Management Accounting	27%	52%	21%
Risk Management	13%	77%	10%
Project Management	5%	78%	17%
Financial Management	2%	54%	44%
Organisation and management of Internal Audit	6%	68%	32%
Internal Control	5%	64%	31%
Corporate Restructuring and Asset Evaluation	19%	62%	19%
Standards of Professional Ethics	5%	50%	45%
Individual Skills of Internal Auditor	24%	69%	7%

Tabel 2. Ervaringsgebieden

Option of issue	Unfamiliar	General understanding	Very familiar
Company Law	6%	72%	22%
Security Law	24%	73%	3%
Tax Law	0%	45%	55%
Accounting Law	0%	37%	63%
Audit Law	0%	16%	84%
Contract Law	1%	73%	26%
Information Disclosure Standards	21%	67%	12%
Corporate Governance Guidelines	31%	60%	9%
Accounting Standards	1%	52%	47%
Independent Auditing Standards	1%	56%	43%
Internal Auditing Standards	7%	69%	24%
International Comparison between the Standards	51%	47%	2%

Tabel 3. Kennisgebieden

Ten slotte is opvallend dat de respondenten op veel terreinen een tekort aan kennis signaleren zoals blijkt uit *tabel 4*.

Werken aan de toekomst

Uit de onderzoeksresultaten blijkt duidelijk dat de onderzochte internal auditafdelingen nog maar weinig gebruikmaken van IT-auditing, ook niet in het kader van de jaarrekeningcontrole. Er lijkt niet veel kennis op dit onderdeel van het vakgebied aanwezig. Om de condities voor het gebruik van IT-auditing te verbeteren werd in 2002 het 'Golden auditing project' (GAP) door de overheid goedgekeurd. Het project werd uitgevoerd in de periode 2002-2011. De doelstellingen van het project waren:

a. *Opbouw van een netwerk en apparatuur* – Auditafdelingen verbeteren hun hardware in hoog tempo en creëren daarmee

Option of issue	Comprehensive analysis capacity of information	Strategy and critical thinking ability	Ability to dynamically acquire new audit principles, concepts and technologies	Ability to identify and understand risks and related opportunities	Customer and market concern ability	Ability to make professional judgements according to audit objectives and special audit objectives	Professional and technical capacity	Ability to use statistical and non-statistical methods to select, collect, assess and manage audit evidences
Quantity	176	128	120	76	71	69	66	66
Proportion	69%	50%	47%	30%	28%	27%	26%	26%

Tabel 4. Tekort aan technische vaardigheden

een omgeving voor het auditen van geautomatiseerde financiele administraties.

b. *Het ontwikkelen en bouwen van programmatuur* – Het gaat hier om twee belangrijke systemen:
   - het 'auditors officesysteem' biedt een soort van workflowmanagementomgeving voor voornamelijk financiële audits. Het biedt vooral plannings- en documentatieondersteuning;
   - het 'audit implementationsystem' biedt daarnaast tools voor het verzamelen en analyseren van data en het opbouwen van rapportages. Ook wordt binnen deze applicatie geëxperimenteerd met online audits waarbij data via internet worden verzameld.

c. *Het opzetten van een database met kerninformatie voor auditors* – Deze database wordt gezien als een noodzakelijke voorwaarde voor het uitvoeren van financiële audits in een geautomatiseerde omgeving. De database is opgebouwd door het National Audit Office of China (CNAO) en omvat drie subdatabases:
   - (macro)economische informatie;
   - auditliteratuur en -expertise;
   - wet- en regelgeving.

   Alle auditafdelingen in China maken gebruik van deze database.

d. *Standaardisatie van IT-audit* – CNAO heeft centrale standaarden voor IT-auditing opgesteld. Daarnaast werden het CNAO-auditproces en de kwaliteitsbeheersing van het proces gestandaardiseerd. Voor het uitwisselen van auditgegevens werden standardformats opgezet en ook de vorm van auditdocumentatie werd gestandaardiseerd. Tenslotte werd een gestandaardiseerd auditmanagementsysteem opgezet.

e. *Human Resources Training* – CNAO ontwierp middenkadertrainingen op het gebied van netwerken, databases, geautomatiseerde verwerking van financiële gegevens, gegevensverzameling en conversie, audit software, et cetera.

f. *Intensief gebruik van IT in financial auditing*.

