AUDIT magazine

Magazine voor internal en operational auditors

nummer 2 juni 2010

thema:

Governance Risk Compliance (GRC)

GRC: een veelbesproken term

De praktijk rondom GRC: wat, waarom en hoe?

Een gebrek aan cultuur?

Instituut van Internal Auditors Nederland

SVRO Stichting Verenigde Operational Auditors

Concurreren wordt steeds verantwoorder*

Wie als ondernemer serieus genomen wil worden, moet tegenwoordig meer laten zien dan alleen transparantie op financieel gebied. Juist openheid en zekerheid over niet-financiële informatie kunnen het verschil maken. Stakeholders, zoals toezichthouders, analisten, maar ook toekomstige medewerkers en potentiële klanten, eisen steeds vaker en nadrukkelijker betrouwbare informatie over zaken als kwaliteit van de dienstverlening en zorg, belasting van het milieu en maatschappelijke verantwoordelijkheid.

Daarom is het nu tijd voor een reset. Tijd om niet-financiële resultaten betrouwbaar en transparant te presenteren. Uit maatschappelijk oogpunt, maar vooral voor de zaak. Want zeker in een nieuwe wereld waarin aanbieders elkaar steeds minder ontlopen, worden openheid en zekerheid over niet-financiële informatie dé onderscheidende factor.

Wie de concurrentie op een transparante verantwoording nu aan gaat, is de winnaar van morgen.

Jan van der Hilst
PricewaterhouseCoopers

*connectedthinking

PRICEWATERHOUSECOOPERS

Assurance • Tax • Advisory pwc.nl

GRC is hot

GRC... een term waar je alle kanten mee uit kunt en waar iedereen iets anders onder kan verstaan. Zoveel is ons als redactie de afgelopen maanden wel duidelijk geworden. Typ 'GRC' in Google in en je komt op ruim 2 miljoen hits. Mocht je al meteen denken GRC is 'governance, risk en compliance' (Google geeft ook weer: GRC: geothermal resources council), dan nog kan de een vinden dat GRC draait om de integratie van deze functies terwijl de ander GRC ziet als een verzameling van allerlei detailed controls.
Hoe het ook zij, GRC is hot. Reden voor de redactie om GRC te verheffen tot het thema van dit nummer. Maar ook volop reden om met de thema-artikelen in kaart te brengen wat GRC nu eigenlijk is, wat er in de praktijk plaatsvindt rondom GRC en welke tools behulpzaam kunnen zijn.

In dit nummer wordt duidelijk wat GRC kan betekenen voor de organisatie en uiteraard ook voor ons als auditors. En dat is niet mis. GRC is, wellicht juist nu met de ervaringen van de kredietcrisis achter ons, een antwoord op de vraag waar risico's nu echt om draaien en hoe daarmee om te gaan. Immers, als vakgebieden binnen een organisatie als silo's functioneren leidt dit niet alleen tot veel inefficiëntie, maar kunnen mogelijk ook die risico's waar het echt om draait, gemist worden. Niet zo vreemd dat GRC daarom volgt na het vorige thema van *Audit Magazine*: 'Waartoe zijn wij op aard?' GRC is geen wondermiddel, geen gemakkelijke pleister die je opplakt, uiteindelijk draait het toch altijd om gezond verstand. Maar met dit gezonde verstand kan met GRC heel veel bereikt worden.

Veel leesplezier!

De redactie van *Audit Magazine*

IT biedt onbegrensde mogelijkheden.

Wat vraagt uw organisatie?

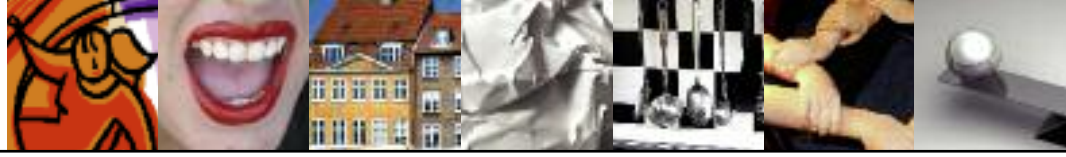
IT Governance en IT Performance vragen aandacht, adviezen zijn er volop en oplossingen lijken grenzeloos. Maar hoe weet u of u de juiste keuze maakt? KPMG IT Advisory adviseert onafhankelijk en deskundig, maakt risico's beheersbaar en zorgt ervoor dat IT optimaal bijdraagt aan uw business. Nu en in de toekomst.

Meer weten? Bel: (020) 656 8021

KPMG

AUDIT ▪ TAX ▪ ADVISORY

inhoud



thema GRC

verder in dit thema

rubrieken

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: Jansen.Ronald2@kpmg.nl **Redactieraad:** F. Steenwinkel (voorzitter), Th. Smit RA CIA, G.M. van Gameren RA RO **Redactie:** drs. R.H.J.W. Jansen RO (voorzitter), drs J.F. Breedveld, drs. N.J. Engel-de Groot, drs. R.J.A.C. Jansen RO, drs. R. Kamstra CIA, drs. H.A. Mulders RA RC, drs. L.Z. Nagy RO EMIA, drs. D.L. Stabel RE 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:** drs. J.Y. Groenink, jeannette@vm-uitgevers.nl **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

GRC: een veelbesproken term

Bij veel organisaties ontstaat een toenemende noodzaak tot transparantie en efficiëntie in risicobeheersing en kwaliteitsverbetering. GRC wordt hiervoor vaak genoemd als oplossing. Maar wat is er met GRC te bereiken? En wat is de eerste stap? In dit artikel wordt GRC in simpele, duidelijke bewoordingen gedefinieerd. Daarnaast wordt beoogd lezers die overwegen de eerste stappen op dit terrein te zetten, of daar inmiddels al mee zijn begonnen, een duwtje in de rug te geven.

M.But en M. Groenenboom

Op verschillende fora en in vakbladen wordt uitgebreid aandacht besteed aan het onderwerp governance risk compliance (GRC). Desondanks blijft vaak onduidelijk wat de term GRC nu precies inhoudt. Wat opvalt aan de publicaties is de terugkerende belofte een definitie van GRC te geven. Hier wordt echter vaak weinig invulling aan gegeven door direct in te gaan op een bepaald aspect van GRC, zoals GRC-software, controlraamwerken of ERM. In die publicaties waarin wel een omschrijving is opgenomen, wordt GRC op verschillende manieren uitgelegd. Enkele voorbeelden:

- Buith en Van Grinsven (2009) zien GRC als een middel om het huidige silodenken te doorbreken tussen business units, functionele processen, geografie en technologie.
- Heijmans (2009) gaat verder in op de raakvlakken tussen de drie gebieden. Zij geeft in haar artikel *Taken en verantwoordelijkheden Governance, Risk & Compliance* aan dat er behoefte is om de verschillende assurancefuncties zodanig te positioneren dat zij elkaar aanvullen en er geen witte vlekken of doublures in werkzaamheden bestaan. De implementatie van een GRC-raamwerk kan dit inzichtelijk maken. Heijmans omschrijft GRC als een gestructureerde aanpak van alle governance-, risk- en compliance-initiatieven in de organisatie.
- Een definitie die gedeeltelijk overeenkomt met de voorgaande komt van Beugelaar en Van Loon (2010) en luidt: ‘GRC betreft een volledig geïntegreerd denken en werken volgens een efficiënt en effectief businessmodel, waarbij eenduidigheid bestaat over alle binnen het GRC-domein uit te voeren werkzaamheden, van strategiebepaling tot en met de uiteindelijke rapportage en effectmeting en een goede samenwerking en afstemming met de activiteiten buiten dit GRC-domein’.
- Ter Heegde (2009) ziet de term GRC breder en benadrukt ook het sturingsaspect in zijn definitie: ‘GRC verwijst naar het meer brede vraagstuk van control (sturing en beheersing) van de maatschappelijke onderneming, waarin begrepen de wijze waarop de maatschappelijke ondernemer sturing geeft aan afdelingen en bedrijfsprocessen, de relatie met de doelstellingen van de maatschappelijke onderneming, de samenhang met de risico’s die het realiseren van doelstellingen in de weg staan, de wijze (overleg, rapportage, audits) van afleggen van verantwoording over het resultaat van het sturen op doelstellingen, de inhoud van die verantwoording en het treffen en naleven van maatregelen die zijn opgenomen in relatie tot mogelijke oorzaken van bepaalde risico’s’.
- BWise definieert GRC als ‘de geïntegreerde benadering die bedrijven toepassen om sterke governance binnen een organisatie neer te zetten door middel van risicomanagement en bewezen compliance’ (www.bwise.nl; 30 maart 2010).

Opvallend aan deze definities is dat in iedere beschrijving in meer of mindere mate aandacht wordt besteed aan het aspect ‘integratie’. Deze integratie kan zich richten op de integratie van raamwerken, kennis of werkzaamheden. Daarnaast wordt vaak verwezen naar een gestructureerde manier van introduceren en implementeren van een bepaalde manier van denken en werken. Voordat er antwoord wordt gegeven op de vraag: wat is GRC? wordt eerst de vraag beantwoord: wat is GRC niet? Dit om te voorkomen dat de term alsnog tot verwarring leidt en een containerbegrip wordt.

Wat is GRC niet?

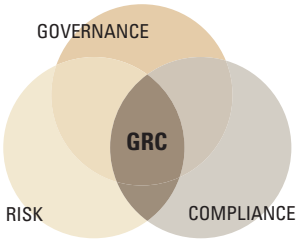
GRC staat voor de drie vakgebieden governance, risk en compliance. Dit geeft aan dat het om een traject gaat waar alle drie de gebieden vertegenwoordigd zijn. Een initiatief dat wordt gestart vanuit een van deze functies en waar slechts deze ene functie profijt van heeft, kan dus niet gezien worden als een GRC-traject. Een dergelijk initiatief zou wel kunnen dienen als startpunt van waaruit GRC zich als een olievlek verspreidt binnen de organisatie.

Hoewel in de definitie de nadruk ligt op de integratie van de functies, betekent dit niet dat de drie functies samengevoegd dienen te worden tot één functie. De nadruk ligt op de samenwerking tussen deze functies terwijl deze onafhankelijk van elkaar blijven opereren. In financiële instellingen is het zelfs een eis dat de functies onafhankelijk blijven.

Er zijn verschillende leveranciers die pretenderen GRC-software te leveren. Echter, na een verdieping in de functionaliteiten blijkt vaak dat deze zich slechts richten op een beperkt aandachtsgebied zoals procesbeschrijvingen, documentmanagement of performancemanagement. De implementatie van een dergelijk pakket maakt het daarmee nog geen implementatie van GRC.

Definitie GRC

Om tot een omschrijving te komen van de term GRC is gebruikgemaakt van de hiervoor genoemde definities. Daarnaast zijn de discussies en het onderzoek van de themadag 'Auditing, compliance en riskmanagement: een drie-eenheid of ieder voor zich?' als input gebruikt. Tot slot hebben onze ervaringen vanuit opdrachten bij verschillende organisaties een bijdrage geleverd. Op basis hiervan is het volgende antwoord geformuleerd op de vraag: wat is GRC? 'GRC is een verzameling activiteiten die zich richt op de integratie van de visievorming op governance, risk en compliance en de integratie van de uitvoering van deze functies binnen een organisatie. Dit met als doel efficiëntie, effectiviteit en transparantie te creëren om te komen tot continue interne beheersing' (zie *figuur 1*).



Figuur 1. GRC

Onder integratie van de uitvoering verstaan wij niet het samenvoegen van de drie functies, maar een betere afstemming van werkzaamheden met behoud van de three lines of defence.

Wat levert GRC op?

Nu er een duidelijk beeld is van hetgeen wel en niet onder GRC wordt verstaan, is de volgende vraag wat dit oplevert voor organisaties. In de nabije toekomst zal de roep om efficiëntie alleen nog maar sterker worden. Dit geldt niet alleen voor het bedrijfsleven, maar wordt ook vanuit de overheid uitgedragen aan bijvoorbeeld instanties in de zorgsector. Zo wordt in het rapport *Zorg voor minder last* gepleit voor een betere regulering van de regeldruk. Verantwoordelijkheden voor de uitvoering van controls worden door de implementatie van GRC duidelijker belegd in de lijnfuncties. Hierdoor worden de controleigenaren niet meerdere keren bevraagd over hetzelfde onderwerp door verschillende functionarissen.

Audit, risk en compliance zullen, onder andere om de onafhankelijkheid te waarborgen, zelfstandig blijven bestaan als functies binnen organisaties. Echter, om de beheersing op een efficiënte en effectieve manier te waarborgen, zullen de werkzaamheden beter moeten worden afgestemd. Door gebruik te maken van elkaars inzichten, resultaten en expertise kunnen de drie functies zich meer gaan richten op de eigen kerntaken.


Illustratie: Roel Ottow

Verantwoordelijkheden die in de organisatie duidelijker belegd zijn en werkzaamheden die niet meer dubbel worden uitgevoerd zullen leiden tot een effectievere en efficiëntere manier van werken. En dit zal uiteindelijk leiden tot kostenbesparing in de beheersing. Zo moet het merendeel van de organisaties voldoen aan zowel de Wet bescherming persoonsgegevens (Wbp) als aan de richtlijnen ten aanzien van informatiebeveiliging. Hier is sprake van doublures. Het realiseren van een geïntegreerd controlraamwerk zorgt voor een efficiëntieslag van minimaal 30 procent. GRC-implementaties en GRC-tooling zorgen ervoor dat inzichtelijk wordt gemaakt waar sprake is van redundantie en hiaten in de werkzaamheden. Daarnaast kan met behulp van GRC-tooling realtime integraal inzicht worden verkregen over de in control-status van de organisatie op ieder willekeurig moment. Met deze inzichten kunnen directie en hoger management waar nodig sturing geven. De gerealiseerde doelen van GRC hebben hiermee

GRC-resultaten

- Realtime inzicht in de in controlstatus
- GRC-functies terug naar kerntaken
- Duidelijk belegde verantwoordelijkheden in de lijn

Figuur 2. Resultaten GRC

effect op zowel het uitvoerend, tactisch als strategisch niveau binnen organisaties (zie *figuur 2*).

Waar te beginnen?

Om van een GRC-implementatie een succes te maken zal allereerst een visie ontwikkeld moeten worden ten aanzien van GRC. In dit artikel is hiervoor een aanzet gedaan. Vorm deze visie in de top van de organisatie om verschil in inzichten te voorkomen, betrokkenheid op hoog niveau te creëren en legitiem de verzuiling te doorbreken. Om een goed startpunt te bepalen is het aan te raden om een aantal inventarisaties uit te voeren. Dit om een goed beeld te krijgen van de omgeving waarin een GRC-traject wordt gestart.

Inventariseer vooraf welke informatie over de in controlstatus reeds beschikbaar is binnen de organisatie. Vraag deze informatie op en voer hier een review op uit om de status van de huidige uitwerkingen van controls te bepalen. Inventariseer ook welke grote projecten, zoals Solvency II of de invoering van VMS, uitgevoerd worden en benoem welke impact ieder project heeft op een GRC-traject. En als laatste, inventariseer hoe het systeemlandschap van de organisatie eruit ziet om aan te geven welke software is geïmplementeerd binnen de organisatie.

Op basis van deze inventarisaties kan het GRC-traject worden aangepast aan de omgeving waarin het traject wordt uitgevoerd. Zoals bij veel veranderingen het geval is, is het zetten van de eerste stap tevens de moeilijkste. Iedere verandering levert weerstand op, ook al betekent dit op termijn vooruitgang. Door te verhelderen wat onder GRC wordt verstaan en welk resultaat het oplevert, hopen we dat de drempel om deze stap te nemen kleiner is geworden en de invulling ervan de kwaliteit krijgt die het verdient.

Marvin But en Merlijn Groenenboom zijn beiden werkzaam bij AuditMatch en GRC.nl. In de rol van consultant hebben zij bij verschillende organisaties ervaring opgedaan met governance-, risk- en compliancevraagstukken.

Literatuur

- Buith, J. en J. van Grinsven, 'GRC nader verklaard', *financieel-management.nl*, 15-12-2009.
- Heijmans, J.M., 'Governance, Risk & Compliance', *Finance & Control*, p. 30, december 2009.
- Beugelaar, B. en W.A.J. van Loon, 'Geslaagd GRC binnen handbereik', p. 11 *Compact.nl*, januari 2010.
- Groenenboom, M. en S. Arnhem,.'Auditing, compliance en riskmanagement: een drie-eenheid of ieder voor zich?' *Audit Magazine*, p. 46-47, maart 2009.
- Heegde, J. ter, 'De maatschappelijke onderneming in zwaar weer', *zbc.nu*, ZBC kennisbank, 27 november 2009.
- *Zorg voor minder last* (rapport), ministerie van Financiën, p. 2, juli 2007.

De praktijk rondom GRC:

wat, waarom en hoe?

GRC is een vakgebied waarbij verschillende partijen betrokken zijn. Adviseurs zien het brede palet bij organisaties, producenten integreren de ontwikkelingen in hun tools en de gebruikers zijn uiteindelijk aan zet om de keur aan adviezen en hulpmiddelen naar hun merites te beoordelen. Wat speelt er zoal rondom GRC? *Audit Magazine* zet de meningen op een rij.

De **ADVISEURS** aan het woord

M. But, Audit Match en GRC.nl

1. Waarom moeten organisaties kiezen voor/nadenken over GRC?
"Wij zien een ontwikkeling in de werkzaamheden van audit-, risk- en compliancefuncties die steeds dichter tegen elkaar aan komen te liggen. Door GRC wordt inzichtelijk gemaakt waar sprake is van redundantie en hiaten in de werkzaamheden. Doordat audit-, risk- en compliancefuncties gebruik kunnen maken van elkaars inzichten, kennis en resultaten wint de organisatie aan efficiency en dat leidt uiteindelijk tot kostenbesparingen. Daarnaast biedt GRC de mogelijkheid om het management realtime integraal inzicht te geven in de controlstatus en daarop te sturen. Dit zorgt voor een verschuiving van periodieke externe verantwoording naar continue interne beheersing."

2. Wat zijn de do's en don'ts ten aanzien van GRC-implementaties?
"De do's zijn:

- Een top-downbenadering om verzuiling van de gebieden audit, risk en compliance te doorbreken.
- Draagvlak creëren bij de top door de quick wins op inzicht en efficiency te tonen en in vervolg hierop structurele kwaliteitsverbetering te realiseren.
- Keypersonen betrekken vanuit de eerste, tweede en derde lijn van de organisatie.
- Software selecteren die zich primair richt op GRC-functionaliteiten in tegenstelling tot software die dit pretendeert zoals procesbeschrijvingstools.
- De implementatiemethode aanpassen naar grootte, volwassenheid en complexiteit van de organisatie.

De don'ts zijn:

- Grootschalig diverse normen, wet- en regelgevingen ineens implementeren aan de hand van een GRC-traject.
- Het GRC-raamwerk als iets statisch beschouwen: met alleen een raamwerk ben je er niet, dit moet continu geëvalueerd en geactualiseerd worden.

> In de toekomst zal de roep om efficiency sterker worden

- Implementatie van GRC enkel beschouwen als een software-implementatie en alleen een GRC-softwareleverancier erbij betrekken.
- Een afwachtende houding aannemen tot zichtbaar wordt dat de beheersing onvoldoende is.
- Van GRC-implementatie een eenzijdige exercitie maken van de derde lijn."

3. Heb je tooling nodig om GRC te implementeren?
"Een tool ondersteunt op verschillende manieren de implementatie van GRC, zoals het doorbreken van de verzuiling. Door de inzet van een tool kan op korte termijn realtime inzicht in de status van beheersing en efficiency worden gerealiseerd. De omvang, samenhang en complexiteit (het creëren van een operationeel raamwerk, hiërarchie aanbrengen in controls, relaties leggen tussen control en meerdere organisatie-entiteiten, de in controlstatus bekijken vanuit verschillende invalshoeken) van GRC-implementaties zorgen ervoor dat de inzet van een tool randvoorwaardelijk is voor het slagen van een dergelijk traject."

4. Welke toekomst voorziet u voor GRC?
"In de toekomst zal de roep om efficiency sterker worden, is het ondenkbaar dat de drie functies audit, risk en compliance onafhankelijk van elkaar zullen blijven opereren en zal er een verschuiving plaatsvinden van periodieke externe verantwoording naar structurele interne beheersing. Om in deze behoefte te voorzien zullen GRC-implementaties en GRC-tooling steeds meer van belang zijn voor organisaties."

Marvin But is werkzaam bij AuditMatch en GRC.nl. In de rol van consultant heeft hij ervaring opgedaan met governance-, risk- en compliancevraagstukken bij verschillende organisaties.

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

1. Waarom moeten organisaties kiezen voor/nadenken over GRC?
"Bedrijven hebben vaak geen idee hoeveel hun interne beheersing wérkelijk kost en wat het ze oplevert. Stafafdelingen helpen de organisatie in control te krijgen en te houden; ieder vanuit de eigen expertise. Onvoldoende samenwerking leidt tot overlap, extra kosten en schijnzekerheid. Inzicht in de echt belangrijke risico's en de mate van beheersing blijken vaak ontransparant of foutief door de veelheid aan risicodefinities, risk- en controlframeworks, loss-, issue- en incidentdatabases, afwijkende risk- en controlratings en assessmentmethodieken. GRC leidt tot beter managen en transparant beheersen van alle risico's en reductie van interne beheersingskosten."

2. Wat zijn de do's en don'ts ten aanzien van GRC-implementaties?
"Implementatie van een sustainable GRC-systeem is geen sinecure. Het verkrijgen van een gezamenlijk gedragen beeld van de organisatierisico's en hoe deze te beheersen is al lastig, het veranderingsproces is nog lastiger. GRC-implementatie kost geld, tijd en commitment. GRC leidt tot verandering in cultuur en gedrag omdat moet worden samengewerkt en bestaande structuren van afdelingen en verantwoordelijkheden worden doorbroken. In de praktijk is het samensmelten van diverse risico- en controlframeworks een goede eerste stap in dit proces. Aandacht voor communicatie en verandermanagement is daarom cruciaal. Zonder uitgesproken commitment en sponsorship vanuit de hoogste leiding mislukt GRC. Een gefaseerde uitrol is vaak ideaal. Start met die GRC-activiteiten die de meeste winst voor de business opleveren. Het ideale GRC-model is afhankelijk van de organisatie."

3. Heb je tooling nodig om GRC te implementeren?
"Ja. GRC beoogt om op een zo efficiënt mogelijke manier aantoonbaar in control te komen en te blijven. De complexiteit van de risico- en controlomgeving is vaak groot. Tooling vereenvoudigt significant het plannen van reviews, audits, product approvalprocessen, procesbeheersing, risico- en controlframeworks, loss-, issue- en incidentdatabases, het vastleggen van de review en de testresultaten en de follow-up."

4. Welke toekomst voorziet u voor GRC?
"GRC zal leiden tot een zo efficiënt mogelijke inrichting van de interne beheersingsfunctie. Discussies zullen ontstaan over het lines of defensemodel, embedded testing en het inrichten van methodieken om op continue basis te monitoren en te auditen (continuous auditing/continuous monitoring). Het huidige machtsblok van finance, hr, planning & control, risicomanagement, interne beheersing en audit wordt grotendeels afgebroken en een nieuwe structuur ontstaat. Ook het management moet mee. Het uitgangspunt is 'doing the right things the first time right': een efficiënte manier van een effectieve beheersing. Interne beheersing zal een belangrijke rol spelen bij de winstgevendheid van de onderneming door kostenverlaging en verhoging van transparant inzicht in mogelijkheden, risico's en effectieve time-to-market."

Drs. W.A.J. van Loon is senior manager bij KPMG Advisory en werkzaam op het vlak van GRC, Internal Audit en (operational) risk management. Daarnaast doceert hij aan de EMIA-opleiding aan de Universiteit van Amsterdam.

J. Buith RE CISA CISSP en ir. D. Janmaat CIA CISA, Deloitte Enterprise Risk Services

1. Waarom moeten organisaties kiezen voor/nadenken over GRC?
"In de meeste organisaties is het thema governance, risk en compliance belegd als een discrete activiteit die losgekoppeld is van de primaire bedrijfsprocessen en het besluitvormingsproces. Governance, risk en compliance als proces heeft duidelijk minder aandacht gekregen vanuit performanceverbetering en procesreengineering dan kernthema's als supply chain, customer centricity, hr en financetransformatie. Slechts recentelijk heeft GRC ook de nodige aandacht gekregen binnen de IT-strategie, IT-projecten en IT-ondersteunende processen. Kortom, de infrastructuur, processen en systemen voor GRC zijn onvoldoende ontwikkeld, met als gevolg dat de meeste ondernemingen risicomanagement en compliance gefragmenteerd hebben ingericht en vanuit 'silodenken' deze programma's beheersen en daar tegen een aantal problemen aanlopen."

2. Wat zijn de do's en don'ts ten aanzien van GRC-implementaties?
"Focus op de daadwerkelijke issues en de uitdagingen voor verbetering. Blijf zeker niet hangen in de discussie rondom de terminologie en de afbakening van deelgebieden. Definieer een duidelijke afbakening, doelstellingen, policies en procedures. Leiderschap rondom GRC moet belegd worden bij het hoogste management om daadwerkelijke verbeteringen mogelijk te maken. Definieer een duidelijk eindplaatje voor geïntegreerde GRC voor de eigen organisatie. Het is nu tijd om andere dingen te doen en dingen anders te doen! Alleen dan zullen ook de voordelen van de integratie van GRC duidelijk worden."

3. Heb je tooling nodig om GRC te implementeren?
"Informatietechnologie is onlosmakelijk verbonden met GRC. Enerzijds door het automatiseren van een GRC-database en het faciliteren van de GRC-functionaliteit zoals het assurancemodel, ondernemingsbrede risico's, het in kaart brengen van controledeficiënties en actieplannen en het rapporteren van de letter of representations. Anderzijds zeker ook door het geautomatiseerd uitvoeren van interne controlehandelingen en het op continue basis monitoren van transactiedata om risico-evenementen direct te rapporteren aan de verantwoordelijke manager of compliance-afdeling, inclusief workflowfunctionaliteit."

