AUDIT magazine

Magazine voor internal en operational auditors

nummer 1 maart 2008

thema:

Risicomanagement

De SVRM heeft kwaliteit hoog in het vaandel!

Auditor en risicomanager: logische bondgenoten

Risicomanagement: wel blijven nadenken!

Instituut van Internal Auditors Nederland

VRO

Risicomanagement

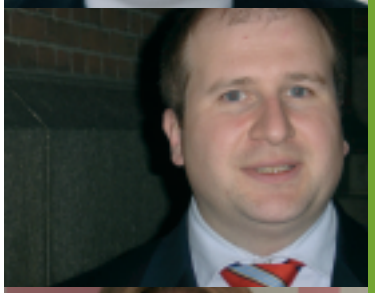

Ronald Jansen voorzitter

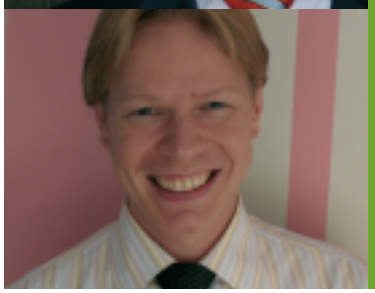

Ronald de Ruiter


Reinier Kamstra


Jolanda Breedveld


Karin Laker


Laszlo Nagy


Rick Mulders

Allereerst wenst de redactie van *Audit Magazine* u een heel goed, gezond en succesvol nieuw (audit)jaar! Dat dit geen holle frase is, blijkt uit het volgende: ten tijde van het afronden van de voorbereidingen van dit eerste nummer is Ronald de Ruiter, één van onze redacteuren, met een hartinfarct in het ziekenhuis opgenomen. Wij wensen Ronald een heel goed herstel én zijn gezin veel sterkte!

Het jaar 2008 begint met enkele redactionele veranderingen. Onze voorzitter, Arjen van Nes, heeft per 1 januari 2008 afscheid genomen van *Audit Magazine* om als secretaris toe te treden tot het dagelijks bestuur van IIA Nederland. Wij willen Arjen hartelijk danken voor zijn jarenlange inzet en toewijding! Ronald Jansen heeft de taak van Arjen overgenomen en wij wensen hem dan ook veel succes in zijn nieuwe rol. Daarnaast is Jolanda Breedveld toegetreden tot de redactie.

Met dit vernieuwde team beginnen we vol energie aan een nieuwe reeks magazines. Een 'tipje van de sluier' over de aanpassingen: het plan is om het aantal interviews te verhogen naar drie per nummer en meer aandacht te besteden aan opinievorming. In een tweetal nieuwe rubrieken willen wij lezers in de gelegenheid stellen hun professionele mening te uiten. De rubriek 'Vlijmscherp' is in dit nummer al opgenomen. Verder willen wij een extra column toevoegen. Om deze vernieuwingen te realiseren en omdat we komend jaar een extra nummer gaan uitbrengen, zijn we op zoek naar versterking van onze redactie. Geïnteresseerden kunnen contact opnemen met de voorzitter (Jansen.Ronald2@kpmg.nl).

Het thema van dit nummer is 'Risicomanagement'. Risicomanagement is een onderwerp dat op vele manieren met het auditvak verbonden is. Veel banken en vermogensbeheerders moeten voldoen aan de eisen geformuleerd door het Bazel Comité om het kredietrisico te beheersen. De auditor kan hierbij een belangrijke rol spelen. Een ander aspect is Business Continuity Management en de rol van de auditor hierbij. En omdat het vakgebied risicomanagement continu in beweging is, in dit nummer een tweetal artikelen over de trends in risicomanagement in de dagelijkse praktijk. In het kader van dit thema licht bijzonder hoogleraar (Enterprise) Risk Management Arjen Ronner in een interview zijn visie op het vakgebied toe.
Naast de thema-artikelen kunt u het verslag lezen van de round-table over het gebruik van standaard auditopinies, georganiseerd door de werkgroep Audit Opinies van IIA Nederland.

Samen met de auteurs heeft de redactie haar best gedaan het jaar goed te beginnen met een interessant en afwisselend *Audit Magazine*. Wij wensen u veel leesplezier!

De redactie van *Audit Magazine*

inhoud

thema Risicomanagement

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 Vereniging van Register Operational Auditors (VRO). De redactie nodigt lezers uit een bijdrage te leveren aan Audit Magazine. Bijdragen kunnen worden gemaild aan: Jansen.Ronald2@kpmg.nl **Redactieraad:** Th. Smit RA CIA (voorzitter IIA Nederland), G.M. van Gameren RA RO (voorzitter VRO) **Redactie:** drs. R.H.J.W. Jansen RO (voorzitter), drs J.F. Breedveld, drs. R. Kamstra, drs. K. Laker, drs. H.A. Mulders RA, drs. L.Z. Nagy RO EMIA, drs. R. de Ruiter RE RA RO CISA **Verenigingsnieuws VRO en Nieuws van de Opleidingen:** N. Arif RO **Verenigingsnieuws IIA Nederland:** drs. D.J.N. van der Hoop **IIA Nederland:** Postbus 7918, 1008 AC Amsterdam, tel.: 020-3010366, fax: 020: 3010392, e-mail: iia@iia.nl, internet: www.iia.nl **VRO:** Postbus 505, 9200 AM Drachten, e-mail: secretariaat@vronet.nl, internet: www.vronet.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.: 020-3010366, e-mail: iia@iia.nl. **Abonnementen:** IIA Nederland, Postbus 7918, 1008 AC Amsterdam, tel.: 020-3010366, fax: 020-3010392, e-mail: iia@iia.nl (zie ook de website: www.iia.nl). Abonnementen kosten € 85 per jaar, losse nummers € 25. Leden van IIA en VRO 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 vijfmaal per jaar.

ISSN: 1570-856X

VM UITGEVERS

BIS II en de rol van Internal Audit

Vele internationale banken en vermogensbeheerders[1] zijn de afgelopen jaren bezig geweest met de invoering van de eisen van het Bazel Comité inzake de nieuwe solvabiliteitsrichtlijnen in het kader van het prudentiële toezicht, kortweg aangeduid met BIS II.[2] In dit artikel wordt ingegaan op het BIS II-raamwerk als basis voor prudentieel toezicht en de invloed van BIS II op de interne bedrijfsvoering. Specifiek wordt ingegaan op de rol van Internal Audit als het gaat om het toetsen van naleving van de nieuwe eisen van BIS II.

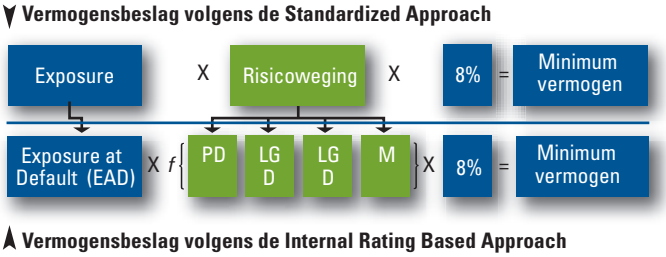
Drs. J. Feijen RA RT CIA

Het Bazel Comité heeft zich vanaf eind jaren negentig ingespannen om het BIS I-raamwerk te herijken en in samenspraak met de sector tot nieuwe richtlijnen te komen voor de rapportage omtrent de solvabiliteit. Het BIS II-raamwerk kent de zogenaamde 3 Pillar-benadering, zoals schematisch is weergegeven in *figuur 1*. De kernpunten uit het BIS II-raamwerk kunnen als volgt worden weergegeven:

- de uitbreiding van de reikwijdte van de solvabiliteitsrichtlijnen met operationeel risico;
- het bieden van meer flexibiliteit voor de solvabiliteitsmeting in het raamwerk, onder meer door het toestaan van interne modellen voor de solvabiliteitsrapportage voor krediet- en operationeel risico op basis van interne en eventueel externe data. De modellen dienen overigens vooraf door de toezichthouder te zijn gevalideerd;
- het gebruik van externe of interne ratings voor de inschatting van het kredietrisico;
- de toepassing van de verwachte waarde van de verkregen zekerheden (onderpand, garanties, et cetera) voor kredietrisico.

Voor instellingen die voor de meer eenvoudige methoden hebben gekozen was de invoeringsdatum 1 januari 2007. Voor de instellingen die voor de geavanceerde methoden hebben geopteerd, was de invoeringsdatum 1 januari 2008. Gedurende een overgangsperiode van twee jaar dient er zowel op basis van BIS I als BIS II te worden gerapporteerd, rekening houdend met bepaalde ondergrenzen voor het minimale solvabiliteitsvermogen (90 procent voor 2008 en 80 procent voor 2009 ten opzicht van BIS I).

Figuur 1. De drie pijlers van het Bazel II Akkoord



PD Probability of Default - de kans op betalingsonmacht bij de kredietnemer (%);
LGD Loss Given Default – het verlies op de zekerheden in geval van default (%);
EAD Exposure at Default – het bedrag waarover risico wordt gelopen (bedrag);
M Maturity – de looptijd van een kredietfaciliteit.

Figuur 2. Solvabiliteitsberekening

Rol van BIS II in de bedrijfsvoering

Onder de BIS II-regelgeving inzake Pillar 1 is rapportage omtrent de solvabiliteit verplicht voor de krediet-, markt- en operationele risico's. Voor ieder van deze risico's is een keuze uit drie methoden mogelijk, variërend van relatief eenvoudig tot geavanceerd. Verder dienen instellingen onder Pillar 2 op basis van een risicoanalyse na te gaan of en in hoeverre een solvabiliteitsbeslag voor andere bedrijfsrisico's nodig is. Instellingen worden zodoende geacht een solvabiliteit boven de minimumnorm van 8 procent aan te houden.

In dit kader kunnen instellingen kiezen voor een integrale benadering voor het interne risico- en solvabiliteitsbeheer op basis van een zogenaamde economic capital-benadering. In de economic capital-benadering wordt beoogd *alle* materiële bedrijfsrisico's te meten en een minimale vermogensbuffer aan te houden om alle onverwachte verliezen op te kunnen vangen. Hierbij kunnen in vergelijking tot de solvabiliteitsrapportage aan de toezichthouder (Pillar 1) andere methoden en een andere betrouwbaarheid worden gehanteerd. In *tabel 1* is een vergelijking gemaakt van de opzet en reikwijdte van de externe eisen voor solvabiliteitsbeheer van het BIS II Akkoord (Pillar 1 en Pillar 2) en de interne normen van economic capital. *Figuur 2* geeft de solvabiliteitsberekening volgens de Internal Rating Bases Approach voor kredietrisico weer.

	BIS II – Pillar 1	BIS II – Pillar 2	Economic Capital
Kredietrisico	√		√
Marktrisico	√		√
Operationeel risico	√		√
Renterisico		√	√
Landenrisico		√	√
Strategisch c.q. bedrijfsrisico		optioneel	√
Concentratierisico		optioneel	√
Verzekeringsrisico		optioneel	optioneel
Pensioenrisico		optioneel	optioneel
Inter-risk diversificatie	Nvt	Nvt	√
Betrouwbaarheid	99,9% (A-rating)	99,9% (A-rating)	Afhankelijk van rating-strategie bank

Tabel 1. Vergelijking BIS II en economic capital

(√ = van toepassing, optioneel = situatieafhankelijk, Nvt = Niet van toepassing)

Rol internal en external auditor

De kernvraag voor een internal auditafdeling (IAD) inzake BIS II audits is of de interne beheersomgeving voldoende waarborgen biedt zodat de solvabiliteitsrapportage voldoende betrouwbaar is. Het integrale solvabiliteitsproces is hierbij object van audit, waarbij ook de kwaliteit van de data, modellen en systemen object van onderzoek dienen te zijn. De Wet op het Financiële Toezicht (WfT) schrijft voor dat de externe accountant van de instelling een verklaring inzake de getrouwheid dient te verstrekken bij een nader door DNB te bepalen kwartaalstaat. De in dit kader relevante kernprocessen (ook wel aangeduid met 'building blocks') staan in *tabel 2*. De volgorde is zo weergegeven dat deze een logische relatie hebben met de drie Pillars van het BIS.

	BIS II – Pillar 1	BIS II – Pillar 2	BIS II – Pillar 3	Economic Capital
BIS II Governance & Implementatie	√	√	√	
Databeheer	√			√
Modellenbeheer	√			√
Systeembeheer	√			√
Operationeel risicobeheer	√			√
Marktrisicobeheer	√			√
Solvabiliteitsbeheersingsproces		√		√
Integratie in bedrijfsvoering		√		√
Interne en externe rapportage			√	√

Tabel 2. Kernprocessen van het integrale solvabiliteitsproces conform BIS II

BIS II Governance en implementatie

Hierna wordt een internal auditaanpak uitgewerkt op hoofdlijnen, overeenkomstig de hiervoor aangegeven kernprocessen c.q. building blocks. Gegeven het feit dat BIS II veelal nog in een (uitfasering van de) projectaanpak verkeert, zijn de projectgerelateerde aspecten onder deze categorie opgenomen. De kernaspecten die in de internal auditaanpak dienen te worden betrokken zijn de volgende:

- toereikendheid van de (project)governance, inclusief de rol van het senior management;
- goede en regelmatige afstemming met de toezichthouders (de zogenaamde home- en hosttoezichthouders) omtrent projectstatus, -knelpunten en verbeteracties;
- toereikendheid projectorganisatie alsmede rapportagestructuur, inclusief projectplanning en -voortgangsrapportage;
- inrichting van de reguliere en bestendige organisatie voor modellen, databeheer en systemen;
- de aanwezigheid van voldoende capaciteit en deskundigheid binnen de organisatie inzake de meer technische BIS II-aspecten;
- heldere instructies en deadlines voor de bedrijfsonderdelen en goede overdracht aan de lijnorganisatie.

Databeheer

Onder databeheer wordt verstaan de verzameling, kwaliteitscontrole en verwerking van gegevens. In dit kader is het nuttig een onderscheid te maken tussen:

- datakwaliteitsbeheer;
- data-integriteitsbeheer.

Datakwaliteitsbeheer omvat de bewaking van de datakwaliteit aan de inputzijde van de bedrijfsprocessen. Kort gezegd gaat het hier om de controles die moeten waarborgen dat de vastlegging van de vereiste data (bijvoorbeeld de PD- en LGD-factoren) aan de randvoorwaarden voldoen van volledigheid, juistheid en tijdigheid qua invoer c.q. onderhoud. Een bijzonder aspect in dit kader is de consistentie in het gebruik van definities en risicomodellen. Een voorbeeld inzake het eenduidige gebruik van definities kan dit illustreren (zie *kader op pag. 8*).

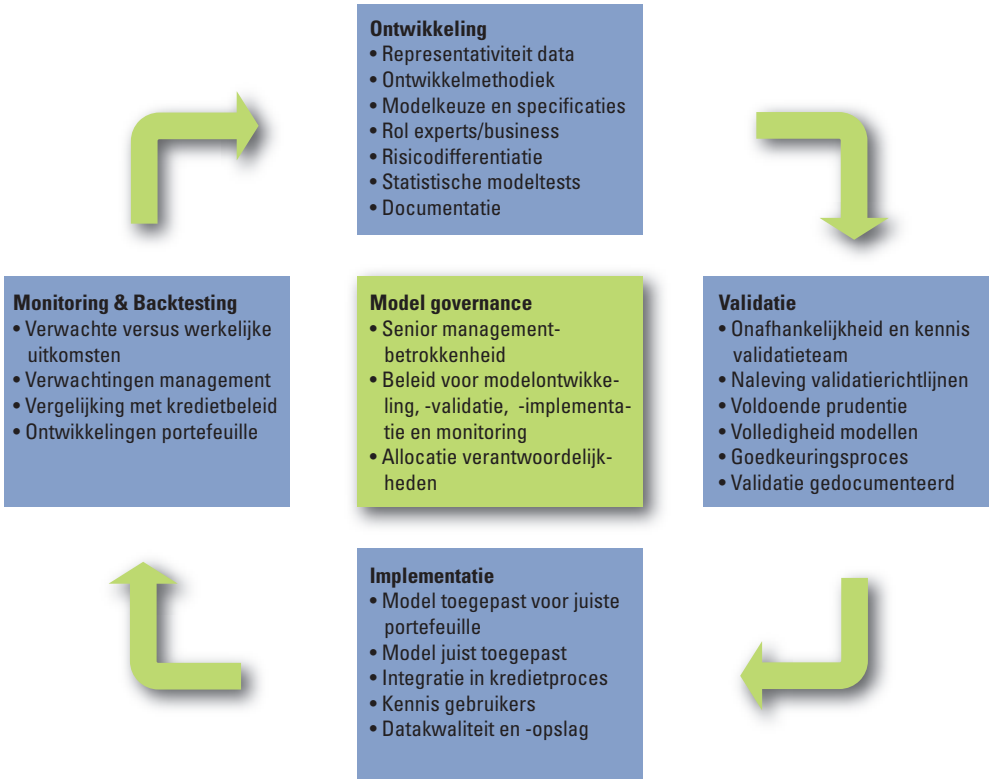
Verder is het data-integriteitsbeheer van groot belang. Dit omvat het beheer van data nadat deze in primaire systemen zijn ingevoerd. Hiermee wordt bedoeld het bestaan/validiteit, de volledigheid en juistheid van de data en de juiste en continue opslag en verwerking van data inclusief de traceerbaarheid van data (audit trail). Het beheer van de data-integriteit wordt in beginsel als een onderdeel van de systeemgerichte controles beschouwd.
Derhalve is de vaststelling van de effectiviteit van de geautomatiseerde controles inzake data-integriteit een essentiëel onderdeel van de Internal Audit. Eventueel zijn additionele controles buiten de systemen om noodzakelijk.

De definitie van exposure

Navraag bij kredietbehandelaars, risicomanagers of senior management wat wordt verstaan onder de gangbare term exposure levert de volgende antwoorden op:

- het feitelijk uitstaande bedrag;
- de limietwaarde volgens het interne systeem;
- de contractuele verplichtingen van de instelling;
- het intern gestelde maximale limietbedrag;
- het naar risico gewogen bedrag c.q. het resulterende solvabiliteitsbeslag.