Gedurende de looptijd van het proces is het gebruik van IT in financial auditing sterk toegenomen. De aandacht die het CNAO schenkt aan dit 'Golden auditing project' weerspiegelt het belang dat men hecht aan het gebruik van IT in auditing. Hoewel IT-auditing zich in hoofdzaak richtte op financial audits in een geautomatiseerde omgeving wordt de laatste jaren ook aandacht geschonken aan het auditen van niet-financiële data en aan het auditen van informatiesystemen in meer algemene zin. Vooral binnen de internal auditafdelingen in Chinese organisaties lijkt er ruimte voor het uitbouwen van IT-auditingactiviteiten in deze brede zin.

Conclusie

Het mag duidelijk zijn dat internal auditing in China nog in de kinderschoenen staat. Op zich is dit niet verwonderlijk gezien het feit dat de economische ontwikkeling in China nog niet zo heel lang geleden op gang is gekomen. Met deze ontwikkeling neemt ook het zelfstandig functioneren van Chinese bedrijven toe. Er komt meer ruimte voor eigen initiatief in plaats van door meerjarenplannen gedreven externe (overheids)aansturing van de bedrijven. Daarbij past ook een Internal Audit die zich ontwikkelt in de richting van het ondersteunen van het bedrijfsmanagement. Op het ogenblik richt Internal Audit in China zich vooral op financial auditing. Ook waar gewerkt wordt aan de ontwikkeling van 'IT-audit' richt zich dat nog vooral op ondersteuning van de jaarrekeningcontrole en standaardisatie van de daarbij gebruikte procedures. Niettemin zijn her en der pogingen tot verbreding te zien en komt ervaring en kennis op een breder gebied aan activiteiten tot ontwikkeling. De Audit University in Nanjing heeft een populatie van bijna 18.000 studenten en werkt, onder andere in samenwerking met buitenlandse universiteiten, aan onderzoek op het vakgebied. Een punt waar wij mogelijk kunnen leren van onze Chinese collega's betreft de economic responsibility audit (het beoordelen van het functioneren van bestuurders van overheidsorganen en bedrijven). Ook in het kader van de Amerikaanse en Europese regelgeving op dit gebied lijkt deze thematiek van belang voor interne auditors.

Zhang Wenxiu (l) is onderzoekster en docente aan de School of International Auditing, Nanjing Audit University in China
zhangwenxiu@nau.edu.cn
Gert J. van der Pijl is hoogleraar IT-Auditing & Advisory aan de Erasmus Universiteit Rotterdam. vanderpijl@ese.eur.nl
Shi Xian is onderzoekster en docente aan de School of International Auditing, Nanjing Audit University in China.

In de ‘Estafettecolumn’ schrijft een auditprofessional op persoonlijke titel over een onderwerp dat hem of haar bezighoudt, irriteert of verbaast. Dit op uitnodiging van de columnist uit het vorige nummer van *Audit Magazine*, om daarna zelf het stokje weer door te geven. Deze keer **Linda van der Lans**, senior auditor van de provincie Zuid-Holland.

Aan de slag met een waarderende CSA

In de vorige Estafettecolumn schreef Anthoon Haagsma over waarderend auditen. Afhankelijk van de wensen van de opdrachtgever, ben ik creatief in het combineren van invalshoeken vanuit diverse vakgebieden. Onlangs heb ik de invalshoeken van control self assessments (CSA) en waarderend auditen bij elkaar gebracht in een workshop. De methode heeft volgens de deelnemers en opdrachtgever goed gewerkt. Met name de korte doorlooptijd en de open benadering zijn pluspunten.

Centraal in de workshop staat de realisatie van een doelstelling zodat successen, kansen en maatregelen in kaart kunnen worden gebracht. Een waarderende insteek betekent een focus op het identificeren van successen (in verleden en heden) en kansen om te verbeteren (in de toekomst). Een (kans op) succes is een gebeurtenis met een (mogelijk) positief effect op de doelbereiking. Er kunnen eveneens maatregelen aan de orde komen die dit succes mogelijk hebben gemaakt of zullen maken.