4. Welke toekomst voorziet u voor GRC?
"Bedrijven zullen zich in de toekomst richten op standaardisatie, betere performance- en risicomanagementcoördinatie, de toenemende verwachtingen van corporate responsibility en belangrijke wijzigingen in GRC-technologieën. GRC-technologie-aanbieders zullen door klanten worden aangespoord additionele functionaliteit te leveren voor ERM, versterkte integratie met business intelligence en betere en meer flexibele performance management applications.

Jacques Buith en David Janmaat zijn beiden werkzaam bij Deloitte Enterprise Risk Services. Buith is partner governance, risk en compliance. Janmaat is senior consultant governance, risk en compliance.

Drs. W.G.M.J. van Haelst RE RA, CSI Netherlands

1. Waarom moeten organisaties kiezen voor/nadenken over GRC?
"De 'GRC-problematiek' is natuurlijk niet nieuw. Echter, door zowel externe als interne factoren komt GRC meer op de agenda van het management en wordt nagedacht over de invulling ervan binnen de organisatie. Externe factoren liggen onder andere in de toenemende wet- en regelgeving met betrekking tot goed ondernemerschap en het zichtbaar in control zijn ('show me' in plaats van 'trust me'). Interne factoren hebben betrekking op de toenemende complexiteit van IT-toepassingen bij bedrijven. De grote afhankelijkheid van dergelijke IT-systemen dwingt bedrijven om risico's en beheersingsmaatregelen inzichtelijk en toetsbaar te maken."

2. Wat zijn de do's en don'ts ten aanzien van GRC-implementaties?
"Bij een GRC-implementatie moet aandacht worden besteed aan de factoren mens, proces en technologie. Hierbij krijgt de factor technologie vaak de meeste aandacht en zijn de andere factoren ondergewaardeerd. Als het om de factor mens gaat wordt het nut en de noodzaak van de GRC-implementatie niet door de organisatie begrepen. Het blijven dan vaak 'speeltjes' van de internal control- en/of internal auditafdeling. Bij de factor proces zijn relevante processen vaak onvoldoende uitgediept. GRC-implementaties vergen meer dan een 'hoog over' risicoanalyse en het vastleggen van zoveel mogelijk interne beheersingsmaatregelen."

3. Heb je tooling nodig om GRC te implementeren?
"De laatste jaren komen veel GRC-producten op de markt. Echter, het adagium 'a fool with a tool is still a fool' geldt ook hier. Waar het bij GRC-implementaties om draait is de inhoud c.q. de content. Zorg dus voor een adequaat fundament dat is verankerd in de organisatie en de processen. GRC-tooling kan vervolgens helpen bij zowel de documentatiefase, de (geautomatiseerde) testfase en het continue monitoringproces. Tooling helpt dus wel degelijk, maar is geen doel op zich."

4. Welke toekomst voorziet u voor GRC?
"Vanuit onze jarenlange ervaring op dit vakgebied voorzien wij een verhoogde aandacht voor GRC. Bedrijven staan te popelen om GRC-projecten te implementeren; de gevolgen van de crisis weerhouden de meeste er echter nog van. Nut en noodzaak begint door te dringen bij het management. Wij verwachten wel dat veel bedrijven de volwassenheidscurve zullen doorlopen: aanvangen met mooi ogende tools en er vervolgens achterkomen dat de inhoudelijke kant nog niet op orde is/was. Bezint eer gij begint!"

Werner van Haelst is managing partner van CSI Netherlands bv. CSI is een team van GRC-professionals die diensten, training en softwareoplossingen levert, gericht op de audit, security & control-aspecten van SAP-omgevingen. Daarnaast doceert hij aan de IT-Auditingopleiding aan de Erasmus Universiteit Rotterdam.

De **PRODUCENTEN** aan het woord

C. Dobbelaar, BWise

1. Wat is de toegevoegde waarde van uw tooling voor de organisatie?

"BWise levert een bedrijfsbreed softwareplatform voor het implementeren en verankeren van GRC-initiatieven in organisaties. Veel voorkomende GRC-initiatieven bij onze klanten zijn om het met behulp van technologie interne controle, risicomanagement en Internal Audit in te richten en te verbeteren. De manier waarop een klant onze software inzet varieert per organisatie. Zo ook de toegevoegde waarde van BWise. Generiek gezien leidt het gebruik van BWise tot de volgende voordelen: 1. beter inzicht/vertrouwen in financiële informatie en rapportage; 2. kostenbesparing door een reductie van dubbele handelingen en key controls; 3. het verminderen van (interne controle) risico's; 4. verbeterde winstgevendheid door betere sturing en minder operationele fouten."

2. Wat is de toegevoegde waarde van uw tooling voor IA?

"BWise biedt een internal auditmodule waarbinnen in een beveiligde auditomgeving werkdocumenten inclusief supporting evidence kunnen worden hergebruikt en men gebruik kan maken van een set van audit best practices. Verder biedt BWise vanzelfsprekend functionaliteiten zoals auditplanning, het inplannen van resources, issuemanagement, audit workflows en uitgebreide auditrapportage met voor alles een volledige audittrail. Het onderscheidend vermogen zit in het feit dat BWise Internal Audit een geïntegreerd onderdeel is van het GRC-platform. Hierdoor kijken alle stakeholders naar één versie van de waarheid: dezelfde data. Deze manier van werken leidt niet alleen tot meer begrip voor elkaars werkzaamheden, ook qua efficiency en benchmarking biedt dit grote voordelen."

3. Op welke wijze dient de tooling geïmplementeerd te worden?

"BWise levert een standaard softwareoplossing die voor elke klant wordt geconfigureerd om aan te sluiten bij de door de organisatie gehanteerde (internal audit)methodologie en reeds bestaande GRC-processen. Onze consultants hebben veel ervaring en maken gebruik van een best practice-aanpak. Dit leidt tot een kortere implementatietijd en verankering in de organisatie waarbij we klanten laten profiteren van onze kennis en ervaring. Waar gewenst kan de best practice worden aangepast aan klantspecifieke eisen, elke organisatie is immers uniek."

4. Welke toekomst voorziet u voor uw tooling?

"Als gevolg van de wereldwijde crisis neemt ook de regelgeving toe. Daardoor wijzigen bedrijven hun risicobeheer van een 'siloaanpak' in een meer holistische benadering. Van Internal Audit wordt verwacht dat zij zekerheid verschaft over de effectiviteit en betrouwbaarheid van de eerste en tweede lines of defense en daarmee het controleren van het beheer van de risico's. De vraag naar een geïntegreerd GRC-platform zal toenemen omdat deze technologie onmisbaar is bij het afbreken van de verschillende silo's en het managen van een multi-complianceframework. Daarnaast worden risico's diepgaander en complexer. Ondernemingen gaan op zoek naar een garantie dat de controles van kracht en effectief geïmplementeerd zijn. BWise loopt op deze ontwikkeling vooruit door continuous controls monitoring (CCM) te integreren binnen het GRC-platform. Voor audits kan dan gekozen worden geen steekproef uit te voeren, maar alle data te analyseren en trends te ontdekken met een voorspellende waarde, zodat niet alleen achteruit wordt gekeken."

Clarinda Dobbelaar is vice president of marketing bij BWise en verantwoordelijk voor de marketing- en telemarketingteams wereldwijd.

F. Hoeben M.Sc., Dynasec

1. Wat is de toegevoegde waarde van uw tooling voor de organisatie?

"Dynasec levert een geïntegreerd systeem. Easy2comply© levert GRC-functionaliteit voor de eerste en tweede line of defense. Easy2audit© levert auditfunctionaliteit voor de derde line of defense. De uitwisseling van informatie tussen organisatie en audit is hiermee gewaarborgd. Immers, beide maken gebruik van dezelfde gegevens. Alleen zijn deze benaderbaar vanuit de verschillende invalshoeken van de diverse functies zoals het lijnmanagement en staffuncties als risk, compliance, security en audit."

2. Wat is de toegevoegde waarde van uw tooling voor IA?

"Traditionele redenen voor de aanschaf van automatiseringsgereedschappen zijn het ondersteunen van het auditproces, het vereenvoudigen van de planning, de opzet van een kennisbron, communicatie binnen het auditteam, registratie van de uitvoering, het verzamelen van (elektronische aangeleverde) bewijzen (evidence), het systematisch vastleggen en evaluatie van bevindingen, het samenstellen van en communicatie over rapportage."

3. Op welke wijze dient de tooling geïmplementeerd te worden?

"Easy2audit is een webdienst (www.easy2audit.nl) waarop een abonnement kan worden genomen. Er kan dus direct worden gestart met een modern systeem tegen lage kosten. Easy2audit vormt een onderdeel van de easy2comply GRC-productlijn voor governance, risk management, compliance en bedrijfscontinuïteit."

4. Welke toekomst voorziet u voor uw tooling?

"Veel organisaties hebben een behoorlijke ontwikkeling doorge-

maakt met betrekking tot hun interne beheersing. Naarmate door de lijnmanagers en staffunctionarissen voor risicobeheer en compliance meer gebruikgemaakt wordt van ondersteunende software voor interne beheersing, komt de elektronische uitwisseling van gegevens in beeld. Daarvoor is een koppeling van de door de organisatie en het auditteam gebruikte systemen noodzakelijk. Easy2audit richt zich op de interactie met een breed scala aan informatiebronnen, en geavanceerde analyse van deze informatie voor betere besluitvorming en onderbouwing van vervolgacties. Het auditsysteem evolueert van een monolithisch systeem naar een systeem dat maximaal integreert in het pluriforme landschap van bedrijfsinformatie."

Frank Hoeben is managing director bij Dynasec.

De **GEBRUIKERS** aan het woord

Ir. J. Heijmans EMIA, Ahold

"Ahold maakt gebruik van het op COSO gebaseerde Ahold Business Controlframework, waarin richtlijnen, procedures en instructies zijn opgenomen die gebruikt worden om Ahold te managen. De belangrijkste GRC-functies binnen Ahold zijn risicomanagement, internal control, compliance en Internal Audit. Risicomanagement heeft binnen Ahold de coördinerende rol voor de groepsbrede risicomanagementactiviteiten. Internal Audit functioneert als de third line of defence.
De hoofden van de GRC-functies rapporteren aan verschillende leden van de raad van bestuur. Dit maakt coördinatie noodzakelijk maar tegelijkertijd het geheel van GRC-functies erg sterk. Binnen Ahold wordt dit als een groot voordeel gezien.
Elk kwartaal is er een GRC-vergadering waarin bestuursleden zitting hebben alsmede de hoofden van de GRC-functies. Hierin worden alle GRC-gerelateerde zaken besproken voordat deze op de agenda van de raad van bestuur komen. GRC is daarmee de coördinator van de GRC-activiteiten met aan de ene kant het management van de werkmaatschappijen en aan de andere kant de raad van bestuur."

Raamwerk

"Om de verschillende GRC-functies effectief en efficiënt te laten opereren heeft Ahold één GRC-raamwerk opgesteld. Hiermee wordt bereikt dat de GRC-functies dezelfde taal spreken, eenzelfde materialiteit gebruiken en vergelijkbare bevindingen rapporteren. Ook is er een risicoacceptatieprocedure ingesteld die het management helpt bij discussies over Ahold's risk appetite. Om deze informatiestromen op een efficiënte wijze tot stand te laten komen en te kunnen gebruiken binnen de hele onderneming is Ahold bezig met het implementeren van GRC-software. Het voordeel van een GRC-tool is dat het management zelf de tool kan gebruiken voor voortgangs- en uitzonderingsrapportages en dat de tool helder inzicht geeft in de relatie tussen de (business) objectives – risico's – controls en de resultaten van de control testactiviteiten."

Jutta Heijmans is senior auditor bij Ahold.

Drs. L. Boogers RA CIA en M. Jongejan, Heineken

"GRC ondersteunt Heineken in haar streven om in control te zijn en in het naleven van relevante regelgeving. Om deze reden is GRC binnen Heineken volledig geïntegreerd in de businessprocessen. De governance- en risicocomponenten van GRC zijn ingevuld via de reguliere planning & controlcyclus en zogenoemde assurance meetings. Het verantwoordelijk management, Internal Audit, business controllers en externe accountants bespreken in de assurance meetings diverse onderwerpen gerelateerd aan risicomanagement en compliance. Het management ondertekent jaarlijks een 'assurance letter' waarin de naleving van geselecteerde 'company rules' wordt bevestigd. Op diverse niveaus in de organisatie bestaan internal controlafdelingen, doch deze vormen geen geïntegreerd geheel.
Een geïntegreerd stelsel van interne controlemaatregelen bestaat voor de belangrijkste businessprocessen. De internal auditors voeren operationele reviews uit waarin de opzet, het bestaan en de werking van de belangrijkste interne controlemaatregelen worden getoetst en geeft hierover een oordeel. Eveneens voert Internal Audit compliance audits uit op geselecteerde 'company rules' en voert het enige internal controlactiviteiten uit. Als laatste activiteit adviseert Internal Audit het management in de inrichting van een effectief risicomanagement- en controlesysteem."

Toetsingsnorm

"Het GRC-raamwerk voorziet in een toetsingsnorm voor Internal Audit. Tevens helpt het raamwerk bij het creëren van eenduidige definities, terminologie en rapportages.
Heineken heeft een verscheidenheid aan systemen ter ondersteuning van de GRC-activiteiten in de business en Internal Audit. Heineken kent geen wereldwijd GRC-systeem maar ziet mogelijkheden om deze systemen verder te integreren om de effectiviteit en efficiency verder te vergroten."

Leonard Boogers en Mark Jongejan zijn beiden werkzaam bij Heineken Nederland. Boogers is regionale auditmanager en Jongejan is manager Internal Audit. Deze bijdrage is op persoonlijke titel geschreven.

De lezer over GRC

In dit themanummer niet alleen de mening van deskundigen maar ook die van u. De redactie van *Audit Magazine* plaatste drie stellingen op de website van het IIA en ontving daarop maar liefst 170 reacties. De uitslag.

Stelling 1
GRC is flauwekul.

	In %
1. Helemaal mee eens	1
2. Mee eens	5
3. Neutraal	10
4. Mee oneens	41
5. Helemaal mee oneens	43

Stelling 2
Door GRC lever ik meer toegevoegde waarde.

	In %
1. Helemaal mee eens	23
2. Mee eens	47
3. Neutraal	20
4. Mee oneens	8
5. Helemaal mee oneens	2

Stelling 3
Organisaties kunnen beter in mensen investeren dan in dure GRC-tools.

	In %
1. Helemaal mee eens	17
2. Mee eens	39
3. Neutraal	27
4. Mee oneens	12
5. Helemaal mee oneens	5

Het is overduidelijk dat internal auditors GRC geen onzin vinden. Sterker nog, het laat internal auditors meer toegevoegde waarde leveren. Echter, in hoeverre GRC-tools hierbij meer helpen dan de inzet van de juiste mensen, levert gemengde reacties op.

Nuttig en relevant

Wat betekent deze uitslag? Ten eerste dat dit themanummer zeer goed gekozen is. Immers, de resultaten uit stelling 1 en 2 laten zien dat GRC relevant en nuttig wordt gevonden. Ten tweede doet het grote aantal respondenten vermoeden dat de term 'GRC' de bezoekers van de IIA-website bezighoudt en dat hun beeld bij GRC voldoende helder is om de stellingen te beantwoorden. Dat doet ons deugd, met name omdat ons tijdens het samenstellen van dit nummer opviel dat GRC een begrip is dat voor velerlei uitleg vatbaar is. Ten slotte blijkt uit de opmerkingen bij de reacties dat 'mensen' zeker zo relevant zijn voor het succes van GRC-tools.

Veel lezers hoeven niet meer overtuigd te worden van de relevantie en het nut van GRC en een ding is zeker, na het lezen van dit nummer zal dit beeld versterkt zijn. GRC leeft!

De redactie wil alle respondenten bedanken. Niet alleen op deze manier uiten we onze waardering, dat doen we ook met een gratis boekenpakket. De gelukkige is dit keer Paul van der Heijdt. Proficiat Paul en veel leesplezier gewenst!

De volgende stellingen komen er aan. Houd de website van het IIA in de gaten en geef uw mening!

Onderzoeksproject:
de relatie tussen de IAF en GRC

In de zomer van 2009 startten IIA Nederland en het NIVRA, vakgroep Interne Accountants (INTAC), een gezamenlijk onderzoeksproject naar de relatie tussen de internal auditfunctie (IAF) enerzijds en het governance-, risk- en compliancevakgebied (GRC) anderzijds. Dit artikel gaat in op enkele opvallende resultaten uit de enquête.

A. Man, S. Cheung, H. van der Wijk, J. Willemstein

Het onderzoek is uitgevoerd door een werkgroep bestaande uit een twaalftal enthousiaste vrijwilligers. Het onderzoek bestond uit een:
1. literatuurstudie,
2. online enquête,
3. serie interviews.

Het eindrapport van het onderzoeksproject zal tijdens een debatsessie met de titel 'Internal Audit en GRC, integrated teamwork?' op 25 mei 2010 en tijdens het IIA-congres in juni aanstaande worden toegelicht. Het eindrapport zal naast bevindingen en conclusies ook best practices bevatten.

Doelsteling, onderzoeksvragen en aanpak

Het doel van het onderzoek is te komen tot een visie vanuit de internal auditvakorganisaties op de relatie tussen GRC en de IAF en – indien mogelijk – tot best practices met betrekking tot de verantwoordelijkheden van en taakverdeling tussen GRC en de IAF. De achterliggende gedachte is dat de IAF een belangrijke rol speelt in het governancevraagstuk binnen organisaties en belang heeft bij een evenwichtig, efficiënt en effectief samenspel met in het bijzonder de afdelingen risk management en compliance.
Op basis hiervan is de volgende onderzoeksvraag gedefinieerd: op welke wijze dient de IAF invulling te geven aan haar verantwoordelijkheden en taakinvulling in relatie tot het governancevraagstuk in organisaties, inclusief de verantwoordelijkheden en taakinvulling van de afdelingen risk management en compliance?
Afgeleide deelvragen zijn:
1. Welke vormen van samenwerking tussen de IAF en GRC zien wij in de praktijk?
2. Wat zijn de voor- en nadelen van deze vormen van samenwerking?
3. Welke invloed heeft de wet- en regelgeving op deze vormen van samenwerking?
4. Welke best practices kunnen geformuleerd worden in de samenwerking tussen de IAF en GRC?
5. Welke veranderingen zijn nodig (in wet- en regelgeving, algemeen aanvaarde normen, opleidingen, et cetera) om de best practices in de samenwerking tussen de IAF en GRC te implementeren?

Wij hebben de scope van ons onderzoek op voorhand beperkt tot ondernemingen in Nederland. De overheid, inclusief zelfstandige bestuursorganen (ZBO's) en dergelijke, hebben we buiten beschouwing gelaten. Deze sector zou eventueel in een vervolgonderzoek meegenomen kunnen worden.
Om de onderzoeksvragen te beantwoorden is eerst een literatuurstudie uitgevoerd. Hieruit bleek dat weliswaar een grote hoeveelheid literatuur beschikbaar is over het onderwerp GRC, maar dat slechts beperkt informatie beschikbaar is over de relatie tussen GRC en de IAF. Op basis van deze literatuurstudie hebben we een aantal thema's gedefinieerd die sturend waren voor de te hanteren vragenlijst. Daarna zijn er per thema vragen gedefinieerd om te komen tot een 'longlist' van mogelijke enquêtevragen. Uit deze longlist is vervolgens de definitieve vragenlijst van 25 vragen voor de enquête samengesteld.
De uitkomsten van de enquête vormden de input voor een serie interviews met hoofden IAF, risk management en compliance.
De uitkomsten van de enquête vormen samen met de interviews en de literatuurstudie de basis voor het eindrapport.

Enkele kernbevindingen uit de online enquête

Respondenten

Van de in totaal 67 respondenten die de enquête hebben ingevuld zijn er 43 (64 procent) werkzaam binnen een IAF, 10 (15 procent) hebben een gecombineerde IAF/riskmanagement- en compliancefunctie, 4 (6 procent) hebben een riskmanagementfunctie en 6 (9 procent) hebben een compliancefunctie. Vier respondenten hebben hun functie niet nader gespecificeerd. Van de respondenten zijn er verder 35 (52 procent) werkzaam in de financiële sector, 31 (46 procent) in de niet-financiële sector en 1 (2 procent) heeft zijn organisatie niet nader gespecificeerd.
Er is een redelijke verdeling tussen grote en kleine ondernemingen en er is ook een goede verdeling tussen de afdelingsgrootte waar de respondenten werkzaam zijn. Vervolgens hebben we onderzocht of er tussen de verschillende groepen (bijvoorbeeld hoofden IAF versus hoofden riskmanagement en compliance, ondernemingen uit de financiële sector versus ondernemingen uit de niet-financiële sector, et cetera) interessante verschillen in antwoorden bestaan.

Verantwoordelijkheid

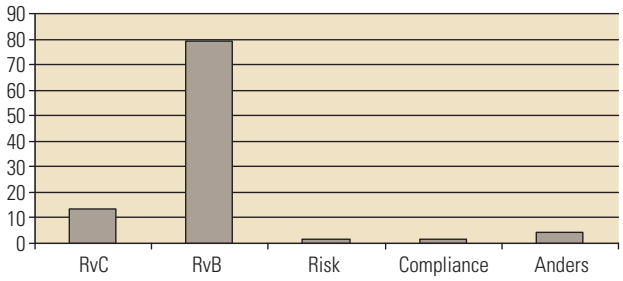
Een ruime meerderheid van de respondenten geeft aan dat de eindverantwoordelijkheid voor GRC bij de raad van bestuur ligt (zie *figuur 1*). Hierbij is er nauwelijks verschil tussen de financiële sector en de niet-financiële sector. Dit beeld geldt zowel voor beursgenoteerde als niet-beursgenoteerde ondernemingen.
Uit de enquête blijkt dat GRC doorgaans op de agenda staat bij de raad van commissarissen (of een subcommissie) en in acht van de tien gevallen bij de raad van bestuur. Hoofden IAF geven in verhouding tot hun collega's van compliance en risk management vaker aan aanwezig te zijn bij de besprekingen van GRC door de raad van bestuur.

Rapportage

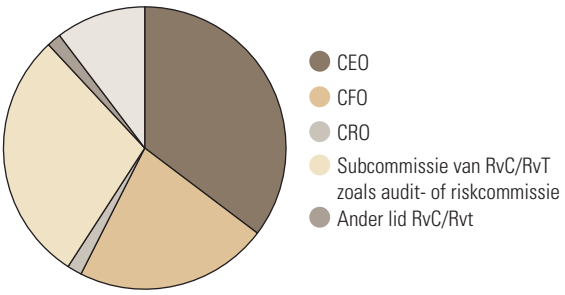
Aan de respondenten is gevraagd aan wie zij rapporteren, met de mogelijkheid om meerdere antwoorden te geven. De bevindingen laten zien dat het meest aan respectievelijk de CEO, een subcommissie van de RvC/RvT en de CFO wordt gerapporteerd (zie *figuur 2*). Blijkbaar heeft tweederde van de hoofden van de IAF of van GRC-functies geen rapportagelijn aan de RvC.

Positionering en informatie-uitwisseling IAF en GRC-functies

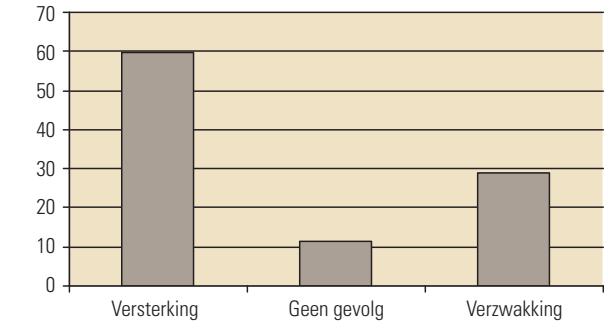
De enquête verschaft een interessant inzicht in de visie van respondenten op de positionering van GRC-functies in de organisatie. De meningen zijn duidelijk verdeeld. Ruim de helft is van mening dat splitsing van GRC-verantwoordelijkheden over meerdere afdelingen leidt tot een versterking van deze functies in de organisatie (zie *figuur 3*). Als we de resultaten verder analyseren dan blijkt dat deze versterking vooral wordt gevoeld door personen die zelf werkzaam zijn op een gecombineerde afdeling (risk en Internal Audit). Het lijkt er dus sterk op dat men een voorkeur heeft voor het model waarbinnen men al werkt. In de interviews is hier verder op ingegaan.



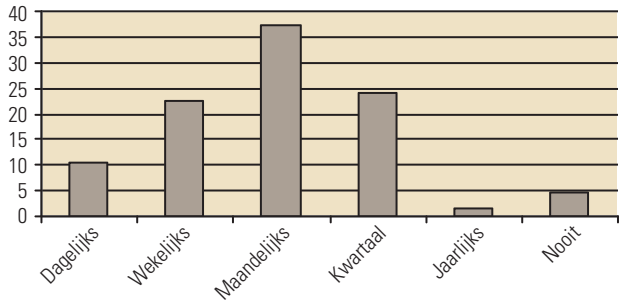
Figuur 1. Eindverantwoordelijkheid GRC



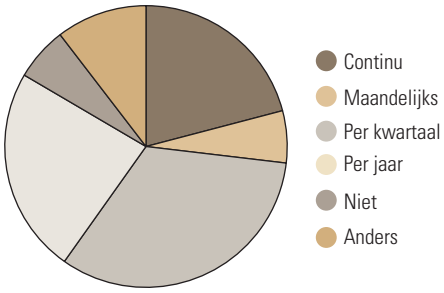
Figuur 2. Rapportagelijnen



Figuur 3. Effect van opsplitsing GRC-functies



Figuur 4. Frequentie informatieuitwisseling



Figuur 5. Bijstelling werkplan

Uit de enquête blijkt verder dat de frequentie van informatie-uitwisseling tussen de IAF en GRC-functies varieert (zie *figuur 4*), waarbij maandelijkse informatie-uitwisseling het meest wordt genoemd.

Aan de respondenten is verder gevraagd om de informatie-uitwisseling tussen de functies te karakteriseren. Daar komt het volgende uit:

- Een ruime meerderheid is tevreden over de gestelde mate van informatie-uitwisseling tussen de IAF en GRC-functies binnen de eigen organisatie.
- Opvallend is dat van alle respondenten die aangeven dat de informatie-uitwisseling tussen IAF en GRC-functies veelvuldig plaatsvindt (dit is ruim 50 procent van de respondenten), vier op de tien dit als een informele wijze van uitwisseling karakteriseert. Dit lijkt te wijzen op een significant belang van informele contacten wat betreft de informatie-uitwisseling tussen de functies onderling.
- Opvallend is wel dat vier op de tien hoofden van de IAF juist aangeeft behoefte te hebben aan meer informatie-uitwisseling met GRC-functies. Dit zou mogelijk verklaard kunnen worden vanuit de gedachte dat de IAF relatief verder van de business staat (ten opzichte van de GRC-functies), wat samenhangt met de specifieke functie van de IAF.