Kortom, er is een noodzaak om op dergelijke punten heldere, eenduidige en toetsbare voorschriften te hebben.



Figuur 3. Enkele auditaspecten per stap van de modelcyclus

Modellenbeheer
Voor het beheer van modellen is door De Nederlandsche Bank (DNB) een modelcyclusbenadering uitgewerkt. Deze omvat de stappen van initiatie, ontwikkeling, validatie/goedkeuring, implementatie, monitoring en onderhoud van modellen door middel van herontwikkeling. In *figuur 3* is de modelcyclus weergegeven en zijn in het kort enkele relevante internal auditaspecten per modelcyclusstap vermeld.
Hierbij is de modelcyclus als geheel het uitgangspunt en niet zozeer een uitgebreide, inhoudelijke toetsing van de individuele modellen. Met andere woorden: de internal auditafdeling zal primair de key controls per cyclusstap moeten kunnen toetsen. In voorkomende gevallen zullen echter ook meer kwantitatieve aspecten aan de orde komen. Voor zover deze expertise niet binnen de IAD aanwezig is, zal deze eventueel moeten worden ingehuurd.

Systeembeheer
Het belang van de effectiviteit van de systeemomgeving is in het kader van de solvabiliteitsrapportage evident. Ten aanzien van systemen doet zich in vergelijking tot bijvoorbeeld de jaarrekeningcontrole overigens een bijzonderheid voor, namelijk dat veelal gebruik wordt gemaakt van de risicomanagementsystemen in plaats van de traditionele financiële systemen. Daar waar voor de jaarrekeningcontrole kan worden gesteund op een omvattende en gesloten financiële administratie, is dit voor BIS II niet zonder meer het geval. De internal auditor zal om die reden de volledigheid van de systeemomgeving inzake BIS II dienen vast te stellen. Twee vormen van aansluitingen zijn daarbij van belang:

- de aansluiting van posities volgens de intern verantwoorde posities (bron: financiële administratie) en de solvabiliteitsrapportage (bron: risicomanagementsystemen);
- de aansluiting tussen de posities volgens de intern verantwoorde posities en de BIS II-modellen, ofwel, wordt iedere portefeuille volledig ondersteund door een bepaald model?

Andere aspecten die voor de systeemgerichte audits in het kader van BIS II relevant zijn, betreffen:

- de toereikendheid alsmede robuustheid van de databasestructuur;
- de effectiviteit van de interfaces tussen de diverse systemen, gericht op integraal ketenbeheer van data;

- de continuïteit van de geautomatiseerde omgeving en daarin verankerde controles;
- de beveiliging tegen ongeautoriseerd gebruik en de bescherming van de vertrouwelijkheid van de data.

Operationeel risicobeheer

Dit onderdeel van het BIS II Akkoord is relevant voor instellingen die voor de meest geavanceerde methode hebben gekozen, de Advanced Measurement Approach. In aanvulling op de hiervoor besproken kernprocessen, kunnen voor dit onderdeel als bijzondere internal auditaspecten worden genoemd:

- de inrichting van de operationele risico-organisatie conform de BIS II-richtlijnen;
- de gestructureerde verzameling en verwerking van interne en externe operationele risicodata conform de BIS II-indeling naar eventtype met het onderscheid tussen operationele en krediet- of marktrisicogebeurtenissen;
- de naleving van ontwikkel- en validatieprocedures voor de operational riskmodellering (inclusief aspecten als het schalen van gebeurtenissen, frequentie- en impactschatting, invloed van verzekeringen, scenario's, et cetera.);
- de periodieke rapportage en evaluatie van operationele risk events in relatie tot de operational risk appetite en het evalueren van de effectiviteit van de interne beheersorganisatie (lessons learned).

Marktrisicobeheer

Voor marktrisico blijven (voor instellingen in de EU) de zogenaamde Capital Adequacy Directive 2 (CAD 2)-richtlijnen van 1996 van kracht. CAD-2 leidde er destijds toe dat interne modellen mochten worden toegepast op de solvabiliteitsrapportage inzake de handelsposities. Deze eisen zijn met BIS II overigens wel aangevuld met additionele eisen betreffende de meting van het zogenaamde specific issuer risk van posities in de financiële markt. De IAD zal, kort weergegeven, om die reden moeten vaststellen dat deze uitbreiding op consciëntieuze en betrouwbare wijze heeft plaatsgevonden.

Solvabiliteitsbeheersingsproces

De solvabiliteitsbeheersing is een integraal onderdeel van de managementcyclus. Belangrijke interne controles die in dit kader relevant zijn en dus een toetsing vergen door de internal auditor, zijn:

- de effectiviteit van het reconciliatieproces van de posities, zoals hiervoor aangegeven;
- de toereikendheid van de analytische interne controles gericht op de voorspelbaarheid van de solvabiliteitscijfers (ex ante, bijvoorbeeld bij model(her)ontwikkeling) en het ex post verklaren van de feitelijke ontwikkeling in de solvabiliteitscijfers. Het analyseren van de uitkomsten van bijvoorbeeld de gemiddelde PD- en LGD-waarden is hierbij een belangrijk onderdeel;
- de toepassing van scenarioanalyses en stresstesting met behulp van de BIS II-modellen en periodieke evaluatie van de uitkomsten. Kernvraag hierbij is of de modeluitkomsten voldoende resistent zijn tegen wijzigingen van kritieke (model)aannamen en veranderende marktomstandigheden.

Een belangrijk aspect bij de bovenvermelde analytische interne controles is het verkrijgen van een intern normenkader, zowel voor de belangrijkste componenten van BIS II voor kredietrisico (PD, LGD en de zogenoemde Exposure at Default – EAD, zijnde de effectieve risicodragende posities). Dit normenkader zal zich gaandeweg ontwikkelen, waarbij interne benchmarking met vergelijkbare portefeuilles zinvol is.

Verder zijn de bepalingen van Pillar 2, die primair gelden voor de toezichthouders, impliciet ook voor rapporterende instellingen van belang. Onder Pillar 2 wordt van de instellingen verwacht dat deze een Internal Capital Adequacy Assessment Process (ICAAP) hebben. Dit omvat onder meer een integraal kapitaalbeheersplan dat met directe betrokkenheid van het senior management is opgesteld en dat leidend is voor de solvabiliteitssturing. De internal auditor dient de ICAAP-eisen in de BIS II-werkzaamheden te betrekken.

De BIS II internal auditaanpak moet zich richten zich op het integrale solvabiliteitsbeheersingsproces

Integratie in de bedrijfsvoering

Onder deze noemer (ook wel aangeduid met de term Use Test) wordt het mechanisme verstaan dat waarborgt dat de belangrijkste componenten van BIS II daadwerkelijk een rol spelen in de bedrijfsvoering. Er wordt in dit kader wel gesteld dat de nieuwe uitdaging van BIS II zit in de integratie in de bedrijfsvoering. Een niet limitatieve opsomming van aspecten die in de internal auditbenadering aan de orde dienen te komen zijn:

- het daadwerkelijke gebruik van de vermelde PD-, LGD- en EAD-componenten in het kredietproces bij de acceptatie en het risicobeheer met behulp van daartoe ontwikkelde modellen;
- het gebruik van interne pricing tools, afgeleid van de specifieke risicomodellen in het kredietproces;
- periodieke analyse en evaluatie van de solvabiliteitscijfers en confrontatie met de risk appetite per risicogebied.

Interne en externe rapportage

Het BIS II Akkoord bevat tevens eisen voor de externe rapportage. Dit betreft zowel kwalitatieve als kwantitatieve aspecten. Het valt buiten het kader van dit artikel om hiervan een limitatieve

opsomming te geven. Volstaan wordt met enkele voorname aspecten die in het kader van de informatie omtrent de solvabiliteit getoetst dienen te worden:

- de hoofdlijnen van de solvabiliteitsstrategie van de instelling;
- de reikwijdte van de solvabiliteitsinformatie qua groepsentiteiten;
- de samenstelling van en ontwikkelingen in de vermogensstructuur;
- het vermogensbeslag ingedeeld naar de afzonderlijke risicocomponenten (krediet-, markt-, operationeel risico en risico's uit hoofde van effectenposities);
- nadere kwalitatieve en kwantitatieve informatie per risicogebied.

De wijze van externe rapportage (jaarrekening, jaarverslag of bijvoorbeeld op andere wijze zoals via internet) is aan de instelling. Verder vindt er in de Nederlandse context nog consultatie plaats als het gaat om de wijze van toepassing van IFRS 7 en Pillar 3 van BIS II inzake de toelichting in de jaarrekening, respectievelijk het jaarverslag alsmede de hiermee samenhangende accountantscontrole.

Uitdaging

De vraag is of de internal auditor een BIS II-expert dient te zijn/worden. Dat is niet noodzakelijk het geval, al zal een zekere basiskennis op het gebied van statistiek, de elementaire begrippen en methoden van BIS II en bovenal risicomanagement, een must zijn. De bestaande gereedschapskist van de internal auditor is echter in beginsel toereikend.

Tot slot kan worden gesteld dat BIS II een interessante uitdaging is voor internal auditors waarbij een belangrijke toegevoegde waarde kan worden geleverd voor de diverse stakeholders. Een goede afstemming c.q. samenwerking met eventuele externe experts (modelaudits), de toezichthouder en de externe accountant, spreekt hierbij voor zich. Ook een actieve en tijdige rapportage aan de interne stakeholders (directie en senior management) is in dit kader een must.

Noten

1. In het vervolg van dit artikel wordt volstaan met de term 'instelling', waarmee zowel (internationaal actieve) banken als vermogensbeheerders worden bedoeld.
2. Als basis voor dit artikel hebben de volgende bronnen gediend: *International Convergence of Capital Measurement and Capital Standards, A Revised Framework, Basel Committee on Banking Supervision*, november 2005. *Common Regulatory Reporting* (CRD) van de Europese Unie, 22 mei 2006 en de Wet op het Financieel Toezicht WfT. Voor het doel van dit artikel worden deze bronnen als één set van regelgeving beschouwd.

Drs. Johan Feijen RA RT CIA is werkzaam bij de Audit Rabobank Groep (ARG) van Rabobank Nederland. Hij fungeert als programmamanager voor de coördinatie van de BIS II-audits binnen Rabobank Groep.
E-mail: j.h.s. feijen@rn.rabobank.nl

De SVRM heeft kwaliteit hoog in het vaandel!

Sinds enige tijd doen risk managers hun intrede in organisaties. Er zijn in Nederland inmiddels dan ook een aantal certified risk managers actief. Risicomanagement is dus duidelijk aan het professionaliseren. Maar wat kun je nu eigenlijk van een risicomanager verwachten? Hoe zit het met de consultants onder ons die zich richten op advisering over risicomanagement? En hoe weet je of je kwaliteit in huis hebt?

Drs. R. Jansen RO

Medio 2007 hakten Ed Mallens en Simon Kooij de knoop door. Zij namen samen het initiatief tot de oprichting van een register voor risicomanagers en anderen die zich in dit vakgebied bewegen, de Stichting Vakontwikkeling Risk Management (SVRM). Een initiatief dat in ieder geval ook aansluit bij ontwikkelingen die in andere vakgebieden plaatsvinden en waar de leden van het IIA zelf middenin zitten.
Op 24 januari jl. organiseerden Mallens en Kooij in Rotterdam een kick off-bijeenkomst met Aon als gastheer. Deze kick off had tot doel steun te krijgen van de gesprekspartners – vertegenwoordigers van de verschillende partijen in de doelgroep – die Mallens en Mooij in de voorbereidingsfase van de oprichting van de stichting hebben gesproken. In het kader van het thema Risicomanagement legde *Audit Magazine* de beide oprichters een aantal vragen voor.

Wat heeft jullie (persoonlijk) bewogen om een stichting voor de vakontwikkeling van risicomanagement op te zetten?
"SVRM is geboren uit de behoefte om de kwaliteit van risicomanagers die werkzaam zijn bij organisaties op een objectieve wijze te kunnen laten zien. Immers, ze krijgen steeds meer verantwoordelijkheid als het gaat om de risicomanagementfunctie, het -profiel en de opvolging van risico's. De noodzaak om bij, zowel publieke als private, organisaties risicomanagers met de juiste kennis, kunde en integriteit in te zetten, groeit gestaag.
Daarnaast is het noodzakelijk om risicomanagement op één uniforme manier te benoemen en toe te passen. De specifieke toepassingen binnen marktsegmenten worden uit het gezichtspunt van risicomanagement benaderd en met elkaar in verband gebracht. De specifieke toepassingen zelf blijven daarbij volledig in tact."

In het businessplan lees ik: 'De missie van SVRM is het borgen van het vakgebied risicomanagement op strategisch, bestuurlijk en politiek niveau in organisaties. Deze organisatie kan zich bevinden in de publieke of private markt met het werken voor een profit-, not-just-for-profit- of non-profitdoelstelling. Risicomanagement is een elementaire functie in elke organisatie. Door de branchegenoten wordt deze visie van harte ondersteund, actief uitgedragen en toegepast.' Hoe belangrijk is deze borging? Ik bedoel, de markt doet toch zijn werk? Of hebben jullie andere ervaringen?
"De borging is belangrijk om daarmee de toegevoegde waarde van risicomanagement voor organisaties te kunnen aantonen. De ontwikkeling van het vakgebied verhoogt de kwaliteit en compleetheid van het risicomanagementhoofdstuk in verantwoordingrapportages en jaarverslagen. Tevens maakt het organisaties robuuster en wordt er geld bespaard."

Jullie hebben als oprichters met verschillende partijen in de doelgroep gesproken. Kunnen jullie aangeven welke partijen het belangrijkste aandeel vormen van de doelgroep? Hoe zijn deze mensen betrokken bij het onderwerp risicomanagement?
"Het grootste aandeel – bij de eerste rondgang langs de marktpartijen – wordt gevormd door die organisaties waar de risico's heel erg groot zijn als het gaat om de frequentie en/of impact. Dit kan worden uitgedrukt in geld, milieuschade, bedrijfscontinuïteit, imago, veiligheid, sterfgevallen. Dus

de financials, de multinationals, de publieke organisaties, de consultants, de opdrachtgevers of aannemers van grote projecten, en last but not least, de risicomanagementopleiders op academisch niveau in Nederland en België."

Wat maakt die verschillende partijen nu tot één groep van risicomanagers? Wat is hun gemeenschappelijke doel?
"Het feit dat het managen van kansen en bedreigingen van of voor een organisatie het uitgangspunt zijn. De risicomanager is capabel om de risicomanagementfunctie te implementeren en te borgen binnen elke soort organisatie. Hij kan aantonen wat de toegevoegde waarde is van risicomanagement voor bestuurders en directies."

Het gaat SVRM ook om het borgen van de kwaliteit van risicomanagers. Dat betekent dat elke geregistreerde risicomanager aan bepaalde eisen zal moeten voldoen. Kunnen jullie een tipje van de sluier oplichten waar de doelgroep aan moet voldoen?
"De gecertificeerde risicomanager, de CRM (Certified Risk Manager), beschikt op een zeer hoog niveau over de juiste kennis, kunde, ervaring en integriteit. De specificaties van deze competenties worden op dit moment uitgewerkt. Degene die (nog niet) aan de criteria voldoet wordt opgenomen in het register van de 'candidates'. Ook hiervoor worden de eisen verder uitgewerkt."

Wanneer gaat de SVRM van start en waar kunnen geïnteresseerden zich melden voor nadere informatie?
"SVRM als stichting bestaat sinds 20 juli 2007. In samenspraak met partijen uit de verschillende branches wordt de organisatie ingevuld, worden de reglementen en procedures volledig uitgeschreven en het ondersteunende apparaat opgezet. SVRM zal zich na de zomer van 2008 presenteren. Iedereen die zich wil registreren als vakbekwaam risicomanager in het Register kan zich tot ons wenden. Dat is ook mogelijk voor de professionele organisaties die risicomanagementdiensten en -producten op de markt brengen. Zij kunnen zich laten registeren in 'de loge' van SVRM. Dat zijn bedrijven die voldoen aan de hoogste kwaliteitseisen voor het vakgebied risicomanagement.

Aanvullende informatie is te vinden op de website van SVRM, www.svrm.eu. U kunt ook telefonisch contact opnemen of via e-mail.

SVRM	SVRM
Simon Kooij	Ed Mallens
06-13213794	06-13214086
s.kooij@svrm.nl	e.a.mallens@svrm.nl

Simon Kooij RRM, RSE is oprichter van SVRM en behaalde een laureaat in risk management bij Amelior België. Hij is Register Risico Manager, (RRM) en Register Security Expert (RSE). Voorheen was Simon bestuurslid NARIM, risk & insurancemanager bij Connexxion en manager Assurantiën bij de Rabo. Simon spreekt en publiceert regelmatig over het vakgebied.
Ed Mallens B.Sc., B.Ba is oprichter van SVRM. Hij is civiel en bedrijfskundig Ingenieur en voorzitter van de landelijke NEN werkgroep voor ISO 31000 Risk Management. Ed werkt als risk & insurance manager bij het Havenbedrijf Rotterdam nv. Voorheen was hij bestuurslid van NARIM en vervulde diverse (project)mangementfuncties bij publieke organisaties. Hij heeft ruime ervaring in de ICT-adviespraktijk ten aanzien van methoden en technieken, tools en quality assurance.

Auditor en risicomanager: logische bondgenoten

Professor Arjen Ronner is de initiator van de vorig jaar september gestarte leergang Enterprise Risk Management aan de Universiteit van Amsterdam. De opleiding besteedt onder meer aandacht aan de portefeuillegedachte, het vergelijken, identificeren, kwantificeren, analyseren en financieren van risico's. Als hoogleraar Financiële Econometrie en door banen bij Philips, Zürich Financial Services en verzekeringsmakelaar Aon vergaarde hij een grote theoretische en praktische kennis over risicomanagement.

Interview: drs. R. Jansen RO en drs. A. van Nes RO
Tekst: B. van Breevoort

Hoe bent u in risicomanagement verzeild geraakt?