Aan de hand van een gestructureerde aanpak vindt een waarderende discussie plaats en wordt informatie uitgewisseld tussen managers en/of medewerkers. De kern is dat alle inbreng waardevol is en systematisch wordt gewaardeerd. De risico’s en problemen kunnen indirect aan bod komen. De facilitatoren en deelnemers hebben een actieve rol om een probleem of risico te herformuleren naar een kans. Het succes is gebaseerd op het creëren van een gezamenlijke waarderende houding in plaats van een kritische houding. Zo ontstaat een lerend klimaat, waardoor deze methode meerwaarde oplevert in de vorm van enthousiasme, acceptatieverhoging en meedenken.

In een waarderende CSA-workshop is een normenkader minder normatief en toetsend van aard. Immers, alles dat wordt ingebracht heeft waarde. Een normenkader wordt ingezet als handvat en om de inbreng van deelnemers te stimuleren en/of te structureren. Het brengt focus aan en bevat idealiter zowel harde als zachte elementen. Mogelijke kaders zijn 7S, INK, KAD+, PRINCE2, COSO of COBIT. Een punt van aandacht is de volledigheid van het kader versus de beschikbare tijd voor de workshop. Afhankelijk van de behoefte van de opdrachtgever en de opzet die je kiest, bepaal je hoeveel structuur de workshop nodig heeft.

Het toetsen van de ingebrachte successen en/of kansen vindt plaats door de deelnemers van de workshop. Iedere deelnemer geeft individueel een score op een scoreformulier, dat na afloop wordt ingeleverd. De score van een (kans op) succes heeft betrekking op de impact op de realisatie van de doelstelling en de waarschijnlijkheid dat deze kans slaagt en tot een succes leidt. Bij successen is de score meer beredeneerbaar dan bij kansen. In de rapportage worden de groepsscores zichtbaar gemaakt en de Top-10-successen en/of kansen kort en krachtig omschreven.

De kracht van de workshop is gebaseerd op het samenspel tussen de opdrachtgever, onderzoekers en deelnemers. De verantwoordelijkheid voor de opdrachtverstrekking, de globale aanpak van de workshop en het vervolg ligt bij de opdrachtgever. Onderzoekers kunnen de behoefte aan een dergelijke workshop bij de intake herkennen, een workshop professioneel voorbereiden en vanuit een onafhankelijke rol een workshop faciliteren en verslaglegging doen over de resultaten. Het is essentieel om te bepalen of het gewenst is dat een auditor een CSA-opdracht oppakt. De uiteindelijke resultaten worden bepaald door de deelnemers en het groepsproces. De deelnemers wordt na afloop gevraagd om hiermee aan de slag te gaan en de vervolgacties op zich te nemen.

De aanpak van een waarderende CSA is vastgelegd in een stappenplan en is mede tot stand gekomen in samenwerking met Frits Engel. Graag draag ik deze column over aan Frits Engel, zodat hij zijn bevlogenheid over CSA met jullie kan delen.

EMIA-RO Masterclass 2012

Op donderdag 29 en vrijdag 30 november 2012 organiseert IIA de tweedaagse EMIA-RO Masterclass. Het thema voor 2012 is: Verbinding. Verbinding tussen internal auditors en hun opdrachtgevers, tussen verschillende concepten van 'control' en tussen het 'oude' en het 'nieuwe' denken over Internal Audit. Prof.dr. Wouter ten Have van Ten Have Change zal ons met de resultaten van zijn proefschrift over organisatiekundige en veranderkundige toepassingen van het in controlconcept inspireren om relaties anders te zien en daardoor ons werk beter te doen.

Inschrijven kan via www.iia.nl.

Buitengewone ALV IIA Nederland

IIA Nederland houdt op maandag 24 september 2012 een Buitengewone algemene ledenvergadering om de strategieherijking nader te bespreken.
Na de ALV op 5 april jl. heeft het bestuur de leden geïnformeerd over de op handen zijnde strategieherijking. Hierna heeft het bestuur de leden in de gelegenheid gesteld te reageren op de conceptstrategienota. De input die het bestuur op deze wijze van de leden heeft ontvangen, heeft zij meegenomen in de aanscherping van de strategieherijking. Vervolgens heeft het bestuur de raad van advies geconsulteerd waarna het bestuur nu de strategieherijking ter instemming aan de leden voorlegt. Hiertoe wordt op 24 september a.s. een Buitengewone algemene ledenvergadering gehouden. Hierbij wordt ook meer specifiek ingegaan op de implicaties van de strategieherijking op het verdienmodel van de vereniging.
Nadere informatie volgt via de nieuwsbrief en op de website.