Tweederde van de hoofden van de IAF of van GRC-functies heeft geen rapportagelijn aan de RvC

Werkplan IAF

De vraag is gesteld hoe vaak het werkplan van de afdeling wordt bijgesteld op basis van de bevindingen op GRC-gebied. Uit de reacties blijkt dat werkplannen vrijwel in alle gevallen periodiek worden aangepast op basis van de bevindingen op GRC-gebied, waarbij de frequentie wel varieert. Slechts in enkele (vier) gevallen werd geantwoord dat in het geheel geen bijstelling van de werkplannen plaatsvindt.

Afsluiting en vervolgstappen

De hier genoemde bevindingen zijn slechts een selectie uit de resultaten van de enquête. De interviews zijn inmiddels afgerond en geven een meer uitgekristalliseerd en nader uitgewerkt beeld. Tevens zijn best practices geformuleerd met betrekking tot de verantwoordelijkheid en taakverdeling tussen de IAF en GRC-functies. De best practices zijn te zien als leidraad voor het verder vormgeven van de onderlinge relatie tussen de genoemde functies. De eindresultaten van het onderzoek zullen worden gereviewd door een redactieraad, bestaande uit de professoren Emanuels, Paape en Van der Poel.

Zoals vermeld in de inleiding van dit artikel, organiseert de projectgroep op 25 mei 2010 een debatsessie over de uitkomsten van het onderzoek. Voor deze sessie zijn naast internal auditors, ook risk- en compliancemanagers uitgenodigd om vanuit verschillende invalshoeken de discussie te kunnen voeren. Tijdens het IIA-congres zullen de eindresultaten bekendgemaakt worden. Het eindrapport zal digitaal verspreid worden onder de leden van het IIA en het INTAC. Voor vragen kunt u zich wenden tot de projectleider, San Croonenberg van het NIVRA,
✉ s.croonenberg@nivra.nl.

Arjan Man is lid van de stuurgroep Project IAF-GRC en senior manager bij PricewaterhouseCoopers/ Internal Audit Services.

Scott Cheung is lid van de werkgroep Project IAF-GRC en hoofd van Group Audit bij Credit Europe Bank nv.

Heiko van der Wijk is lid van de werkgroep Project IAF-GRC en manager Internal Control bij Office KLM.

Jeroen Willemstein is data-analist online enquête en senior associate bij PricewaterhouseCoopers/Regulatory Compliance.

Coördinatie van GRC-activiteiten: een kans voor Internal Audit!

Goverance-, risk- en complianceconvergentie staat in het middelpunt van de belangstelling en refereert naar de integratie en coördinatie van GRC-activiteiten. De theorie klinkt eenvoudig maar de praktijk is weerbarstig. De internal auditfunctie kan hier een significante rol spelen maar grijpt zij deze kans ook? En hoe zou zij deze rol kunnen vervullen?

M. van der Sanden RA RO CIA

Hoewel verschillend uitgelegd in verschillende organisaties, omvat GRC doorgaans de activiteiten met betrekking tot het identificeren, analyseren, beheersen van organisatiebrede risico's (waaronder de naleving van wet- en regelgeving) én de monitoring van de effectieve werking van de interne beheersing. Governance vormt de paraplu van voorgaande activiteiten en definieert de organisatorische structuur, de infrastructuur, het beleid en de procedures.

Dubbel werk

In veel organisaties bestaan naast de operationele afdelingen (first line of defense) tal van afdelingen in de tweede en derde line of defense die zich bezighouden met risicomanagement, interne beheersing en compliance (zie *figuur 1*). Hierbij kan gedacht worden aan de afdelingen risk management, treasury, compliance, health & safety en Internal Audit. De afzonderlijke afdelingen gebruiken vaak verschillende benaderingen voor de beheersing van risico's die mogelijk resulteren in dubbel werk of lacunes in risicodekking. Uit recent onderzoek[1] blijkt dat:

- 73 procent van de respondenten aangeeft zeven of meer risicofuncties te hebben;
- 67 procent overlappende dekking met twee of meer risicofuncties heeft;
- 50 procent hiaten in de dekking tussen risicofuncties heeft.

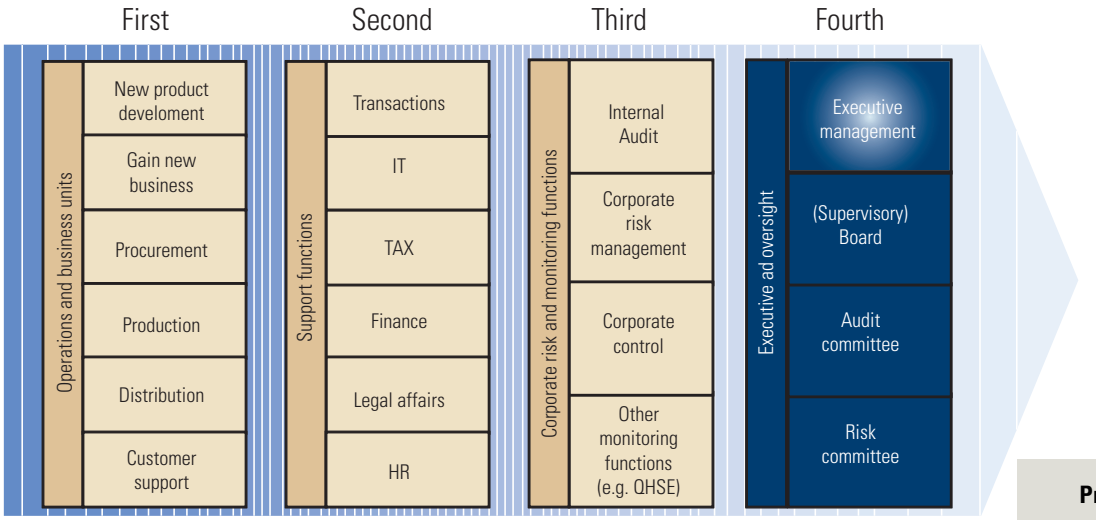
Internal Audit is een van de risicofuncties en haar rol binnen GRC is vooral gericht op het geven van assurance over de effectiviteit van de interne beheersing. In dit artikel wordt eerst ingegaan op de rol die Internal Audit kan spelen bij de coördinatie van assuranceactiviteiten en vervolgens op de coördinatie van het bredere GRC-raamwerk.

IIA Practice Advisory 2050 Coordination

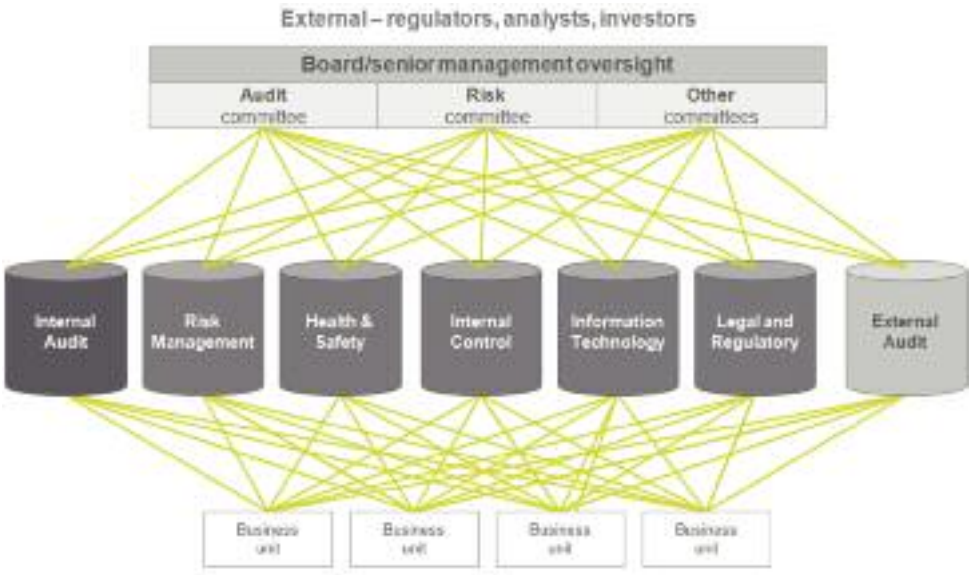
De IIA Standaard 2050 schrijft voor dat de chief audit executive zijn activiteiten moet coördineren met andere interne en externe assurancefuncties. In juli 2009 heeft het IIA een Practice Advisory (PA) gepubliceerd met guidance voor het voldoen aan deze standaard. De PA onderkent dat de meeste organisaties een veelheid aan afdelingen of functies hebben die assurancewerkzaamheden uitvoeren zoals compliance, quality assurance, health & safety en uiteraard Internal Audit. Het IIA verdeelt de assurancefuncties in drie groepen:

1. Degenen die rapporteren aan het management zoals kwaliteitsauditors (ISO 9000), milieuauditors (ISO 14001) alsmede personeel dat control self assessments uitvoert.
2. Degenen die ook rapporteren aan de raad van commissarissen of het audit committee zoals Internal Audit.
3. Degenen die rapporteren ten behoeve van externe belanghebbenden zoals de externe accountant en externe certificerende instellingen.

De raad van bestuur (RvB) en het audit committee wensen de zekerheid dat het overall assuranceproces adequaat en efficiënt is en dat alle significante risicogebieden worden afgedekt. Echter, bij de meeste organisaties opereren de verschillende assurancefuncties veelal onafhankelijk in silo's naast elkaar (zie *figuur 2*).



Figuur 1. De lines of defense (Bron: Ernst & Young)



Figuur 2. Een veelvoorkomende huidige situatie (Bron: Ernst & Young)

Praktijkvoorbeeld

Een CEO van een Fortune 500-onderneming stelde in het kader van een externe kwaliteitstoetsing van de internal auditfunctie: 'Er zijn vele assurancefuncties binnen de groep en het is niet duidelijk wie wat doet. De assurancefuncties moeten de business gecoördineerd benaderen om het tijdsbeslag van de business te minimaliseren. Ik zou graag één overall rapportage zien met de conclusie, thema's en trends vanuit de verschillende assurancefuncties. Aangezien Internal Audit de enige assurance-functie is met een mandaat vanuit het audit committee ligt het voor de hand dat zij een proactieve rol speelt bij deze coördinatie.'

Een overall beeld van de uitkomsten van de activiteiten van deze assurancefuncties, zoals de resultaten van risicoanalyses en uitgevoerde audits, is zelden beschikbaar. Hierdoor bestaat het risico dat bepaalde activiteiten, processen en afdelingen binnen een organisatie meerdere malen aan een audit worden onderworpen door verschillende assurancefuncties met overlappende auditscopes. Uiteraard leidt dit tot veel frustratie in de business en hoge kosten. Daarnaast bestaat het risico dat significante risicogebieden helemaal niet worden afgedekt.

De internal auditfunctie is in de unieke positie dat het vaak de enige assurancefunctie is met een mandaat vanuit het audit committee. In deze rol is Internal Audit veelal verantwoordelijk voor het verschaffen van assurance over de gehele organisatie. Dit omvat dus de gehele GRC-omgeving waaronder de activiteiten van andere assurancefuncties. De chief audit executive wordt door de IIA Standaard 2050 aangespoord om een coördinerende rol te vervullen met betrekking tot alle assuranceactiviteiten binnen een organisatie.

Assurance map

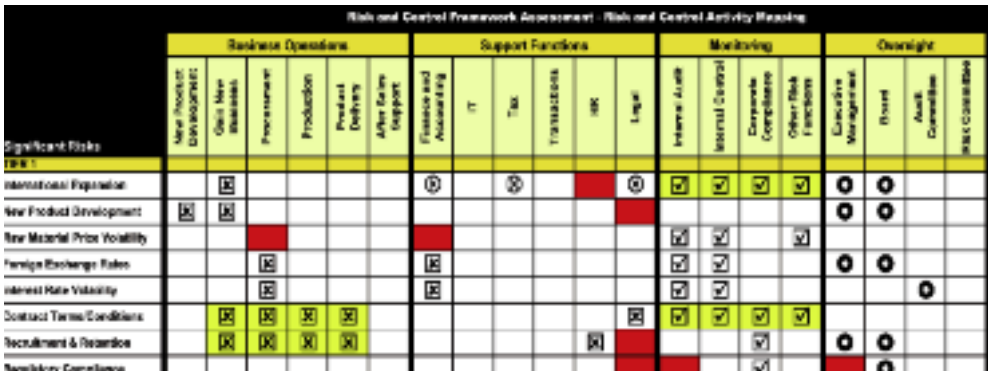
De IIA Practice Advisory stelt dat een assurance map een effectieve tool is om invulling te geven aan de coördinatie van assuranceactiviteiten én hierover te communiceren. Met behulp van assurance maps worden de activiteiten van alle assurancefuncties gekoppeld aan de belangrijkste risicogebieden voor de organisatie. Dit stelt de internal auditor in staat om eventuele lacunes en inefficiënties te identificeren en vervolgens te adresseren. Zo heeft de internal auditfunctie van een Nederlandse onderneming in de vervoerssector efficiëntieverbeteringen geïdentificeerd met betrekking tot de assuranceactiviteiten op veiligheidsrisico's. Naast Internal Audit voerde ook de verbijzonderde afdeling Veiligheid regelmatig audits uit op dit risicogebied. Door de auditplannen af te stemmen kon men de business benaderen met

Maurice van der Sanden is senior manager bij Ernst & Young en gespecialiseerd in Internal Audit, risicomanagement en internal control.

een gecoördineerde aanpak en het tijdsbeslag op de business tot een minimum beperken.
Ten slotte kan de assurance map als communicatiemiddel gebruikt worden. Met behulp van de assurance map kan een internal auditfunctie haar belanghebbenden laten zien dat alle belangrijke risicogebieden zijn afgedekt door assuranceactiviteiten.

Internal Audit kan bijdragen aan een efficiënter GRC-raamwerk, lagere kosten én een verbeterde reputatie in de business

Practice Advisory 2050 geeft internal auditors zeer concrete richtlijnen om invulling te geven aan de IIA Standaard 2050. Daarnaast biedt het internal auditors enorme mogelijkheden om de assurancelast voor de business te minimaliseren en hierdoor een bijdrage te leveren aan een efficiënter assuranceraamwerk. Echter, Practice Advisory 2050 gaat vooral in op de coördinatie van assuranceactiviteiten binnen de third line of defense. Zoals hiervoor reeds genoemd bestaan er bij veel organisaties mogelijkheden voor een integratie van GRC over *alle* lines of defense.



Figuur 3. Vereenvoudigde weergave van een geïntegreerde GRC-map

Internal auditors hebben een kans om hier een significante bijdrage te leveren door de assurance mapconcepten uit de Practice Advisory 2050 toe te passen over alle lines of defense heen.

Geïntegreerde GRC-maps

De belangrijkste uitbreiding van de assurance maps over alle lines of defense betreft het inzichtelijk maken van de rollen en verantwoordelijkheden van vooral de first line of defense. Uit de praktijk blijkt dat succesvol risicomanagement afhankelijk is van de mate waarin de business eigenaarschap voelt voor het beheersen van risico's. Het volledig 'delegeren' van risicomanagement naar afzonderlijke afdelingen is een van de kenmerken van falend risicomanagement. De business (first line of defense) behoort de primaire verantwoordelijkheid te dragen voor het identificeren, analyseren en beheersen van risico's. Hierbij kunnen verbijzonderde functies of afdelingen (second line of defense) de business ondersteunen bij deze taken. Denk hierbij bijvoorbeeld aan treasury en juridische zaken.
Voordat internal auditors zich storten op audits op operationeel of procesniveau is het daarom van belang dat zij inzicht verkrijgen in wie verantwoordelijk is voor de beheersing van de organisatiebrede risicogebieden. Een analyse van deze rollen en verantwoordelijkheden zal (vaker dan men denkt) uitwijzen dat verschillende afdelingen of functies zich verantwoordelijk voelen voor het beheersen van dezelfde risico's. Wanneer deze verschillende afdelingen zich hier niet van bewust zijn kunnen de maatregelen die zij afzonderlijk nemen zelfs tot nieuwe risico's leiden. In het ergste geval is er sprake van risicogebieden waar niemand zich binnen de organisatie verantwoordelijk voor voelt.
Geïntegreerde GRC-maps kunnen internal auditors helpen bij het identificeren van deze inefficiënties en lacunes binnen de first line of defense. Vervolgens kunnen internal auditors hier effectief over communiceren en eventueel het auditplan aanpassen om bijvoorbeeld bepaalde niet afgedekte risico's (tijdelijk!) te monitoren. Deze uitbreiding ten opzichte van een (IIA Practice Advisory 2050) assurance map kan de RvB en het audit committee duidelijk inzicht geven over hoe de belangrijkste risicogebieden worden beheerst en hoe verantwoordelijkheden zijn verdeeld over alle lines of defense.
Figuur 3 geeft een illustratie van een vereenvoudigde weergave van een geïntegreerde GRC-map.

Ten slotte kunnen geïntegreerde GRC-maps internal auditors helpen om assuranceactiviteiten binnen de onderneming beter te coördineren. Na het inzichtelijk maken van inefficiënties en lacunes kan

de internal auditfunctie een rol vervullen bij het:

- waarborgen dat assuranceactiviteiten zijn gealloceerd aan specifieke risicogebieden;
- bewaken dat de verschillende assurancefuncties optimaal samenwerken in het belang van de business;
- regelmatig uitwisselen van perspectieven, auditplannen en issues tussen de assurancefuncties (bijvoorbeeld via een protocol) om tot een geïntegreerd assuranceplan te komen;
- zorgen voor consistente, geïntegreerde risico- en assurancerapportages teneinde consistentie in rapporteren door de verschillende functies te realiseren;
- bestuur en commissarissen voorzien van een geconsolideerde rapportage over de ontwikkeling van de belangrijkste risico's en audituitkomsten.

Noot

1. *The Future of Risk*, Ernst & Young, 2009.

Conclusies

Internal auditors hebben een unieke kans om met de concepten uit IIA Practice Advisory 2050 een significante bijdrage te leveren aan de integratie en coördinatie van GRC-activiteiten. Met behulp van een geïntegreerde GRC-map kunnen internal auditors die gebieden waar verbeterde integratie en coördinatie van GRC mogelijk is, inzichtelijk maken. Een geïntegreerde GRC-map geeft een holistisch, bottom-up inzicht in wie wat doet ten aanzien van de belangrijkste risicogebieden binnen de onderneming. Het geeft in één overzicht weer wie verantwoordelijk is voor het identificeren, analyseren en beheersen van de belangrijkste inherente risicocategorieën alsmede wie de aanvullende zekerheid verschaft over de interne beheersing.

Met dit inzicht kunnen internal auditors een actieve rol spelen in de coördinatie van de organisatiebrede GRC-activiteiten. Dit betekent concreet de realisatie van een efficiënter GRC-raamwerk met een lagere assurancelast voor de business wat zal leiden tot een kostenbesparing van GRC-activiteiten. Een actieve rol hierin biedt Internal Audit de kans om haar reputatie in de business nog verder te vergroten.

Samengevat zijn de voordelen van de toepassing van een geïntegreerde GRC-map:

- Het geeft de RvB en het audit committee een duidelijk beeld van hoe de belangrijkste risicogebieden worden beheerst en hoe verantwoordelijkheden zijn verdeeld over alle lines of defense.
- Het geeft het management op alle niveaus inzicht in de beheersomgeving waar zij verantwoordelijk voor is en hoe deze verantwoordelijkheid zich verhoudt tot de rest van de organisatie.
- Het verschaft duidelijkheid aan de verschillende risico- en assurancefuncties binnen de onderneming over waar ieders verantwoordelijkheden liggen. Dit stelt betrokkenen beter in staat om de gebieden te identificeren waar zij elkaar kunnen ondersteunen of aanvullen.
- Het identificeert hiaten in de dekking van de belangrijkste risicogebieden (exposure) en overlap in taken, rollen en verantwoordelijkheden (inefficiëntie en meer dan noodzakelijke belasting van de business).

In de vorige editie van *Audit Magazine* werd stilgestaan bij ISO 31000. Ook deze standaard predikt samenwerking en coördinatie tussen de verschillende risico- en assurancefuncties. Zullen internal auditfuncties de kans grijpen om hier een leidende rol in te spelen?

Personalia

Berichten kunt u mailen naar iia@iia.nl

- **Drs. R.E. van Ballegooijen RA** is overgestapt van Millennium Finance Corporation Ltd. Dubai International Financial Centre naar Royal Boskalis Westminster nv (Sharjah, UAE) (Lamnalco Group).

- **J.H.J. Brakenhoff RA RO** is werkzaam bij Heineken International bv. Hij komt van Ahold.

- **Drs. G.H.A. Grimbergen RE RO** maakte de overstap van Rabobank Randmeren naar ProRail bv.

- **Drs. P.X. Hooijschuur RE CIA CISA** is overgestapt naar Royal Bank of Scotland (RBS). Voorheen was zij werkzaam bij ABN Amro Bank nv.

- **Drs. R.S. de Heus RO EMIA** is door de Voedsel en Waren Autoriteit aangetrokken. Hij komt van CIAD bv.

- **Drs. J. de Ridder RA** versterkt nu Shell International bv. Voorheen was hij werkzaam bij het Openbaar Ministerie.

- **Drs. P. de Leeuw RO CIA** komt in dienst van Philips Corporate Internal AuditBuilding VS-1A. Zijn vorige werkkring was Ernst & Young Business Risk Services.

- **S.U. Annema-Killop RO EMIA** maakte de overstap van AEGON Nederland naar de De Nederlandsche Bank nv.

- **W. Sonneveld EMIA RO** versterkt Het Expertise Centrum. Voorheen was zij werkzaam bij het ministerie van Financiën.

- **Drs. E. Stoelhorst EMIA RO** is overgestapt naar BWise bv. Hiervoor werkte hij bij Ernst & Young Accountants Nederlandse Antillen.

Een gebrek aan cultuur?

Over governance, risk management en compliance (GRC) is nog altijd veel onduidelijkheid. In dit artikel zal gesteld worden dat de GRC-cultuur (in tegenstelling tot de GRC-tools) centraal dient te staan in het inrichten van governance en management van organisaties.

R. Voet RA

GRC lijkt nog niet zo oud en toch voelt het al als een oud vakgebied. Dat komt omdat de drie elementen op zichzelf al redelijk zijn doorontwikkeld maar in hun samenhang pas sinds enkele jaren als zodanig worden beschouwd. Gezien de recente ontwikkelingen en schandalen en niet in de laatste plaats de crisis, is het nog maar de vraag of GRC zoals we dat vandaag de dag kennen, niet toe is aan upgrade: GRC 2.0! GRC 2.0 is nodig, GRC 1.0 is oude wijn in nieuwe zakken en mist toch de noodzakelijke verfrissende kijk op integrale sturing, risico en waardecreatie!

OESO, hoezo?

Binnen de OESO is veel kennis en ervaring verzameld, gedeeld en verwerkt tot geadviseerde best practices waar het gaat om public management, een deelgebied van GRC. Al sinds 1990 bestaat het 'Support for Improvement in Governance and Management' (SIGMA) programma, dat onder andere een rol speelde bij de voorbereiding tot de toetreding van de Oost-Europese EU-lidstaten.

De door de OESO gemaakte statements dat de cultuur van de organisatie en dan met name de risk managementcultuur gemonitord moet worden, dienen ter harte genomen te worden. Waar het gaat om GRC-tools, dient vooral in deze richting een ontwikkeling plaats te vinden. GRC 2.0 zal meer handen en voeten geven aan een effectieve control environment dan het nu doet.

Het werk van de OESO verdient het om onder de aandacht gebracht te worden. Waar het gaat om het delen van kennis en ervaring richten velen onder ons zich allereerst op de binnen de beroepsorganisaties (bijvoorbeeld NIVRA en IIA) aanwezige bronnen. Men realiseert zich vaak niet dat veel belangwekkend inventariserend en vergelijkend onderzoek, met inbreng van vele deskundigen vanuit allerlei richtingen en landen (inclusief vertegenwoordigers van de genoemde beroepsorganisaties), bij de OESO beschikbaar is voor consultatie.

OESO

De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) is een samenwerkingsverband van dertig democratische landen met een markteconomie. De aangesloten landen wisselen en vergelijken onderling ervaringen, zoeken oplossingen voor gemeenschappelijke problemen, identificeren good practices en coördineren het nationale en internationale beleid.

OESO en corporate governance best practices

Na de toetreding van de eerste golf nieuwe EU-lidstaten heeft de OESO het public management committee geïntegreerd in het





directorate for public governance and territorial development (GOV). Daarnaast bestaat er binnen de OESO het directorate for financial and enterprise affairs (DAF), waar veel aandacht wordt besteed aan corporate governance.
Veel publicaties van de OESO bevatten good practices. De waarde hiervan gaat verder dan een deskundig advies aan de administraties van de dertig aangesloten lidstaten. Door een stelselmatige opbouw van 'peer pressure' worden de adviezen uiteindelijk meestal geïmplementeerd. Hierbij gaat het om langdurige trajecten. De OESO brengt zelf geen wetgeving tot stand, maar modellen die binnen deze denktank tot standkomen zijn input voor besluitvoorbereidend werk binnen bijvoorbeeld de EC, WTO, IMF en Wordbank.
Zo bestaan er OESO *Principles of corporate governance* (1999) en als resultaat van het periodieke doorlichten en bijstellen van de onderzoeksresultaten is er ook een *Revision of the principles* (2004). In 2006 publiceerde de OESO een *Methodology for assessing implementation of the OECD principles on corporate governance*. Deze methodologie geeft onder andere een kader voor beleidsdiscussies op nationaal en internationaal niveau.