Ronner: "Ik heb Econometrie gestudeerd aan de Universiteit van Groningen en er daarna ook college in gegeven. Na een jaar een hoogleraarschap te hebben vervuld in Amerika, besefte ik dat er meer was dan Groningen. Ik heb het bedrijfsleven opgezocht. Ik begon als consultant Kwaliteit & Logistiek bij Philips. Uiteindelijk kwam ik in de Treasury afdeling van de Lichtdivisie terecht. Hier kreeg ik nadrukkelijker te maken met risicomanagement. Later werd ik hoofd van de Research & Consultancygroep bij de Treasury en was ik onder meer verantwoordelijk voor het valutabeleid. Door de activiteiten van veertig productdivisies in zestig landen speelden bij Philips allerlei valutarisico's. Er bestond geen eensluidend idee bij de productdivisies over waar die risico's afgedekt moesten worden.
Toen ik in 1993 hoogleraar Financiële Econometrie werd aan de VU Amsterdam heb ik samen met de studenten onderzoek verricht naar de aanpak van de valutaproblematiek van Philips. In zo'n concern worden miljarden dollars omgezet maar ook uitgegeven. Doordat er zestig verschillende winst- en verliesrekeningen zijn, is consolidatie niet erg eenvoudig. Het hedgen van de dollargeldstroom is niet afdoende, omdat het sterke bewegingen in de verlies- en winstrekening teweegbrengt, waarover vervolgens uitleg verschuldigd is aan de aandeelhouders. We zijn gekomen tot drie strategieën: het afdekken van de risico's van de cash flow, van de winst- en verliesrekening of op centraal niveau. Het bleek dat ze niet alledrie tegelijk uitgevoerd konden worden. De literatuur leert ons bijvoorbeeld dat de waarde van de onderneming in de toekomstige cashflow zit en deze dus beschermd dient te worden. Door de boekhoudregels is men echter huiverig om dat te doen vanwege de geweldige verschuivingen in de winst- en verliesrekening."

IFRS heeft dat niet veranderd.

"Inderdaad niet. Een kleine onderneming kan het risico nog afdekken, maar een grotere onderneming is gedwongen alle onderliggende financiële instrumenten te gaan waarderen en dat is een hele klus. Risicomanagement voor financiële en operationele risico's heeft mij sindsdien niet meer losgelaten. Na de verhuizing van het hoofdkantoor van Philips naar Amsterdam ben ik gaan werken voor Zurich Financial Services, een grote verzekeraar voor de industriële sector. Daar hebben we verzekeringsprogramma's ontwikkeld die meer risico's in één polis afdekken: een all-in polis voor een onderneming. Het was een heel ongebruikelijk product en ook best lastig voor multinationals, omdat het een gedetailleerde analyse vereist van de verschillende risico's en de interactie ertussen. Het is wel een mooi instrument voor risicospreiding."

Bestaat er met zo'n polis geen gevaar voor een cumulatie van risico's?

"Dat is precies het argument dat verzekeraars vaak gebruikten. Echter, wiskundig gezien is de volatiliteit van de polis altijd kleiner dan de som van de volatiliteit van alle risico's, tenzij ze 100 procent gecorreleerd zijn. In andere woorden: niet iedere brandschade heeft een aansprakelijkheidschade tot gevolg. Er zit een dempend effect in de volatiliteit en dat resulteert in een lagere premie. De polis heeft twee jaar redelijk verkocht, maar na 11 september 2001 is men er van teruggekomen en is het gestopt. Mede dankzij de discussie met verzekeraars over een all finance polis werd duidelijk dat er behoefte was aan een universitaire module over risicomanagement in de verzekeringssector. Er zijn wereldspelers actief in die sector, maar toch weten weinig mensen van het bestaan van herverzekeraars en verzekeringsmakelaars.

Na Zurich Financial Services ben ik bij Aon begonnen. Aon is een verzekeringsmakelaar en consultant op het gebied van het in kaart brengen van risico's. Wij maken analyses van verzekerbare risico's, we helpen bedrijven om een eigen verzekeringsmaatschappij op te richten en op verzoek benchmarken wij risicomanagementprogramma's van soortgelijke bedrijven. Mede door de steun van Aon heb ik de leergang Enterprise Risk Management aan de Universiteit van Amsterdam kunnen opzetten."

Waarom is specifiek gekozen voor de invalshoek van verzekeringen?

"In de bestaande opleiding zaten al modules verzekeringskunde, recht, actuariaat, daar sloot risicomanagement mooi bij aan. De opleiding beperkt zich echter niet tot verzekerbare risico's. Het behandelt tevens financiële risico's, wetgeving, compliance en de publieke regels voor de rapportage. Het is een Executive Master-opleiding, waarvoor een bachelordiploma en minimaal twee jaar praktijkervaring is vereist. Na voltooiing krijg je een master of science-diploma. Hbo'ers kunnen na een schakeljaar instromen, mits ze voldoende praktijkervaring hebben. Het is daarnaast mogelijk om bepaalde modules te volgen. 1 September 2007 zijn we van start gegaan."

Risicomanagement lijkt heel dicht tegen het werkveld van de internal auditor aan te liggen, vooral voor operational auditors. Komt het voor dat het actuariaat buiten de financiële sector samenwerkt met internal auditors?

"Dat is een actuele vraag. Risicomanagers zouden goed kunnen samenwerken met auditors, omdat zij dezelfde bedrijfsprocessen analyseren en omdat daarbij automatisch financiële risico's ter sprake komen. Hoewel de invalshoek verschilt, zijn risicomanagers en auditors logische bondgenoten voor het in kaart brengen van risico's en voor het naar buiten brengen van de kwaliteit van het risicomanagement. Een risicomanager gaat een stap verder door scenario's te maken van de gevolgen van bepaalde ingetreden risico's. Nu speelt er bij niet-financiële instellingen nog niet de intensieve rapportageplicht zoals bij financiële instellingen, maar de laatstgenoemden leggen die druk wel in toenemende mate op aan hun klanten. Daarnaast zie je in de publieke sector dat overheden, gemeenten en ziekenhuizen aan toezichthouders moeten aangeven of ze voldoende kapitaal hebben gereserveerd als buffer. De Nederlandsche Bank kijkt naar de modellen die de

Illustratie: Roel Ottow


Professor Arjen Ronner.

banken zelf hebben ontwikkeld en of die geschikt zijn om het kapitaal te berekenen dat nodig is om voldoende garanties aan het publiek te geven. De Nederlandsche Bank hanteert daarbij de portefeuillegedachte. Men hoeft niet het totale garantiekapitaal voor alle risico's maar een bepaald gemiddelde te reserveren, vanwege de gedachte dat de risico's zich niet alle tegelijk zullen manifesteren."

Valt alles te berekenen? Er zit toch meer achter de cijfers? Bestaat er niet het risico dat hiermee een schijnzekerheid wordt gecreëerd?
"Daar ben ik het mee eens. Risicomanagement is meer dan alleen getallen. Net als beleggingsanalisten is contact met het bedrijf noodzakelijk om te begrijpen of de organisatie op orde is. Het gevoel hoort erbij, maar daar valt wel lastiger over te rapporteren. Historische gegevens kunnen helpen om een toekomstig risico cijfermatig neer te zetten."

Neem de hypotheekcrisis in Amerika. Nederlandse financiële instellingen betoogden in eerste instantie dat ze er niet door geraakt werden. Nu wordt echter duidelijk dat het wel degelijk invloed heeft door de nauwe verwevenheid tussen financiële instellingen. In hoeverre is een afdeling risicomanagement in staat om deze zaken te kunnen bevatten of te herkennen? Is het ook een taak voor risicomanagers?
"Een risicomanager moet meer bezig zijn met de toekomst dan met het verleden. Naast het kwantificeren van risico's moet hij nadrukkelijk bezig zijn met scenarioanalyse. Denk aan het begrip 'value at risk'. In 95 procent van de gevallen blijft de exposure van bijvoorbeeld de dollar binnen een bepaalde bandbreedte, maar in 5 procent van de gevallen gaat hij er overheen, maar wanneer treedt dat op? 'Value at risk' draagt een schijnzekerheid in zich en daarom is er veel discussie over. Spreiding van de meer serieuze risico's op basis van scenarioanalyse kan een praktische oplossing zijn. In Amerika zijn hypotheken verstrekt tegen lage rentes die al snel zijn verhoogd, waardoor de hypotheeknemer ze niet meer kon betalen. Intussen hebben de hypotheekverstrekkers die rechten op de hogere rente doorverkocht, terwijl ze konden weten dat de hypotheeknemers waarschijnlijk in betalingsproblemen zouden komen. Tegelijkertijd had de hypotheeknemer zich wel twee keer moeten bedenken om zo'n hypotheek af te sluiten.
Het is merkwaardig dat deze hypotheekcrisis het financiële bouwwerk wereldwijd in elkaar doet storten. Het geeft een enorme deuk in het vertrouwen bij alle stakeholders. Toch heeft de klant belang bij liquiditeit. Opties op de AEX zijn courant en heel goed verhandelbaar en kunnen in een risicomanagementstrategie een nuttige rol spelen. Niemand heeft daar problemen mee, ook al heeft de leek geen idee hoe de prijs tot stand komt. Als een verzekeraar het brandrisico op een polis te groot acht, kan hij het laten afdekken bij een herverzekeraar. Daar zie je dat in risico wordt gehandeld. Men heeft kennelijk interesse in het risico en is bereid om het over te nemen. Bij verzekeren blijkt de wet van het afnemend grensnut op te gaan. Zekerheid heeft een bepaalde waarde boven onzekerheid, ook al heeft de onzekere

gebeurtenis eenzelfde verwachte waarde als de zekere gebeurtenis. Stel: je kunt óf 2 miljoen euro óf niets winnen met het gokken op kop of munt. In de kansberekening win je even vaak dan dat je verliest, dus maak je kans op gemiddeld 1 miljoen euro. Nu blijkt het voor mensen meer nut te hebben als men direct voor die 1 miljoen euro kan kiezen zonder aan het spel mee te doen. Voor een bedrijf is het niet anders. Het zal nuttiger zijn om zich voor een premie in de buurt van de gemiddelde schade te verzekeren in plaats van te gokken en, indien het risico optreedt, de schade te betalen uit de eigen cashflow. In het eerste geval valt er bovendien minder uit te leggen aan de aandeelhouders."

In het werk van de auditor moet de kwantificering van risico's een belangrijkere rol gaan spelen. Daarvoor leent zich de samenwerking met risicomanagers bij uitstek

Hoeveel risicomanagers zijn er? Hoe ontwikkelt het vakgebied zich?
"Momenteel hebben alle grote multinationals en bedrijven in de industriële sector afdelingen risicomanagement opgezet. Verder is er een Nederlandse Associatie van Risk Managers (NARIM) en een Europese vereniging, de Ferma, die eveneens bestaat uit risicomanagers, die niet zelden afkomstig zijn uit de verzekeringsbranche. Industriële bedrijven hebben nogal uiteenlopende disciplines, waardoor het risicomanagement vaak verdeeld is over verschillende afdelingen. Overigens is het niet nodig om één persoon verantwoordelijk te maken voor risicomanagement. Zolang er maar een open structuur is waarin er over de risico's kan worden gecommuniceerd. De verschillende afdelingen rapporteren wel alle veelal aan de CFO. Aon heeft laatst een enquête gehouden onder 250 risicomanagers wereldwijd en daaruit bleek dat 20 procent van de respondenten verwacht dat er een Chief Risk Officer (CRO) in de onderneming wordt aangesteld."

Een risicomanager als coördinatiepunt en initiator klinkt mooi, maar moet het management niet bovenop de risico's zitten?
"Is risicomanagement een vak of is het een eigenschap die elke manager moet bezitten? Beide zijn waar. Ondernemen is risico lopen, dus een manager moet gevoel voor risico hebben. Echter, er kleven zoveel professionele en specialistische aspecten aan de risico's dat daar toch een hoogwaardige staffunctie voor nodig is. Zo is het in een financiële instelling vanwege de gecompliceerde regelgeving en rapportage-eisen gerechtvaardigd om een CRO aan te stellen."

Tabaksblat verlangt onder meer een risicobeheersingsysteem, een rapportage over de risico's en stelt de bestuurders daarvoor verantwoordelijk. De Monitoringscommissie Frijns heeft dit onlangs afgezwakt door te zeggen dat men zich moet richten op de financiële verantwoording. Wat vindt u daarvan?
"Tabaksblat was een stap in de goede richting. Voor wat betreft professor Frijns zou ik iets anders willen uitlichten. Frijns is jurylid van de FD Henri Sijthoff-prijs voor het beste jaarverslag. Bij de jurering voor die prijs gaat men veel verder dan Tabaksblat. In het juryrapport wordt namelijk expliciet aandacht besteed aan de risicoparagraaf. Ondernemingen zouden daar zo uit kunnen citeren. Natuurlijk is er geen verplichting om aan die wedstrijd mee te doen, maar bedrijven willen wel graag goed voor de dag komen bij die prijs. Feit blijft wel dat ondernemingen niet altijd even open willen zijn over hun risico's omdat het de beurskoers nadelig kan beïnvloeden."

Analisten geven ratings af. Maken die gebruik van dezelfde theorieën als risicomanagers? En moeten accountants in de toekomst ook ratings gaan afgeven?
"Analisten zijn voor risicomanagers zeker belangrijke partners. Alhoewel analisten doorgaans betrekkelijk voorzichtig zijn in het stellen van vragen over risico's. Ze kijken meer naar winstverwachtingen. Voor met name verzekeraars speelt bij rating agencies de vraag naar de solvabiliteit: is het geld veilig?"

Is het niet beter als een accountant meer prospectieve verslaggeving gaat afgeven? Hij zou inzicht kunnen bieden in de te verwachten toekomstige ontwikkelingen door te toetsen of een onderneming zich voldoende heeft ingedekt voor mogelijke risico's. Momenteel kijkt een accountant alleen maar terug.
"Als toekomstige ontwikkelingen invloed hebben op materiële zaken van het bedrijf kan een accountant deze inderdaad omschrijven."

Hebt u nog suggesties en tips voor internal auditors?
"De kracht van internal auditors is dat ze nauwkeurig de bedrijfsprocessen en de risico's onder de loep nemen. Ook voor internal auditors geldt dat vooruitkijken van belang is voor de analyse. In hun werk moet verder de kwantificering van risico's een belangrijkere rol gaan spelen. Daarvoor leent zich de samenwerking met risicomanagers bij uitstek. Mede in dat licht kijk ik uit naar cursisten met een auditachtergrond maar zie ik tevens een auditor als docent graag komen praten over een onderwerp als compliance." ❑

Criteria voor de beoordeling van de FD Henri Sijthoff-prijs zijn beschikbaar in pdf op: http://www.junglerating.nl/upload/public/file/2007/Criteria%20FD%20Henri%20Sijthoff-Prijs%20februari%202007.pdf

Business Continuity Management:

Prepare for the worst, hope for the best

Onder de ondernemingsdoelstellingen van organisaties valt bijna per definitie het streven naar operationele excellentie en continuïteit. Dit vindt zijn weerslag in mission statements, pay offs, welluidende oneliners en brochureteksten. Maar hoewel er onder invloed van nieuwe dreigingen en toenemende afhankelijkheden steeds meer waarde wordt toegekend aan maatregelen om de veiligheid en continuïteit te waarborgen, is de praktijk echter weerbarstig.

L. Knegtel MBCI
J. Franke FBCI

Gepercipieerde complexiteit, selectieve risicobeleving en een kennelijk gebrek aan tijd en geld, weerhouden nog altijd veel organisaties ervan structureel maatregelen te treffen om de continuïteit te waarborgen. Toch is het om een calamiteit te kunnen overleven noodzakelijk vooraf over de gevolgen daarvan na te denken en om vooraf te bezien welke risico's de organisatie schade kunnen toebrengen. Een crisis, van welke aard of op welk gebied dan ook, laat zich immers niet eenvoudig voorspellen. In de onheilspellende, bedreigende en onzekere situatie die zich voordoet tijdens een crisis krijgt een organisatie zelden een tweede kans. Het risico van een onherstelbare reputatieschade ligt op de loer. Echter, iedere crisis biedt een organisatie de mogelijkheid deze het hoofd te bieden en als 'winnaar uit de strijd' tevoorschijn te komen.

Miele: er is geen betere. (1957)

Philips: 'We dragen bij aan een beter bestaan door op het juiste moment zinvolle technologische innovaties op de markt te brengen'

Denk vooruit

In lijn met de overheidscampagne 'Denk Vooruit' waarin de burger wordt aangespoord zich voor te bereiden op calamiteiten, zouden ook organisaties zich dezelfde proactieve houding eigen moeten maken. Een dergelijke attitude vindt in een organisatie zijn beslag in het proces Business Continuity Management (BCM). BCM is het geheel aan activiteiten dat er op is gericht de continuïteit van een organisatie te waarborgen. Hierbij worden primair 'high impact-low probability'-risico's in ogenschouw genomen. Dit zijn de verstoringen in het bedrijfsproces waar het dagelijks management niet primair op is ingericht en vaak niet op is voorbereid.

Nu vinden de activiteiten binnen BCM niet uitsluitend plaats ná het manifest worden van risico's. Het is vooral in de preventieve sfeer waar directe waarde wordt gecreëerd. Door vroegtijdige betrokkenheid van BCM bij besluitvorming kan kapitaalvernietiging worden voorkomen: bij aankoop van unieke en onvervangbare bedrijfsmiddelen, bij het ontwerpen en invoeren van nieuwe processen of systemen, of bij de introductie van nieuwe producten of product/marktcombinaties.

Voor die risico's die niet (verder) kunnen worden gereduceerd en waarvan de impact tot desastreuze gevolgen kan leiden, zullen maatregelen moeten worden getroffen. Voorbeelden hiervan zijn het continuïteitsplan, het pandemiescenario, een uitwijkplan, bedrijfshulpverlening, crisismanagement, mediaplanning of reputatiemanagement. Deze maatregelen vormen een verzekering.

Bij verzekeren is de gedachte dat een risico tegen betaling van een premie wordt overgedragen aan een derde partij. Indien een risico manifest wordt, zal op basis van polisvoorwaarden worden

overgegaan tot uitkering. De verzekeringspremie bestaat in dit geval uit in de inspanningen die worden geleverd in de implementatie van het BCM-proces. De uitkering, in de vorm van bedrijfscontinuïteit, wordt zichtbaar na een calamiteit.