Activiteitenkalender

CIA-examentraining najaar 2012
21-28 sep. en 4-5-12 okt. 2012

Training Administratieve Organisatie (AO), klassiek en modern!
24-25 sep. en 1-2 okt. 2012

Training Zelfsturend leren in auditing
2 okt. 2012

Seminar Overtuigende auditprofessionals
4 okt. 2012

Seminar Uncontrolled social media
8 okt. 2012

Round table Samenwerking tussen operational- en IT-auditor
10 okt. 2012

Training Governance, risk management & compliance (GRC)
10 & 11 okt. 2012

Training Tools & techniques for the new auditor in charge
12 & 17 okt. 2012

Training Introductie NLP
18 okt. 2012

Seminar Leiderschap en loyaliteit
25 okt. 2012

Seminar Projecten – de menselijke factor
1 nov. 2012

Seminar Risicoparagraaf & in control statement
5 nov. 2012

Seminar Actualia fraude en witwassen
6 nov. 2012

Training Auditen van projecten
7 en 8 nov. 2012

Training IIA toolbox voor interne auditdiensten
13 nov. 2012

GAIN-bijeenkomst: Internal Audit en sustainability
14 nov. 2012

Training Introductie waarderend onderzoeken
22 nov. 2012

Training Professioneel Kritische Instelling (PKI)
22 nov.-6 dec. 2012 en 15 jan. 2013

Training Beginning auditor tools & techniques
26-27 nov., 10-11 dec. 2012

Training Financial auditing
29 en 30 nov. 2012

Seminar EMIA-RO Masterclass 2012
29 en 30 nov. 2012

Training Administratieve organisatie (AO), klassiek en modern!
3, 4, 17 & 18 dec. 2012

Training Leiderschap bij misleiding
6 & 7 dec.

Training Governance en management control
10 dec. 2012

Seminar (Corporate) Governance en de internal auditor
13 dec. 2012

Uitreiking kwaliteitscertificaten

Stork

Alex Nieman, risk management & Internal Audit van Stork: "De internal auditafdeling van Stork Technical Services is zeer vereerd om als eerste kleine internal auditafdeling het certificaat naar aanleiding van de kwaliteitstoets te ontvangen. Dit bewijst dat ook kleine IAD's kunnen voldoen aan de algemeen aanvaarde normen voor beroepsuitoefening. Het is goed om van tijd tot tijd een externe bril naar je organisatie te laten kijken. Zowel de aanbevelingen als de discussies bieden nieuwe aanknopingspunten om hierover door te denken en waar nodig de kwaliteit verder te verbeteren. Wij kunnen een dergelijke toets dan ook van harte aanbevelen en ondersteunen de doelstelling om door middel van deze kwaliteitstoetsen het niveau van Internal Audit in Nederland naar een hoger plan te brengen."

NIBC

Hoofd Internal Audit NIBC, Marc Verberne: "De externe toetsing door IIA is voor Internal Audit een belangrijk onderdeel van het continu voldoen aan de professionele kwaliteitseisen en bevestigt uiteindelijk de kwaliteit van ons werk en van de interne auditors. De gecombineerde toetsing door IIA aan de eisen van het NIVRA, de NOREA en IIA is voor ons efficiënt en vlot verlopen. Managing board en audit committee zijn nadrukkelijk betrokken en hechten zeer aan het oordeel over Internal Audit. Tot slot is voor de organisatie de vraag: who audits the auditor? met deze toetsing opnieuw expliciet beantwoord."