Financiële crisis

Als gevolg van de financiële crisis publiceerde de OESO *Corporate covernance lessons from the financial crisis* (2009) en *Corporate governance and the financial crisis: key findings and main messages* (2009). Deze rapporten zijn beslist aan te bevelen. Zo valt er bijvoorbeeld te lezen dat riskmanagers vaak apart gehouden werden van het management en niet gezien werden als essentieel voor het implementeren van de strategie van het bedrijf. Of nog opvallender: leden van de bestuursorganen waren zich soms niet bewust van de risico's waaraan de organisatie bloot stond. De les die getrokken wordt is dat het als een good practice gezien moet worden dat het bestuur van de organisatie betrokken is bij zowel de inrichting als het monitoren van de structuur van het risk management. In Nederland zal de Commissie-De Wit haar onderzoek binnenkort afronden en naar verwachting op 10 mei 2010 de conclusies presenteren. Het zal interessant zijn te vernemen of deze commissie andere of aanvullende conclusies heeft dan de OESO reeds in 2009 rapporteerde.

Internal Audit

In relatie tot het onderwerp Internal Audit merkt de OESO onder andere op dat het niet duidelijk is of risk management tot de taken van het audit committee behoort, maar wel dat het zich behoort te informeren over de risk managementstructuur. Dit roept de vraag op of er nu wel of niet een functiescheiding zou moeten bestaan tussen Internal Audit en risk management. Het binnenkort te verwachten rapport van de projectgroep van het NIVRA/IIA die de relatie tussen de internal auditfunctie en GRC onderzocht, gaat hier nader op in.
In ieder geval lijkt het duidelijk dat in gevallen waar de IAF en GRC nauw verweven zijn, soms onder leiding van eenzelfde manager, de audit van risk management systems beter overgedragen kan worden aan externe auditors opdat auditors niet hun eigen werkzaamheden auditen.

Risk management

De volgende uitspraak heeft een belangrijke boodschap in zich: 'Reflecting the lack of adequate standards, disclosure of foreseeable risks is often poor and can be mechanical and boiler plate in nature (e.g. a list of umpteen possible risks). More important is adequate disclosure about the mechanisms of risk management and the risk management culture.'[1]
Hierin staat een aantal conclusies in één volzin:
- er is een gebrek aan adequaste standaarden (voor risk management);
- er is geen adequate openbaarmaking;
- niet alleen de risk managementmechanismen, maar ook de risk managmentcultuur dient beschreven te worden.

Het lijkt er ook op dat de OESO de risk management standards van ISO (31000:2009) niet ziet als de bedoelde standaarden. De reden daarvan is niet gespecificeerd, maar de aanwijzing ligt besloten in het woord 'culture'. Te vaak nog wordt risk management benaderd als een welhaast mechanisch systeem waar met hulp van richtlijnen, checklists en GRC-tools een oplossing voor te vinden is. Veel softwareleveranciers spelen in op deze meer technische benadering en brengen specifieke GRC-modules van hun product op de markt.

Uitdagingen voor IA

De relatie tussen de internal auditfunctie en GRC is hier onbesproken gelaten omdat daar vanuit het perspectief van de NIVRA/INTAC- en de IIA-projectgroep elders in dit magazine aandacht aan wordt besteed. Opvallend is dat in de OESO-rapporten bijzonder weinig aandacht geschonken wordt aan de rol

van Internal Audit. Hierin ligt op zich reeds een uitdaging...
Het gebrek aan adequate standaarden zal – als de OESO het bij het rechte eind heeft – toch zeker door vele internal auditors opgemerkt en gerapporteerd zijn. De vraag is welk effect dat heeft gesorteerd? En als we het gevoel hebben dat het effect gering was, hoe kunnen internal auditors hun werk meer effectief maken?
En dan is er de vraag of internal auditors wel voldoende zijn voorbereid om te beoordelen of de disclosure met betrekking tot de risk managementcultuur adequaat is? Deze vraag leidt tot de gedachte dat we de internal auditfunctie moeten versterken met meer sociaal-psychologisch deskundigen. In dat verband verwijs ik graag naar het gedachtegoed van collega Arthur Izeboud RA, die onder de vlag *Culture governance* betoogt dat cultuur 'een organisatie niet overkomt' maar dat cultuur wel degelijk, en expliciet, een plaats heeft in het management control framework van de boardroom en de organisatie. Cultuur wordt hiermee een bewust stuurinstrument dat wordt gepland, uitgevoerd, gemeten en gecorrigeerd.
De GRC-tools die derhalve met urgentie ontwikkeld moeten worden – en waar internal auditors een bijdrage kunnen leveren – zijn:

- meer ook cultuurgerichte risk managementstandaarden;
- verbeterde openbaarmaking, inclusief een effectievere bijdrage van Internal Audit;
- ontwikkeling van audit op de risk managementcultuur, met bijdragen van human capital en human behavious assessors.

Toekomstige ontwikkelingen GRC 2.0

Als kritiek op de Sarbanes-Oxley-wetgeving, waar het met name gaat over de key-controls over financial reporting, is vaak naar voren gebracht dat geen van de schandalen (Enron, Worldcom, Tyco etc) door de SOx-regelgeving voorkomen had kunnen worden. Zonder afbreuk te willen doen aan alle initiatieven betreffende integrated risk management dient er meer en expliciet aandacht gegeven te worden aan de factor 'cultuur', zoals reeds door de OESO aangegeven. De invulling hiervan is niet simpel, want cultuur lijkt een containerbegrip, afhankelijk van vele soms minder beïnvloedbare factoren. Vanuit die gedachte is cultuur een resultante van 'systemen en processen', maar vooral ook van 'mensen', 'geschiedenis', et cetera. Leiderschap en tone at the top in dit kader is dan onderdeel van de mensfactor in de cultuurbepaling. De toegenomen belangstelling voor soft controls de afgelopen jaren gaat hierbij in de goede richting.
Waar veel van de GRC-tools zich richten op de factor systemen en processen, zal ik mij meer willen richten op de factor mensen om de oorzaak van de schandalen bij de wortel aan te pakken. Culture control met als deelgebied hr-control zou met name ook in de top van organisaties een andere geschiedenis tot gevolg hebben gehad. Waren we in staat geweest om het overtreden van morele en ethische waarden door Jeffrey Skilling (Enron), L. Dennis Kozlowski (TYCO), Bernie Ebbers (Worldcom), et cetera, een halt toe te roepen, dan zou de wereld er nu heel anders uitzien.
In samenwerking met HermansNieuwenhuis, bedrijfspsychologen, werk ik aan de ontwikkeling van een benadering waarbij het weten en meten van integriteit centraal staat. Natuurlijk blijven de overige GRC-tools ook nodig, al is het maar ter voorkoming en opsporing van fouten. De gedachte is dat wanneer mensen integer zijn, ze integer handelen. Of in de woorden van Pieter Hermans: 'Integriteit, daar is geen pil voor'. Dit is een geringe stap maar wellicht een met belangrijke consequenties. Ook hier geldt een oude wijsheid: stilstand is achteruitgang: GRCC 2.0: governance, risk & compliance culture!

Conclusie

Internal Audit dient zich sterk te maken voor het beheersen van de GRC-cultuur als een GRC-tool en daar hun eigen vaardigheden op aan te passen. Ook is het zaak het om de functie van Internal Audit en de betekenis die deze kan hebben in de context van GRC meer en beter over het voetlicht te brengen en zeker internationaal meer aan de weg te timmeren.

Noot

1. *Corporate Governance and the Financial Crisis: Key Findings and Main Messages,* OECD, juni 2009.

Rudy Voet is zelfstandig adviseur. Daarvoor was hij werkzaam in diverse internal auditfuncties en als deputy financial controller en governance councillor bij de OESO respectievelijk SIGMA. Hij is lid van de INTAC/IIA-projectgroep Internal Audit en Governance, Risk & Compliance.




Naar een 'paperless audit'

Zelfstandig adviseurs Tom Koning en Konstantinos Karathanasis prediken een internetrevolutie voor het auditvak. Wat hen betreft worden SAS 70-verklaringen en internal control statements voortaan volledig digitaal gefaciliteerd met hun web-based product Audit Navigator. Nu is dit anno 2010 wellicht niet opzienbarend. Echter, de Audit Navigator biedt auditors een verfrissende aanpak door ze op een gestructureerde wijze naar de beheersomgeving te laten kijken. Ze kunnen met het product slim en gefundeerd de risico's van een organisatie selecteren in plaats van mechanisch een checklist na te lopen. Kortom, een nuttige, nieuwe tool voor het toepassen van GRC.

Interview: drs. R.H.J.W. Jansen RO
Tekst: B. van Breevoort

Er zijn momenteel heel wat applicaties op de markt voor GRC. De Audit Navigator is een nieuwe loot aan de stam. Wat is de aanleiding voor jullie geweest om dit product te ontwikkelen?
Koning: "De Audit Navigator is het resultaat van een veelheid aan ervaringen die we beiden tijdens onze auditpraktijk bij KPMG hebben opgedaan en in later zelfstandig advieswerk. Wat telkens opviel is dat alle bij een audit betrokken spelers eigen systemen en spreadsheets gebruiken. Doordat de systemen veelal niet overeenkomen is het delen van informatie lastig en inefficiënt. Mijn ogen zijn pas echt open gegaan toen ik voor een bedrijf een SAS 70-verklaring hielp maken. Het bedrijf verwerkte de data in Excel en voegde het toe aan een dik rapport. Dit werd vervolgens aan de externe accountant gegeven, die daarna grote delen ging overtypen in het eigen elektronisch dossier. Toen dacht ik: dit moet effectiever en efficiënter kunnen. Daarnaast bevreemdde het mij dat het rapport van een externe accountant doorgaans begint met een uitleg van de context van het bedrijf, gevolgd door een uitvoerige procesbeschrijving, terwijl dan ergens achterin een checklist staat."

Hoe werkt het product in de praktijk?
Koning: "Het product begint met open vragen waarmee je de relevante aspecten die het risicoprofiel van de onderneming bepalen, boven water krijgt. Bij de open vragen wordt uitleg gegeven over de reden van een vraag, maar het geeft ook extra informatie die van belang kan zijn voor de beantwoording van de

vraag. Overigens, het is vereist om zelf te blijven nadenken. Het programma kauwt de antwoorden niet voor. Daarnaast kan men zelf ook vragen toevoegen die zijn toegesneden op de specifieke aspecten van een organisatie. Met de selectie vooraf kan het risicomanagement worden gestuurd en kan op een veel effectievere wijze een in control statement worden afgegeven. Hiermee voorkom je dat je een complete procesbeschrijving nodig hebt. Denk bijvoorbeeld aan een pensioenfonds dat aan de Nederlandsche Bank (DNB) moet laten zien dat men de risico's begrijpt en dat men precies weet welke maatregelen er nodig

zijn. DNB hanteert daarvoor een aantal standaardmaatstaven. Echter, het ene fonds is het andere niet. Pensioenfondsen kunnen in het beheer van hun beleggingsportefeuille hemelsbreed verschillen. In de Audit Navigator wordt door het vooraf beantwoorden van open vragen afgeleid of de organisatie in een hogere of lagere risicocategorie zit. Op basis daarvan kan nauwkeurig worden bepaald welke controlemaatregelen nodig zijn.
Het product vraagt de auditor om te beargumenteren of het interne beheersingssysteem effectief genoeg is om alle risico's af te dekken. In de applicatie vermeld je hoe je de gekozen controlemaatregelen gaat testen en wat uiteindelijk de uitkomst is van die test. Dat staat in je overzicht procesanalyse, wat een dynamisch overzicht van alle risico's, controlemaatregelen en werkzaamheden toont. Het beleid en de stuurmechanismen komen in een apart overzicht. Als wordt geconstateerd dat een stuurmechanisme niet werkt wordt er een key risk aangemaakt."

> Papieren vastlegging wordt als achterhaald beschouwd ten opzichte van een goed beveiligde elektronische vastlegging

Hoe is de toegang tot het product geregeld?
Karathanasis: "De applicatie is volledig web-based. Alle betrokken partijen kunnen inloggen met een wachtwoord en gebruikersnaam die gekoppeld zijn aan het IP-adres van de gebruiker. De loggegevens van alle gebruikers worden bewaard, zodat gecontroleerd kan worden wie wat heeft toegevoegd of heeft nagelopen. De voortgang van de reviews wordt getoond en men kan documenten toevoegen als onderbouwing van een antwoord."
Koning: "Organisaties kunnen de Audit Navigator gebruiken voor een SAS 70-verklaring, risicomanagement of een in control statement. Zij kunnen de externe accountant, die participeert in dat onderzoek, vervolgens toegang geven tot bepaalde onderdelen van het pakket. Omgekeerd kan een externe accountant het pakket gebruiken voor zijn boekenonderzoek en het object van zijn onderzoek bepaalde velden in de applicatie laten invullen. Het product geeft dus verschillende gebruikers toegang en autoriseert hen op individuele basis tot bepaalde onderdelen van het programma. Hiermee creëer je een centraal dossier waarin de betrokken partijen, waar relevant, hun commentaar kunnen geven op de verschillende aspecten van de audit."
Karathanasis: "Zo is het hele proces van een SAS 70-verklaring en een in control statement volledig gestructureerd en transparant gemaakt."

Is het een continu proces of meer een momentopname?
Koning: "Het is het meest effectief als er elk kwartaal een follow-up wordt gedaan. Risico's blijven gedocumenteerd, samen met de benodigde controlemaatregelen, de uitvoering en de uitkomst."

Is het product ook in een internationale context toepasbaar, mede in het licht dat bepaalde regelgeving per land kan verschillen?
Koning: "Audit Navigator is op het COSO-model gebaseerd en dat is, evenals andere auditstandaarden, internationaal geaccepteerd. Dus ja, het is toepasbaar in andere landen. Bovendien bevat de applicatie ook een Engelse versie. Risico's op het gebied van specifieke nationale regelgeving kan men kwijt in de toelichting, dus dat verloopt niet zozeer via de open vragen."

Hoe kan het dat er nu pas een systeem op basis van internettechnologie is ontwikkeld?
Koning: "Het is een typisch voorbeeld van de wet van de remmende voorsprong. Veel bedrijven hebben eigen pakketten gebouwd en na zo'n investering stapt men niet zomaar over op een nieuwe technologie."

Wat biedt het product voor internal auditors wiens takenpakket veel breder ligt?
Koning: "Ik ben een keer door een internal auditdienst gevraagd om te adviseren over de opzet van een operational audit. De IAD wilde van een 'ist'-positie naar een 'soll'-positie. De internal audit bestond uit een analyse of de vereiste controlemaatregelen aanwezig waren en indien niet, wat er aan gedaan werd. Ik vond dat een verkeerde aanpak, aangezien je eerst met de context moet beginnen. De soll-positie simpelweg als uitgangspunt nemen is geen due process. Eerst dienen er vragen over de interne processen beantwoord te worden, zoals: welke producten bieden ze aan? Welke afnemersgroepen zijn er? Welke systemen draaien er? Welke kwaliteitseisen gelden er?, et cetera. Zo leer je alle aspecten van het proces kennen en kun je daarna de soll-positie bepalen. Op basis daarvan kan vervolgens de ist-positie worden bekeken. Dit kan allemaal met behulp van de Audit Navigator."

Wat betekent het voor auditors dat zij naar een web-based applicatie gaan en niet meer werken op papier?
Koning: "Men ziet inmiddels in dat dit de manier van werken is voor de toekomst. Papieren vastlegging wordt als achterhaald beschouwd ten opzichte van een goed beveiligde elektronische vastlegging. Men is overtuigd geraakt van het op afstand samenwerken zonder eindeloos documentatie heen en weer te hoeven sturen."

Bij GRC en in control statements worden adequate controlemaatregelen bepaald door de context van het bedrijf. Wie heeft die context in de Audit Navigator bepaald?
Koning: "De context wordt gestuurd door de antwoorden op de

open vragen, die veelal gebaseerd zijn op (wettelijke) richtlijnen, controlestandaarden en handboeken. Daarnaast laten we de vragen ook toetsen door ervaren gebruikers."

In hoeverre verschilt de Audit Navigator van andere tools voor GRC?

Koning: "Andere producten maken in de regel alleen onderscheid tussen laag, midden en hoog complexe risico's. Wij betrekken ook het vraagstuk van de subjectiviteit erbij, want een risico kan laag complex zijn maar tegelijkertijd hoog subjectief. Gedrag en eigenschappen van werknemers en management zijn lastig te testen. Ze hebben echter een belangrijke invloed op het risicoprofiel van een organisatie. Het management kan bijvoorbeeld heel streng zijn. Dit kan enerzijds tot gevolg hebben dat mensen beducht zijn om fouten te maken en anderzijds dat men probeert zaken uit het zicht van het management te houden. Uit de beantwoording van de voormelde open vragen kan meer dan één risico volgen. Het onderzoek vindt echter plaats per risico. De ervaring heeft geleerd dat zaken fout gaan omdat ze complex, subjectief, fraudegevoelig of bewerkelijk zijn. Daarbij bepaalt het type ziekte het medicijn. Bij een complex vraagstuk zijn controleberekeningen, change management en scenario-analyses nodig. Bij een hoog subjectief risico zit het veel meer in onderzoek naar de kwaliteit en ervaring bij mensen, autorisatieschema's en referentiedatabases. Die referentiedatabases maken het mogelijk om de eigen risicoanalyse te vergelijken met die van bedrijven die actief zijn in hetzelfde vakgebied, dezelfde industrietak of soort dienstverlening. Deze benchmark helpt een organisatie om atypische risico's te duiden, waar additioneel onderzoek op kan worden uitgevoerd. Je kunt ook de verschillen herkennen en op basis daarvan onderzoeken wie de beste controlemaatregelen treft. Dit stimuleert het zelflerend vermogen van een organisatie."

> De Audit Nagivator is innovatief en maakt controle een stuk goedkoper en efficiënter

Wat is de kans dat andere partijen participeren als één partij voorstelt om met de applicatie te gaan werken?

Koning: "Ik schat die kans hoog in. Met of zonder het systeem: men heeft voor de SAS 70-verklaring of de in control statement deze onderzoeksinformatie toch nodig. Het systeem biedt bovendien gebruiksgemak en transparantie doordat alle relevante informatie geïntegreerd valt te raadplegen en er op relatief eenvoudige wijze rapporten uit kunnen worden gegenereerd."

Karathanasis: "Er is ook een duidelijke efficiënctieslag te behalen voor bijvoorbeeld internal auditors van een groot concern die op verschillende locaties gevestigd zijn. De Audit Nagivator is innovatief, maakt controle een stuk goedkoper en efficiënter en is tot nu toe ook het enige pakket waarmee een fatsoenlijke story of the audit kan worden gegenereerd."

Koning: "Voor de externe accountant en zijn opdrachtgever is er een bijkomend voordeel. De accountant kan voorafgaand aan het onderzoek reeds adviseren om de accenten te verleggen. Daardoor kan op voorhand al voor de organisatie inzichtelijk worden gemaakt welke kosten daarmee gemoeid zijn."

Konstantinos Karathanasis (l) en Tom Koning: "De Audit Navigator is het resultaat van een veelheid aan auditervaringen die we beiden hebben opgedaan."

Hoe komt een organisatie tot die afstemming met een externe accountant?

Koning: "De externe accountant kan voor zijn dossiervorming uit het systeem putten. Hij hoeft niet allerlei documenten op te vragen bij de klant of dagenlang door ordnerkasten heen te ploegen. Er is bovendien een andere reden waarom deze stap naar een meer efficiënt werkproces broodnodig is. Het vak auditing spreekt steeds minder tot de verbeelding bij jongeren. Dus alleen daarom is het oppakken van meer geavanceerde technologie voor het vakgebied van belang om het saaie spitwerk terug te dringen en mensen effectiever in te zetten."

De zin en onzin van auditaanbevelingen

Het IIA stelt op haar website dat internal auditors aanbevelingen moeten geven en actieplannen moeten aanleveren, en dat de internal auditor maximale inspanningen zal doen om te bevorderen dat de aanbevelingen daadwerkelijk worden doorgevoerd. Er zijn opvattingen dat de uitgangspunten van het IIA te rule based zijn. Zo zien we ook in de auditliteratuur dat er verschillende zienswijzen bestaan op het al dan niet geven van aanbevelingen in internal auditrapporten. Het is dan ook de vraag of de verantwoordelijkheid voor het opleveren van actieplannen bij internal auditors ligt of bij het management zelf.

Drs. M. van Raam EMIA CAMS

In het verlengde van deze discussie gaat dit artikel in op de situatie waarin internal auditors bij het vaststellen van inconsequenties tevens aanbevelingen doen aan het management voor het oplossen van die inconsequenties. Hierbij geldt dat wanneer internal auditors aanbevelingen doen zij zich zouden moeten afvragen of het doen van een aanbeveling op zichzelf voldoende is of dat er bepaalde randvoorwaarden zijn voor effectieve aanbevelingen. Tevens is het doel van dit artikel om inzicht te geven in de effectiviteit van aanbevelingen in een internal auditrapport, zodat de aanbeveling een bijdrage kan leveren aan organisatieverbetering. Hierbij hanteer ik de volgende vraagstelling: wanneer is een aanbeveling in een internal auditrapport effectief en wanneer is de aanbeveling onzinnig? Om deze vraag te beantwoorden kijk ik naar de randvoorwaarden die we aan aanbevelingen kunnen stellen, de mate waarin aanbevelingen effectief kunnen zijn en hoe de effectiviteit gemeten kan worden.

Randvoorwaarden voor aanbevelingen

Aanbevelingen moeten worden opgesteld binnen stakeholdergerichte, technische en situationele randvoorwaarden. Het opstellen van aanbevelingen binnen de stakeholdergerichte randvoorwaarden houdt in dat internal auditors vooraf hebben vastgesteld welke strategie (wegbewegende, meebewegende, gemengde of tegenbewegende strategie) het best passend is om ervoor te zorgen dat de ontvanger de aanbeveling zo goed mogelijk accepteert (Ezerman, 1983) (zie *tabel 1*).

> ‘If you want to change the world, change the way you speak about it’
>
> (Van Nistelrooij, 1999)

Een *wegbewegende strategie* kan betekenen dat een aanbeveling in zijn geheel wordt weggelaten en de internal auditor enkel de constatering doet dat de ontvanger afwijkt van de norm. Een reden om deze strategie te kiezen is dat het doen van een aanbeveling soms niets toevoegt omdat deze het omgekeerde van de constatering is.

Wegbewegende strategieën	Meebewegende strategieën	Gemengde strategieën	Tegenbewegende strategieën
Ontwijken	Informeren Faciliteren Ondersteunen Participatie	Gemeenschappelijke visie Onderhandelen	Overtuigen Macht/dwang/pressie

Tabel 1. Acceptatiestrategieën (Ezerman, 1983)

Voorbeeld wegbewegende strategie

Constatering: we hebben tijdens de audit geconstateerd dat afdeling X de richtlijnen uit de Wet bescherming persoonsgegevens niet naleeft.

Bij *meebewegende strategieën* stelt de internal auditor zich naast de ontvanger op bij het doen van een aanbeveling en wordt de ontvanger om een inbreng gevraagd (bijvoorbeeld een managementreactie).

Voorbeeld meebewegende strategie

Constatering: we hebben tijdens de audit geconstateerd dat afdeling X de richtlijnen uit de Wet bescherming persoonsgegevens niet naleeft.
Aanbeveling: wij bevelen afdeling X aan om samen met Legal te inventariseren aan welke richtlijnen nog niet wordt voldaan om hier alsnog aan te kunnen voldoen.
Response ontvanger: wij erkennen deze afwijkingen en zullen de aanbeveling opvolgen. De eerste afspraak voor het inventariseren met Legal is reeds gepland.

In *gemengde strategieën* is de invloed van de internal auditor en de ontvanger even groot en hebben beiden een inbreng in de aanbeveling. Hierbij stellen de ontvanger en de internal auditor de aanbeveling gezamenlijk op.

Voorbeeld gemengde strategie

Constatering: we hebben tijdens de audit geconstateerd dat afdeling X de richtlijnen uit de Wet bescherming persoonsgegevens niet naleeft.
Agreed management action: met het management is overeengekomen dat afdeling X samen met Legal zal inventariseren aan welke richtlijnen nog niet wordt voldaan en aan welke richtlijnen wel voldaan zou moeten worden.

Bij *tegenbewegende* strategieën is de internal auditor degene die de aanbeveling bepaalt of in sterke mate beïnvloedt. De internal auditor schrijft in dit geval de aanbeveling voor en brengt eigen ideeën krachtig naar voren en stelt zo nodig sancties op voor het niet opvolgen van de aanbeveling.

Voorbeeld tegenbewegende strategie

Constatering: we hebben tijdens de audit geconstateerd dat afdeling X de richtlijnen uit de Wet bescherming persoonsgegevens niet naleeft.
Aanbeveling: het College bescherming persoonsgegevens beveelt aan om aan de richtlijnen uit de Wet bescherming persoonsgegevens te voldoen voor 1 november 2009. Indien de richtlijnen uit de Wet bescherming persoonsgegevens niet voor 1 november 2009 voor 100 procent worden nageleefd zal afdeling X een boete ontvangen van €1000.

Per situatie moet worden gekeken welke strategie het best past om ervoor te zorgen dat de ontvanger de aanbeveling accepteert. Ik hanteer hiervoor een ruime opvatting van acceptatie, omdat in sommige gevallen acceptatie van de aanbeveling door de ontvanger niet zal plaatsvinden. In die gevallen kan het nodig zijn dat de internal auditor een wegbewegende of tegenbewegende strategie toepast. Bij het geven van internal auditaanbevelingen kunnen bovendien factoren meespelen die een bepaalde strategie uitsluiten. Indien de internal auditor bijvoorbeeld niet over sancties beschikt kan deze de machtsstrategie niet toepassen. Tevens geldt dat als een tegenbewegende strategie wordt toegepast de internal auditor de ontvanger moet kunnen overtuigen dan wel macht moet kunnen toepassen.