> When planning for business continuity, remember Noah started building the ark before it began to rain

Fundamentele aanpak

Continuïteit verdient en behoeft binnen organisaties een fundamentele aanpak. Deze wordt gerealiseerd door BCM als secundair proces met een primaire functie in te richten. De werking van het proces vindt plaats op verschillende niveaus in de organisatie (zie *figuur 1*).

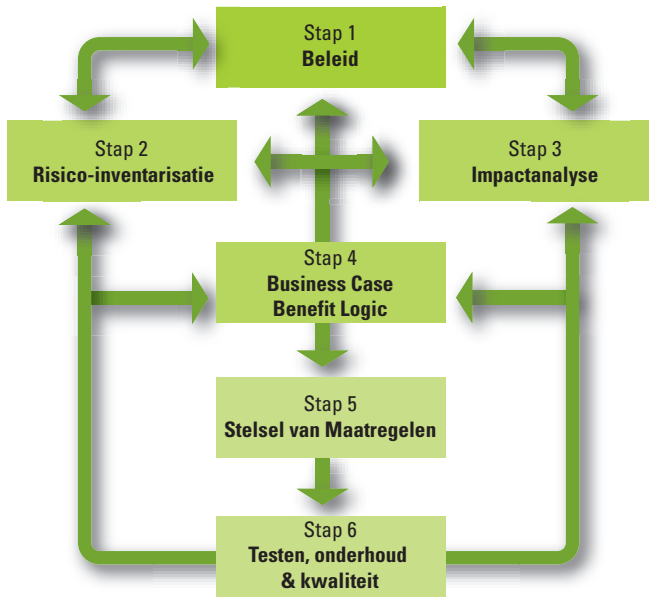
Het beleid rondom BCM wordt op strategisch niveau vastgesteld. De scope van het proces wordt bepaald, de positionering van het proces geformaliseerd en de organisatorische verankering van BCM mogelijk gemaakt. Vervolgens worden er beslissingen genomen ten aanzien van de eisen die moeten worden gesteld aan de continuïteit van de bedrijfsprocessen. Een vereiste is dat binnen de strategie en beleidsbepaling, proactief met continuïteitsaspecten wordt omgegaan. Het eigenaarschap van het proces en de eindverantwoordelijkheid voor het resultaat liggen op strategisch niveau. De besluitvorming die op strategisch niveau heeft plaatsgevonden, vormt op tactisch niveau het kader voor de inrichting en het management van het BCM-proces. Hier vindt de regie plaats over organisatiebrede activiteiten die gerelateerd zijn aan continuïteit. Aan het proces dat op tactisch niveau is ingericht, wordt op operationeel niveau organisatiebreed uitvoering gegeven.

Figuur 1. De werking van het BCM-proces

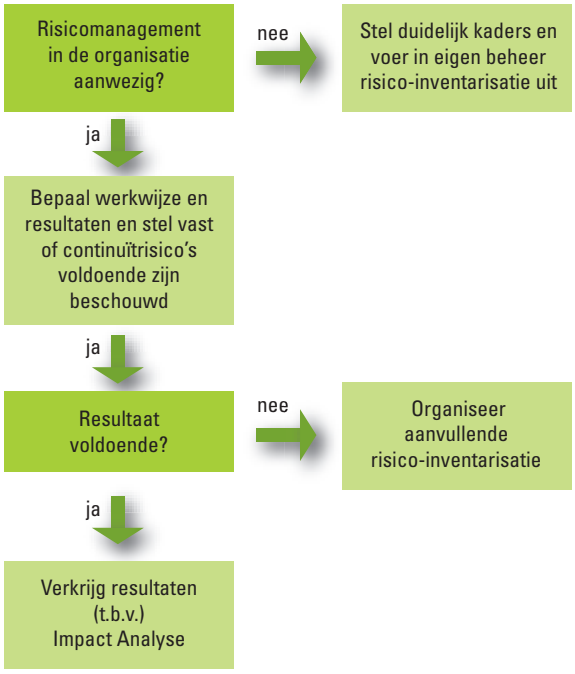
Beleid en risico-inventarisatie

Het BCM-proces start met de vormgeving van het beleid (zie *figuur 2*). Doel van het BCM-beleid is dat het strategisch management zich uitspreekt over en committeert aan de wijze waarop, hoe en waarmee de continuïteit van de organisatie wordt veiliggesteld. De positie van het proces wordt in deze fase vastgesteld, overeenkomstig de cultuur, visie en missie van de organisatie en de aard van de 'industry'.

Door het uitvoeren van een risico-inventarisatie wordt inzicht verkregen in de risico's die de continuïteit van de bedrijfsvoering kunnen bedreigen. De risico-inventarisatie behoort traditioneel tot het werkveld van risicomanagement. Op de vraag of de uitvoering hiervan binnen het domein van de risicomanager valt, is het antwoord dan ook: 'ja, tenzij'. Zie voor de invulling van het 'tenzij' *figuur 3*.



Figuur 2. De vormgeving van het BCM-proces



Figuur 3. Invulling van het domein van de risk manager

Omdat veel risico's onbekend zijn, vraagt het om inbeeldingsvermogen om hier goede invulling aan te geven. Vaak kan één enkele bron onmogelijk het hele spectrum aan risico's aangeven en worden er meerdere sporen gevolgd: bijvoorbeeld een interactieve brainstormsessie (brown paper-sessie), locatieonderzoek, desk research (branche-onderzoeken, benchmarks, et cetera) en focusinterviews. Bij ieder risico wordt tegelijkertijd vastgesteld of er al maatregelen zijn getroffen in de risicobeheersende sfeer of de calamiteitenbeheersende sfeer, alsmede welke maatregelen mogelijkerwijs het risico zouden kunnen afdekken. De belangrijkste bron voor het identificeren van risico's is de kennis en ervaring die aanwezig is bij de eigen medewerkers. Door het personeel te laten putten uit eigen ervaring en overtuiging, wordt duidelijk wat het actuele risicoprofiel van de organisatie is.

Business Impact Analyse

De Business Impact Analyse (BIA) heeft tot doel de gevolgen te bepalen van die risico's die een lage waarschijnlijkheid van optreden kennen en een hoge mate van impact hebben op het bedrijfsproces (de calamiteitenrisico's). De BIA geeft inzicht in de financiële en niet-financiële impact per proces, afdeling of businessunit. Voordat een BIA kan worden uitgevoerd is het noodzakelijk inzicht te krijgen in de werking van de bedrijfsprocessen en de mensen en middelen die voor de uitvoering van dat proces nodig zijn. Onderlinge afhankelijkheden tussen processen worden geïdentificeerd en de prioriteiten daarbinnen vastgesteld.
De uitvoering van een BIA is in veel organisaties de eerste echte hindernis bij het inrichten van BCM. De impact van calamiteitenrisico's is immers niet altijd goed te kwantificeren. Het wordt als ingewikkeld ervaren om schade in geld uit te drukken. In het geval van niet-financiële schade blijkt de factor reputatieschade lastig te interpreteren. Als echter voldoende kwalitatieve invulling is gegeven aan de processtap 'beleid', is er op strategisch niveau draagvlak om met de onzekerheden die voortkomen uit de resultaten van de BIA, om te gaan. Met andere woorden, de organisatie bepaalt zelf de mate van acceptatie voor de resultaten van de BIA. De BIA maakt inzichtelijk en transparant wat de impact van een calamiteit is en welke kwetsbaarheden zich waar in de organisatie bevinden. Het uitgangspunt in een BIA is de vraag: welke gevolgschade treedt op als er uitval van het proces plaatsvindt? Omdat de aard van een calamiteit daarbij niet van primair belang is, is het niet beslist noodzakelijk voorafgaand aan de BIA een risico-inventarisatie uit te voeren. De risico-inventarisatie kan ook na de BIA plaatsvinden.

Business case & benefit logic

De risico-inventarisatie heeft inzicht verschaft in de risico's en kwetsbaarheden van de organisatie. Het resultaat van de BIA toont aan welke gevolgschade per proces te verwachten is als zich een calamiteit voordoet. De uitkomsten worden geaggregeerd tot een hoger niveau. In de 'business case' en 'benefit logic' wordt aan beleidsmakers en besluitvormers informatie verstrekt op basis waarvan beslissingen over de eventueel te treffen maatregelen kunnen worden genomen.

Fase	Maatregelingen & Activiteiten		
	Strategisch	*Tactisch*	*Operationeel*
Alameringsfase	Herkenning en erkenning	Escalatie en alarmerings-procedures	Escalatie en alarmerings-procedures
Activeringsfase	Analyse en besluitvorming	Opstarten BCP	Bedrijfshulp-verlening & ontruiming. Schade inventarisatie
Uitvoeringsfase	Terugdringen gevolgschade & formulieren herstelstrategie	Uitvoering geven aan BCP en management van de organisatie in uitwijk	Disaster Ricovery Noodprocedures Reconstructie Inhalen achterstanden
Nazorg en evaluatie	Besluitvorming terugkeer naar business as usual. Nazorg en evaluatie	Management van de inwijk	Herstel van normale operatie

Tabel 1. Maatregelen en activiteiten bij een crisis

Tegenover de resultaten van de BIA – de schade die wordt geleden – worden de kosten van maatregelen geplaatst waarmee de schade kan worden vermeden. In de business case wordt de balans opgemaakt van kosten en baten. In de benefit logic, letterlijk te vertalen als de logica achter de baten, wordt het geheel van cijfermateriaal getoetst aan minder of anders kwantificeerbare, organisatorische en omgevingsafhankelijke gevoeligheden.

> A business continuity plan is like an insurance policy – nobody wants it until the house burns down

Stelsel van Maatregelen

Bij een crisis verandert de wereld in chaos. De vertrouwde omgeving die we denken te kennen, verandert direct in een vreemde en mogelijk vijandige wereld. Het is 'ieder voor zich'. De dagelijkse praktijk, de business as usual, functioneert niet meer. Routines, gewoonten en procedures werken niet meer. Als daardoor communicatielijnen veranderen maakt hiërarchie uit bittere noodzaak plaats voor kennis en inzicht en is samenwerking essentieel. Op een dergelijke situatie moet de organisatie zich voorbereiden. Dit gebeurt door het realiseren van een Stelsel van Maatregelen op strategisch, tactisch en operationeel niveau (zie *tabel 1*).

Testen, onderhoud en kwaliteit

Het testen en onderhouden van het Stelsel van Maatregelen vindt plaats op operationeel niveau. De resultaten hiervan (de test- en auditresultaten) worden op tactisch niveau geanalyseerd en

beoordeeld om vervolgens op strategisch niveau input te zijn voor nieuwe beleidsvorming.

• *Testen*

Om de organisatie bekend te maken met het Stelsel van Maatregelen en de werking op bruikbaarheid en juistheid te verifiëren, moet deze worden getest. Uitsluitend door frequent te testen blijft de organisatie voorbereid op haar taken bij een calamiteit. Ook kunnen tijdens testen onvolkomenheden worden geconstateerd die aanpassing vereisen in de maatregelen.

• *Onderhoud en kwaliteit*

Er wordt te vaak vanuit gegaan dat een calamiteit aan de eigen deur voorbij gaat, waardoor de aandacht voor de noodzaak van BCM verloren gaat. Door wijzigingen in de omgeving van de organisatie bestaat de kans dat getroffen maatregelen niet meer werken, niet meer beschikbaar zijn, of dat procedures niet meer actueel zijn. Periodiek dient daarom het beleid te worden getoetst op actualiteit en moet het Stelsel van Maatregelen zonodig worden aangepast.

Voor het reguliere onderhoud op maatregelen moeten procedures worden vastgesteld. Als er personele wijzigingen zijn, moeten deze worden doorgevoerd in de organisatorische voorzieningen van het CMT en BCP. Hetzelfde geldt voor verhuizingen, wijzigingen in processen, nieuwe processen of het verdwijnen van activiteiten. Omdat het niet ondenkbaar is dat veranderingen niet consequent worden doorgevoerd, vindt er naast regulier onderhoud ook periodiek onderhoud op de plannen plaats. Voor het periodieke onderhoud op maatregelen geldt hetzelfde als voor het testen. Ook hier zijn de intern gestelde kwaliteitscriteria leidend. In de meeste organisaties vindt, aanvullend op het reguliere onderhoud, één of twee keer per jaar periodiek onderhoud plaats.

Audit van het BCM-proces

Een goede werking van elk proces wordt bedreigd door risico's, ook het BCM-proces. Als deze risico's niet optimaal worden beheerst, komen de doelstellingen van het proces in gevaar. Voor BCM is het auditproces één van de maatregelen om risico's te beheersen. In dit geval wordt de kwaliteit beoordeeld van het BCM-proces. Het doel is het management van de organisatie zekerheid te verschaffen over de werking van het proces. Het niet uitvoeren van audits kan leiden tot:

- het in gevaar komen van de doelstelling van het proces: continuïteit van de bedrijfsvoering;
- kapitaalvernietiging omdat maatregelen op het 'moment suprême' niet blijken te werken (schijnzekerheid);
- het verdwijnen van het proces in de anonimiteit.

Voor een proces dat door risiconegatie en risicoperceptie de kans loopt om na een zekere periode van management attention in de vergetelheid te raken, is de rol van de auditor van essentieel belang. De auditor wordt geholpen door het beschikbaar komen van normen en standaarden op het gebied van BCM, op basis daarvan kan gecertificeerd worden. De belangrijkste standaard op dit moment is de Britse standaard BS25999:2006.

Conclusie

Business Continuity Management is een professie waarvoor inhoudelijke kennis en specifieke competenties zijn vereist. Het is een vak te kunnen voorzien in specifieke, op de eigen situatie afgestemde oplossingen en maatregelen; de balans aan te brengen tussen preventief en repressief; waarde toe te voegen door op integere basismaatregelen te ontwikkelen overeenkomstig de aard van de business, de organisatie en haar processen.

The Business Continuity Institute vertegenwoordigt wereldwijd de professionals die werkzaam zijn binnen het vakgebied en voorziet in de certificering van haar leden. Business Continuity Management is dan ook een proces van mensen, niet alleen van maatregelen.

Joop Franke is Principal Educational Services bij BCM Academy en Fellow of the Business Continuity Institute en heeft meer dan twintig jaar ervaring in BCM. Hij is bij BCM Academy verantwoordelijk voor het samenstellen van opleidingen en leergangen en het uitvoeren ervan. Tijdens zijn dienstverband bij het toenmalige Computer Uitwijk Centrum verzorgde hij talloze trainingen. Joop traint regelmatig strategische managers in crisismanagement en is spreker op seminars.
E-mail: jfranke@bcmacademy.nl.

Louise Knegtel is directeur van BCM Academy, het Europese kennisinstituut voor Business Continuity & Crisis Management en beschikt over meer dan vijftien jaar ervaring binnen het brede vakgebied van 'continuïteit'. Na een carrière als management consultant binnen multinationale ondernemingen, specialiseerde zij zich in BCM-vraagstukken. Het trainen van crisisteams en het genereren van Business Continuity awareness op alle bedrijfsniveaus behoort tot haar specialisme.
E-mail: lknegtel@bcmacademy.nl.

Het auditen van Business Continuity Management (BCM)

Door het toegenomen gebruik en de toepassing van ICT convergeren steeds meer bedrijfsprocessen en ondersteunende productiemiddelen. De integratie met ICT draagt bij aan een grotere efficiëntie, lagere kosten, hogere kwaliteit en toegenomen productiviteit. Echter, de keerzijde van deze integratie is een toegenomen complexiteit en een toegenomen afhankelijkheid van ICT.

Drs.ing. A. Ratelband RE CISA
P. Nieuwenhuizen RE RA

De grote afhankelijkheid van ICT zorgt ook voor een toenemend risico en toenemende impact indien die ondersteuning wegvalt en het risico manifest wordt. Om die dreigingen en risico's het hoofd te bieden, ontwikkelen bedrijven continuïteitsplannen en implementeren ze continuïteitsmaatregelen. Zo wordt vooraf nagedacht over te nemen acties ten tijde van een onderbreking of wellicht een calamiteit. Hierdoor is men beter geëquipeerd als een incident zich daadwerkelijk voordoet én wordt op deze wijze voorkomen dat een incident een calamiteit wordt.

Continuïteitsplanning

Vanwege die grote afhankelijkheid van IT en de potentieel grote impact bij uitval van IT, spelen IT-auditors steeds vaker een belangrijke rol bij het beoordelen van één of meerdere aspecten van continuïteitsplanning. Vandaar dat in dit artikel wordt uitgegaan van de inzet van een IT-auditor voor deze beoordeling. Aspecten waar bijvoorbeeld naar wordt gekeken zijn het continuïteitsplan zelf, het totstandkomingproces, of de gekozen maatregelen ook daadwerkelijk zijn geïmplementeerd en of de plannen en maatregelen worden getest en onderhouden. Een oordeel van een onafhankelijke auditor met betrekking tot één van deze aspecten geeft aanvullende zekerheid aan interne en externe stakeholders dat het proces goed is doorlopen en dat de juiste maatregelen zijn getroffen.
De rol van de IT-auditor is des te belangrijker aangezien het beschermen van de organisatie in het geval (een deel van) de operatie wegvalt een doelstelling van continuïteitsplanning is, alsmede het herstellen van de effecten van de gebeurtenis.

Aangegeven wordt wat de rol is van een IT-auditor in relatie tot bedrijfscontinuïteitsplanning en welke aandachtsgebieden in de scope van een onderzoek door de IT-auditor aan bod komen.

Wat is BCP?