The governance challenge: a first exploration for internal auditors

In June 2012 the Professional Practices Committee of IIA Netherlands released its latest report on the role internal auditors may play related to the assessment of governance.
Governance is a hot topic. It is the basis of how an organisation is structured, how it operates and how it is managed. So it is essential for internal auditors to understand it, analyse it and assess it. And many of us have to provide an opinion on it. But strangely enough, not many detailed publications are yet available to assist the internal auditor in his or her assessment. This document aims at filling in some of these gaps: it provides a clear overview of all related definitions of the term, it brings a clear framework that could act as a starting point for the analysis, and it formulates a lot of questions that need to be asked when assessing governance.
Positive reaction from Richard Chambers, President and CEO of The Institute of Internal Auditors: "IIA Netherlands recently published what I think is a well written whitepaper on The Governance Challenge." U kunt de publicatie downloaden via www.IIA.nl/vaktechniek.

Gratis Quality Assurance Review

Ook dit jaar voeren de tweedejaarsstudenten bij de module 'Quality Assurance Review' weer praktijkopdrachten uit, waarbij zij een internal auditfunctie aan de hand van de Standards van IIA beoordelen. In groepen van vier personen onderzoeken de studenten, door middel van interviews en het bestuderen van documentatie, zowel de inrichting als het functioneren van de internal auditfunctie.
Doel van deze opdracht is enerzijds om de studenten te laten ervaren hoe een andere dan hun eigen internal auditafdeling in de praktijk functioneert. Anderzijds helpt het de deelnemende organisaties om zich een beeld te vormen van in hoeverre zij conform de IIA Standards werken.

Toetsing
Deelnemende organisaties zien de toetsing als een goede voorbereiding op een periodieke toetsing door IIA. Zij zijn enthousiast over de mogelijkheid die hen wordt geboden om hun IAD tegen het licht te laten houden. Met name de concreetheid van aanbevelingen en de inleving van de studenten in de specifieke situatie waar de desbetreffende auditdiensten zich in bevinden, wordt door de organisaties zeer op prijs gesteld.
De opdrachtgevers bepalen zelf welke medewerkers worden geïnterviewd en welke documentatie ter beschikking wordt gesteld. Verdere factfinding hoeft niet te worden gedaan. Ook worden afspraken gemaakt over vertrouwelijkheid en geheimhouding en het tussentijds afstemmen van bevindingen. Tijdens het laatste college vindt de eindpresentatie door de studenten aan de deelnemende organisaties plaats.
De volgende reviewronde vindt plaats in de periode december 2012-februari 2013. Organisaties die zich voor een review van hun auditdienst willen aanmelden kunnen dit doen door een mail te sturen aan r.kamstra@uva.nl.

Buluitreiking

Op 25 mei 2012 hebben we weer enkele studenten kunnen feliciteren met het behalen van hun bul. In totaal werden zes bullen uitgereikt.
Hassan Khosravi, die helaas niet op de buluitreiking aanwezig kon zijn, schreef een scriptie over het auditen van shared service centres. Jan Somers keek naar de rol van Internal Audit bij control selfassessments, terwijl Heino Lageveen zich richtte op de betekenis van zachte indicatoren op de beheersing van risico's bij bancaire instellingen. Diederic Salis schreef een scriptie over de beheersing van reputatierisico's die kunnen voortkomen uit sponsoractiviteiten en schetste daarbij een model dat de internal auditor kan gebruiken bij het beoordelen van reputatierisico's. Erwin Blom pakte het onderwerp GRC op en ging nader in op de aandachtsgebieden bij de invoering van GRC vanuit het oogpunt van de internal auditor. Steeds vaker wordt de internal auditor gevraagd te kijken naar de beheersing van (grote) projecten; een onderwerp dat door Erik Dijkhuizen werd uitgewerkt.

V.l.n.r.: Erik Dijkhuizen, Heino Lageveen, Diederic Salis, Erwin Blom en Jan Somers

UNIVERSITEIT VAN AMSTERDAM

Uitbreiding Programme Board

Gerben Everts, AFM

Met veel genoegen laten we weten dat per 1 september 2012 Gerben Everts is toegetreden tot de programme board van onze opleiding. Gerben Everts is directeur bij de Autoriteit Financiële Markten (AFM) en verantwoordelijk voor het toezicht op accountantsorganisaties en financiële verslaggeving. Met zijn toetreding is de programme board weer compleet, na het vertrek van prof.dr. Steven Maijoor naar de European Securities and Markets Authority (ESMA).
De programme board van EIAP fungeert als een toetsend en adviserend orgaan ten behoeve van de opleiding en is zodanig samengesteld dat het complete werkgebied van internal auditing wordt afgedekt. Naar functie zijn de leden werkzaam als toezichthouder, voorzitter van een audit committee, CEO, CFO of CRO en hoofd Internal Audit. Ook een hoogleraar op het vakgebied maakt deel uit van de programme board.
De toegevoegde waarde van de programme board voor EIAP zit in het tijdig signaleren en monitoren van relevante ontwikkelingen in de praktijk. Deze ontwikkelingen worden tijdens de vergaderingen besproken en waar nodig doorvertaald naar nieuwe en/of aanvullende opleidingseisen.