Technische randvoorwaarden

Technische voorwaarden zie ik als de argumentatie-eisen waaraan een aanbeveling moet voldoen. Naast de stakeholdergerichte randvoorwaarde moet de aanbeveling technisch goed in elkaar zitten en moet de argumentatie in de aanbeveling kloppen. Om te bepalen aan welke argumentatie-eisen een aanbeveling moet voldoen, is gekeken naar de argumentatieschema's die Steehouder e.a. (1999) hebben onderscheiden. Deze argumentatieschema's kunnen worden gekoppeld aan de SPROA (Situatie, Probleem, Risico, Oorzaak en Aanbeveling) rapportagemethodiek:

- *Argumentatie op basis van gedragsregels:* dit speelt vaak een rol als het gaat om handelingen en beleid (wat dient men wel/niet te doen en wat is wel/niet geoorloofd) en is te typeren als de norm of situatie waartegen de constatering wordt afgezet (Situatie).
- *Argumentatie op basis van waarderingsregels:* als het gaat om oordelen spelen waarderingsregels vaak een rol, hetgeen gezien kan worden als de constatering van het probleem (Probleem).
- *Argumentatie ter voorspelling:* hierbij wordt op basis van een bepaald verschijnsel voorspeld dat een ander verschijnsel zich voor zal doen en dit kan gezien worden als het risico van de constatering (Risico).
- *Argumentatie ter verklaring:* deze wordt gebruikt om een bepaald verschijnsel in het verleden te verklaren en kan worden gezien als de oorzaak van de constatering (Oorzaak).
- *Pragmatische argumentatie:* hierin worden bepaalde maatregelen, handelingen en adviezen verantwoord, hetgeen te typeren is als de aanbeveling (Aanbeveling).

Bij het doen van aanbevelingen worden handelingen, maatregelen en adviezen verantwoord. In de aanbevelingen zullen hierdoor dikwijls pragmatische argumentaties worden gehanteerd. Hierbij moeten internal auditors zich het volgende afvragen (Steehouder e.a., 1999):

- Is de maatregel in de aanbeveling uitvoerbaar en toelaatbaar?
- Zijn er nog niet genoemde alternatieven die zouden kunnen worden meegenomen in de aanbeveling?

Voorbeeld randvoorwaarde

Steehouder et al. (1999) expliciteren deze randvoorwaarde aan de hand van het volgende voorbeeld uit een interne beleidsnotitie van een ziekenhuis:
Constatering: uit de kwaliteitscontrole bleek dat de kwaliteit van het eten te wensen overlaat. 80 procent van de patiënten geeft aan dat het eten te eenzijdig en te koud is als het bezorgd wordt.

Aanbeveling: we stellen voor maatregelen te nemen op personeelsgebied door:
- een deskundiger koksteam aan te stellen;
- de huidige twee chefkoks te ontslaan;
- naast huishoudelijk personeel ook verpleegkundigen in te zetten voor het rondbrengen van het eten.

- Is de maatregel in de aanbeveling uitvoerbaar en toelaatbaar?
  - Uitvoerbaar: het is niet mogelijk de huidige koks te ontslaan, daar is niet voldoende juridische grondslag voor. Daarnaast is het niet mogelijk meer verpleegkundigen in te zetten voor het rondbrengen van het eten, omdat zij al tijd te kort komen voor hun kerntaken.
  - Toelaatbaar: de huidige koks kunnen niet zomaar worden ontslagen. Zij hebben immers nooit te horen gekregen dat zij hun werk niet goed doen. Bovendien zouden zij de mogelijkheid moeten krijgen zich om te scholen en hun werk te verbeteren.
- Zijn er nog niet genoemde alternatieven die zouden kunnen worden meegenomen in de aanbeveling?
  - Het aanstellen van een derde kok die gespecialiseerd is en het huidige kokteam zou kunnen aansturen is wellicht een beter alternatief. Daarnaast kunnen logistieke verbeteringen worden aangebracht in de wijze van het bezorgen van maaltijden om te voorkomen dat deze koud op de plaats van bestemming aankomen.

Om aanbevelingen op te stellen binnen de situationele randvoorwaarden maken internal auditors vooraf een inschatting van de kennis en expertise van de ontvanger alvorens te bepalen of de aanbeveling open dan wel concreet dient te worden opgesteld. In het geval de ontvanger over voldoende of zelfs meer kennis en expertise voor het oplossen van de geconstateerde afwijking beschikt dan de auditor, volstaat een *open aanbeveling*.

Voorbeeld open aanbeveling
Constatering: de afdeling hypotheken identificeert haar klanten niet conform de Wet ter voorkoming van Witwassen en Financiering Terroristen (WWFT), omdat er geen procedures zijn.
Aanbeveling: wij bevelen de afdeling Compliance aan om procedures in te richten zodat medewerkers weten hoe zij hun klanten moeten identificeren.

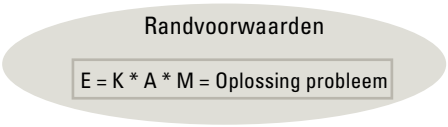
Indien de ontvanger niet beschikt over voldoende kennis en expertise, heeft deze behoefte aan een meer *concrete aanbeveling*. Immers, de ontvanger was voor het constateren van de afwijking hier niet van op de hoogte en moet bij het oplossen van de afwijking geholpen worden door de internal auditor.

Voorbeeld concrete aanbeveling
Constatering: de afdeling hypotheken identificeert haar klanten niet conform de Wet ter voorkoming van Witwassen en Financiering Terroristen (WWFT), omdat er geen procedures zijn.
Aanbeveling: wij bevelen aan om procedures op te stellen in naleving op de WWFT, waarbij tenminste wordt opgenomen dat klanten bij het aangaan van een hypotheek:
- worden geïdentificeerd op naam en adres;
- op naam en adres worden geverifieerd door middel van een kopie van een legitimatiebewijs;
- een risicoanalyse ondergaan.

Daarnaast bevelen we aan dat de hiervoor genoemde punten tevens bij reeds bestaande klanten worden uitgevoerd.

Effectiviteit van aanbevelingen

Nu rest nog de vraag wanneer aanbevelingen effectief dan wel onzinnig zijn. Een veelvoorkomende valkuil is dat internal auditors veronderstellen dat een aanbeveling effectief is als deze is geïmplementeerd door de ontvanger en is afgemeld bij de internal auditor. Het implementeren van de aanbeveling zelf is niet altijd een garantie voor het daadwerkelijk oplossen van het probleem en daarom vereist de effectiviteit van aanbevelingen een andere begripsbepaling. *Figuur 1* is een visie op hoe de effectiviteit van aanbevelingen bepaald kan worden. Hierbij wordt met de effectiviteit van een aanbeveling bedoeld dat deze het probleem heeft opgelost (O) en dat dit wordt bepaald door de kwaliteit van de aanbeveling (K), de mate waarin de aanbeveling door de ontvanger wordt geaccepteerd (A), de mate waarin een adequate follow-up plaatsvindt op de aanbeveling (M) en het voldoen aan de randvoorwaarden bij het opstellen ervan. Een aanbeveling is onzinnig als deze niet binnen de randvoorwaarden is opgesteld en niet effectief is.



Figuur 1. Effectiviteit van aanbevelingen

De effectiviteit van aanbevelingen kan aan de hand van de volgende vragen worden vastgesteld:
- Kwaliteit (K): sluit de aanbeveling aan op de constatering?
- Acceptatie (A): is de ontvanger het met de aanbeveling eens?
- Management (M): heeft follow-up plaatsgevonden?
- Oplossing probleem (O): wijst analyse door de internal auditor uit dat het probleem daadwerkelijk is opgelost na het opvolgen van de aanbeveling door de ontvanger?
- Randvoorwaarden (R): om vast te stellen of de aanbeveling binnen deze randvoorwaarden is opgesteld, kunnen de volgende vier vragen worden gesteld:
  - Welke acceptatiestrategie is het meest geschikt: wegbewegen, meebewegen, gemengde strategie of tegenbewegen? (stakeholdergerichte randvoorwaarde)
  - Is de maatregel in de aanbeveling uitvoerbaar en toelaatbaar? (technische randvoorwaarde)
  - Zijn er nog niet genoemde alternatieven die zouden kunnen zijn meegenomen in de aanbeveling? (technische randvoorwaarde)

- Over welke kennis en expertise beschikt de ontvanger en is gezien deze kennis en expertise een open aanbeveling of een concrete aanbeveling het meest geschikt? (situationele randvoorwaarde)

Gepoogd is antwoord te geven op de vraag wanneer auditaanbevelingen effectief zijn. Hierbij zijn echter verschillende kanttekeningen te plaatsen. Er zijn meerdere factoren denkbaar die overwogen hadden kunnen worden in dit artikel, waaronder:

- Politiek en macht: politiek en macht spelen een rol bij de effectiviteit van aanbevelingen, omdat de raad van bestuur en/of het audit committee kan besluiten dat een aanbeveling niet hoeft te worden opgevolgd. Politieke en machtsfactoren kunnen ertoe leiden dat een zinnige aanbeveling niet wordt opgevolgd.
- Risicoweging: een hoge risicoweging zal ertoe kunnen leiden dat de ontvanger de aanbeveling eerder oppakt dan wanneer een lagere risicoweging van toepassing is.
- Risicobereidheid: de ontvanger kan besluiten het geconstateerde probleem te accepteren en een bepaalde mate van risicobereidheid tonen, ongeacht de aanbeveling.
- Aanbevelingen die zijn opgelost voordat het rapport is uitgebracht: aanbevelingen hebben niet alleen betrekking op het rapportageproces, aanbevelingen worden eerder in het internal auditproces geboren. Het inschatten van bijvoorbeeld het kennisniveau van de ontvanger moet al bij het plan van aanpak zijn ingeschat en niet pas bij het rapportageproces.

Mischa van Raam werkt sinds 2007 als internal auditor bij ABN Amro Group Audit, waarbij zij operational- en compliance audits uitvoert. Van Raam is ook lid van de seminarcommissie van het IIA. Daarnaast is zij als vrijwilliger verbonden aan de Kindertelefoon.
Mocht u vragen hebben of geïnteresseerd zijn in het referaat *De Zin en Onzin van Auditaanbevelingen* (2009) waarop dit artikel is gebaseerd dan kunt u mailen.
✉ mischa.van.raam@nl.abnamro.com

Literatuur

- Ezerman, G., 'Zeven strategieën om leiding te geven aan veranderingen' in *Leren en leven met groepen*, Samsom, Alphen a/d Rijn, 1983.
- Nathans, H., *Adviseren als tweede beroep: resultaat bereiken als adviseur*, Kluwer Bedrijfsinformatie, 2002.
- The Institute of Internal Auditors, *International standards for the professional practice of internal auditing*, Altamonte Springs: The Institute of Internal Auditors, 2009.
- Nistelrooij, A.T.M. van, *Collectief organiseren. Een sociaal-constructionistisch onderzoek naar het werken met grote groepen*, Lemma, 1999.
- Steehouder, M., Jansen, C., Maat, K., Staak, J., van der, Vet, D., de, Witteveen, M. en E. Woudstra, *Leren communiceren. Handboek voor mondelinge en schriftelijke communicatie*, Wolters-Noordhoff, 1999.

De rol van IA bij risicomanagement?

De vraag stellen is hem niet beantwoorden!

Als gevolg van de financiële crisis zijn de rapporten en commentaren over het functioneren van risicomanagement binnen de financiële sector niet meer weg te denken. Dit alles om het risicomanagement van de organisatie te versterken, maar bovenal om het vertrouwen in de sector terug te brengen.

Drs. J. Velzen RO

Beroepsinstanties als het NIVRA en IIA buigen zich over de vraag hoe de huidige crisis kon ontstaan en welke rol de betrokken beroepsgroepen hadden kunnen spelen en in de toekomst zouden moeten spelen. Wat opvalt aan de reactie van de verschillende partijen (bestuurders, commissarissen, accountants), is dat zij zich vooral verdedigen en aangeven hún rol afdoende ingevuld te hebben. Maar gaat het bij het leren van deze crisis om de verdediging van de vragen die (aan een beroepsgroep) gesteld worden of is het nu eens tijd om zelf het initiatief te nemen en kritisch naar het eigen werk te kijken? Wat zou de internal auditor in het vervolg anders of meer moeten doen om het risicomanagement van de organisatie beter te laten functioneren?

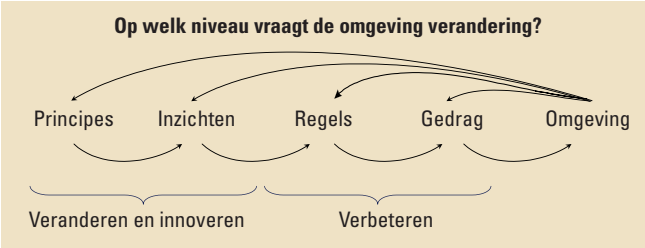
Discussie

Wat opvalt is dat veel er veel gediscussieerd wordt over wie welke taak had en hoe deze taken nu beter ingericht kunnen worden. Hiermee wordt een poging gedaan de verantwoordelijkheden beter te beleggen in de hoop dat risicomanagement beter uitgevoerd zal worden. Ook voor Internal Audit kan deze vraag gesteld worden. Wat volgt is een discussie over de verhouding tot de overige controlfuncties en de noodzaak van Internal Audit om onafhankelijk te blijven.

Met het opnieuw beleggen van verantwoordelijkheden wordt aangenomen dat de oorzaak van de problemen zit in het duidelijk beschrijven en toewijzen van de verantwoordelijkheden. Maar is deze aanname zelf niet het probleem? Door het benoemen en toewijzen van verantwoordelijkheden wordt een essentieel aspect uit het oog verloren: het nemen van verantwoordelijkheid!

De Commissie Maas zegt het als volgt: ‘Een gezonde risicocultuur moet weer het uitgangspunt zijn bij het besturen van iedere bank en van iedere bankbestuurder’.

Bij het beleggen van verantwoordelijkheden spreken we vooral over structuren en niet over de cultuur die door de Commissie Maas als uitgangspunt wordt benoemd. We moeten daarom een niveau dieper zoeken om van goed gestructureerd risicomanagement naar goed werkend risicomanagement over te gaan. Kernmerkend voor dit onderscheid is misschien wel de term risk awareness. Deze term is jarenlang gebruikt als vertegenwoordiger van het ‘zachte’ aspect van risicomanagement. De letterlijke vertaling van het woord legt bloot waar het probleem zit. Risico*bewustzijn* blijkt duidelijk niet voldoende om een adequaat risicomanagement te voeren. Vanuit risicobewustzijn moet ook een verdiepingsslag gemaakt worden naar het doorvertalen van bewustzijn in gedrag, van cognitie naar handelen.



Figuur 1. Cocreatie van verandering (naar A.F.M.Wierdsma)

Verbetering

Om daadwerkelijk tot verbetering van risicomanagement te komen zal dus een diepere verandering nodig zijn en moet de toevlucht niet gezocht worden in het aanpassen van beleidsdocumenten en TVB's (taken, verantwoordelijkheden en bevoegdheden).
Wat daadwerkelijk nodig is, is een diepe gedragsverandering van de betrokkenen en de institutionalisering daarvan in de vorm van de organisatiecultuur. Hiervoor moeten de principes van medewerkers en organisaties aangesproken worden in plaats van de (cognitieve) inzichten en bijbehorende formele regels (zie *figuur 1*).
Veranderingen op het niveau van principes zijn diepgaand en gaan daarbij ook gepaard met meer onzekerheid en onduidelijkheid over het eindpunt van de verandering.

> Door het benoemen en toewijzen van verantwoordelijkheden wordt een essentieel aspect uit het oog verloren: het nemen van verantwoordelijkheid!

In tegenstelling tot de strak geplande veranderingen op het gebied van regels en deels ook op het gebied van inzichten, vraagt dit om een grotere persoonlijke betrokkenheid en durf om naast de rationele en bewuste processen ook de irrationele en onbewuste processen van de organisatie te raken. Dit is nu juist de essentie van principle based organiseren en risico's beheersen: handelen op basis van een duidelijke set aan principes die altijd en op elk niveau van het persoonlijk functioneren geldig zijn. Deze principes moeten dan ook het onderwerp van aandacht, management en toetsing zijn. Aan die principes heb je je altijd te houden en op basis hiervan onderbouw je waarom je bepaalde regels wel (comply) of niet (explain) toepast. Maar let wel, comply of explain kan alleen betrekking hebben op regels en nooit op principes. Daarmee zijn de principes zelf rule based, zij zijn de altijd geldende leefregels voor de organisatie en haar medewerkers.

Leefregels

Welke leefregels zijn dan nodig om zwakten in risicomanagement het hoofd te kunnen bieden? Als eerste is al genoemd het nemen van verantwoordelijkheid. In plaats van zich af te vragen wie verantwoordelijk is voor een bepaald onderwerp of proces, moet elke individuele medewerker zich afvragen hoe hij kan bijdragen aan het nemen van zijn individuele verantwoordelijkheid, maar ook aan het vertegenwoordigen van de verantwoordelijkheid van de totale organisatie.
Uit het nemen van verantwoordelijkheid volgt als tweede: samenwerking. In plaats van te focussen op verantwoordelijkheidsgebieden en het afbakenen hiervan moet de aandacht worden verlegd naar onderwerpen die mogelijk tussen de wal en het schip kunnen geraken. Zo worden de snijvlakken binnen de organisatie eerder dubbel belicht in plaats van vergeten.
Ten derde is het noodzakelijk om een cultuur te hebben waarin medewerkers elkaar op hun verantwoordelijkheid kunnen en zullen aanspreken. Sterke principes hebben een sturend effect op de organisatie, maar dit ontslaat de organisatie niet van haar taak om de naleving door de organisatie te bewaken. Voorwaarde voor het aanspreken op verantwoordelijkheden is om dit vanuit een betrokken houding te doen en niet vanuit de drang om de ander eens even op zijn fouten te wijzen.

Implicaties

Welke implicaties heeft dit alles nu voor de internal auditor? De internal auditor zal zich op zijn minst de aanbeveling van de Commissie Maas voor de externe accountant aan moeten trekken: 'De externe accountant dient zich een grondig oordeel te vormen over het feitelijk functioneren van de governance binnen een bank'. Wat hier van de externe accountant gevraagd wordt, is de kern van het werk van de internal auditor. De vraag is echter op welke wijze dit grondige oordeel tot stand kan komen. Kan dit door op de huidige wijze de rolinvulling te continueren? Mijns inziens moeten de internal auditors een ommezwaai maken en zich meer gaan richten op het toetsen op het niveau van de principes van de organisatie. Leeft de organisatie haar eigen leefregels wel na en worden activiteiten ondernomen om het naleven van deze leefregels te borgen?
Concreet hebben internal auditors hier meerdere handreikingen voor. Handreikingen die niet nieuw zijn, maar waarschijnlijk wel onderbelicht. Als eerste noemen we het aanspreken van het management. Traditioneel is dit een lastig onderwerp in verband met de afhankelijke relatie tussen de auditors en het bestuur en de focus op de onafhankelijkheidsdiscussie binnen het internal auditvakgebied. Daarnaast blijkt in overleg met internal auditors dat zij veelal terughoudend zijn in het aanspreken van het management op en het adviseren over haar verantwoordelijkheden.
Echter, het hogere (en ook lagere) management heeft een dominante rol in het opstellen, uitdragen en voorleven van de principes van de organisatie. Niets werkt zo destructief op het naleven van de organisatiewaarden als managers die leefregels met voeten treden. Dit wetend is het extra belangrijk dat internal auditors zich

meer toeleggen op het aanspreken van het management op hun leidende positie in risicomanagement.
Ten tweede zal de aandacht voor de snijvlakken in de organisatie nog groter moeten worden. Audits naar specifieke afdelingen herbergen het gevaar dat de belangrijkste bevindingen buiten beeld zullen blijven. Vanuit de financiële crisis kan bijvoorbeeld de relatie tussen de financial en operational riskafdelingen genoemd worden. Door deze gescheiden te houden werden simpele vragen aan financial riskafdelingen regelmatig niet gesteld, waardoor fouten in de complexe modellen slopen. Fouten die met voldoende samenwerking over (afdelings)grenzen heen en voldoende collegiale toetsing voorkomen hadden kunnen worden. Vanuit Internal Audit zou dit ondersteund kunnen worden door specifiek ook te toetsen op de verbanden tussen afdelingen vanuit een perspectief van integrale beheersing, één governance-, risk- & complianceframework.

Voor gedragsverandering van de betrokkenen en de institutionalisering daarvan moeten de principes van medewerkers en organisaties aangesproken worden

Ten derde is er het auditen van soft controls. Ook dit is een onderwerp waar auditors mee blijven stoeien. Niet omdat dit onmogelijk is, maar omdat dit een stevige verdieping van het werk vereist en het de nodige moeite kost om variabelen te bedenken die een goede indicatie geven van het gewenste gedrag en de onderliggende principes. Door dit (deels) links te laten liggen wordt de essentie (de cultuur, waarden, uitgangspunten, et cetera) van het principle based organiseren buiten beschouwing gelaten, waardoor fundamentele afwijkingen van de leefregels niet worden geïdentificeerd en het grondige oordeel over de governance van de organisatie niet tot stand komt. Kijk bijvoorbeeld naar de Enron-case waar de ‘zachte’ informatie zoals de sturing vanuit de top en de wilde, bijna mythische verhalen over de ‘off sites’ van de kaderleden een veel nauwkeuriger beeld gaven over de beheersing dan de beoordeling van het formele, keurig opgezette beheersingsraamwerk.
Uit de hiervoor genoemde punten komt nog een implicatie naar voren: in welke mate komt het competentieprofiel van auditors overeen met het competentieprofiel dat nodig is voor het toetsen van principes in de organisatie? In dit artikel wordt hier niet uitgebreid bij stilgestaan, maar het ligt voor de hand dat een psycholoog minder moeite heeft met het bedenken van indicatoren voor de gewenste organisatiecultuur dan de gemiddelde accountant. De organisatie zal zich dus kritisch de vraag moeten stellen of haar auditafdeling voldoende is toegerust met kennis en vaardigheden om de essentie van de governance te kunnen toetsen.

Jelte Velzen is manager bij KPMG Advisory en is organisatiepsycholoog en operational auditor. Vanuit deze achtergrond houdt hij zich bezig met governancevraagstukken, vooral op het gebied van leiderschap, organisatieontwikkeling, teamprestatie en individuele gedragsverandering.

Conclusie

Als eerste moet geconcludeerd worden dat de rol van Internal Audit op zich niet belangrijk is. Veel belangrijker is het dat Internal Audit haar rol speelt binnen het totale speelveld van de organisatie en ook onderdeel is van het totale samenwerkingsverband. Het grondige oordeel over de beheersing van de organisatie (governance) is van belang, niet de beoordelaar zelf. Zoals eerder gezegd moet er in de totale samenwerking op het gebied van beheersing gedacht worden. Een integraal GRC-gedachtegoed kan hier zeker een goede bijdrage aan leveren door naar het totaalplaatje van de beheersing te kijken, maar dit gedachtegoed moet niet eenvoudigweg tot een volgende oppervlakkige herstructurering leiden.
Ook kan worden geconcludeerd dat om de governance van de organisatie daadwerkelijk te verbeteren, de onderliggende principes aangepakt moeten worden. Welke gedrag ligt ten grondslag aan het falen van risicomanagement? En welke mechanismen houden dit ‘oude’ gedrag in stand? En welke onbewuste en irrationele processen liggen hieraan ten grondslag? Er is al veel geschreven over beloningsstructuren en dit is niet zonder reden. In een relatief sterk individueel en transactiegerichte maatschappij heeft de (financiële) beloning een sterke impact op het gedrag en uiteindelijk ook op de ontwikkeling van principes. Maar zoals eerder aangegeven is het voorbeeldgedrag door het management en specifiek de top van de organisatie, van minstens zo groot belang.
Ten slotte moeten de principes die de basis voor de organisatie vormen consequent en constant worden toegepast. Een organisatie, specifiek de top, moet geloven in de principes waar zij voor staat. Dit moet dan ook tot uiting komen in de besturingsfilosofie van de organisatie. Als principle based de besturingsfilosofie is zal dit in de praktijk ook tot uiting moeten komen. Dit betekent dat de principes duidelijk gemaakt en voorgeleefd worden én dat de leiding het vertrouwen geeft om medewerkers hun verantwoordelijkheid te laten nemen. Zo belegt een organisatie niet in rollen en verantwoordelijkheden maar in principes en vertrouwen.

Machtsverhoudingen in organisaties:
wat moet en kan de auditor hiermee?

Henry Mintzberg zei ooit: 'Inzicht in machtsverhoudingen is essentieel om het functioneren van organisaties te begrijpen en om de organisatie van binnenuit en van buitenaf te controleren'. Mintzberg stelt dat wij organisaties niet zullen begrijpen, laat staan kunnen controleren, als we niet weten hoe de macht is verdeeld. Auditors hebben de taak om het management te ondersteunen bij het in control zijn. Willen ze toegevoegde waarde hebben voor het management, dan moeten ze inzicht hebben in de machtsverhoudingen in en om de organisatie.

J. Adriaanse

Het spel om de macht wordt in vrijwel iedere organisatie gespeeld, of het nu overheids- en politieke organisaties of banken en verzekeringsmaatschappijen zijn. Kennis van macht en inzicht in de machtsverhoudingen zorgen ervoor dat je begrijpt welk spel wordt gespeeld. De auditor heeft een bijzondere plaats in de organisatie. De auditafdeling zou een onafhankelijke dienst moeten zijn. Hoewel auditors zich uiteraard niet volledig aan het politieke spel in organisaties kunnen onttrekken, hebben ze de positie om als buitenstaander de machtsverhoudingen te observeren.
In mijn afstudeerscriptie[1] voor de opleiding Internal/Operational Auditing beoog ik inzicht te geven in de invloed van machtsverhoudingen op de effectiviteit van organisaties, met als doel de kennis en bewustwording bij de auditor te vergroten en zo de relevantie en de kwaliteit van operational audits te verbeteren. Het uitgangspunt is dat machtsverhoudingen in organisaties van grote invloed zijn op het functioneren en de effectiviteit van organisaties en tegelijkertijd in operational audits onderbelicht zijn.
Het analysekader is gebaseerd op een literatuurstudie van verschillende sociaalwetenschappelijke theorieën van machtsverhoudingen in en om organisaties. De belangrijkste geraadpleegde auteurs zijn C.J. Lammers, W.F.G. Mastenbroek en H. Mintzberg.

In dit artikel ga ik in op de uitgangspunten van Lammers en de theorie van Mastenboek. Het theoretisch kader dient als basis voor een lijst van aandachtspunten die de internal auditor kan gebruiken, in het bijzonder bij het in kaart brengen van de auditcontext en bij het oriënterend gesprek met de opdrachtgever.