Het vooraf nadenken over wat de kwetsbaarheden voor een organisatie zijn met betrekking tot continuïteit en hoe te continueren in geval zich een incident of calamiteit voordoet, wordt continuïteitsplanning genoemd. Vroeger sprak men veelal van IT-disaster recovery. Wegens de hiervoor genoemde convergentie van IT en bedrijfsprocessen en het toenemende belang van ICT, spreekt men tegenwoordig veelal over bedrijfscontinuïteitsplanning of Business Continuity Planning (BCP) waarmee het bedrijfsbrede en integrale karakter wordt onderstreept.
Dit vooraf plannen en voorbereiden gaat in een aantal stappen. De stappen bestaan uit het uitvoeren van een risicoanalyse waarin dreigingen en kwetsbaarheden worden geïdentificeerd die richtinggevend zijn voor de te ontwikkelen plannen. Het maximaal toelaatbare verlies, uitgedrukt in een hersteltijd of Recovery Time Objective (RTO) wordt bepaald in een uit te voeren Business Impact Analyse (BIA). Op basis van de BIA vindt daarna de (continuiteits-)strategieselectie plaats. Vervolgens wordt alles gedocumenteerd en onderhouden. Tot slot, om verzekerd te zijn van de werkbaarheid van het geheel, verdient het

Illustratie: Roel Ottow

aanbeveling om met enige regelmaat een test te doen.
Het uiteindelijke resultaat van deze inspanningen is een continuïteitsplan bestaande uit een set gedocumenteerde procedures voor het handelen ten tijde van een onderbreking of calamiteit. Met een goed continuïteitsplan kunnen de gevolgen van een calamiteit beter in de hand worden gehouden, zodat de uiteindelijke impact voor een organisatie beheerst kan worden.

Risicoanalyse
Het belangrijkste vertrekpunt voor continuïteitsplanning is de risicoanalyse. In de risicoanalyse worden de potentiële dreigingen en kwetsbaarheden met betrekking tot de continuïteit van de bedrijfsprocessen van de organisatie geïdentificeerd en geanalyseerd. Het resultaat van de kwetsbaarhedenanalyse is een overzicht van relevante dreigingen, het resultaat van de dreigingenanalyse is een overzicht van de relevante kwetsbaarheden. Om dit te verduidelijken een voorbeeld: de kans op een brand. Of dit een relevante dreiging is hangt af van de mate van kwetsbaarheid: zijn er rookmelders, zijn er sprinklers, zijn er branddeuren en brandmuren in het gebouw?
Deze twee onderwerpen (kwetsbaarhedenanalyse en dreigingenanalyse) moeten nadrukkelijk in samenhang beoordeeld worden. De aandacht zal zich voor het vervolg van het traject moeten richten op die dreigingen die potentiële en manifeste kwetsbaarheden uitbuiten. De kans dat een dreiging optreedt, de mate van kwetsbaarheid en de mate van impact, worden gecombineerd in het volbrengen van de risicoanalyse.

In deze fase van het BCP-traject richt de IT-auditor zich op de gehanteerde reikwijdte en de aanpak van de risicoanalyse zoals uitgevoerd door de organisatie. Wie zijn er betrokken geweest bij de analyse, welke dreigingen zijn onderdeel van de analyse geweest? Et cetera.

Business Impact Analyse
De Business Impact Analyse (BIA) is een exercitie waarin de impact van het verlies van middelen als gevolg van het manifest worden van een dreiging, op de bedrijfsprocessen wordt geanalyseerd. De centrale vraagstelling in een BIA is welke bedrijfsprocessen kritisch zijn voor de organisatie en welke niet, of minder. Deze analyse wordt gedaan door de gevolgen van uitval of stilstand te vertalen in financiële en operationele impact of impact op de reputatie. Vooral de laatste is de laatste jaren voor steeds meer bedrijven een belangrijk immaterieel of 'intangible' goed geworden dat gekoesterd moet worden.
Het belangrijkste criterium om de gecumuleerde impact weer te geven is het uitdrukken van een maximale uitvalsduur of een 'Recovery Time Objective' (RTO) per proces. Deze brengt tot uitdrukking hoe lang het bedrijfsproces 'uit de lucht' mag zijn voordat er schade ontstaat voor de organisatie. Dit is over het algemeen een kwalitatieve exercitie waarbij het belangrijk is dat proceseigenaren, of functionarissen met veel kennis van het proces, erbij betrokken zijn. Naast de RTO's worden in deze fasen veelal nog andere zaken vastgelegd per proces. Te denken valt aan de benodigde middelen om een proces te herstellen en het maximale dataverlies (ook wel Recovery Point Objective genoemd, RPO) per systeem.
Ervaring leert dat veel organisaties de, overigens geheel natuurlijke, neiging hebben de RTO's vrij strak te definiëren, maar dat onder invloed van een daaraan gekoppeld kostenplaatje blijkt dat daar nog 'lucht' in zit. Deze kosten komen aan bod in de strategieselectie als de maatregelen, inclusief kosten/baten, worden gedefinieerd. Onderzoeksvragen waar een IT-auditor zich op zal richten zijn onder andere:
- Hoe is de BIA tot stand gekomen, zijn daar bijvoorbeeld de juiste personen bij betrokken geweest?
- Wat is de scope van de BIA, zijn door middel van een preselectie al specifieke processen als niet-relevant bestempeld?

- Zijn de RTO en RPO eenduidig en op consistente wijze bepaald?
- Sluit de BIA aan op de bedrijfsdoelstellingen en contractuele afspraken (SLA's)?

Strategieselectiefase

Nadat de BIA is afgerond dienen de daarin geformuleerde uitgangspunten en conclusies te worden vertaald naar oplossingsrichtingen. Deze fase wordt de strategieselectiefase genoemd. In deze fase gaat het erom de juiste combinatie van technische maatregelen, hulpmiddelen, voorzieningen en procedures te kiezen die aansluiten bij de BIA.

Het belangrijkste resultaat uit de strategieselectiefase is een overzicht van genomen en nog te nemen maatregelen die in de juiste samenhang voldoende waarborg moeten bieden voor het kunnen weerstaan van een incident of onderbreking. Daarnaast is het belangrijk, zoals al gemeld in de BIA-fase, om een kosten/batentoets te doen om te voorkomen dat 'een kwartje wordt uitgegeven om een dubbeltje te beschermen'. In deze fase kijkt de auditor of de gekozen maatregelen voldoen aan de uitgangspunten zoals geformuleerd in de BIA. Hoe de keuzen gemaakt zijn en of een gekozen oplossing ook in de praktijk adequaat is geïmplementeerd.

In veel organisaties komt na een langdurig proces een eerste draaiboek tot stand, maar vindt er daarna geen onderhoud meer plaats

Planontwikkeling

Nadat alle maatregelen zijn geïdentificeerd, is het van belang om te zorgen voor documentatie in de vorm van een actiegeoriënteerd draaiboek. In het draaiboek dienen alle rollen, taken en verantwoordelijkheden kort en krachtig geformuleerd te zijn evenals wie welke acties op welk moment neemt.

De grootste valkuil waar organisaties mee te maken krijgen is een 'overbeschrijving' van details. Omdat praktische hanteerbaarheid een groot goed is in tijden van een calamiteit dient het draaiboek inzichtelijk ingedeeld te worden en de te nemen acties in de tijd dienen uit het draaiboek te blijken. Een bekende stelregel is dat het draaiboek voldoende details moet bevatten zodat een onbekende er mee moet kunnen werken en de acties op een juiste wijze moet kunnen uitvoeren.

Aspecten die binnen de reikwijdte van een audit vallen als het om het draaiboek gaat, zouden kunnen zijn:

- identificatie: hoe worden dreigingen en incidenten geïdentificeerd?
- notificatie: wie dient genotificeerd te worden indien zich iets voordoet?
- escalatie: hoe, wanneer en naar wie wordt er geëscaleerd?
- implementatie: beschrijft de uitvoering van alle te nemen acties vlak na het incident?
- herstel: beschrijft de herstelprocessen en acties die genomen moeten worden om terug te keren naar een normale bedrijfsvoering?

Daarnaast kijkt een auditor altijd naar de actualiteit van het draaiboek. In veel organisaties komt na een langdurig proces een eerste draaiboek tot stand, maar vindt er daarna geen onderhoud meer plaats. Doordat organisaties veranderen, mensen van functie veranderen, de technologie verandert, systemen veranderen, et cetera, is het van belang dat al die veranderingen hun weg vinden in het draaiboek voor zover het impact heeft op de continuïteit van de organisatie.

Testen van plannen

Het laatste onderdeel van BCM is het testen van de continuïteitsmaatregelen. Het belang hiervan wordt nog steeds door veel organisaties onderschat. Het welbekende stigma 'het zal toch nooit gebeuren' viert nog steeds hoogtij. Het testen van de uitwijkvoorziening is vaak contractueel geregeld en gebeurt dan ook één of twee maal per jaar. Daarnaast dienen technische voorzieningen als noodstroomaggregaten, gasblusinstallaties en dergelijke, conform de voorschriften van de leverancier onderhouden en getest te worden.

Naast zekerheid over de technische werking van deze maatregelen is het ook van belang om te testen in hoeverre het draaiboek adequaat is, of betrokkenen weten hoe te handelen in geval van een calamiteit en of betrokkenen dit in bepaalde complexe situaties ook kunnen omzetten in echte actie. Dit kan verschillende vormen aannemen, variërend van een zogeheten table top test ('droogtest'), waarbij het draaiboek stap voor stap wordt doorgelopen aan de hand van een scenario, tot een volledige crisissimulatie waarbij een calamiteit wordt nagespeeld. Het belangrijkste uitgangspunt voor het uitvoeren van testen is dat een test zorgvuldig wordt ontworpen en dat deze niet zelf de bedrijfsprocessen onderbreekt waardoor alsnog een echt incident ontstaat.

Voor wat betreft de betrokkenheid van een IT-auditor, richt deze zich in de meeste gevallen op testverslagen en testrapporten als evidence voor het feit dat er getest is. Ook kan een IT-auditor een beoordeling uitvoeren op het testplan. Dan gaat het om de volledigheid van hetgeen wordt getest, gegeven de doelstelling van het continuïteitsplan. Daarnaast is voor de auditor een rol weggelegd in het bewaken van de opvolging van de bevindingen die

voortkomen uit een test. Daarbij is belangrijk dat deze bevindingen worden geïncorporeerd in de maatregelen en/of het draaiboek.

Normenkader

Een belangrijk onderdeel van iedere audit is het vaststellen van het normenkader waartegen het te onderzoeken auditobject wordt getoetst. Hiervoor kunnen enkele veelgebruikte raamwerken handvatten bieden, zoals:

- *BS25999*. De BS25999 is de vroegere PAS56 standaard (Publicly Available Standard 56) waarin de best practices van het Britse Business Continuity Institute geformaliseerd zijn. Deze standaard beschrijft het BCM-proces in vijf stappen en bevat per processtap best practices.
- *CobiT*. Control Objective DS4 'Ensure Continuous Service' beschrijft doelstellingen in de vorm van dertien control objectives die een organisatie dient na te streven om continuïteit te waarborgen.
- *NFPA 1600*. De NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs is een Amerikaanse standaard en beschrijft programma-elementen, technieken, processen en best practices voor BCM. De NFPA-standaard onderkent vier stappen in het BCM-proces: mitigation, preparedness, response en recovery. Per stap worden de best practices en programma-elementen beschreven.
- *ISO 27002*. ISO 27002 is de opvolger van de Code voor Informatiebeveiliging en de latere ISO 17799. ISO 27002 bevat best practices voor de implementatie van informatiebeveiliging. Binnen de ISO 27002 is ook een apart hoofdstuk gewijd aan continuïteitsmanagement, de te hanteren aanpak, de risicoanalyse en de test en het onderhoud van een plan.

Naast deze publieke normenkaders zijn er ook veel methodieken van diverse dienstverleners die op het terrein van BCM actief zijn. Deze methodieken maken op de een of andere wijze gebruik van publieke normenkaders.

Competentie van de IT-auditor

Het auditen van continuïteitsmanagement is bedrijfsspecifiek. Naast het feit dat de auditor over de juiste auditkennis en -ervaring dient te beschikken alsmede objectdeskundigheid dient te hebben voor wat betreft continuïteitsplanning, is het ook van belang dat de auditor een gedegen inzicht heeft in de bedrijfsomgeving van de organisatie. Wat is de missie van de organisatie, wat zijn de doelstellingen, wat zijn de kritische bedrijfsprocessen, op welke wijze is IT ingericht en is dat in lijn met de bedrijfsstrategie van de organisatie?

Conclusie

Meer dan louter een verplichting of een overlevingsmiddel dienen BCP en continuïteitsplanning integraal onderdeel uit te maken van de bedrijfsprocessen om op verantwoorde wijze de belangen van interne en externe stakeholders te waarborgen. Stakeholders steunen steeds meer op onafhankelijk verstrekte zekerheden van een audit professional, zo ook bij het onderwerp BCP. Op de schouders van veel IT-auditors rust de taak om door middel van een BCM-audit bij een organisatie inzichtelijk te maken in hoeverre de continuïteitsdoelstellingen en maatregelen in lijn zijn met de bedrijfsdoelstellingen. De beschreven raamwerken kunnen hierbij goed als normenkader dienen.

Peter Nieuwenhuizen is als director werkzaam bij PricewaterhouseCoopers Accountants nv bij het onderdeel Systems & Proces Assurance. Hij is verantwoordelijk voor IT-auditopdrachten bij cliënten in verschillende sectoren; voornamelijk in de technologie industry, financial services en de publieke sector. Deze opdrachten betreffen onder andere Third party Mededelingen zoals SAS 70-onderzoeken en opdrachten op het gebied van continuïteit en uitwijk.

Arnout Ratelband is senior manager binnen PricewaterhouseCoopers. Zijn aandachtsgebieden zijn naast de IT-audit voor enkele grote beursgenoteerde ondernemingen, IT-governance en revenue management. Arnout heeft een uitgebreide ervaring in BCM. Tot zijn werkzaamheden behoren het maken van risicoanalyses, impactanalyses, het ontwikkelen van plannen, alsmede het geven van trainingen, workshops en het houden van crisissimulaties voor opdrachtgevers in diverse sectoren.

Risicomanagement in de internal audit spotlights

Er is een toenemende belangstelling voor risicomanagement waar te nemen bij internal auditafdelingen. Dit artikel geeft naast de achtergronden een aantal handvatten om de verschuiving in de auditaanpak in de praktijk te kunnen realiseren. Het onderscheidende vermogen om te excelleren lijkt vooral te liggen in het verkrijgen en behouden van de juiste talentvolle medewerkers.

Ir. M. Prinsenberg CIA, mr.drs. C. de Witte RA RO CIA EMIA en S. van Adrichem

De toenemende belangstelling voor risicomanagement blijkt uit de door PricewaterhouseCoopers uitgevoerde *State of the Profession survey 2007*, een onderzoek onder een groot aantal hoofden Internal Audit van voornamelijk Amerikaanse ondernemingen (inclusief de Fortune 500) en een aanvullend onderzoek gericht op de internal auditfunctie in 2012 (Internal Audit 2012).[1] Deze groter wordende belangstelling is met name zichtbaar daar waar het de verschuiving van een controle based auditaanpak naar een risk based auditaanpak betreft.

Achtergrond

Ongeveer tien jaar geleden waren er slechts enkele ondernemingen die een volwaardige, op risicoanalyse gebaseerde aanpak hadden voor wat betreft het opstellen van hun auditplan. Uit het recentelijk door ons gehouden onderzoek *State of the Profession survey 2007*, ('het onderzoek') blijkt dat vandaag de dag meer dan 80 procent van de respondenten de uitkomsten van ondernemingsbrede risicoanalyses gebruikt als basis voor hun jaarlijks terugkerend internal auditplanningsproces. Vooral de recente fraudes bij een aantal grote beursgenoteerde ondernemingen hebben een bredere toepassing van een op risicoanalyse gebaseerde auditplanning versneld.

Mede als gevolg van deze fraudes is de focus van de eisen die toezichthouders, investeerders en andere belanghebbenden stellen aan een onderneming veranderd, er is meer en meer nadruk komen te liggen op het voorkomen en tijdig signaleren van fraude. Het spreekt voor zich dat Internal Audit hierbij een belangrijke rol speelt. Tevens blijkt uit het onderzoek gericht op Internal Audit in 2012, dat meer dan de helft van de respondenten verwacht dat in 2012 het belang van een risicogerichte aanpak voor Internal Audit zal zijn toegenomen. Dit naast 36 procent van de respondenten die aangeeft dat het slechts iets belangrijker zal zijn dan nu.

Daarbij zal als gevolg van het toenemende belang van continuous monitoring de nadruk voor Internal Audit komen te liggen op concepten als continuous auditing en continuous assessments, met als doel het stroomlijnen en verbeteren van het auditproces. Gelet op het feit dat risicoanalyses en het monitoren van risico's real-time zal moeten gaan plaatsvinden, zullen audits dan ook eerder op basis van behoefte worden uitgevoerd dan volgens een vaste planning.

Uiteenlopend

Uit het onderzoek blijkt dat de manier waarop risicoanalyses en risicomanagement worden toegepast binnen ondernemingen nogal uiteenloopt. Bij sommige ondernemingen houdt Internal Audit toezicht op de risicomanagementfunctie, bij andere ondernemingen is Internal Audit verantwoordelijk voor risicomanagement en in sommige gevallen is er helemaal geen sprake van (formeel) toezicht op de risicomanagementactiviteiten.

Gezien deze variëteit in aanpak kan worden geconcludeerd dat de implementatie van risicomanagement bij veel organisaties op zijn best als onvolwassen en op zijn slechtst als ongestructureerd kan worden beschreven. Dit is zeker het geval bij ondernemingen waarbij risicomanagementactiviteiten door meerdere afdelingen worden uitgevoerd en waar risicoanalyses niet noodzakelijkerwijs gebaseerd zijn op de strategische doelen dan wel niet noodzakelijkerwijs in lijn zijn met elkaar.

Verantwoordelijk voor de uitgevoerde risicoanalyse	
Internal auditafdeling (IAD)	36%
Chief Risk Officer (CRO)	12%
IAD en CRO	13%
Andere afdeling/businessunit binnen de onderneming	15%
Externe accountant	6%
Niemand	18%

Tabel 1. Voor de risicoanalyse verantwoordelijke functies

Facts & Figures

Volgens de IIA standaard 2010[2] dient het hoofd van de internal auditafdeling een audit op te stellen die gebaseerd is op een minimaal op jaarbasis uitgevoerde risicoanalyse en waarbij de input van senior management en de raad van bestuur wordt verkregen. Uit ons onderzoek komt duidelijk naar voren dat er bij de ondervraagde ondernemingen verschillende functies verantwoordelijk zijn voor het uitvoeren van de risicoanalyse. *Tabel 1* laat zien wie binnen de bij het onderzoek betrokken ondernemingen voor de risicoanalyse verantwoordelijk zijn.