Openingscollege

Op 31 augustus 2012 is officieel gestart met de nieuwe lichting studenten van het EIAP. Tijdens het openingscollege hebben de nieuwe studenten kennis kunnen maken met elkaar en met de docenten en is een inleiding gegeven op de opbouw en samenhang van het curriculum. Ook IIA en de alumnivereniging Auditor presenteerden zich aan de studenten.

Kopjaren RO en RE

De opleidingen Internal Auditing & Advisory (RO) en IT-Auditing & Advisory (RE) hebben een kopjaar voor kandidaten die al een postinitiële opleiding hebben afgerond. Zo kunnen RE's, RA's en RC's/CPC's instromen in het kopjaar RO en kunnen RO's en RA's instromen in het kopjaar RE. RC's kunnen via een instroommodule worden toegelaten tot het kopjaar RE. Voor meer informatie: www.esaa.nl of bel met Miranda Snel, tel.: 010-4082437.

Terugblik Toekomst van de public auditor

Mark van Twist (l) en Winfried Beekmans

ESAA organiseerde op 10 mei een bijeenkomst over de 'Toekomst van de public auditor' in Den Haag. Prof.dr. Mark van Twist, wetenschappelijk directeur van de opleiding Internal Auditing & Advisory, sprak over (paradoxen in) de positionering, professionalisering en performance van de public auditor. Drs. Winfried Beekmans MPA, lid van de directie van de Auditdienst Rijk, ging in op de ontwikkelingen in auditing bij de rijksoverheid en de toekomst van de public auditor. Als slot gaf hij de toehoorders mee dat het niet gaat om controle versus advies, om RA, RE of RO, of om wettelijke taken of opdrachten op verzoek, maar om het dienen van het publieke belang. Daarbij staat niet het product centraal, maar de vraag wat de opdrachtgevers daarmee kunnen in een steeds veranderende samenleving.

Module Auditing

Vanaf november 2012 tot en met februari 2013 wordt op vrijdag overdag de module Auditing gegeven. Deze module bestaat uit veertien colleges en maakt deel uit van de reguliere opleiding. Het is mogelijk om voor deze module los in te schrijven.
Voor meer informatie zie www.esaa.nl

Terugblik slotcollege 'Realisatie van Strategie'

Peter Bakhuizen, Havenbedrijf Rotterdam

Het jaarlijks feestelijk aangeklede slotcollege, waarbij ook de bazen en collega's van de studenten worden uitgenodigd, stond 22 juni jl. in het teken van het Havenbedrijf Rotterdam (HbR). Danielle van der Sluijs, concerncontroller, ging in op de strategievorming van het HbR en de betrokkenheid van de auditors in dit proces. Kees Eveleens Maarse (informatiemanager) en Arno Grund (IT-consultant) gaven een kijkje in de keuken van een groot ICT-project dat een bijdrage moet leveren aan de realisatie van de strategie. Ten slotte vertelde Peter Bakhuizen, hoofd Interne Accountantsdienst, dat het jaarverslag van het HbR transformeert naar een verslag waar niet hoofdzakelijk financieel verantwoording wordt afgelegd, maar juist over de realisatie van de strategie. Verder lichtte hij toe dat operational en IT-auditors een steeds grotere rol krijgen naast de registeraccountants.

Aanschuifcolleges

De opleidingen Internal Auditing & Advisory en IT-Auditing & Advisory bieden geïnteresseerden voor de opleidingen de mogelijkheid aan te schuiven bij een regulier college. De colleges worden op vrijdag gegeven. U kunt zich aanmelden voor een college van onder andere de module Governance & Risk Management en Informatiebeveiliging. Zie www.esaa.nl voor meer informatie of neem contact op met Marco van de Meugheuvel, vandemeugheuvel@ese.eur.nl of 010-4082217.