Zienswijze op organisaties

Lammers meent dat organisaties een 'dubbelkarakter' hebben, dat wil zeggen dat zij zowel een samenwerkingsverband als een arena zijn. Lammers stelt dat er twee fundamentele analysemodellen van organisaties zijn, het systeemmodel dat de organisatie als samenwerkingsverband ziet en het partijenmodel waarin de organisatie als markt of arena wordt gezien (zie *tabel 1*).[2] Een monistische visie is eenzijdig en een verarming aan verklaringsmogelijkheden voor problemen waar organisaties mee kampen. Een synthese van beide modellen doet volgens Lammers recht aan het dubbelkarakter van organisaties.

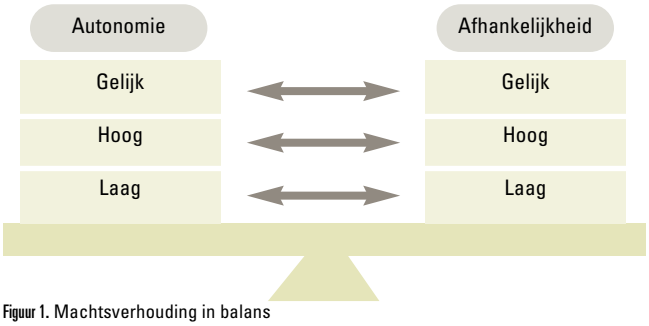
	Partijenmodel	**Systeemmodel**
Eenheid van analyse	Deelgroeperingen met eigen belangen	Organisatie als geheel met bepaalde functionele vereisten
Duurzaamheid van een organisatie	Labiel verband, hooguit een belangengemeenschap, coalitie	Stabiel verband met inherente krachten tot zelfhandhaving
Drijfkrachten	Dwang- en lokmiddelen	Norm- en saamhorigheidsbesef
Mensbeeld	Koel/berekenend, op eigen belangen gericht zijn	Sociaal zijn, gericht op organisatiebelang
'Gevoelstoon' van de analyse	Cynisch/realistisch	Idealistisch

Tabel 1. Het partijenmodel versus het systeemmodel

De meeste door auditors gebruikte modellen gaan uit van een rationele organisatie waarbij het regelkringdenken (plan, do, check, act) centraal staat en er een logische aansluiting is tussen strategie, doelen en processen. Deze zienswijze past binnen het systeemmodel. De uitgangspunten zijn, al dan niet expliciet, dat de medewerker gericht is op het organisatiebelang en voorspelbaar handelt, dat de organisatie een stabiel verband is en dat het norm- en saamhorigheidsbesef hoog is. In het partijenmodel ligt de nadruk vooral op belangen en macht. Organisaties kunnen worden geanalyseerd vanuit beide zienswijzen. Ook bij audits geldt dat voor een afdoende verklaring van organisatieproblemen een integratie van beide analysemodellen nodig is.
Mastenbroek legt een relatie tussen de machtsverhoudingen in organisaties en de effectiviteit en gaat hierbij uit van de integratie van het systeem- en het partijenmodel. Zowel Mastenbroek als Mintzberg stellen dat het meest kenmerkende aspect van macht de relatie is met afhankelijkheid. Macht en afhankelijkheid zijn dan ook sterk aan elkaar gekoppeld.

Macht en afhankelijkheid zijn onlosmakelijk met elkaar verbonden

Machtsverhoudingen in organisaties
Mastenbroek[3] verklaart de interne machtsverhoudingen, in navolging van Lammers, met behulp van het dubbelkarakter van organisaties. Het uitgangspunt is dat sociale betrekkingen gemengd van aard zijn: in relaties is de mens zowel op zichzelf gericht (autonoom) als afhankelijk van anderen. Deze behoefte aan afhankelijkheid (systeemmodel) en autonomie (partijenmodel) komt terug in het dubbelkarakter.
Mastenbroek benadrukt het belang van de balans tussen autonomie en afhankelijkheid (zie *figuur 1*). Hij legt een directe relatie tussen de machtsbalans en het (dis)functioneren van organisaties. De veronderstelling hierbij luidt: 'de ineffectiviteit van organisaties kan worden veroorzaakt door een verstoring in de machtsverhoudingen. Een zwakke wederzijdse afhankelijkheid tussen partijen leidt tot suboptimalisatie van de organisatie'.



Figuur 1. Machtsverhouding in balans

Deze veronderstelling is uitgewerkt voor drie typen relatiepatronen:
- gelijk versus gelijk (gelijkwaardige afdelingen);
- hoog versus laag (het management ten opzichte van de werkvloer of de machtige ten opzichte van de minder machtige afdelingen);
- hoog versus midden versus laag (verbijzondering van hoog versus laag, hierbij zit het middenkader tussen hoog en laag in).

Machtsverhouding gelijk versus gelijk
De effectiviteit van organisaties hangt samen met een sterke wederzijdse afhankelijkheid van gelijke partijen. Sterke wederzijdse afhankelijkheid leidt tot samenwerking. Een zwakke wederzijdse afhankelijkheid uit zich in een vechtsituatie en eindeloze onderhandelingen, wat leidt tot suboptimalisatie.

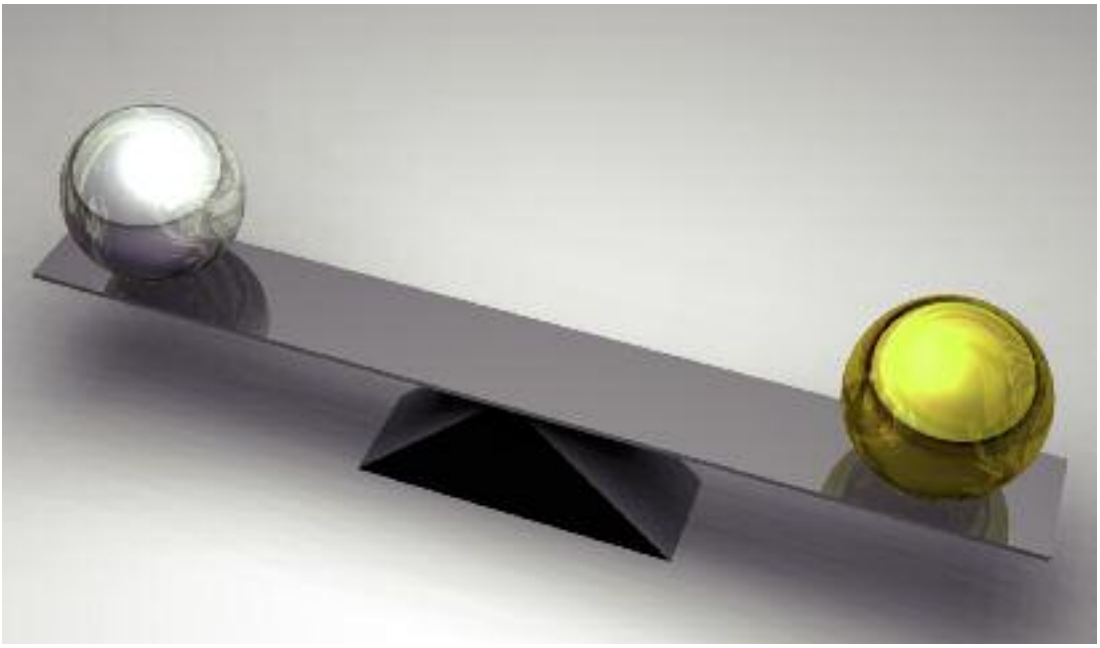
Bij de machtsverhouding *gelijk versus gelijk* hebben de organisatieonderdelen (formeel) evenveel macht. De werkelijke (informele) macht wordt bepaald door factoren als prestige, grootte of mate van succes. Tussen onderdelen bestaat vaak een neiging tot competitie. Dit kan leiden tot een vechtsituatie of tot eindeloze onderhandelingen. Als partijen wederzijds afhankelijk zijn, is er sprake van een machtsbalans. Dit leidt tot samenwerking omdat men elkaar nodig heeft.
Interventies die kunnen worden gepleegd als blijkt dat de machtsverhoudingen uit balans zijn, bestaan uit het creëren van machtsevenwicht (bijvoorbeeld door alle partijen ongeveer evenveel invloed op de besluitvorming toe te kennen), het instellen van een machtscentrum (één partij die boven de partijen staat, met de bevoegdheid om knopen door te hakken), duidelijkheid verschaffen over taakafbakening en -afstemming en het ontwikkelen van onderhandelings- en communicatievaardigheden.

Gelijk versus gelijk: een praktijkvoorbeeld

De topleiding van een ministerie heeft een probleem met verschillende directies die samen verantwoordelijk zijn voor een effectieve en efficiënte informatievoorziening binnen het departement. Er wordt veel met elkaar gediscussieerd en eindeloos onderhandeld. De problemen waarmee de top te maken heeft zijn trage besluitvorming, onduidelijkheid over taken en verantwoordelijkheden en geldverspilling. De leiding vraagt zich af wat de oorzaak van deze problemen is.

Machtsverhouding hoog versus laag
De effectiviteit van de organisatie hangt samen met de machtsbalans tussen hoog en laag. Er is sprake van een machtsbalans als de beheersing door hoog en de autonomie van laag in balans zijn.

Het relatiepatroon *hoog versus laag* betreft het management en de medewerkers, maar is ook aan de orde tussen hogere en lagere



organisatieonderdelen. Bij dit relatiepatroon is de tendens dat het management de organisatie wil beheersen door uitbreiding van de macht of inperking van de autonomie op de werkvloer. Bij de medewerkers bestaat de neiging om de autonomie te vergroten. Managers maken vaak gebruik van hun hiërarchische positie om macht uit te oefenen. Zij kunnen hiertoe bijvoorbeeld dwang- en lokmiddelen inzetten om doelen te bereiken, ingewikkelde inspraaksystemen creëren of zaken van de agenda weren. De medewerkers beschermen de autonomie vaak op een subtiele wijze. Hierbij kan worden gedacht aan het vaag houden van afspraken, het oneigenlijk gebruikmaken van kennis en vaardigheden of de leidinggevenden tegen elkaar uitspelen.
Interventies bij problemen in de machtsbalans hoog versus laag kunnen er als volgt uitzien: persoonlijke macht vervangen door (onpersoonlijke) regels en procedures, een verandering van de leiderschapsstijl en het ontwikkelen van inzicht bij alle partijen in de dynamiek die zich voordoet bij hoog versus laag.

Hoog versus laag: een praktijkvoorbeeld

De directeur van een zorgorganisatie maakt zich zorgen over een specifieke unit binnen de instelling. Er zijn signalen opgevangen dat medewerkers het niet (meer) naar hun zin hebben. Dit blijkt onder andere uit een recent medewerkerstevredenheidsonderzoek en uit de toename van het ziekteverzuim. Tevens blijkt dat (duidelijk meer dan bij vergelijkbare afdelingen) het middenmanagement beheersingsproblemen heeft die zich uiten in bijvoorbeeld de moeizame implementatie van een nieuw kwaliteitssysteem.

Machtsverhouding hoog versus midden versus laag

Dit relatiepatroon is een verbijzondering van het relatiepatroon hoog versus laag. Voor de effectiviteit van de organisatie is het van belang dat er sprake is van een machtsbalans tussen hoog, midden en laag. Rolconflicten, rolonduidelijkheid en stress zijn signalen van een situatie waarbij het middenkader klem zit tussen hoog en laag.

Bij het relatiepatroon *hoog versus midden versus laag* zit het middenkader tussen het hogere management en de werkvloer in.
*R*olonduidelijkheid door onduidelijkheid over functie en verantwoordelijkheden en slechte communicatie en rolconflicten door de tussenpositie van het middenkader doen zich regelmatig voor. Rolonduidelijkheid en rolconflicten leiden tot stress bij het middenmanagement.
Mogelijke interventies bij hoog versus midden versus laag zijn het creëren van duidelijkheid over taken, verantwoordelijkheden en bevoegdheden, het stimuleren van een open communicatie en het ontwikkelen van vaardigheden bij het middenkader om niet klem te raken tussen hoog en laag.

Hoog versus midden versus laag: een praktijkvoorbeeld

Het bestuur van een grote onderneming realiseert zich dat het middenkader van de organisatie zich in een lastige positie bevindt. Dit blijkt onder andere uit veel verloop, een hoog werkgerelateerd ziekteverzuim en veel ad-hocoplossingen door het middenkader. De directeur heeft zojuist kennis genomen van het theoretisch kader van Mastenbroek en vraagt zich af of het middenkader last heeft van rolconflicten en rolonduidelijkheid.

Bruikbaarheid en relevantie voor de auditor

Op basis van de inzichten van Mastenbroek en Mintzberg is een analysekader opgesteld en geoperationaliseerd in de vorm van een aandachtspuntenlijst. Per relatiepatroon is een aantal punten genoemd die kunnen duiden op problemen in de machtsbalans. De lijst met aandachtspunten is geen checklist, maar dient als denkmodel om mogelijke verklaringen te bieden voor signalen die zich voordoen in de onderlinge verhoudingen. De lijst is door een groep auditors beoordeeld op relevantie, bruikbaarheid en toepasbaarheid bij operational audits.
Bij *gelijk versus gelijk* kan een zwakke wederzijdse afhankelijkheid blijken uit het volgende:

- de doelen en belangen van de onderdelen zijn verschillend en onderling strijdig;

- er wordt voortdurend onderhandeld over de toedeling van budgetten;
- er zijn (bij voortduring) communicatieproblemen tussen de onderdelen.

De neiging tot beheersing door *hoog* bij *hoog versus laag:*
- het inzetten van dwang- en lokmiddelen om doelen te bereiken;

Auditors zullen organisaties niet begrijpen, laat staan controleren, als ze niet weten hoe de macht is verdeeld

- gebruikmaken van overtuigingskracht (demagogie of propaganda) om voorstellen of ideeën in de organisatie doorgevoerd te krijgen;
- het hanteren van korte reactietermijnen.

Het beschermen van de autonomie door *laag:*
- oneigenlijk gebruikmaken van kennis en vaardigheden om zichzelf onmisbaar te maken of doelstellingen van de organisatie te beïnvloeden;
- misbruik maken van rechten ten koste van het organisatiebelang;
- de omgeving op de hoogte stellen van misstanden: de vuile was buiten hangen of klokkenluiden.

De volgende signalen duiden op mogelijke problemen in het patroon *hoog versus midden versus laag:*
- overspannenheid en/of een hoog ziekteverzuim bij het middenkader;
- spanningen tussen het middenkader en het hogere management en problemen op de werkvloer;
- klachten en ontevredenheid over het functioneren van het middenkader.

Vooronderzoek/contextanalyse

De internal auditor kan de aandachtspuntenlijst gebruiken tijdens het vooronderzoek van de audit, om na te gaan of er verstoringen zijn in de machtsbalans die de effectiviteit van de organisatie schaden. Bij een brainstormsessie met het auditteam kunnen de volgende zaken aan de orde komen: welke partijen zijn betrokken bij de audit? Wie is opdrachtgever, wie is auditee? Wat is hun rol/plaats in de organisatie? Hoe is de onderlinge verhouding? Hebben de spelers een geschiedenis met elkaar, positief of negatief? Wie heeft welke belangen? Wat zijn de (in)formele machtsmiddelen van de betrokkenen? In het gesprek met de opdrachtgever kan worden bepaald of deze openstaat voor een analyse van de machtsverhoudingen in zijn organisatie.
Als tijdens het onderzoek blijkt dat er mogelijk sprake is van een disbalans in de machtsverhoudingen, kan dit gevolgen hebben voor de keuzen die worden gemaakt tijdens het vervolg van de audit.
- Het opstellen van een normenkader: als de gewenste situatie (norm) over de interne machtsverhoudingen kan worden vastgelegd en wordt gedragen door de opdrachtgever, dan kan een audit uitgevoerd worden naar de bestaande machtsverhoudingen (ist) en deze worden gerelateerd aan de wenselijke verhoudingen (soll).
- De onderzoeksmethodiek: welke wijze van materiaalverzameling is het meest passend: interviews of een (anonieme) enquête? Welke vragen worden gesteld? Met wie worden interviews gehouden? Aan welke groepen worden enquêtes voorgelegd? Aan wie worden de bevindingen en conclusies voorgelegd? Dit zijn uiteraard vragen die bij iedere audit spelen, maar de keuzen die hierbij worden gemaakt zijn mede afhankelijk van de geconstateerde machtsverhoudingen.

Tot slot

Auditors zijn er om organisaties een spiegel voor te houden om zo een bijdrage te leveren aan het beter functioneren van de organisatie. De klassieke auditaanpak is door de accentuering van het regelkringdenken waardevol, maar ook eenzijdig. Organisaties zijn namelijk niet alleen een samenwerkingsverband maar ook een arena. Wil een auditor een goed beeld schetsen van het functioneren van organisaties, dan is aandacht voor machtsverhoudingen onontbeerlijk. Belangen, macht en politiek moeten dan ook een centrale plaats innemen in audits.

Noten

1. Adriaanse, J., *Machtsverhoudingen in en om organisaties, een handvat voor de operational auditor*, ESAA, 2009.
2. Lammers, C.J. e.a., *Organisaties vergelijkenderwijs: ontwikkeling en relevantie van het sociologisch denken over organisaties,* 2000.
3. Mastenbroek, W.F.G. *Verandermanagement door betere sturing en meer zelforganisatie, organisatievernieuwing als het managen van interdependenties,* 1996.

Jacomien Adriaanse is operational auditor bij de Audit Dienst van het ministerie van Defensie. In het verleden heeft zij diverse functies bekleed in de GGZ en welzijn (uitvoering, beleid & kwaliteit en toezicht). Adriaanse heeft Bestuurskunde gestudeerd aan de Universiteit Leiden en is recent afgestudeerd aan de opleiding Internal/ Operational Auditing aan de Erasmus Universiteit Rotterdam.

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 **Thierry Meulenbroek**, senior auditor bij de Departementale Auditdienst van het ministerie van Verkeer en Waterstaat en **Marco Kuijper**, strategieontwikkelaar bij de Waarderingskamer. Beiden zijn tevens oprichter van Auditwise.

De wereld in een sneeuwbol

Een deugdelijke auditopzet en een adequaat normenkader zijn essentieel voor de kwaliteit van een audit. Maar er zijn meer variabelen die de kwaliteit beïnvloeden. Zo kan gekozen worden voor een lagere kwaliteit uit kosten- en/of tijdoverwegingen. Echter, als de kwaliteit van de audit het succes bepaalt, waarom zien we er dan zo weinig expliciet van terug in de rapportages?
Op dit terrein is er een parallel met meer kwantitatief georiënteerde vakgebieden als geodesie (landmeetkunde). Voordat metingen worden verricht, wordt de kwaliteit van het te verwachten meetresultaat bepaald. Daarbij wordt onderscheid gemaakt tussen ‘precisie’ en ‘betrouwbaarheid’. Precisie is de nauwkeurigheid van een meting. Het meten met een laser heeft immers een hogere precisie dan het meten met een liniaal. Het begrip betrouwbaarheid duidt op de ‘mate van gecontroleerdheid’. Meerdere metingen leiden tot een hogere betrouwbaarheid.
Beide begrippen kunnen eenvoudig worden vertaald naar het auditproces. Zo hebben interviews over het algemeen een lagere precisie dan een cijferanalyse en zal de betrouwbaarheid van een bevinding op basis van twintig interviews groter zijn dan op basis van één interview. Hoewel de auditor heel goed weet dat het hanteren van andere audittechnieken invloed heeft op de kwaliteit, zien we echter dat keuzen op dit terrein impliciet worden gemaakt.

Uit onderzoek[1] in de gezondheidszorg blijkt daarnaast dat inspecteurs in 52 procent van de gevallen onterecht een (te) positief oordeel geven. Een van de redenen ligt in het instrumentarium. De werkelijkheid is immers nooit volledig te vatten in een instrument. Opvallend is wel dat oordelen eerder te positief dan te negatief zijn als er geen aansluiting is met het normenkader. De reden daarvoor ligt bij de auditor. Zo worden aspecten meegenomen die voor de inspecteur van belang zijn, maar die niet in de normatiek staan. Daarnaast speelt dat harmonisatie prettiger is dan confrontatie. Elementen die direct invloed hebben op de kwaliteit.

Concluderend weten we dat (operational) auditors voornamelijk kwalitatief onderzoek doen. Hierbij geldt dat niet alle situaties in een normenkader passen. Een auditvraag past evenmin in een vast normenkader als de wereld in een sneeuwbol. Ook is de auditor juist opgeleid om met discretionaire ruimte om te gaan. Hoe borg je dan de kwaliteit van de audit? Naar onze mening door meer grip te krijgen op het begrip kwaliteit, bijvoorbeeld door de termen betrouwbaarheid en precisie te introduceren en nadrukkelijk bespreekbaar te maken. Voer voor de start van de audit én bij het opstellen van de eindrapportage de discussie over de auditkwaliteit en leg gemaakte keuzen en conclusies vast. Als we dit beter in de vingers krijgen kunnen we ook meer gaan vertrouwen op andere methoden en technieken binnen ons werkveld.

Het volgende dat we bespreekbaar willen maken is de overdracht van de verantwoordelijkheid voor de column. Wij dragen de verantwoordelijkheid over aan Joyce Teunissen. Joyce werkt als programmamanager innovatie bij ProRail, doceert aan de Rijksacademie en is eigenaar van Joy Consultancy & Education.

Noot

1. Tuin, S.M., Berg, H. van den, Robben, P.B.M. en F.J.G. Janssens, *De relatie tussen normen en oordelen in het toezicht op de gezondheidszorg*, 2009.

Joop Brakenhoff komt tegenwoordig met bier thuis in plaats van worteltjes, omdat hij zijn baan bij Ahold verruilde voor een internationale internal auditfunctie bij Heineken. Hij vertelt waarom hij de overstap heeft gemaakt.

Joop: "Ik ben mijn werkzame leven begonnen in 1985 bij KPMG Accountants in Den Haag. Na mijn afstuderen in 1994 als NIVRA-registeraccountant ben ik via Heerema International, waar ik head of Internal Audit was, en Burg Industries, waar ik na group controller in 1996 statutair financieel directeur ben geworden, in de zomer van 2002 begonnen bij Ahold als vice president Internal Audit Europe. Dat was een half jaar voor de openbaring van het 'drama Ahold'. 2003 was een jaar van branden blussen en het corrigeren van de gevonden tekortkomingen in de wereldwijde beheersingsstructuur en met name in de financiële rapportage. Dat was een zeer enerverende en leerzame periode waarin vanaf 2003 de gehele accounting-, reporting- en internal controlorganisatie opnieuw werd ingericht en waar ik vanaf begin 2004 als vice president Accounting & Control verantwoordelijk was voor de wereldwijde implementatie van onder andere IFRS, SOx, de Finance Acadamy en het aantrekken en ontwikkelen van financieel talent voor deze activiteiten."

Politieman

Nadat in 2005 Ahold had afgerekend met de nasleep van begin 2003, werd Joop in de zomer van 2005 gevraagd om eindverantwoordelijk te worden voor de wereldwijde Ahold internal auditfunctie. "Het was onder andere mijn taak om na de crisis de positionering van de internal auditfunctie te veranderen van de toenmalige 'politieman'-rol naar de 'business partner'-rol. Dat betekende dat veel meer dan voorheen de relatie met het locale management en de businesskennis van de auditors belangrijk werd. Daarnaast namen de taken van Internal Audit toe en naast ons oordeel over de financiële beheersingsmaatregelen (financial controls) werd ook ons oordeel gevraagd over strategische, operationele en IT-beheersingsmaatregelen. Internal Audit werd gepositioneerd als duidelijke third line of defense waarbij wij ook de governance-, risk management- en de internal controlactiviteiten (de second line of defense) beoordeelden. Ook de auditaanpak werd aangepast, met meer aandacht voor een transparant en consistent auditproces, korte en bondige rapportages, en in het algemeen met meer toegevoegde waarde voor het management.
Dit alles kon natuurlijk niet gebeuren zonder dat ook goed werd gekeken naar de personele invulling van de afdeling. Het succes en de erkenning die Internal Audit, en vooral de individuele auditors, de afgelopen jaren hebben gekregen van zowel het het locale management als het executive management gaf mij veel voldoening. Na vijf jaar kan ik met een goed gevoel zeggen dat Internal Audit succesvol gepositioneerd is binnen Ahold en klaar is voor de volgende groeifase waarin Ahold is beland."

Natuurlijk moment

Dit was voor Joop dan ook een natuurlijk moment om te kijken naar een volgende uitdaging. "Een uitdaging die ik heb gevonden bij Heineken. De internal auditfunctie bij Heineken kent een bredere agenda dan die bij Ahold en omvat bijvoorbeeld ook de faciliterende rol bij de inrichting van governance-, risk- and compliance-activiteiten. Heineken kent in tegenstelling tot Ahold geen aparte risk management- en internal controlafdelingen. Heineken groeide de laatste paar jaar sterk door recente overnames in Europa, Mexico en Brazilië en met nieuwe samenwerkingen in andere delen van de wereld zoals in Indië en het Verre Oosten. De als gevolg van de groei ontstane vraagstukken over de inrichting van de governance-, risk-, compliance- en auditactiviteiten bij Heineken zijn voor mij dan ook een mooie uitdaging waarbij ik de ervaringen die ik heb opgedaan bij mijn vorige werkgevers goed kan gebruiken."

Positief

Zijn gezin is positief over deze nieuwe uitdaging. "Mijn kinderen (14, 16 en 19 jaar) zien de meerwaarde van een vader die met bier thuiskomt in plaats van met worteltjes. Mijn vrouw heeft een wat meer gebalanceerd oordeel, zij vindt het een prachtige kans om bij een parel als Heineken te werken, maar begrijpt ook dat ik wat meer zal gaan reizen. Ze zijn het reizen echter wel gewend en het is een logisch gevolg als je in dit kikkerland werkzaam bent bij multinationals en je een baan hebt met mondiale verantwoordelijkheid. Ik ben dan ook blij met de steun die mijn gezin en vooral mijn vrouw mij altijd heeft gegeven bij het maken van de keuze voor een werkgever. De mensen die dicht bij ons staan zullen bevestigen dat zonder haar onvoorwaardelijke steun mijn carrière er wellicht minder mooi zou hebben uitgezien."
Gezien de korte tijd dat Joop bij Heineken werkzaam is, is het moeilijk om nu al ervaringen te delen. "Wel herken ik de trots van de werknemers op hun bedrijf. Net zoals het hoge 'Hollands Glorie'-gehalte van Heineken dat ik eerder heb mogen meemaken bij Heerema, Burg Industries en bij Ahold, en de positieve en pragmatische instelling bij het oplossen van problemen. Een wereldspeler met een duidelijke 'can do'-mentaliteit, met respect voor het verleden en niet bang om (beheerste) veranderingen door te voeren die van belang zijn om de korte- en langetermijndoelstellingen te realiseren.
Als ik over vijf jaar terugkijk en kan zeggen dat Heineken zijn doelstellingen heeft gehaald, waarbij Heineken Internal Audit een zodanige positie heeft dat het wordt gezien als onderdeel van dat succes en wordt gewaardeerd voor de ondersteuning aan het management en de RvC, ben ik een gelukkig man."