Positief is dat het onderzoek aantoont dat 82 procent van de respondenten op jaarlijkse basis een ondernemingsbrede risicoanalyse uitvoert. Daar staat tegenover dat 18 procent van de respondenten aangeeft helemaal geen risicoanalyse uit te voeren, wat toch als verrassend mag worden beschouwd. Nemen we het percentage van de externe accountant mee, (aangezien deze analyse niet intern wordt uitgevoerd) dan kan worden geconcludeerd dat bijna een kwart (24 procent) van de 717 ondernemingen die hebben meegewerkt aan het onderzoek eigenlijk niet in staat is om één van de belangrijkste basisprincipes van het internal auditberoep toe te passen.

De implementatie van risicomanagement kan bij vele organisaties op zijn best als onvolwassen worden beschreven

Worden er binnen een afdeling/groep in één onderneming meerdere risicoanalyses uitgevoerd, dan is het van belang dat deze in lijn zijn met elkaar en op elkaar zijn afgestemd. Slechts door een derde van de aan het onderzoek deelnemende ondernemingen worden meerdere analyses binnen een groep of afdeling uitgevoerd. Van deze ondernemingen geeft 20 procent aan dat de analyses goed op elkaar zijn afgestemd en in samenwerking zijn uitgevoerd, 50 procent geeft aan dat ze enigszins op elkaar zijn afgestemd, waarbij de resultaten en verschillen worden besproken, en 30 procent geeft aan dat ze slecht op elkaar zijn afgestemd en er nauwelijks sprake is van samenwerking.

Daarnaast blijkt uit het onderzoek dat van de ondernemingen die jaarlijks een risicoanalyse uitvoeren slechts 24 procent frequent (minimaal op kwartaalbasis) hun risicoanalyse herzien. *Tabel 2* laat zien met welke frequentie de risicoanalyse wordt herzien. Het spreekt voor zich dat wanneer wij de resultaten van het onderzoek als representatief zien voor alle ondernemingen, we kunnen stellen dat er ruimte voor verbetering van het risicoanalyseproces is.

Hoe vaak wordt de risicoanalyse herzien?		
Continu (gedefinieerd als meer dan maandelijks)	7%	24% best in class ten aanzien van de frequentie van herziening
Maandelijks	2%	
Kwartaalbasis	15%	
Halfjaarlijks	11%	
Waneer nodig (zonder vaste interval)	49%	
Niet	15%	

Tabel 2. Frequentie van herziening van de risicoanalyse

Een effectieve risicoanalyse

Om een effectieve risicoanalyse te kunnen uitvoeren, moeten de volgende zes stappen worden doorlopen.

1. Pas een procesmatige aanpak toe

Om aan de verwachtingen van de stakeholders te kunnen voldoen, moet zowel het audit committee als het senior management goed geïnformeerd zijn over de wijzigingen in risico's, evenals over de genomen/te nemen beheersmaatregelen. Een procesgedreven aanpak voor het uitvoeren van risicoanalyses verdient dan ook de voorkeur boven een enkel door individuele gebeurtenissen gedreven aanpak. Bij een procesgedreven aanpak is er een continue focus op risico's, waarbij, indien nodig, het risicoprofiel van een organisatie tussentijds kan worden herzien en men niet hoeft te wachten op het jaarlijkse planningsproces. Het spreekt voor zich dat de planning van de internal auditafdeling flexibel dient te zijn, om zo te kunnen inspelen op belangrijke aspecten die uit de risicoanalyse naar voren komt.

2. Herzie de risicoanalyse minimaal op kwartaalbasis

Gelet op de huidige risico-omgeving, die als dynamisch kan worden omschreven, is het voor de internal auditor noodzakelijk om de risicoanalyses minimaal op kwartaalbasis uit te voeren dan wel te herzien. Er dient te worden bepaald of de reeds eerder geïdentificeerde risico's nog van belang zijn voor de organisatie en in welke mate dat het geval is. Daarnaast dient te worden bekeken of er nieuwe risico's zijn die een bedreiging (kunnen) vormen voor de organisatie. Door het proces van risicoanalyses

te definiëren en te formaliseren en daarbij gebruik te maken van ondersteunende technologieën, is het inzichtelijk welke aandachtsgebieden er zijn en kan een effectievere planning van audits worden gerealiseerd. Daarnaast wordt het gemakkelijker om vroegtijdig risico's te signaleren en te analyseren.

3. Maak gebruik van de resultaten van voorgaande risicoanalyses

Voor het realiseren van een effectieve risicoanalyse is het van belang om te leren van het verleden (bijvoorbeeld via incidentrapportages) en gebruik te maken van binnen de organisatie opgedane ervaringen.

4. Stem risicoanalyses op elkaar af

Het is van belang om een eenduidige boodschap te geven richting het audit committee en het senior management over de risico's die de onderneming loopt. Dit wordt vooral lastig als er meerdere analyses worden uitgevoerd binnen de onderneming, met ook nog eens significante verschillen in uitkomsten. Binnen een organisatie (en organisatieonderdelen) moet men dan ook dezelfde 'taal' spreken en kennis met elkaar te delen om te komen tot een consistente en geïntegreerde aanpak.

5. Verkrijg de benodigde expertise

De bij het onderzoek betrokken hoofden van internal auditafdelingen maken zich vooral zorgen over hun mogelijkheden om strategische en bedrijfsrisico's, alsmede risico's gerelateerd aan fraude en technologie, te kunnen analyseren. Om deze risico's effectief te kunnen beoordelen moet namelijk een procesmatige aanpak te worden ontwikkeld, waarbij kennis en ervaring op de kritieke gebieden zoals fraudepreventie en -detectie, en technologie nodig is. Om de benodigde expertise te verkrijgen zullen dan ook zowel interne als externe kennisbronnen/expertises moeten worden aangeboord.

6. Verbeter de samenwerking met andere risicomanagement afdelingen/groepen

Uit het onderzoek blijkt dat er zeer beperkt sprake is van samenwerking en informatie-uitwisseling tussen de internal auditafdeling en andere groepen die verantwoordelijk zijn voor risicomanagement. Slechts 11 procent van de respondenten geeft aan dat er een formeel proces is ingevoerd om samenwerking te bewerkstellingen. Daarnaast geeft 38 procent aan dat er sprake is van een informeel proces. Positief is dat 41 procent van de hoofden Internal Audit heeft aangegeven actief bezig te zijn om dit samenwerkingsproces te verbeteren. Gezien het belang van stap vier is juist dit het mechanisme om niet alleen succesvol, maar ook efficiënt, integraal en op de dagelijkse praktijk toegesneden invulling te geven aan risicomanagement

Gevolgen voor de toekomst

Bij het doorlopen van de bovengenoemde stappen is een efficiënte en effectieve uitvoering van werkzaamheden van belang. Daarbij zal het de komende jaren voor internal auditors belangrijk zijn om technologische hulpmiddelen, bijvoorbeeld voor data-extractie en -analyse, te gebruiken en deze te combineren met een goed analytisch inzicht. Hierbij kan gebruik worden gemaakt van key risk indicators (KRI's) om op deze manier effectief (en in een vroeg stadium) risico's te kunnen monitoren. Een niet te onderschatten stap in het proces om te komen tot een effectieve risicoanalyse is het verkrijgen van voldoende capaciteit, expertise en vaardigheden op dit gebied. De verwachting is namelijk dat deze, hoewel de meer traditionele accounting en auditingvaardigheden van groot belang zullen blijven in de toekomst, zullen moeten worden aangevuld met:

- vaktechnische expertise om grote hoeveelheden data te analyseren, bijvoorbeeld daar waar het frauderisico's betreft;
- vaardigheden om complexe IT-omgevingen alsmede ondernemingsbrede risico's en corporate governance-structuren te kunnen analyseren;
- kennis van en ervaring met beheersstructuren van bedrijfsprocessen om voldoende zelfverzekerd te kunnen deelnemen aan gesprekken met het senior management, uitvoerend management, maar ook met het audit committee;
- (culturele) diversiteit gezien de toenemende globalisering van ondernemingen.

Noten

1. Beide studies zijn te verkrijgen via de website van Pricewaterhouse-Coopers: www.pwc.com
2. De internationale standaard voor 'Professional Practice of Internal Auditing, ©2007, The Institute of Internal Auditors, Altamonte Springs, Fla.

Marcel Prinsenberg is binnen PricewaterhouseCoopers Advisory verantwoordelijk voor de dienstverlening op het gebied van Internal Audit in Nederland en actief binnen het brede werkveld van governance, risk en compliance, in het bijzonder risicomanagement.

Cuno de Witte is binnen PricewaterhouseCoopers Advisory al een groot aantal jaren betrokken bij de dienstverlening op het gebied van Internal Audit, zowel co-sourcing, strategie, methodologie als technologie (Teammate) en dan met name in de industriële en technologie sector.

Susan van Adrichem is werkzaam binnen PricewaterhouseCoopers Advisory en heeft naast brede financiële en controlervaring een groot aantal internal audits uitgevoerd binnen diverse sectoren, zowel nationaal als internationaal.

Risicomanagement: wel blijven nadenken!

Op zich is de toenemende aandacht voor risicomanagement een goede ontwikkeling, maar de vraag is of het instrument risicomanagement wel voldoende tot haar recht komt. Gebaseerd op praktijkervaringen beschrijft dit artikel hoe risicomanagement vorm gegeven kan worden en waarde toe kan voegen aan een organisatie. Daarnaast komt een vijftal praktische uitdagingen rondom risicomanagement aan de orde.

Drs. R. Jansen RO en mr.drs. A. van Krimpen

De steeds grotere behoefte aan risicomanagement kan voortkomen uit de wens van het management om beter inzicht te hebben in risico's, maar kan ook meer extern gedreven zijn door corporate governance-codes. De Code Tabaksblat geldt voor Nederlandse beursgenoteerde organisaties, maar er komen steeds meer branchespecifieke codes. Zo zijn er bijvoorbeeld corporate governance-codes voor zorginstellingen, voor woningcorporaties, et cetera.

Sommige organisaties zeggen dat zij risicomanagement hebben geïmplementeerd. Wij kennen echter ook nogal wat organisaties die enthousiast zijn begonnen met risicomanagement maar nooit tot een volwaardige implementatie zijn gekomen. Na een aantal workshops en inventarisaties van risico's kwamen aan het eind van het eerste jaar onvermijdelijk vragen naar boven als: 'Hoe nu verder?' 'Hoe zorgen wij voor continuïteit?' 'Hoe gaan wij de gekozen managementacties monitoren?' 'Moeten wij hierover rapporteren in het jaarverslag en waarom?'

Wat is van invloed?

Risicomanagement houdt in dat risico's niet alleen worden geïdentificeerd maar dat ook daadwerkelijk acties worden geformuleerd en opgevolgd. De vormgeving en inrichting verschilt per organisatie en per branche. Om goed te functioneren moet risicomanagement namelijk aansluiten op de omgeving waarin zij functioneert. Voor de ene branche, bijvoorbeeld financiële sector, kan dit betekenen dat risicomanagement op geavanceerde wijze is ingericht met een zelfstandig risicomanager en de mogelijkheid om de risicobeheersing dagelijks te monitoren aan de hand van KSF'en en KPI's. In minder gereguleerde omgevingen, bijvoorbeeld bij een middelgroot productiebedrijf, volstaat een meer lean en mean-aanpak die aansluit bij de bestaande P&C-cyclus.

Een verklaring voor de verschillen in de inrichting van risicomanagement moet vooral worden gezocht in de doelstellingen van de organisatie en de daaruit voortvloeiende risico's, de volwassenheid van de organisatie zelf en de mate waarin binnen de branche afspraken en regels zijn overeengekomen. Ook de meetbaarheid van risico's is verklarend. Sommige risico's zijn goed en frequent meetbaar. Denk aan de invloed van rentestanden of

Element van het KPMG- risicomodel	Basis Voldoen aan wet- en regelgeving	Volwassen Een management proces	Geavanceerd Een strategisch instrument
Risicobeleid	Een centraal risicomanagement-beleid om te voldoen aan externe eisen	Een risicomanagementstructuur met duidelijke meetpunten om de risico-managementdoelstellingen te onder-steunen	Meetbaar risicomanagement geïntegreerd met prestatie-management
Risico-assessment	Jaarlijkse risico-assessment met beperkte analyse en interpretatie van risico's	Frequente risico-assessments in lijn met managementrapportage, inclusief analyse van risico's	Risico- en beheersactiviteiten geïntegreerd in organisatie-processen
Kwantificering en aggregatie	Kwantificeren van geselecteerde risico's	Kwantificeren van procesrisico's; geavanceerd kwantificeren van geselecteerde risico's	Organisatiebrede aggregatie tussen alle risicogebieden
Monitoren en rapporteren	Rapportage over organisatierisico's is ontworpen om te voldoen aan externe eisen	Uitgebreide rapportage aan de raad van bestuur en RvC/audit commissie over huidige risiconiveaus en toe-komstige risico-issues	Risicorapportages zijn op elkaar afgestemd om één samenhangend risicobeeld te geven
Optimaliseren balans risico's en maatregelen	Weinig verrassingen door het mana-gen van belangrijkste risico's *(key risks)*	Toegenomen vertrouwen van belanghebbenden en verbeterde risicomitigerende strategieën	Strategie, prestatie evaluatie en allocatie van middelen afgestemd op risico's

Figuur 1. Risicomanagement Maturitymodel (bron: KPMG Nederland 2007)

wisselkoersen. Andere risico's daarentegen zijn moeilijker meetbaar, bijvoorbeeld het risico op imagoschade.
Naast deze wat zakelijke verklaringen zijn ook hele menselijke factoren van invloed. Herkenbaar is de situatie waarin het management het enthousiasme verliest. Als geïdentificeerde risico's zich niet voordoen, wordt de relevantie van het instrument namelijk niet meer gezien.

De inrichting

Om risico's goed te managen zal de inrichting moeten aansluiten bij de verwachtingen van het management. Onvrede over het functioneren van risicomanagement hangt voor een belangrijk deel samen met een matig geformuleerde behoeftestelling. Hier hebben we meteen de eerste oorzaak voor minder goed functionerend risicomanagement benoemd. Hierna beschrijven wij nog vijf andere aspecten van risicomanagement die naar onze mening een oorzaak kunnen zijn voor een niet-optimaal functionerend risicomanagementsysteem.

1. Volwassenheid en ambitie

Net als bij andere keuzen die het management maakt, moet ook bij risicomanagement worden nagedacht over het doel en de haalbaarheid daarvan. Het maakt nogal een verschil of je kiest voor een minimale invulling of dat je een geavanceerd model voor risicomanagement nastreeft. Ook de snelheid waarmee je dat wilt realiseren is van belang. Daarbij komt dat afstemming met toezichthouders, waaronder raad van commissarissen en andere belanghebbenden, noodzakelijk is. Investeren in deze beeldvorming – voorafgaand aan de feitelijke inrichting van het risicomanagementproces – voorkomt verstoringen in het vervolgtraject. *Figuur 1* laat drie volwassenheidsniveaus zien en geeft een toelichting op het verschil in ambitie per volwassenheidsniveau voor de vijf logische bouwstenen van het risicomanagementmodel.

2. Denken in kansen

Bij het benoemen van risico's worden de organisatiedoelstellingen als uitgangspunt genomen. Vaak worden risico's in verband gebracht met gebeurtenissen die het realiseren van de doelstelling negatief beïnvloeden. Maar het tegendeel is ook waar. Het aangrijpen van kansen hoort ook bij risicomanagement en stelt de organisatie in staat proactief om te gaan met nieuwe ontwikkelingen. Hierdoor kan een belangrijk concurrentievoordeel worden opgebouwd. Om het instrument risicomanagement goed te laten functioneren, kan een SWOT-analyse worden geïntegreerd in het risicomanagementsysteem.

3. Risk appetite (risicobereidheid)

Veel organisaties managen hun risico's door het benoemen van maatregelen om alle risico's te reduceren. Dit is over het algemeen niet efficiënt. Door het benoemen van de risk appetite (risicobereidheid) van de organisatie, wordt inzichtelijk gemaakt welke risico's binnen deze risicobereidheid vallen en welke risico's niet. In het laatste geval zijn (aanvullende) maatregelen nodig om de risico's te reduceren. In het eerste geval is de organisatie mogelijk 'overcontrolled' en kan een efficiëntiewinst worden geboekt door het beperken van maatregelen. Een analyse per risicocategorie blijkt in de praktijk wenselijk omdat een algemene uitspraak over de risicobereidheid over kwalitatief geformuleerde risico's niet haalbaar is. In een situatie waarin risico's worden gekwantificeerd, kunnen risico's met elkaar worden vergeleken en kan het management 'gemakkelijker' de grens bepalen tussen acceptabel en niet-acceptabel.

Impact	Score				
	1	2	3	4	5
	laag		midden		hoog
Financieel	Minder dan € 1 mln omzetverlies of extra kosten		Omzetverlies of extra kosten tussen € 1 mln en € 10 mln		Meer dan € 10 mln omzetverlies of extra kosten
Operationeel	• Beperkte impact op het bereiken van de operationele doelstellingen • Minimaal verlies van kwaliteit van producten en/of diensten • Minimaal verlies van mensen en/of middelen		• Grote impact op het bereiken van de operationele doelstellingen • Gematigd verlies van kwaliteit van producten en/of diensten • Gematigd verlies van mensen en/of middelen • Kortstondige onderbreking sleutelproces		• Grote impact op het bereiken van de strategische (en operationele) doelstellingen • Significant verlies van kwaliteit van producten en/of diensten • Significant verlies van mensen en/of middelen • Langdurige onderbreking sleutelproces
Reputatie	• Lage politieke en/of maatschappelijke gevoeligheid • Geen negatieve aandacht in de media, slechts interne bekendheid		• Gematigde politieke en/of maatschappelijke gevoeligheid • Negatieve aandacht in de lokale media • Bijzondere aandacht van toezichthouder		• Significante politieke en/of maatschappelijke gevoeligheid (maatschappelijke onrust) • Negatieve aandacht in de nationale media • Waarschuwing van toezichthouder

Figuur 2. Referentiematrix voor het scoren van de impact van risico's
Dit is een voorbeeld van een referentiematrix, weergegeven voor het inschatten van de impact van de risico's. In de voorbereiding van de workshop stemmen wij als facilitator de schaal af in samenspraak met het management. Een impact van € 10.000.000 betekent voor de ene organisatie een faillissement maar voor een andere organisatie 'slechts' een serieuze tegenvaller.