Verdiepingscolleges

Ook dit jaar krijgen de studenten van onze auditingopleidingen binnen een aantal modules een keuzemogelijkheid tussen verdiepingscolleges publieke sector of verdiepingscolleges financiële instellingen.

CIA-examentraining (PE)

De opleiding Internal Auditing & Advisory organiseert in de periode september tot en met begin november 2012 een zestal colleges ter voorbereiding op de CIA-examens part I, II en III. De colleges worden op vrijdag (overdag) op de Erasmus Universiteit Rotterdam gegeven en worden verzorgd door Siebe de Jager. Tijdens de colleges/training wordt gebruikgemaakt van de CIA-reviewboeken van Gleim. Meer informatie over data, kosten en aanmelding op www.esaa.nl of u kunt contact opnemen met Miranda Snel, wsnel@ese.eur.nl of tel.: 010-4082437.

Too big to fail

Dr. J.R. van Kuijck*

Dit jaar is het precies honderd jaar geleden dat de Titanic voor de eerste reis vertrok vanuit Southampton, UK. Destijds het grootste bewegende object ooit geproduceerd door de mensheid. Symbool van de industrialisatie. Badend in weelde waanden vele passagiers zich in veiligheid. Maar helaas, tijdens de 'maiden voyage' op 14 april 1912 zonk het schip na een aanvaring met een ijsberg. In 1985 werden de resten van het schip op de bodem van de Atlantische Oceaan teruggevonden op een diepte van 4 kilometer. Een treurig einde van een onzinkbaar geacht, onoverwinnelijk schip. Je zou een parallel kunnen trekken met de huidige financiële crisis waarin grote banken ten ondergaan, landen failliet dreigen te gaan en er zelfs wordt gespeculeerd over de val van de euro. Of misschien de klimaatverandering die onvermijdelijk rampspoed zal brengen. Mensen denken vaak dat zij de situatie de baas zijn, ja zelfs alwetend zijn. En dat met het uitoefenen van invloed of druk alles maakbaar is. Een grondig misverstand!

Als auditor proberen we een situatie zo goed mogelijk in te schatten en een oordeel te geven dat juist is. Het imago van de onfeilbare auditor. Dat wordt van ons verwacht door de buitenwacht. Maar is dat oordeel wel altijd juist? Het probleem is dat een auditor als basis voor de analyse een beeld creëert van de werkelijkheid. Helaas kan dat door allerlei factoren afwijken van de werkelijkheid. Ja, het kan zelfs ons begrip van de werkelijkheid vertekenen. Niet in de laatste plaats door het gebruik van metaforen en gebruikte formuleringen. We kaderen immers ons begrip van de situatie in, wat kan leiden tot een eenzijdige of onjuiste belichting van de problematiek. In feite is het beeld dat ontstaat van de werkelijkheid gekleurd, en dus persoonsgebonden. De auditor zal dus maatregelen moeten nemen om de objectiviteit ook hier te borgen en ervoor te waken dat geen vertekening optreedt. In dit kader is het aardig om nog eens *Images of organization* van Gareth Morgan te lezen.

Op verschillende momenten in het beoordelingsproces van de auditor kan het fout gaan. De waarneming van de auditor is selectief en de interpretatie kan arbitrair zijn. De auditor graaft in zijn geheugen en interpreteert de nieuwe gegevens in het licht van de bij hem aanwezige kennis. Maar is die kennis wel juist of is deze misschien achterhaald? Immers, de kennis van de auditor is ook weer een subjectieve interpretatie van de werkelijkheid. Kortom, onzekerheid troef. Daarom is het belangrijk dat de auditor nadrukkelijk oog heeft voor het objectiveren van zijn oordeel. De essentie ligt uiteraard in een grondig onderzoek. Een aanpak gebaseerd op principes van triangulatie en een analyse met objectieve criteria. Daarnaast helpt het als een betrokken collega of expert het oordeel beoordeelt en het ermee eens is. Echter, als iedereen het ermee eens is, wil dat nog niet zeggen dat daarmee het ware beeld is geschapen. Consensus of intersubjectiviteit alleen is een slechte raadgever voor een auditor.