De harde realiteit van soft controls

Audit Magazine (4-2009) behandelde uitgebreid het thema soft controls, onder meer door een interview met James Roth. Hij zei dat in Nederland soft controls meer worden (h)erkend dan waar ook. Dat is natuurlijk een mooi compliment, maar wordt deze (h)erkenning ook naar de praktijk vertaald? Bijvoorbeeld bij het managen van risico's?

E. Kleijn

In de (audit)literatuur is veel geschreven over de onderwerpen soft controls en risicomanagement. De combinatie van beide onderwerpen in één artikel komt echter minder vaak voor. Laat staan de toepassing van soft controls in de praktijk, zoals door Jan Vink (Algemene Rekenkamer) wordt bevestigd in datzelfde *Audit Magazine*. Voor mij was dit 'gebrek' aan literatuur over de combinatie van beide onderwerpen de reden om onderzoek te doen naar de expliciete toepassing van soft controls in risicomanagement en mijn scriptie over dit onderwerp te schrijven. De onderzoeksvraag was: in hoeverre worden soft controls expliciet toegepast bij de beheersing van risico's in de vervoerssector?

Wat zijn soft controls?

Om de vraagstelling te kunnen beantwoorden, moet eerst worden vastgesteld wat soft controls precies zijn. De literatuur is hier niet eenduidig over: naast verschillende definities kom je ook verschillende benamingen tegen. Voor het onderzoek is de volgende definitie gehanteerd: soft controls zijn controls gericht op het bewust beïnvloeden van het innerlijke (persoonlijkheid en overtuigingen) van de medewerker, tot uiting komend in het gedrag van de medewerker bij het realiseren van de gestelde doelen van de organisatie.

Voor risicomanagement heb ik de definities van COSO en Chapman gecombineerd, omdat deze combinatie beter de lading dekt. Mijn definitie van risicomanagement luidt als volgt: risicomanagement is het proces dat organisatiebreed wordt uitgevoerd om risico's te identificeren, te analyseren en te prioriteren om vervolgens door middel van een set aan controls de kans en impact te managen en zo de continuïteit van de organisatie te borgen.

Onderscheid

Om de toepassing van soft controls in risicomanagement te kunnen onderzoeken, is het onderscheid tussen hard en soft controls belangrijk. Om dit onderscheid te kunnen maken, moet worden vastgesteld wat het doel of beoogd werkingsgebied van de control is. Het doel van de control kan gericht zijn op verschillende niveaus van persoonlijk functioneren: het gedrag van de betreffende persoon, de vaardigheden of de persoon zelf (persoonlijkheid en overtuigingen) (Nathans). Op basis van deze niveaus van persoonlijk functioneren kan onderscheid worden gemaakt tussen drie typen controls: hand (hard), hoofd (semisoft), hart (soft) (zie *figuur 1*).

> Soft controls zijn niet de eerste keus bij het managen van risico's

Tot zo ver de soft controls. Nu de risico's nog. Waar anders dan in risicoregisters zijn risico's beschreven, inclusief de wijze waarop de risico's worden beheerst? Voor dit onderzoek zijn (delen van) de risicoregisters van drie organisaties in de transportsector onder de loep genomen: Schiphol Groep, Havenbedrijf Rotterdam en ProRail. Daarnaast heb ik de hoofden van de auditafdelingen, managers risicomanagement en managers reporting van de organisaties geïnterviewd. Per onderzocht risico is vastgesteld of de control hard, semisoft dan wel soft is.

Tijdens het onderzoek bleek al snel dat niet voor alle controls gemakkelijk vast te stellen was welk type control het was (hard, semisoft of soft). Dit werd veroorzaakt door de vaak summiere beschrijving van de controls. Op basis van de omschrijving kon niet eenduidig worden vastgesteld wat het beoogd werkingsgebied van de control was en dus niet of het een hard of een (semi) soft control betrof.
De harde realiteit van soft controls in de Nederlandse vervoerssector is dat de daadwerkelijke toepassing van soft controls in risicomanagement beperkt is. Slechts 6 tot 10 procent van alle controls zijn 'pure' soft controls. Voeg je daar ook de semisoft controls aan toe, dan wordt dat 20 á 35 procent. Dat betekent dat het percentage hard controls ongeveer 65 procent is (zie *figuur 2*).

Bevindingen

Wat betekenen deze cijfers en wat betekenen ze niet? Wat ze zeker niet betekenen, is dat risico's in de Nederlandse vervoerssector onbeheerst zijn. Wat de cijfers wel betekenen, is dat de vervoerssector meer hard controls dan soft controls toepast. Hierbij moet de kanttekening worden geplaatst dat het onderzoek beperkt is gebleven tot de beschrijving van controls in de risicoregisters. Of de beschreven controls daadwerkelijk in de praktijk zijn toegepast, is buiten de scope van het onderzoek gebleven. Ook de werking van de beschreven controls is dus niet onderzocht. Het onderzoek heeft daarnaast tot een aantal andere bevindingen geleid. De belangrijkste zijn:

a. De verschillen tussen de organisaties met betrekking tot de betekenis en toepassing van risicomanagement, risicoregisters en soft controls zijn minimaal.
b. De verschillen tussen bedrijfseenheden binnen één organisatie met betrekking tot de toepassing van soft controls in risicomanagement zijn echter aanzienlijk.
c. Communicatie en samenwerking zijn de meest toegepaste (semi)soft controls.
d. Soft controls worden niet altijd toegepast waar je dat zou verwachten.

a. De verschillen tussen de organisaties met betrekking tot de betekenis en toepassing van risicomanagement, risicoregisters en soft controls zijn minimaal

Naast de Code Tabaksblat speelt bij alle drie de organisaties de ambitie tot verdere professionalisering een belangrijke rol bij de implementatie van risicomanagement. Het Enterprise Risk Managementmodel van COSO en control risk self assessments zijn belangrijke bouwstenen van het risicomanagementproces. Ook hebben alle drie de organisaties een zogenaamd risicoregister. De verschillen tussen de risicoregisters zijn minimaal.

b. De verschillen tussen bedrijfseenheden binnen één organisatie met betrekking tot de toepassing van soft controls in risicomanagement zijn echter aanzienlijk

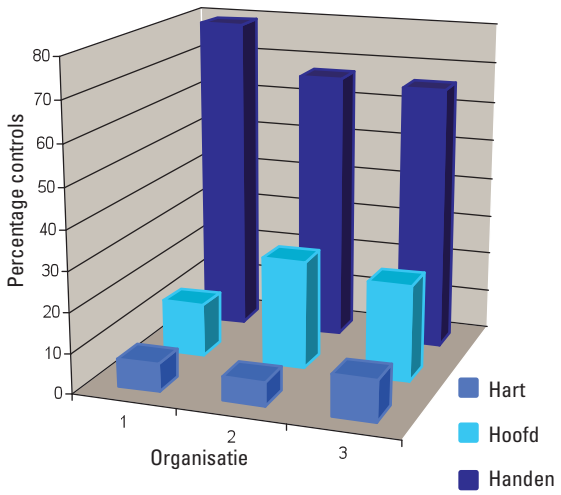
Als we binnen de drie organisaties naar de verschillende bedrijfseenheden kijken die zijn onderzocht, zien we grote verschillen in de toepassing van soft controls. De percentages soft

Handen (hard)
Controls zijn direct gericht op het beïnvloeden van het gedrag van de medewerker. Bijvoorbeeld procedures, handleiding, planning.

Hoofd (semisoft)
Controls zijn gericht op de kennis en vaardigheden van de medewerker. De kennis en vaardigheden van de medewerker komen vervolgens tot uiting in het gedrag. Bijvoorbeeld training, opleiding, overleg, presentatie.

Hart (soft)
Controls zijn gericht op de medewerker zelf (de persoonlijkheid en overtuigingen). Het handelen wordt indirect beïnvloed door de medewerker te overtuigen, te stimuleren en te motiveren waarna de medewerker 'uit zichzelf' het gewenste gedrag vertoont. Bijvoorbeeld integriteit, loyaliteit, samenwerken.

Figuur 1. De drie typen controls



Figuur 2. Verdeling controls totaal (in %)

controls in de onderzochte bedrijfseenheden van organisatie 1 lopen uiteen van 3 tot 27 procent, in organisatie 2 van 0 tot 15 procent en in organisatie 3 van 7 tot 12 procent. Het percentage soft controls in organisatie 3 is gemiddeld hoger dan in de andere organisaties. Mogelijke verklaringen voor deze verschillen tussen bedrijfseenheden zijn de aard van het hoofdproces en de cultuur. De verklaringen zijn echter niet onderzocht.

c. Communicatie en samenwerking zijn de meest toegepaste (semi)soft controls

Voor alle drie de organisaties geldt dat communicatie (overleggen, afstemmen, terugkoppeling, et cetera) en samenwerking de meest toegepaste soft controls zijn.

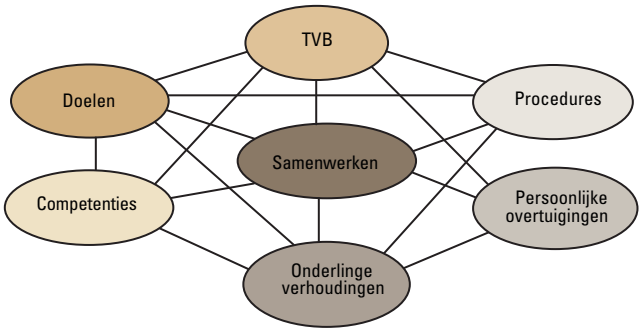
d. Soft controls worden niet altijd toegepast waar je dat zou verwachten

In meerdere gevallen zou te verwachten zijn dat in de risicoregisters, op basis van de risico-omschrijving, een andere control (hoofd/hart) dan de beschreven control (handen) wordt toegepast. Bijvoorbeeld voor het risico 'miscommunicatie tussen partijen' zijn procedures, werkcontracten en voorschriften als (hard) controls genoemd. Dit lijkt echter maar een deel van de oplossing te zijn. Wellicht dat (semi)soft controls als communicatietraining, wederzijdse stages, bedrijfsbezoeken of 'kijkjes in de keuken' het risico effectiever kunnen beheersen.

Soft controls zijn geen harde realiteit

Een beetje lef

En dan nu de belangrijkste vraag voor auditors: wat betekenen deze resultaten voor het werk van de auditor? Hoewel slechts een klein percentage van de controls soft is, zullen auditors over kennis en vaardigheden moeten beschikken om ook de effectiviteit van deze soft controls te kunnen beoordelen en het management te kunnen adviseren over het toepassen van soft controls. Een veel gehoord nadeel van soft controls is echter dat ze niet meetbaar zijn en dat niet in alle gevallen eenduidige normen kunnen worden vastgesteld. Dit is echter geen excuus om 'dus maar geen audits op soft controls uit te voeren'. Met creativiteit en een pragmatische aanpak kunnen ook soft controls prima worden beoordeeld. Een beetje lef van de auditors en goede afstemming met het verantwoordelijk management zijn ook belangrijk.
Binnen ProRail wordt het auditen van soft controls ook zeker niet uit de weg gegaan. Een voorbeeld van hoe ProRail Audit de soft controlsamenwerking heeft geaudit. Binnen ProRail wordt, net als bij de meeste organisaties, veel samengewerkt tussen bedrijfseenheden of afdelingen. Samenwerking is een soft control. Samenwerking wordt immers niet alleen procedureel vastgelegd, maar wordt ook vanuit de overtuiging van de medewerker gevoed dat samenwerking tot de beste resultaten leidt. Om de effectiviteit van de samenwerking tussen bedrijfseenheden te auditen, hebben we in de bij ons bekende managementliteratuur gezocht naar 'effectieve samenwerking' om te bepalen wat de (minimale) voorwaarden zijn voor samenwerking. Op basis van een model voor effectieve samenwerking (uit *Toolbox Teamontwikkeling* van Rubin, Plovnick en Fry, 1981) hebben we het 7-S Raamwerk (McKinsey) gevuld met die elementen van samenwerking die volgens ons als meest effectief mogen worden beschouwd (zie *figuur 3*).



Figuur 3. Normenkader samenwerking

We hebben de samenwerking getoetst voor een drietal MIRT-projecten (Meerjarenprogramma Infrastructuur, Ruimte en Transport), waaronder de aanleg van de Hanzelijn. Voorbeelden van deze elementen waren:

- TVB (taken, verantwoordelijkheden en bevoegdheden): TVB's zijn bekend, worden begrepen en zijn conflictloos.
- Doelen: doelen zijn bekend, worden begrepen en nagejaagd.
- Procedures: procedures zijn vastgelegd, afwijkingen van de procedures worden beargumenteerd en gecommuniceerd.
- Samenwerken: betrokkenen voelen zich eigenaar van het project en benutten elkaars kennis en vaardigheden.
- Competenties: betrokkenen zijn resultaatgericht, nemen verantwoordelijkheid/initiatief, zijn klant- en omgevingsgericht en betrouwbaar.
- Persoonlijke overtuigingen: betrokkenen kennen elkaars overtuigingen, doelen en de context, ze begrijpen het (niet) handelen van collega's.
- Onderlinge verhoudingen: betrokkenen vertrouwen elkaar, voelen zich prettig bij het samen uitvoeren van het project.

Workshops

Evenals in het 7-S Raamwerk zijn in het model van *figuur 3* naast harde (bijvoorbeeld procedures, TVB) ook zachte (bijvoorbeeld persoonlijke overtuigingen, onderlinge verhoudingen) elementen van samenwerking opgenomen. De zeven elementen van samenwerking hebben we afgestemd met het verantwoordelijk management van de betrokken bedrijfseenheden en als 'norm' gehanteerd voor de audit. Vervolgens hebben we drie workshops georganiseerd en gefaciliteerd, waarvoor per MIRT-project medewerkers uit minimaal drie verschillende bedrijfseenheden zijn uitgenodigd.

Tijdens de workshops is aan de deelnemers gevraagd om in multidisciplinaire groepen aan te geven welke acties, afspraken, middelen, et cetera, positief en negatief hebben bijgedragen aan de samenwerking tussen de bedrijfseenheden en daarmee tot een succesvolle uitvoering van het MIRT-project. Hierbij is de focus gelegd op de positieve aspecten, omdat we vooral van elkaars kwaliteiten willen leren en niet van elkaars fouten.

Soft controls zijn te auditen met creativiteit en lef

Omdat wij als auditors toen nog geen ervaren facilitators waren, hebben we ter voorbereiding van de workshops gesproken met een externe facilitator. Hij heeft ons aanwijzingen gegeven en met ons de belangrijkste do's en don'ts van workshops besproken. Na elke workshop hebben we een korte evaluatie gedaan met de deelnemers en gevraagd naar tips (wat kan beter aan de workshop?) en kicks (wat vonden jullie goed aan de workshop?). Deze tips en kicks hebben we vervolgens in de volgende workshop toegepast. Na drie workshops hadden we negen flipovervellen met positieve en negatieve punten voor samenwerking. Met behulp van de mind-maptechniek hebben we de punten geclusterd naar de zeven elementen van samenwerking en de rode draad van (positieve elementen van) samenwerking binnen MIRT-projecten in kaart gebracht.

Enquête

Naast de workshop hebben we ook alle deelnemers gevraagd een korte enquête in te vullen. Met behulp van een vragenlijst hebben we meer inzicht verkregen in de werking van de zeven elementen. De resultaten van de workshops (elementen van effectieve samenwerking) en de enquête zijn gepresenteerd aan het verantwoordelijk management en vastgelegd in een rapportage. Nu, ongeveer een jaar na afronding van de audit, krijgen we nog steeds verzoeken om de resultaten van de audit in projectteams toe te lichten. Dit zijn natuurlijk mooie resultaten van de audit, maar wat minstens zo mooi is, is de terugkoppeling van de deelnemers over de workshop. Alle deelnemers vonden de workshops erg waardevol. Niet eerder hadden ze in een dergelijke setting met elkaar gesproken over samenwerking. Het heeft hen nieuwe inzichten gegeven en meer begrip gecreëerd voor elkaars standpunten en beweegredenen. Hoewel de normen waaraan we de samenwerking hebben getoetst niet heel concreet waren en zeker niet meetbaar, heeft deze audit veel toegevoegde waarde voor ProRail. En voor ons als auditors was het een bevestiging dat niet alles hoeft te worden gemeten om het te weten. Met creativiteit en lef kun je jezelf, maar vooral ook anderen overtuigen van de effectieve werking van (soft)controls.

Ellen Klijn is senior auditor bij ProRail bv. In het kader van haar afstudeerscriptie voor de EMIA-opleiding aan de UvA heeft zij het hier besproken onderzoek uitgevoerd. Het voorbeeld van de auditsamenwerking is een voorbeeld uit de ProRail auditpraktijk en was geen onderdeel van de scriptie. Het voorbeeld toont aan hoe auditors met creativiteit en lef soft controls kunnen auditen.
✉ Ellen.klijn@prorail.nl.

Ongelofelijke megalomane persoonlijkheden

Eric Smit • Nina • Prometheus • ISBN 9789044614657 • Marja Bontekoe • De dossiers Lakeman • Prometheus • ISBN 9789044616606

Nina en *De dossiers Lakeman*, twee boeken over 'grootheden' uit de zakelijke wereld. Twee boeken waar veel reclame voor is gemaakt. Bij diverse radio- en tv-programma's zijn de schrijvers uitgebreid aan het woord geweest. In het geval van het boek over Lakeman leidde dit prompt tot een kort geding met een uitspraak over de slagingskansen van zijn rechtszaken waarover in het boek de juiste data staan, maar waarin de schrijver zich vergaloppeerde in haar uitspraken. Eric Smit moest zich ook direct bij de rechter melden na de publicatie van zijn boek. En bij Lakeman en Nina Brink is dat altijd gevaarlijk, want beide grootheden zijn extreem bedreven in rechtszaken.

Het is voor gewone stervelingen nauwelijks voorstelbaar dat je dingen doet die zulke enorme gevolgen hebben. In het geval van Nina Brink waren er de heel behoorlijke financiële gevolgen voor haarzelf en voor de aandeelhouders van de WorldOnline-beursgang en bij Lakeman was het zijn beruchte DSB-uitspraak. Groots, bijna megalomaan en met verbazingwekkend grote gevolgen. Ik heb mij er nog het meest over verbaasd dat in beide boeken te lezen is hoe ongelooflijk veel vertrouwen mensen geven aan andere mensen die alleen maar hoeven te pretenderen iets te kunnen. En het lijkt net of dat geschonken vertrouwen groter wordt naarmate de risico's groter worden.
Bij veel van wat ik las verbaasde ik mij over het gemak waarmee de grootste besluiten worden genomen. Bijna omgekeerd evenredig aan de omvang van het risico. Toen ik een kennis in de advocatuur vroeg of men dan in dergelijke zaken geen borgstellingen vraagt, vertelde hij dat de ego's van dergelijke figuren zo groot zijn dat dat eigenlijk not done is. Zo van: hoezo moet ik een borgstelling betalen, weet je niet wie ik ben? Je zou blij moeten zijn dat ik met mijn case bij jou kom… Kortom, arrogant, zelfverzekerd… en vertrouwenwekkend.

Nina is geschreven met een journalistieke, zij het wat cynisch, achtergrond. Dat maakt het een heel leesbaar boek. Het krijgt daardoor vaart en snelheid. Maar je moet er wel van houden. Het is alsof je een lang krantenartikel aan het lezen bent. Er worden veel namen gebruikt en feiten weergegeven. Soms kijkt de schrijver wat van een afstand maar uiteindelijk wint de journalist, die met een kritische blik naar de details kijkt, het. Het boek over Pieter Lakeman is veel negatiever. De schrijfster pretendeert onafhankelijk te zijn, maar van ongeveer alles wat in het boek staat druipt het wantrouwen af en lijkt ze meer en meer een grumpy old lady. Niets van wat Lakeman doet is goed. Het boek leest daardoor veel minder door, je verlangt echt naar het einde.

Ik kreeg beide boeken toegestuurd ter recensie en zat me tijdens het lezen af te vragen of ik ze ook zelf zou kopen. Ik was nieuwsgierig, maar dat is op zichzelf geen goed argument. Ik ben ook nieuwsgierig naar de diverse koppen die op de cover van de *Privé* en de *Story* staan, maar om nu te zeggen dat dat een reden is om die bladen te kopen of te lezen?
Na het lezen van beide boeken kan ik me voorstellen dat *Nina* een boek is dat ik zou willen lezen en ook wel in mijn bibliotheek zou willen hebben. Het komt dan naast de bibliografie van Jan Baan te staan en naast wat boeken van Manfred Kets de Vries over megalomane managers. Het boek over Lakeman is gewoon te mager en te negatief. Je leert dat je niet te veel vertrouwen moet hebben in dure adviseurs en je leert wat de jongeren van de MiniOnderneming op de plaatselijke ROC al leerden: als je gemaakte afspraken niet vastlegt, kom je jezelf ooit een keer tegen. Dat kan spannende lectuur opleveren, maar vaker levert het uiterst saaie vervelende verhalen op die niemand echt verder brengen.
In het boek van Kets de Vries over megalomane managers worden schetsen gegeven van diverse ego's. Die zijn dan zo gericht op hun eigen succes dat alles daarvoor moet wijken. Het bewijs van die stelling zag ik in de schets van Nina Brink. Maar, hoewel de schrijfster haar uiterste best doet, herkende ik Lakeman niet in die schetsen. Hooguit is het een wat zonderling mens.

De marketing van beide boeken is uitstekend. En het maakt niet uit hoe je genoemd wordt als je maar genoemd wordt, aldus de algemene marketingregel. Ik kan me voorstellen dat een financieel auditor wel geïnteresseerd is in *Nina* om de vraag te beantwoorden hoe hij om kan gaan met dergelijke ongebreidelde megalomanie en anderen te waarschuwen voor de nadelige gevolgen van onterecht gesteld vertrouwen. Het boek over Lakeman wordt verstoord door de negatieve sfeer en biedt nauwelijks inzage in de persoon en de drijfveren van Lakeman-achtige persoonlijkheden en heeft daardoor eigenlijk geen plaats in mijn boekenkast verdiend.

Renze J. Klamer is management consultant bij Sentle bv (www.sentle.nl)
Duinvoet 8, 8242 RB Lelystad,
0320-231280,
✉ klamer@sentle.nl

Samen werken aan stevige pijlers

Sander Weisz is tegelijkertijd met zijn aantreden als nieuwe voorzitter van het IIA begonnen aan een verbouwing van een recent aangekocht huis uit 1923. Werkelijk alles wordt vernieuwd behalve de vier buitenmuren. Weisz is van plan het nodige zelf te doen, maar erkent dat zijn vrouw handiger is en dat hij daarnaast ook professionele hulp heeft ingeschakeld. Ook het IIA gaat een nieuwe fase in met een vernieuwd bestuur. Weisz voorspelt geen grootscheepse 'verbouwing', want de basis is solide. Toch wil hij met hulp van het bestuur, de commissies en de leden nieuwe pijlers voor de toekomst slaan. Daarvoor zijn alle ideeën en suggesties welkom. Het IIA blijft tijdens de verbouwing dan ook open voor alle leden.

Interview: drs. R.H.J.W. Jansen RO
Tekst: B. van Breevoort

Wie is Sander Weisz?
"Ik woon samen met mijn vrouw en twee dochters van tien en dertien in Sassenheim, midden in de Bollenstreek."

Wat doe je momenteel voor werk?
"Sinds september 2007 werk ik bij USG People als corporate director Internal Audit, waar ik sinds kort ook leiding geef aan het opzetten van de functie risk management. USG People is een uitzendorganisatie met merken als Creyfs, Content, Unique en Start. Wij zijn actief in veertien landen in Europa met het hoofdkantoor in Almere. Ik ben bij USG People gaan werken omdat ik daar een internal auditafdeling van de grond af mocht gaan opbouwen. Vanuit Almere beoordelen we de risico's in de werkmaatschappijen en SSC's verspreid over Europa en analyseren we waar mogelijke kansen liggen. USG People ondersteunt mijn voorzitterschap van het IIA van harte, omdat die functie natuurlijk ook afstraalt op ons bedrijf."

Hoe ben je in het auditvak gerold?
"Ik ben ooit begonnen op de Optiebeurs. Daarna heb ik gewerkt voor Vluchtelingenwerk en het ministerie van Justitie. In die banen had ik nooit een echt bevredigend gevoel. Totdat ik op een dag les kreeg van Arie Molenkamp tijdens de opleiding Operational Auditing. Ik was meteen verkocht. Het principe dat een internal auditor kijkt naar een organisatie en deze een spiegel voorhoudt, sprak mij enorm aan en Molenkamp kan er ook zo mooi over vertellen. Ik was zo enthousiast dat ik hem aan het eind van de opleiding vroeg of hij mij kon introduceren bij

> Als internal auditor ben je continu bezig te analyseren waar het beter kan. Er spelen telkens andere politieke en strategische belangen

bedrijven waar ik operational audits zou kunnen doen. Hij wilde dat best, maar vroeg me waarom ik niet bij hem kwam werken. Zo kwam ik terecht op de afdeling management services van KPMG. Molenkamp was en is nog steeds een groot voorbeeld voor mij. Ik heb in die tijd veel geleerd doordat je allerlei verschillende bedrijven adviseert. Maar op een gegeven moment wilde ik de internal auditfunctie echter in één bedrijf gaan uitoefenen. Het werd KPN. Daar heb ik vijf jaar audits gedaan en drie jaar als manager 'in de fabriek' gewerkt waar KPN de dienstverlening voor de zakelijke markt bouwt en beheert."

Wat vind je leuk aan het auditvak?