4. Kwalificeren en kwantificeren van risico's

Veel organisaties hebben moeite met het beschrijven (definiëren) van risico's. Als onduidelijk is wat de verschillende oorzaken en gevolgen zijn van een risico, wordt het definiëren van adequate maatregelen en daarmee het managen of beheersen, ook een lastige zaak. Een goede analyse leidt tot een meer eenduidig beeld van risico's zonder hinderlijke overlap tussen de risico's. De analyse leidt tot een concretere formulering en betere afbakening van risico's. Containerbegrippen als bijvoorbeeld 'veranderingen in wet- en regelgeving', 'imagoschade' en 'politieke besluitvorming' moeten zoveel mogelijk worden vermeden omdat deze geen duidelijke richting geven om de risico's te managen.

Het is 'per definitie' gebruikelijk om geïdentificeerde risico's te prioriteren, bijvoorbeeld tijdens een workshop en met ondersteuning van stemapparatuur. Bij een dergelijk assessment is het belangrijk om een gedeeld beeld te hebben van de kans en impact van risico's (zie *figuur 2*). Wanneer is de impact hoog en wanneer laag? Onze praktijk wijst uit dat er meer behoefte ontstaat om risico's te kwantificeren. Het onderscheid tussen een hoog, midden en laag risico blijkt vaak te weinig specifiek. Op vrij eenvoudige wijze kunnen risico's meer kwantitatief worden ingeschat. Wij gebruiken meestal een semi-kwantitatieve methode. Daarvoor gebruiken we dan een schaal die de deelnemers aan het assessment in staat stelt om de risico's meer kwantitatief te scoren. 'Echte' kwantitatieve methoden worden buiten de financiële sector (banken, pensioenfondsen en verzekeringen) nog maar weinig gebruikt. Het gebruik van kwantitatieve methoden (onder andere simulatiemodellen) stelt hoge eisen aan de beschikbaarheid van informatie over de gevolgen van de risico's voor de doelstellingen van de organisatie. Hiervoor worden 'loss databases' gebouwd die bottom-up gevuld moeten worden met alle gegevens die over de ontstane risico's bekend zijn, de gevolgen

Arie van Krimpen werkt als adviseur bij KPMG Business Advisory Services. Hij richt zich in het bijzonder op risicomanagement en internal auditing.
Ronald Jansen werkt bij KPMG Business Advisory Services. Hij is binnen deze groep verantwoordelijk voor de risicomanagementpropositie.

(veelal in euro's) en de maatregelen die zijn toegepast. De volledigheid en juistheid van deze database moet natuurlijk ook worden vastgesteld. Deze databases worden interessanter als de dienstverlening een zekere standaardisatie en een hoge frequentie kent. Kwantitatieve methoden worden veelal in hogere fasen van volwassenheid gebruikt omdat de cultuur, het denken en het handelen van de organisatieleden meer risicogericht zal moeten zijn.

5. Monitoring en rapporteren

Zoals in de inleiding aangegeven, is risicomanagement meer dan het identificeren en prioriteren van risico's en het benoemen van de bijbehorende maatregelen. Risico's moeten ook daadwerkelijke gemanaged worden. Het feitelijke managen vindt plaats onder verantwoordelijkheid van de (lijn)managers. Periodiek zouden zij moeten rapporteren over de voortgang van de implementatie van overeengekomen maatregelen en de effecten daarvan. Bij voorkeur zoekt men hierbij aansluiting bij de reguliere P&C-cyclus. Op deze wijze wordt risicomanagement geïntegreerd in het dagelijkse management en de bestaande communicatie- en verantwoordingsstructuur. Deze integrale benadering vergroot het inzicht in en de samenhang tussen de gezamenlijke doelen en risico's. Integratie in de P&C-cyclus houdt de beheerslast beperkt.

Toch werkt het in de praktijk vaak anders. Managers besteden het eenvoudig uit aan risicocoördinatoren en assistenten zonder zelf voldoende aandacht te schenken aan de (periodieke) resultaten en rapportage. Dit beeld ontstaat in een omgeving waarin het management niet adequaat wordt aangesproken op haar rol en de invulling daarvan. Vaak beseft men onvoldoende het belang en de mogelijkheden van risicomanagement. Het gaat immers over de belangrijkste zaken die managers bezig zouden moeten houden. Toch?

Conclusie

In de Nederlandse praktijk is het instrument risicomanagement over de hele lijn nog niet tot volledige ontwikkeling gekomen. Gelukkig zijn er ook gunstige uitzonderingen. Laten we vooral leren van elkaar om de ontwikkeling van risicomanagement te stimuleren en daarmee de kwaliteit van (interne) beheersing te bevorderen, want daar is het allemaal om te doen.

Wij spreken internal auditors dan ook aan om zich nadrukkelijker in dit proces te verdiepen en om op professionele wijze tot oordeelvorming te komen. Wij hebben een paar van onze inzichten met u willen delen en hopen dat anderen dit voorbeeld zullen volgen.

Standaard auditopinies:

een dwaling of een stap op weg naar volwassenheid?

In de dagelijkse praktijk hanteren de meeste interne auditdiensten een stelsel van auditopinies om hun conclusies bij een operational audit te communiceren. Tegelijkertijd zijn er prominente vertegenwoordigers die voor terughoudendheid van het gebruik van opinies pleiten.

B. Vis en S. van Verseveld

Op 27 september 2007 organiseerde de IIA NL-werkgroep 'Audit Opinies' een goed bezochte round-table voor managers van interne auditdiensten. De aanleiding voor de round-table was de wens van het IIA Commissie Professional Practices om vast te stellen 'waar we staan in Nederland' en te onderzoeken of er behoefte is aan verdere guidance. De door de werkgroep gemaakte inventarisatie en de discussies bij de round-table leverden interessante uitkomsten op.

Aanpak en werkwijze

De werkgroep Audit Opinions stelde vast dat er weinig onderzoek is gedaan naar het gebruik van audit opinions bij operational audits en naar de wenselijkheid tot meer standaardisatie te komen. In verwante vakgebieden zijn die standaarden er wel, zoals bij registeraccountants die voor hun financial auditwerkzaamheden al jaren met een standaard stelsel van oordelen werken. Ook de register EDP-auditors zijn al enige tijd bezig met een onderzoek naar de haalbaarheid van een stelsel van oordelen.
De werkgroep stuurde als voorbereiding op de round-table een questionnaire naar hoofden van in Nederland werkzame interne auditdiensten. Tijdens de round-table hield de werkgroep een presentatie waarbij het accent lag op de voordelen van het gebruik van standaard opinies. Tevens was er de inbreng van een externe deskundige, die een tegengeluid liet horen. Aan de hand van een aantal stellingen en interactieve stemronden werd gediscussieerd.

De argumenten voor

Voorafgaand aan de round-table had de werkgroep de positie ingenomen dat het nuttig zou zijn wanneer er een richtlijn of handreiking op het gebied van auditopinies bij operational audits zou komen. Auditopinies hebben tot doel het (top)management te voorzien van eenduidige en transparante informatie over de mate waarin het object van onderzoek in control is en of de bedrijfsdoelstellingen kunnen worden behaald. De werkgroep is zich ervan bewust dat voor een goed gebruik van standaards een aantal vragen beantwoord moet worden. Het gaat daarbij om vragen als:

- Zijn beoordelingen gebaseerd op meetbare normen? wie bepaalt deze normen?
- Zijn auditobjecten onderling vergelijkbaar?
- Zijn interne en/of externe omgevingsfactoren meegenomen?
- Wordt gewerkt met wegingsfactoren en zijn deze inzichtelijk?
- Hebben alle gebruikers/stakeholders een zelfde kennisniveau?

> "Het is voor de internal auditor cruciaal dat er voorafgaand aan de hantering van de ratings overeenstemming is tussen opdrachtgever, auditee en auditor over de grondslag van de rating. Dit om onnodige en zinloze discussies te voorkomen."
>
> Jan Driessen

Professionele auditorganisaties (zoals het IIA Inc.) stellen expliciete eisen omtrent de rapportage van (de uitkomsten van) assurance-opdrachten en de communicatie daarover. IIA, Standard

2410.A1: ‘Final communication of results should, where appropriate, contain the internal auditor’s overall opinion or conclusions’. De werkgroep was en is van mening dat standaardisatie als nadere invulling van deze richtlijn een volgende stap is op weg naar volwassenheid van het vakgebied van internal audit.
Standaardisatie van de bij opinies gebruikte bewoordingen komt de transparantie, vergelijkbaarheid en eenduidigheid naar de gebruikers ten goede. De werkgroep noemde de volgende specifieke argumenten in haar pleidooi voor het gebruik van (standaard) auditopinies bij operational audits:

- Duidelijkheid verschaffen aan de stakeholders. Standaardisatie van (de bewoordingen van) het oordeel geeft inzicht in de aard en ernst van de bevindingen en het belang daarvan voor het object van onderzoek (criteria/scope). Een consistent begrippenapparaat bevordert de communicatie over de risico- en controlstatus van een organisatie. Ergo, de chief audit executive in plaats van de gebruiker interpreteert.
- Vergelijkbaarheid van oordelen vergroten. Standaardisatie vormt een benchmark voor het evalueren van de control effectiveness van auditobjecten ten opzichte van elkaar en in de tijd (referentie) en biedt de mogelijkheid om in vogelvlucht (snapshot) auditresultaten herkenbaar weer te geven.

De argumenten tegen

Jan Driessen was bereid gevonden om een tegengeluid te laten horen. In beginsel herkende hij de voordelen van standaardisatie, zeker als de keuze is gemaakt om een expliciet oordeel uit te spreken. In zijn betoog benadrukte hij echter dat de wenselijkheid van het koppelen van een auditopinie aan de uitkomsten van een operational audit, ter discussie moet worden gesteld. Immers, bij operational audits is in zijn ogen sprake van ‘maatwerk’.
Hij trok in zijn betoog een parallel met een wijncasus. Hij had een fles wijn gekocht met een perfecte beoordeling, maar dat bleek geen garantie voor een goede afdronk. Daarbij spelen immers meer aspecten een rol dan sec de kwaliteit van de wijn (zoals de persoonlijke voorkeur, temperatuur, combinatie met voedsel, et cetera). Bij een audit is dat niet anders, daar spelen bijvoorbeeld aspecten als reikwijdte van het onderzoek, risk appetite en control environment een rol. Bovendien geldt bij operational audit dat namens de topleiding getoetst wordt of de controls in het proces werken zoals bedoeld. Dus eigenlijk moet de topleiding een opinie geven (‘van de wijn proeven’); niet de auditor.

> “Uiteraard is elke schaal arbitrair en niet zaligmakend. Als je dat maar uitlegt en de criteria helder maakt, lijkt me dat geen probleem. Ik ben zelf niet zo’n voorstander van veel gebruikte ratings, althans, ik zou voor enige voorzichtigheid willen pleiten.”
>
> Leen Paape

Bij het gebruik van standaard opinies binnen de beroepsgroep bestaat er volgens hem een reëel risico dat onvoldoende recht wordt gedaan aan de specifieke omstandigheden. Zo bezien is het gebruik van standaard opinies voor het management eerder een schrikbeeld dan een geruststelling (nog meer ‘rule based’). Ratingsystemen zijn arbitrair en leiden volgens Driessen af van de kern: waar het om draait is dat er tussen de auditor en de gebruiker overeenstemming wordt bereikt over de aandacht- en verbeterpunten en de hierbij gehanteerde maatstaf. Het gaat primair om het verbeteren van de controls, maar door gebruik van opinies bij operational audits verschuift de aandacht van de inhoud van de boodschap naar de systematiek van oordeelsvorming. De auditee wordt dan afgeleid van het werkelijke probleem: kan ik de uitkomsten van oranje niet naar groen praten? Kan ik van die twee geen drie maken, et cetera.

De praktijk in Nederland

Begin 2007 presenteerde Audit Directors Round-table de resultaten van een wereldwijde inventarisatie onder leden aangaande het gebruik van auditopinies.[1] Om inzicht te krijgen in de situatie in Nederland benaderde de werkgroep de hoofden van interne auditdiensten om hun systematiek rondom af te geven oordelen kenbaar te maken. De belangrijkste uitkomsten van de inventarisatie zijn:

- 73 Procent van de respondenten hanteert intern standaardoordelen. Er zijn duidelijke verschillen per sector:
  - in de financiële sector maakt 100 procent van de respondenten gebruik van standaard opinies;
  - bij de (semi-)overheid worden vrijwel geen standaard opinies gebruikt.
- Er is veel variatie in de uitwerking van de standaarden. Dat blijkt bijvoorbeeld uit:
  - de gehanteerde schaal (3/4/5 punt);
  - de gebruikte presentatie vorm (kleuren/cijfers/letters/woorden). Meest voorkomend is een 4-puntsschaal met gebruik van woorden, vaak in combinatie met kleuren. Bijvoorbeeld: onvoldoende/matig/voldoende/goed.
- Er is geen consistentie bij het gebruik van begrippen. Dat blijkt bijvoorbeeld uit het feit dat:
  - hetzelfde begrip niet overal dezelfde inhoud heeft (een veel gehanteerd begrip als 'voldoende' betekent dan niet overal hetzelfde);
  - verschillende begrippen worden gebruikt voor dezelfde inhoud (voor een onderzoek waarbij belangrijke tekortkomingen zijn geconstateerd gebruikt men wezenlijk andersluidende omschrijvingen).

Voorbeelden van 'hetzelfde begrip maar verschillende inhoud':

- Bij onderneming A is 'adequate' de beste score op een schaal van drie met als omschrijving: 'the operations are assessed to have an adequate system of internal controls and procedures in all areas within the scope of this audit. The impact of any weaknesses identified in the control environment imposes the business or function to limited risk'.
- Bij onderneming B is 'adequate' de tweede score op een totaal van vier mogelijk te geven scores met als omschrijving: 'voldoet aan de norm, geen (bedrijfskritische) verbeteringen noodzakelijk'.

> "Belangrijk is dat we operational audit in de breedte blijven positioneren en niet alleen vanuit de (financial) in control voor de top, met de nadruk op vergelijkbaarheid. Die ratings passen bij vergelijkbaarheid en dat is slechts een manier om toegevoegde waarde te leveren. "
>
> Ron de Korte

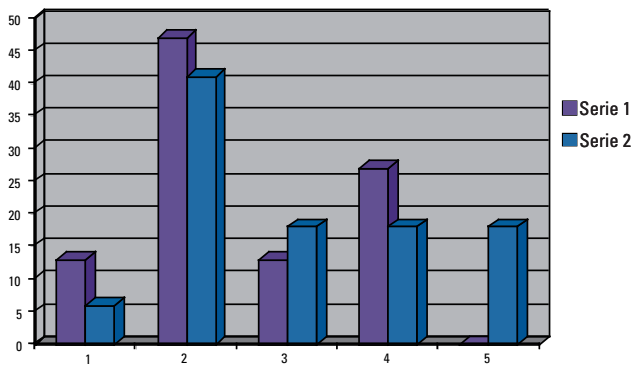
Voorbeelden van 'verschillende begrippen voor dezelfde inhoud':

- Bij onderneming C is de derde score op een schaal van vier mogelijk te geven scores aangeduid als 'insufficient'.
- Bij onderneming D wordt voor een vergelijkbare score de term 'qualified' gehanteerd.

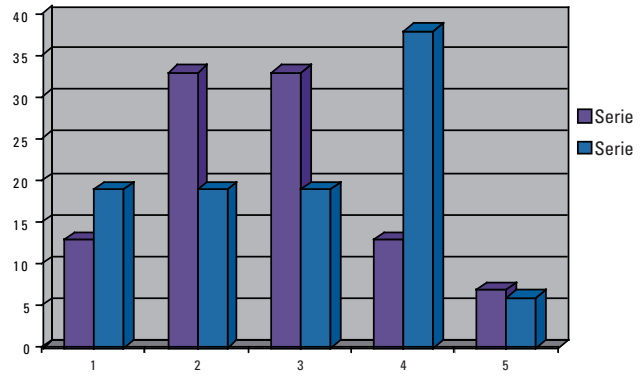
Round-table: discussie over stellingen

Tijdens de round-table konden de deelnemers zich uitspreken over een aantal stellingen. Door middel van stemkastjes konden de deelnemers hun mening geven. De normering was hierbij steeds een 5-puntsschaal (1 = helemaal mee eens, tot 5 = helemaal niet mee eens. De werkgroep heeft ook nagegaan in hoeverre de door de werkgroep en Jan Driessen ingebrachte argumenten tot bijstelling in de meningen van de deelnemers leidde.

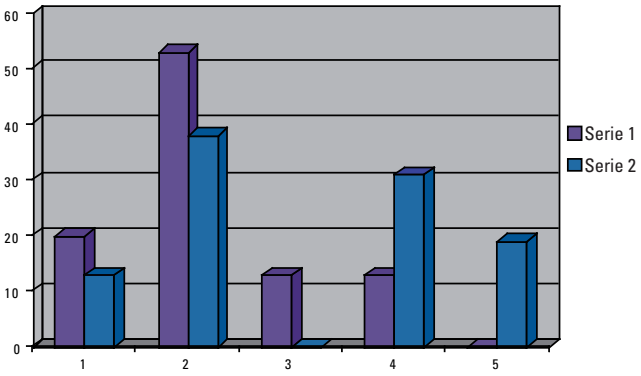
- ***Stelling 1:*** *het geven van een oordeel in een operational audit draagt bij aan het verbeteren van de beheersing van bedrijfsprocessen.*



Figuur 1. Stemresultaten eerste stelling voor (serie 1) en na (serie 2) inbreng van argumenten



Figuur 2. Stemresultaten tweede stelling voor (serie 1) en na (serie 2) inbreng van argumenten



Figuur 3. Stemresultaten derde stelling voor (serie 1) en na (serie 2) inbreng van argumenten

Uit de stemresultaten blijkt aan het begin van de round-table een ruime meerderheid het met de stelling eens te zijn. Na inbreng van de argumenten voor en tegen is een tendens richting 'niet mee eens' zichtbaar. Belangrijkste argument daarbij was dat een oordeel afleidt van de kern (zie *figuur 1)*.