Daarom is het belangrijk dat we als auditor over onze schaduw heen durven te stappen. We moeten onze beeldvorming nadrukkelijk challengen. De tijd nemen en bereid zijn om te twijfelen aan het eigen oordeel: zie ik het wel goed? Is de conclusie hetzelfde als ik het vanuit een andere invalshoek of een ander perspectief bekijk? Kan ik andere relevante criteria toepassen? Daarmee kan de onfeilbaarheid van ons oordeel toenemen en zal dit bijdragen aan een solide imago!

* Actief in Serum Consultancy (www.serum.nl), Orange Executive Search (www.orangesearch.nl) en Lime Tree Research & Education (bvk@limetree-research.nl).

Unlocking the power of GRC technology

Organizations today are struggling with managing risks across the enterprise. External and internal requirement are becoming increasingly complex and intrusive, while demand for more comprehensive consolidated and actionable governance, risk and compliance (GRC) information continues to increase. In order to keep up with these requirements, and to prevent risk management from becoming an operational and financial burden, an integrated approach to your organization's infrastructure, processes and resources is essential.

This is the right time to learn about opportunities to transform your risk management program by enabling GRC technology that can:

- Create improved visibility and integration by linking risk and control frameworks
- Lower the cost of risk management through the elimination of duplicate and fragmented risk activities and minimization of manual processes
- Increase efficiencies through automation and end-to-end process centralization

Our recent Ernst & Young's Global survey of more than 250 leading organizations found a direct link between effective risk management practices and improved financial performance. Harnessing the power of GRC technology to improve risk information, streamline processes and reduce costs was both the biggest opportunity and challenge in achieving the needed risk management maturity.

Ernst & Young has the knowledge and practical experience in processes, risks and GRC technology to assist you to turn your risks and opportunities into results.

For more information, please visit www.ey.com/nl

Partners in Sport

Tonny Dekker
Risk Advisory Leader
+ 31 (0)88-407 10 04
tonny.dekker@nl.ey.com

Frank Leenders
GRC Leader
+ 31 (0)88-407 88 12
frank.leenders@nl.ey.com

BWise® Internal Audit

In control met de meest geavanceerde Governance, Risicomanagement en Compliance software

Take control
Stay ahead

BWise® Internal Audit, onderdeel van het geïntegreerde BWise Governance, Risicomanagement en Compliance (GRC) Platform, is een software oplossing die de internal audit processen ondersteunt. Om de toenemende verantwoordelijkheden van internal audit te stroomlijnen zorgt BWise ervoor dat audit kan werken in hetzelfde systeem als andere afdelingen zoals risk, compliance en de business, met behoud van haar onafhankelijkheid.

Dit helpt internal audit om in een veilige omgeving te werken en gebruik te maken van dezelfde risico taxonomie en risico terminologie binnen de organisatie. Op deze manier wordt het audit proces geoptimaliseerd en worden dezelfde doelen nagestreefd. Ann Green en haar collega's hebben BWise® Internal Audit geselecteerd om op efficiënte wijze de jaarlijkse audit plannen en documentatie te kunnen creëren en efficiënt de audit te kunnen uitvoeren voor de opvolging van bevindingen en aanbevelingen. BWise® Internal Audit is voorzien van moderne technieken, zoals **Audit Analytics** en **Continuous Monitoring**, om alle audit activiteiten te automatiseren.

Vraag voor meer informatie over BWise® Internal Audit de brochure "A Day in the Life of Ann Green" aan, of ga naar www.bwise.nl/grc-library

BWise® Internal Audit is één van de zes, op rollen gebaseerde, software oplossingen die BWise biedt. De andere rollen zijn Risk Management, Internal Control, Compliance en Policy management, IT GRC en Sustainability Performance Management.

BWise, een NASDAQ OMX onderneming, is wereldwijd marktleider op het gebied van Governance, Risicomanagement en Compliance software. BWise ondersteunt organisaties wereldwijd bij het traceren, meten en managen van alle bedrijfsrisico's in één geïntegreerd systeem.

gebruik uw smartphone om de QR-code te scannen voor meer informatie

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY
www.bwise.nl