"Er is zo veel variatie. Ook al ga je iedere keer het auditproces door, het object van de audit wisselt steeds. Er spelen telkens andere politieke en strategische belangen. Als internal auditor ben je continu bezig te analyseren waar het beter kan. Als je binnen één bedrijf het auditvak uitoefent, gaat de audit steeds gemakkelijker. Dat komt omdat je de organisatie beter leert kennen. Dit opent de mogelijkheid om je veel meer te verdiepen en meer klussen op te pakken dan dat je als external auditor zou kunnen doen. Zo kun je als internal auditor bijvoorbeeld in de voorfase van een beoogde fusie of overname er al bij betrokken worden.

Bij USG People zijn we momenteel bezig om Content en Unique samen te voegen tot één bedrijf. Ook daar heeft de internal auditafdeling een duidelijke stem en kunnen we toegevoegde waarde bieden. Een ander voorbeeld is dat USG People in Nederland bezig is met de implementatie van een SAP-systeem. Dat heeft een behoorlijke impact, dus ook daar houden wij de spiegel voor op zowel inhoud als proces. Het houdt dus wat mij betreft niet op bij bijvoorbeeld de compliance aan declaratieregelingen. Er is veel meer wat een internal auditafdeling bezighoudt en moet houden. Binnen het IIA werken we derhalve aan een veelzijdige invulling van de functie Internal Audit. Het is de taak van de internal auditor dat hij in een breed scala aan onderwerpen toegevoegde waarde kan bieden aan het management door middel van zijn auditrol. Men moet je niet als last of kostenpost ervaren. Als het management de internal auditor niet meer vraagt voor interessante opdrachten, dan is het mis. Dan is of de inhoud van je output niet goed of je verkoopt je niet goed binnen de organisatie. Er zijn tal van aspecten waar de internal auditor bij betrokken hoort te zijn: compliance, toepassing van nieuwe wet- en regelgeving, systeemgerelateerde opdrachten, opdrachten voortkomend uit verandermanagement en ad-hocopdrachten bij onregelmatigheden of bij speciale gebeurtenissen zoals overnames, fusies of samenvoegingen van bedrijven. Dat hele palet hoort als auditonderwerp bij de internal auditafdeling thuis."

Bij USG People heb je een brede internal auditafdeling opgezet. Leefde dat idee al bij USG People?

"Eerlijk gezegd niet. Sterker nog, bij de sollicitatie bleek dat men zich op financial audits wilde gaan richten. Ik gaf aan dat ik dan niet de juiste man was, aangezien ik geen RA ben. Ik voegde daar echter aan toe dat het in mijn ogen beter is om de auditfunctie breder op te zetten. Kijk niet alleen naar de financiële verantwoording, want dat is het sluitstuk van de hele bedrijfsvoering. Er zijn veel meer onderdelen die een audit verdienen. In de uitzendbranche gaat het om effectiviteit en efficiency in de backoffice en om kwalitatieve marketing, verkoop en communicatie in de frontoffice. Het is toen even stil gebleven maar twee maanden later bleken ze overtuigd van mijn visie en kreeg ik de vrijheid om een multidisciplinair auditteam samen te stellen, hangend onder de CEO en met een korte communicatielijn naar het audit

committee. Het werd een leerproces, want de organisatie moest wennen aan het fenomeen audit."

Is de bredere inzet van de auditfunctie inmiddels gangbaar in het bedrijfsleven?

"Ja, USG People is geen uitzondering. Er zijn volgens mij juist vrijwel geen internal auditafdelingen meer die zich puur en alleen met compliance of financial audits bezighouden. De crux blijft echter of het management of de CEO de bredere invulling van de internal audit toejuicht en ondersteunt. Daarom is het goed om audits te laten evalueren door de betrokkenen. Daarmee kan naderhand worden aangetoond of de audit inhoudelijk als goed is ervaren en professioneel is uitgevoerd."

Is het voorzitterschap een uit de hand gelopen hobby of een erebaan?

"Het is zeker een erebaan waar je stevig voor aan de bak moet en ik heb niet van meet af aan gedroomd van het voorzitterschap van het IIA. Ik kom oorspronkelijk uit de VRO en was voor het samengaan van het IIA en VRO redactielid van *dit* Magazine, dat werd uitgegeven door de VRO en het IIA. Ik heb later zitting genomen in het bestuur van het IIA om als een van de bruggenbouwers te fungeren. Ik was toen nog niet eens lid van het IIA. Wat mij direct opviel was de andere sfeer. Het was een grotere vereniging en anders georganiseerd. Toch heeft de fusie van de VRO en het IIA nog heel wat voeten in de aarde gehad. Uiteindelijk is het gelukt. Ik heb nu de functie geruild met Fred Steenwinkel, hij was voorzitter en ik vicevoorzitter. We hebben dit gedaan om continuïteit te borgen. Het is namelijk funest als een voltallig bestuur aftreedt en een heel nieuw bestuur moet worden samengesteld."

Sander Weisz: "We moeten oppassen dat we alleen een langetermijnvisie bouwen terwijl we op de korte termijn onvoldoende presteren."

Wat gaat de toekomst ons brengen met jou als voorzitter van het IIA?

"Het zal een bestendiging van de lijn betekenen die de voorgaande jaren reeds is ingezet. We doen dat gezamenlijk met het algemeen bestuur als vertegenwoordigers van de IIA-leden. De commissies moeten daarbij onder een zekere autonomie kunnen opereren. Het is wel de bedoeling dat het bestuur de richting aangeeft waar we in de toekomst naartoe willen. We streven naar een verdere verbetering van de onderlinge samenwerking en een nog betere dienstverlening naar de leden. We zullen drie pijlers neerzetten die we zowel intern als extern gaan uitdragen:
Pijler 1: de internal auditor is onmisbaar in corporate governance. Dit betekent dat niet alleen zijn rol en positie in de organisatie duidelijk is, maar dat men Internal Audit ook ziet en ervaart als cruciale schakel in (corporate) governance.
Pijler 2: het IIA ontwikkelt en bewaakt de hoogwaardige professionaliteit van het internal audit vakgebied. Het gaat om een optimale ondersteuning van het vakgebied door het IIA. Wij zijn van driehonderd naar 2500 leden gegroeid en van tien trainingen naar meer dan veertig trainingen en seminars per jaar. We hebben een zeer gewaardeerd congres en een goed gelezen full-colour *Audit Magazine*. We hebben veel bereikt en willen nu nog een stap verder.
Pijler 3: IIA is de leidende autoriteit inzake internal auditing in Nederland en wordt als zodanig ook door de stakeholders in de maatschappij en het bedrijfsleven gezien en benaderd. Deze pijler hebben we nog niet geslagen. Het IIA speelt nog geen prominente rol in de diverse discussies. Het begint wel te komen, maar we moeten die plaats in het debat actiever gaan opeisen.

Het kiezen van de richting is relatief het eenvoudigst, maar de richting vasthouden is het moeilijkst. En we moeten oppassen dat we niet alleen aan een langetermijnvisie bouwen terwijl we op de korte termijn onvoldoende presteren. Dus, nadat de richting is aangegeven moet dat meteen een vervolg hebben in het samen met de leden actief oppakken van initiatieven om bij het gewenste toekomstdoel te komen. Daar gaan we met het algemeen bestuur en de commissies concreet aan werken. Volgens mij zijn er alleen al in de commissies genoeg waardevolle ideeën om de volgende stappen te zetten. Maar wij staan uiteraard open voor elke suggestie van ieder lid. We gaan naar verdere ontwikkeling en groei in omvang en kwaliteit. Het vertrekpunt is uitstekend: een prachtige vereniging met een solide basis van actieve leden, gezonde financiën en een goede inhoudelijke invulling. Op zo'n fundament is het goed bouwen."

Nieuwe voorzitter

Op het presidents dinner van 24 april jl is bekendgemaakt dat Sander Weisz de nieuwe voorzitter is van IIA. Sander Weisz neemt het stokje over van Fred Steenwinkel, die afscheid neemt als voorzitter en zitting neemt in het bestuur als vicevoorzitter. Wij danken Fred vanaf deze plek voor zijn inzet van de afgelopen jaren.

Sander Weisz, de nieuwe voorzitter.

Jaarverslag 2009

Voor het jaarverslag 2009 zijn we afgestapt van het verstrekken van de ledenlijst in gedrukte vorm. Op het moment van drukken zijn de gegevens namelijk alweer achterhaald. Vandaar dat u de actuele ledengegevens alleen via de website kunt raadplegen. Daarnaast is het jaarverslag in een nieuw jasje gestoken. U kunt een exemplaar van het jaarverslag aanvragen via het bureau: iia@iia.nl.

Presidents dinner

Jaarlijks organiseert IIA Nederland het presidents dinner. Jefferson Wells is al een aantal jaren sponsor van dit diner, dat traditiegetrouw in een aansprekende omgeving wordt georganiseerd. Op 24 april jl. werden onze vrijwilligers welkom geheten te kasteel Doorwerth nabij Arnhem. Een prachtige locatie die de dresscode 'black tie' eer aandoet en waardoor de genodigden al meteen in een feestelijke stemming verkeerden.
Voor de gelegenheid werd tussen de bedrijven door een aantal kleine acts opgevoerd om de gasten te vermaken. Fred Steenwinkel, die afscheid nam als voorzitter om de rol van vicevoorzitter te gaan vervullen, droeg symbolisch de voorzittershamer over aan Sander Weisz. De laatste handeling die Steenwinkel als voorzitter verrichtte, was afscheid nemen van Wilma Bakker. Zij heeft door de jaren heen de notulen van de ALV's en de bestuursvergaderingen verzorgd.
Het was prachtig weer en dat zorgde voor een fantastische avond. Voor een aantal genodigden luidde dit een heerlijk weekend in de buurt van Doorwerth in, aangezien zij bleven overnachten. Zij hebben ongetwijfeld de volgende dag nog nagenoten in deze mooie omgeving.

Sander Weisz neemt de hamer over van Fred Steenwinkel.

Afscheid van Wilma Bakker.

Bibliotheek

De bibliotheekcollectie van IIA Nederland is ondergebracht bij het bureau van het IIA in Naarden. De bibliotheek is toegankelijk voor alle leden van het IIA. De verzameling omvat ruim tweehonderd publicaties, voornamelijk van de IIA Research Foundation van de afgelopen twaalf jaar. De catalogus is te raadplegen op de website van het IIA onder het kopje 'vaktechniek'.
Als u de bibliotheek wilt bezoeken kunt u vooraf een afspraak maken via het bureau, tel.: 088-0037100. U kunt een informatieverzoek ook per mail richten aan: iia@iia.nl.

Nieuwe aanwinsten

- *Externe verslaggeving van publieke organisaties. Een multidisciplinair theoretisch kader vanuit een verticaal verantwoordingsperspectief*, drs. M. Dees RA.
- *Using Surveys in Internal Audits*, IIA Research Foundation, Hernan Murdock DBA, CIA with James Roth PhD, CIA, CCSA, ISBN 978089413677.
- *Auditing International Entities*, 2nd Edition, IIA Research Foundation, David O'Regan CIA, FCA, ISBN 9780894136740.

IIA-Congres 2010 All on board

Op 21 en 22 juni 2010 organiseert het IIA wederom het jaarlijkse congres. Dit jaar vindt het congres op een wel zeer unieke locatie plaats, namelijk op de SS Rotterdam. Op 20 april jl. bracht de commissie Congres met enkele genodigden een werkbezoek aan de SS Rotterdam. De unieke ligging met zicht op de skyline van Rotterdam vanaf het dek en de compleet in stijl van de jaren vijftig gerenoveerde inrichting zorgden ervoor dat iedereen zin heeft gekregen om een bijzonder evenement te mogen beleven.
Het congres bestaat uit plenaire sessies en substreamsessies. Tijdens het plenaire gedeelte komen gerenommeerde sprekers aan het woord. De substreams hebben als thema fraude, maatschappelijk verantwoord ondernemen (mvo) en de audit professional. De chief audit executives van auditdiensten kunnen deelnemen aan een speciale, exclusieve substream op het gebied van governance, risk en compliance (GRC) (D). Het volledige programma kunt u vinden op www.iia.nl.

SS Rotterdambezoek.

Algemene ledenvergadering

De algemene ledenvergadering vond plaats op 8 april jl. bij het ministerie van Financiën in Den Haag. Het was een goed bezochte vergadering met een aantal hoogtepunten.

Kurt Aulman, penningmeester, presenteerde een positief financieel resultaat over 2009. IIA heeft de zaken weer goed op orde en is tevreden over de werkzaamheden van het secretariaatsbureau, APPR. Daarnaast deelde voorzitter Fred Steenwinkel mee dat hij na het presidents dinner vicevoorzitter zal zijn en Sander Weisz voorzitter. Michel Kee is benoemd als algemeen bestuurslid.

De algemene ledenvergadering.

Activiteitenkalender 2010

Juni	
7	Workshop Doen Nederlandse bedrijven massaal aan kapitaalvernietiging?
6 t/m 9	International conference – Atlanta 2010
9-10	Training Introductie Operational Auditing
17	Seminar Succesvol organiseren van de internal auditfunctie
21-22	IIA Jaarcongres 2010: All on board!
24-25	Creativiteit, onmisbaar voor auditors

September	
3	Seminar Leiderschap/Management
14	Seminar Internal Audit How to audit your business strategy?
15-16	Control self assessment: facilitation skills
16	Round-table Trends en ontwikkelingen op de arbeidsmarkt
23	Seminar Ontwikkelingen in Internal Auditing
23-24	Introductie IT Auditing
29-30	Training Financial auditing voor internal auditors

Oktober	
6-7	Effectief strategisch risicomanagement
7	Overtuigende audit professionals
7-8	Training Practical coaching voor auditors

UNIVERSITEIT VAN AMSTERDAM

Buluitreiking EMIA

Afgelopen najaar hebben zeventien studenten hun bul gehaald aan de EMIA-opleiding. De lijst met namen en afstudeeronderwerpen is als volgt:

Saskia **Sprengers**	De rol van Internal Audit bij overnames
Linda **Midgley**	Ethical Issues in the Application of Soft Controls and Implications for Managers and Auditors
Roxanne **van der Beek**	De rol en de toegevoegde waarde van de internal auditor bij het tot-standkomingsproces van een publiekprivate samenwerking
Mischa **van Raam**	De zin en onzin van auditaanbevelingen
Jacqueline **Can**	Interactief leren & auditkwaliteit
Sandra **Annema**	Risk management & Internal Audit en de kredietcrisis bij financiële instellingen: lessons learned
Sander **van den Broek**	De rol van projectcontrollers en projectauditors bij infrastructurele megaprojecten
Jutta **Heijmans**	Governance, risk & compliance en de internal auditfunctie
Sacha **le Feber**	Geschikt of ongeschikt? Een zoektocht naar een model voor het toetsen van een integriteitbeleid
Tessa **de Haas**	Een framework voor het selecteren van auditobjecten ten behoeve van het risk-based auditjaarplan
Michiel **van Schieveen**	Auditen van luchtemissies
Maarten **van der Linden**	Leuker kunnen ze het niet maken, wel makkelijker
Ellen **Klijn**	De harde realiteit van soft controls - De expliciete toepassing van soft controls in risicomanagement in de vervoerssector
Sjoerd **Jansen**	XBRL en continuous monitoring/continuousauditing
Marc **van Estrik**	Soft controls bij professional servive firms... Een uitdaging voor Internal Audit?
Martijn **Knottnerus**	Het auditen van de tone at the top – een utopie binnen organisaties?
Klaas **Pool**	De relatie van risk appetite van de onderneming tot de oordeelvorming van de internal auditor

De geslaagden.

EQUIS heraccreditatie voor Amsterdam Business School

Met trots kondigt de Amsterdam Business School (ABS) (waar de EMIA-opleiding onderdeel van uitmaakt) aan dat de EFMD (European Foundation for Management Development) de prestigieuze EQUIS-accreditatie – een Europees kwaliteits-keurmerk voor business schools – verlengd heeft met een periode van drie jaar. Met deze heraccreditatie sluit de Amsterdam Business School aan in de rij van 122 andere topinstituten uit 34 landen, waaronder de London Business School, INSEAD en IMD.

Duidelijke erkenning

Het is een duidelijke erkenning van de ontwikkeling die de ABS de afgelopen drie jaar heeft doorgemaakt. Het EQUIS Peer Review Team dat de ABS in december 2009 bezocht was niet alleen onder de indruk van het visitatierapport, maar ook van het studentenrapport dat door een groep ABS-studenten was samengesteld.

De investering van de ABS in nieuwe onderwijsprogramma's en studentenaantallen en de vooruitgang die geboekt is met het stimuleren van internationaal onderzoek, zijn specifiek genoemd in de rapportage van het EQUIS-team. Zij noteerden ook vooruitgang in transparantie van structuren, beleid en verantwoordelijkheden, alsmede vooruitgang in de managementstructuur, het bestuur van de ABS en in de bedrijfscontacten. Het nieuwe gebouw van de ABS werd gezien als indrukwekkend, niet alleen wat betreft de faciliteiten, maar ook als symbool.

ERASMUS UNIVERSITEIT ROTTERDAM
ESAA
ERASMUS SCHOOL OF ACCOUNTING & ASSURANCE

Buluitreiking Internal/Operational Auditing en IT-Auditing

Op maandag 22 maart 2010 vond de buluitreiking plaats voor afgestudeerden van de postinitiële masteropleidingen Internal/Operational Auditing en IT-Auditing. Studenten die in de periode november 2009 tot en met maart 2010 zijn afgestudeerd, konden op de Erasmus Universiteit Rotterdam hun bul in ontvangst nemen uit handen van de program directors Ron de Korte en Gert van der Pijl. Elke student werd persoonlijk toegesproken en ontving de bul met de titel executive master in Internal Auditing respectievelijk executive master of IT-Auditing. De voorzitter van het curatorium van de beide opleidingen, Lex van der Drift, sprak namens het curatorium tot de studenten. Namens de studenten voerde Nico Jan de Rooij het woord. Hij gaf een korte schets van wat de IT-Auditing-opleiding voor hem had betekend. Samengevat zei hij: "Deze studie is geweldig interessant en verbreedt en verdiept je wereldbeeld".

De afgestudeerden.

Voorlichtingsavond

ESAA organiseert op 8 juni 2010 een voorlichtingsavond voor geïnteresseerden in het opleidingenaanbod, waaronder de postinitiële masteropleidingen IT-Auditing en Internal/Operational Auditing. Tijdens deze avond krijgt u uitleg over de inhoud en de opbouw van de opleiding. U kunt zich aanmelden via www.esaa.nl. Voor meer informatie over de opleidingen kunt u contact opnemen met Miranda Snel, tel.: 010-4082437.

Nieuwe brochures 2010/2011 I/OA en IT-Auditing

De nieuwe brochures van de IT-Auditing en I/OA-opleidingen staan op www.esaa.nl of zijn aan te vragen via esaa-it@ese.eur.nl en esaa-ioa@ese.eur.nl.

Inschrijving kopjaar IT-Auditing (RE)

Naast de reguliere tweejarige opleidingen Internal/Operational Auditing en IT-Auditing gaat ook het kopjaar IT-Auditing eind augustus van start. Studenten die de Internal/Operational Auditing-opleiding hebben gevolgd (RO's) kunnen instromen in het kopjaar van de opleiding IT-Auditing, wat betekent dat de studie in één jaar kan worden afgerond. Ook afgestudeerde RA's (tot en met het theoretisch examen) en RC's kunnen een verkorte opleiding IT-Auditing volgen. Voor RE's, RC's en RA's bestaat natuurlijk ook de mogelijkheid om het kopjaar tot EMIA (RO) te volgen. De kopjaren worden voorafgegaan door een precourse (van een tiental colleges) die start op 25 augustus 2010.

Verslag (alumni)bijeenkomst Balanced Change Card

Op 15 april jl. organiseerde ESAA een bijeenkomst voor alumni en andere geïnteresseerden waarin werd ingegaan op de Balanced Change Card, een raamwerk voor het inrichten en evalueren van veranderorganisaties. Wim Bouman, een van de bedenkers van deze Change Card, ging daarbij in op de overeenkomsten en verschillen tussen de welbekende Balanced Scorecard van Kaplan en Norton en de Balanced Change Card. De Balanced Change Card maakt bovendien gebruik van de ideeën van Quinn.
Door evenwichtig aandacht te geven aan de interne en externe aspecten van verandering, beheersing en flexibiliteit kunnen veranderprojecten en programma's op een evenwichtige manier worden beoordeeld
Peter Hartog liet zien hoe hij de Balanced Change Card in de praktijk gebruikt in (operational) audits naar de kwaliteit van de beheersing van veranderprojecten en programma's. Naar zijn mening maakt het instrument het mogelijk om op een concrete en evenwichtige manier aandacht te geven aan de harde en zachte aspecten van verandering.

Aristoteles terug van weggeweest

Dr. J.R. van Kuijck*

De Griekse filosoof Aristoteles leefde van 384-322 voor Christus. Naast Plato en Socrates wordt hij gezien als de meest invloedrijke klassieke filosoof. Wat had hij te melden? Voor de gymnasiasten onder u begint er wellicht vaag iets te dagen. Maar laten we kijken naar een belangrijk werk van hem dat heden ten dage nog veelvuldig wordt aangehaald in de moderne filosofie: *Ars Rhetorica*. En wat blijkt? In meerdere disciplines – van verkooptechniek tot journalistiek – hebben de inzichten van Aristoteles niet aan relevantie ingeboet. Laten we eens stilstaan bij het belang van de inzichten voor auditors.

Waar gaat de *Ars Rhetorica* over? Aristoteles bespreekt in dit werk de manieren waarop een spreker zijn medemens kan overtuigen van iets. Daarbij maakt hij onderscheid tussen technische en niet-technische middelen om te overtuigen. De niet-technische middelen hebben betrekking op alle middelen die los staan van de spreker. In feite gaat het hier om blote feiten die voor zich spreken. Bij de technische middelen onderscheidt hij drie categorieën, te weten *ethos, logos* en *pathos*.
De *ethos* wordt gevormd door de autoriteit van de spreker of schrijver, de mate waarin de toehoorders deze zien als gekwalificeerd. Met *pathos* wordt ingespeeld op de emoties van degenen die moet worden overtuigd, in casu de opdrachtgever of lezer van een rapport. Tot slot is de *logos* gericht op de logische redenering die wordt gevolgd in een betoog om iemand te overtuigen.
Deze drie overtuigingsmiddelen kunnen elkaar overigens versterken maar ook verzwakken. Om dit laatste te verduidelijken een voorbeeld. De viroloog – en adviseur van de Nederlandse regering – Ab Osterhaus kwam vorig jaar veelvuldig in de publiciteit omtrent de Mexicaanse griep. Zijn autoriteit (ethos) werd echter aangetast doordat hij belangen bleek te hebben bij de verkoop van vaccins. Bovendien is er openlijk twijfel ontstaan over de ernst van de Mexicaanse griep. Wat denkt u dat de overtuigingskracht is van deze viroloog bij het uitbreken van een pandemie in de toekomst?

Volgens sommige wetenschappers zijn ethos en pathos echter taboe en worden zij afgedaan als drogredenen. Immers, zo stellen zij, brengen deze technische middelen ons geen stap dichter bij de waarheid. Zij stellen dat het gebruik ervan geen bewijs levert voor de juistheid van een stelling in een betoog; het voegt niets toe aan de argumenten. Als bijvoorbeeld Dutroux tijdens het proces zegt dat hij spijt heeft van zijn daden doet dat niets af aan het feit dat hij een moordenaar is die jarenlang gruwelijke misdaden met kinderen heeft gepleegd.

Het voorgaande mag dan wel zo zijn, maar dat neemt niet weg dat gebruik van ethos en pathos de efficiency van het overtuigingsproces kan laten toenemen. Het is mijn overtuiging dat het gebruik van ethos en pathos in het algemeen toelaatbaar is en mutatis mutandis ook voor auditors. Daar zijn echter wel belangrijke voorwaarden aan verbonden. Allereerst zal de argumentatie (logos) die centraal staat sterk moeten zijn. Daarnaast moet men erop kunnen vertrouwen dat een auditor geen knollen voor citroenen verkoopt. De auditor zal moralistisch moeten handelen en geen zwakke redenatie moeten compenseren met oneigenlijke elementen. Een auditor is immers geen autoverkoper.

In de aanloop naar de Tweede Kamerverkiezingen hebben we de afgelopen maanden veel politici gehoord. Weinig logos, maar veel pathos en soms ook ethos. Maar politici hebben niet dezelfde moraal als auditors. Ik hoop dan ook vurig dat de logos voor u leidend zal zijn als u uw stem uitbrengt!

* Actief in SERUM Corporate Finance en LIME TREE Research & Education. Tevens is hij verbonden aan de Vrije Universiteit als UHD voor onderzoek op het gebied van auditing (vankuijck.bob@hetnet.nl).

Independent research firm named BWise a Leader in Enterprise GRC Platforms*

Let BWise make *you* the GRC leader.

BWise
BUSINESS IN CONTROL

BWise biedt uw organisatie een software oplossing van wereldformaat voor Governance, Risk en Compliance (GRC) uitdagingen. Met GRC uitdagingen bedoelen we ondermeer het efficiënt voldoen aan wet- en regelgeving, zoals Solvency II, Sarbanes-Oxley, ISO 31.000 en Code Tabaksblat. Ook kunt u denken aan onderwerpen zoals het krijgen van grip op Internal Control, Risk Management, Internal Audit en (IT) Governance. Door onze unieke procesgerichte aanpak, bereikt u met BWise niet alleen voordelen op het gebied van proces-optimalisatie, u bespaart ook aanzienlijk op compliancekosten.

Vraag het Forrester rapport gratis aan via **www.bwise.nl**.

**The Forrester Wave™: Enterprise Governance, Risk and Compliance Platforms, Q3 2009*

FORRESTER®

Finding the right balance?

The world is changing rapidly. The continuously changing risk environment requires executives to look at risk from a new perspective. They cannot afford any other surprises. They need assurance that systems are working effectively. Today is the moment for executives to find the right balance and direction for the future.

A partnership with Deloitte enables you to supplement your organization's capabilities with our expertise and experience to optimize your risk management and internal audit function. This provides you a balanced and objective assurance over your organization's key risks and responses to the issue driven requirements of your key stakeholders.

Hence you can take rewarded risks and preserve value creation through assurance plans that provide the right combination of compliance, risk management and opportunity development.

For more information, please contact Wim Eysink or Marcel van Raan, Deloitte Enterprise Risk Services
+31 (0)88 288 9711

Deloitte.