• ***Stelling 2:*** *het is in het belang van de internal auditor dat er een richtlijn komt die het gebruik van standaard oordelen voorschrijft.*

Uit de stemresultaten blijkt het percentage tegenstemmers na inbreng van de argumenten voor en tegen meer dan verdubbeld, maar nog altijd minder is dan 50 procent. De deelnemers gaven aan met name gecharmeerd te zijn van de duidelijkheid en grotere consistentie die kan worden bereikt met een algemeen geldende standaard. Tegelijkertijd ontstond er toenemende weerstand tegen een verplicht karakter van een richtlijn (zie *figuur 2*).

Conclusie

Uit de geanimeerde discussies tijdens de round-table bleek dat het onderwerp '(standaard) auditopinies' leeft binnen de beroepsgroep. Een meerderheid van de deelnemers is voor het gebruik van opinies, maar er bestaat nadrukkelijk verschil van inzicht over de wenselijkheid en (met name) de mate van standaardisatie.

Op basis van de argumenten tijdens de presentaties en de daarop volgende discussies is een verschuiving waarneembaar in de richting van terughoudendheid in de mate van standaardisatie. Bij de deelnemers kon het beschikbaar maken/gebruiken van best practices wel rekenen op support. De suggestie om tot meer richtlijnen/verplichte aanwijzingen vanuit de beroepsinstanties (zoals het IIA) te komen, werd door de meerderheid van de deelnemers niet gesteund.

De werkgroep wil als vervolgstap komen tot een meer vrijblijvende handreiking (practice advisory) op het gebied van standaard te hanteren opinies. Met name bij beginnende auditfuncties is er duidelijk vraag naar guidance op dit vlak.

• ***Stelling 3:*** *Het gebruik van een beperkt aantal standaard oordelen zal leiden tot een beter begrip van de betekenis ervan bij het management/de auditee.*

Uit de stemresultaten blijkt aan het begin van de round-table een meerderheid het met de stelling eens te zijn. Na inbreng van de argumenten voor en tegen is een tendens richting 'niet mee eens' zichtbaar. De deelnemers gaven aan dat het vooral de argumentatie is die zorgt voor het begrip bij het management en de auditee, niet zo zeer het oordeel (zie *figuur 3*).

Serge van Verseveld maakt als audit manager deel uit van de afdeling Group Audit & Risk Services van Eureko/Achmea.
Bas Vis is senior audit manager van de afdeling Professional Practices van Corporate Audit Services bij de ING Groep.
De IIA Werkgroep Audit Opinions bestond verder uit Harrie de Poot (voorzitter werkgroep, Rabobank), Jaap de Vries (NS) en Gerard Zwiers (Mitsubishi Motors).

Noot

1. Survey of Rating Systems for Audit Reports and Audit Findings, maart 2007, Angelina Chin, GM Audit Services.

Mark Jongejan trad per 1 januari 2008 in dienst als manager Internal Audit bij Heineken Nederland. Daarvoor was hij manager Internal Audit bij Connexxion.

Huck Chuah is vanaf 1 januari 2008 werkzaam bij Randstad als risk manager. Voorheen was hij hoofd Internal Audit bij Samas nv.

Sytske Breedveld startte per 1 januari 2008 bij Akzo Nobel.

Arjen van Nes is per 1 januari jl. werkzaam als corporate risk manager bij Cordares. Voorheen was hij chief internal auditor bij GWK Travelex.

Vlijmscherp Private equity?

Drs. A. van Nes RO*

De afgelopen maanden hebt u in de kranten het nodige kunnen lezen over de effecten van private equity op het Nederlandse bedrijfsleven. Op basis van onderzoek van de Erasmus Universiteit (een inventariserend literatuuronderzoek, voornamelijk gebaseerd op artikelen uit de VS geschreven in de jaren tachtig van de vorige eeuw), verklaarde onze minister van Financiën in november vorig jaar dat investeringsmaatschappijen gemiddeld genomen positief zijn over de winstgevendheid van de bedrijven. Bos zei blijkens een artikel in de *NRC* (3 november 2007) verder: "Ook het beeld dat bedrijven na private equity-overnames slechter presteren, bijvoorbeeld door verhoging van de schuld, is gebaseerd op zeldzame gevallen." Dit baseerde hij op hetzelfde onderzoek. Onze minister wilde hiermee een antwoord geven op negatieve uitspraken over de effecten van private equity en hedge funds, onder andere na de verkoop van ABN Amro.

De *NRC* biedt in hetzelfde artikel weerwoord: alle grootschalige gezichtsbepalende recente overnames door investeerders in Nederland leveren een ander beeld op. Bij de meer dan tien grootste recente overnames waar cijfers van beschikbaar zijn (gezamenlijke overnamesom ruim 29 miljard euro) is er slechts één bedrijf dat winst maakt. Alle andere ondernemingen lijden verlies. Hun schulden namen met 12 miljard toe.

Het beeld van private equity als de harde heelmeester voor de Nederlandse economie die van onze achterblijvende 'watjes'-bedrijven weer 'echte mannen' maakt, is dus niet eenduidig. In de tweede week van januari volgde een uitspraak van de Ondernemingskamer. De private equity-aanbieder die PCM overnam, APAX, toonde volgens de Ondernemingskamer 'onvoldoende committment bij PCM, het belang van de vennootschap en de continuïteit van de bedrijfsvoering. De nadruk was vooral gericht op het eigen rendement.

Wat nu betekent de komst van private equity voor een auditafdeling? Natuurlijk heeft schrijver dezes geen onderzoek gedaan. Maar helaas wel enige ervaring op dit gebied. Laten we uitgaan van de gang van zaken zoals beschreven bij PCM. De met schuld overladen onderneming zal op een streng kostenbesparend dieet worden gezet. De schuld is aangegaan tegen een hoog rentepercentage (bijvoorbeeld 15 procent). Doel van de investeerder is het terugverdienen van de lening en het bedrijf klaarmaken voor doorverkoop. Eventuele investeringen worden niet vanuit ondernemen (klanten en toekomstige klanten), maar vanuit portfoliobeheer gedaan (hoe kan de verkoopwaarde verbeterd worden). Voor de auditfunctie betekent dit dat ze moet bezuinigen, net als alle andere afdelingen. Die andere afdelingen gaan met minder mensen (en ook met minder gemotiveerde mensen) meer doen. Aspecten als het volgen van procedures, klantgerichtheid, oog voor kwaliteit, samenwerking en motivatie kunnen dan in de knel komen. Operational audits die uitgaan van ondernemingsdoelen die in deze termen zijn geformuleerd, worden lauw of slecht ontvangen. Het beleid geldt namelijk niet meer, maar de net vernieuwde top heeft er geen belang bij nieuwe doelen duidelijk te formuleren voor de medewerkers. Besparen, bezuinigen en uitstellen met het oog op de hoge rentelasten zijn geen motiverende ondernemingsdoelstellingen, nietwaar? Mogelijkheden voor fraude gaan zich voordoen. De veelal nieuwe ondernemingsleiding, daar geplaatst door de private equity-investeerder met de belofte van een hoge bonus, is bovenal gericht op de financiële resultaten.

De auditafdeling zal daarom al snel het verzoek krijgen zich op de ondersteuning van de nieuwe doelen en strategie te richten en de aandacht te richten op financial audits en fraudeonderzoeken. Dit alles onder het motto: ga zoeken naar besparingen. Dit gaat natuurlijk wel ten koste van de andere stakeholders: personeel, leveranciers, huidige klanten en toekomstige klanten. En van het plezier in het werk (want die bonus is er niet voor de auditor).

* Arjen van Nes was voorheen redacteur van *Audit Magazine*. Hij schrijft deze column op persoonlijke titel.

Audit u al innovatie?

Je kunt geen tijdschrift of krant openslaan of je komt het onderwerp innovatie tegen. Seminars en congressen zijn eraan gewijd en allerlei prijzen worden onder dit motto toegekend. Is dit een 'ver-van-ons-bed-show' of moet de auditor innovatie wel degelijk tot zijn werkterrein maken?

B.A.C. de Vries EMIA RO CIA

Innovatie is hot. De media staan er bol van. De Europese Unie wil in 2010 de meest dynamische, concurrerende kenniseconomie ter wereld zijn en Nederland moet binnen Europa tot de top gaan behoren. In 2003 is een Innovatieplatform opgericht en sindsdien is er een jaarlijkse top 10 van meest innovatieve landen, Nederland staat daarin nu op de zesde plaats dankzij de mp3-speler, TomTom en Bluetooth. Bedrijven hebben er belang bij te innoveren om zodoende hun continuïteit te waarborgen. Innoveren maakt steeds meer deel uit van de strategie.
Ook in auditland wordt het belang van innovatie onderkend: 'Internal auditors zouden niet alleen bewakers van het gevestigde beleid en procedures moeten zijn, maar ook voorvechters van positieve verandering en continue verbetering'.[1]
Maar is innovatie te meten en dus te auditen? In dit artikel eerst een nadere beschouwing van het begrip innovatie, daarna volgt een aanzet tot discussie waarom innovatie een onderwerp van audit zou moeten zijn. Afsluitend wordt een aantal mogelijke invalshoeken voor een audit op innovatie aangereikt.

Wat is innovatie
Het begrip innovatie werd in 1912 als eerste gebruikt door de Oostenrijkse econoom Schumpeter. Innovatie wordt vaak als synoniem gebruikt voor verandering. Hoewel elke innovatie per definitie een verandering is, is niet elke verandering een innovatie. De dikke Van Dale definieert innovatie als volgt: invoering van iets nieuws. En juist de aanduiding 'iets nieuws' is onderscheidend van verandering. De Jong en Brouwer (1999) geven in hun definitie van innovatie uitsluitsel wat onder 'iets nieuws' verstaan moet worden: 'An innovation is the development and successful implementation of a new or improved product, service, technology, work process or market condition, directed towards gaining a competitive advantage'.
Het gaat derhalve om het *invoeren* van *nieuwe*, nog niet in gebruik zijnde (combinaties van) toepassingen *binnen een bepaalde context*. Het toepassen van robots was in de ruimtevaart al gemeengoed terwijl het toepassen van deze techniek in de zorg en bij operatietechnieken een innovatie was. De ontwikkeling van een driebenige panty is echter niet als innovatie te betitelen aangezien dit (nog) niet is ingevoerd.
Er wordt ook onderscheid gemaakt in de vorm van innovatie. Het object waarop de innovatie is gericht, bepaalt dit onderscheid (van der Voort, 2006):

- Procesinnovatie, de meest bekende vorm, waarbij het vizier van de vernieuwing is gericht op het behalen van efficiencyvoordelen ofwel dezelfde dingen steeds goedkoper doen.
- Productinnovatie is gericht op het vergroten van de omzet door in te spelen op de (veranderende) behoefte van de klant ofwel andere dingen doen voor dezelfde klant.
- Marktinnovatie is eveneens gericht op het vergroten van de omzet, maar dan door bestaande producten op nieuwe markten af te zetten (al dan niet door aanpassing van het product) ofwel, bijna dezelfde dingen doen voor andere klanten.

Waarom auditen?
De vorm van innovatie is echter van minder groot belang dan de mate en variatie waarin een organisatie innoveert: 'Het zijn niet degenen die het sterkst of het snelst zijn die uiteindelijk overleven, maar degenen die zich het best aanpassen aan nieuwe omstandigheden' (Charles Darwin, 1859).
Het 'aanpassen aan nieuwe omstandigheden' is daarom te zien als een maatregel voor het beheersen van het bedrijfsrisico. Doff (2006) definieert dit risico immers als volgt: 'Het risico van verliezen die ontstaan uit veranderingen in de concurrentieomgeving of het tekortschieten van de interne flexibiliteit'. Auditen van innovatie is daarmee een audit op de beheersing van het bedrijfsrisico.
In verhouding tot risico's als liquiditeits-, markt- of kredietrisico blijft het in kaart brengen van het bedrijfsrisico echter onderbelicht ondanks de erkenning van het belang van innovatie voor het voortbestaan van de organisatie (Bijvoet, 2007; *Het Financieele Dagblad*, 18-6-2007; Prahalad en Ramaswamy, 2004;

Lonkhuyzen, 2007; Pickford, 2006; Chan Kim, 2007). In bijvoorbeeld Solvency II is het meten van het bedrijfsrisico zelfs niet opgenomen. Niet omdat het als minder belangrijk wordt gezien, maar omdat het kwantificeren ervan veel lastiger zou zijn dan bijvoorbeeld markt- of kredietrisico (Doff, 2006).
Juist hier kan Internal Audit een toegevoegde waarde leveren. Auditjaarplannen dienen in toenemende mate risicogebaseerd zijn. Gezien de geringe aandacht voor beheersing van het bedrijfsrisico verdient een onderzoek naar de omvang en de eventuele beheersmaatregelen voor dit risico een plaats op de auditagenda.
Daar waar Doff (2006) het beheersen van dit risico defensief insteekt (periodieke strategische analyses van de concurrentiepositie, marktanalyses, analyses van de kostenstructuur) is het inbedden van innovatie in de organisatie te beschouwen als een offensieve manier om dit risico te beheersen.

Invalshoeken

Deze inbedding vormt bij uitstek het onderwerp voor een audit en kan vanuit verschillende invalshoeken benaderd worden.
- Is het vermogen om te innoveren aanwezig binnen de organisatie?
- Is innovatie als proces aanwezig?
- Wordt op innovatie gestuurd?

Per invalshoek levert de enorme hoeveelheid literatuur op het gebied van innovatie verschillende auditvariabelen (zie *figuur 1*)[2] waarvan ik er enkele wil noemen. Naast het uitvoeren van een audit naar deze vorm van risicobeheersing kan de bijdrage van Internal Audit echter ook bestaan uit het aanzetten tot discussie en besluitvorming door het management over de norm voor de hierna genoemde variabelen.

Innovatievermogen

Om de auditvariabelen voor de invalshoek van het innovatievermogen te kunnen bepalen (zie *figuur 2*), moet eerst gedefinieerd worden wat onder innovatievermogen wordt verstaan. De Jong en Brouwer (1999) definiëren dit als volgt: 'Het vermogen van de werknemers van een organisatie om ideeën te genereren en deze toe te passen teneinde nieuwe of verbeterde producten, diensten, technologieën, werkprocessen of markten te ontwikkelen'.

Figuur 2. Auditvariabelen voor innovatievermogen

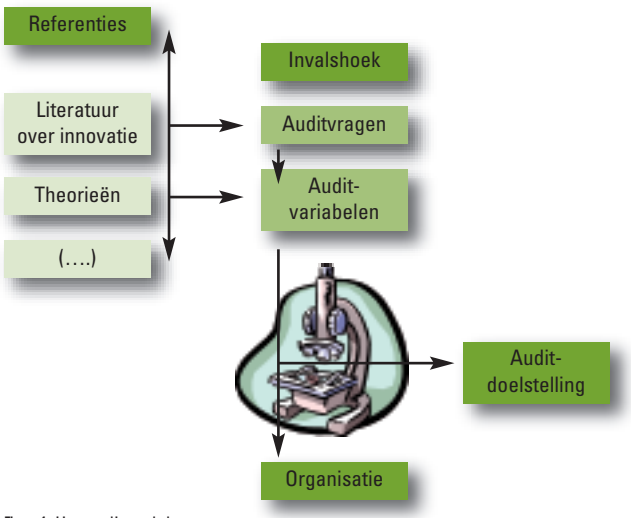
De medewerker vervult dus een centrale rol in het innovatief vermogen van een organisatie. Daarom is het van belang te weten welke factoren het genereren van ideeën bij medewerkers beïnvloeden. In het onderzoeksrapport van De Jong, Kemp en Snel (2001) worden 38 factoren onderzocht, 13 daarvan zijn significant, met als belangrijkste de bereidheid van de medewerker om risico's te nemen om zodoende zijn creatieve vermogens te benutten. Allereerst dienen medewerkers met creatieve vermogens binnen de organisatie aanwezig te zijn. De werving en selectie dient zich daar dan ook op te richten (à auditvariabele 1).
Daarnaast dient de medewerker ook de gelegenheid te krijgen deze eigenschap aan te spreken (en dan wel gericht op de bedrijfsbelangen). Tolerantie voor fouten, mislukkingen en/of suboptimale productie is dan essentieel omdat het dit type medewerker toegestaan moet worden zijn ideeën uit te proberen terwijl er toch een resultaatgerichte cultuur heerst (à auditvariabele 2). Deze werknemers zijn dan ook niet gebaat bij strikte handhaving van voorgeschreven procedures omdat dit geen beroep doet op hun creatieve vermogens wat juist één van de motivatiefactoren voor dit type werknemer is. Het belang van een juiste, daarop afgestemde managementstijl heb ik al in een eerder artikel uiteengezet[3] (à auditvariabele 3).
In hetzelfde onderzoeksrapport worden ook multifunctionele teams (à auditvariabele 4) en autonomie (à auditvariabele 5) genoemd als factoren die van significante invloed zijn op het innovatievermogen.

Het beschikbaar hebben van innovatievermogen is één voorwaarde voor innoveren. Een tweede voorwaarde is het vervolgens benutten van dat vermogen door innovatie enerzijds als proces te onderkennen en anderzijds op innovatie te sturen.

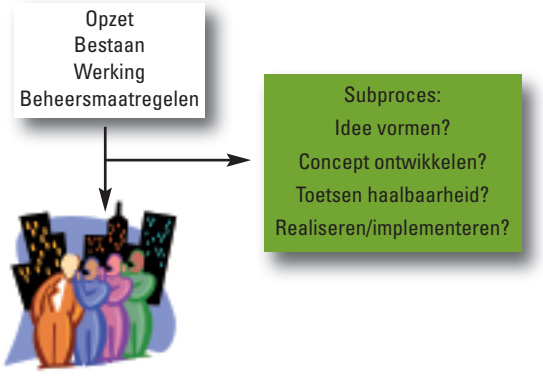
Innovatie als proces

Innovatie als proces valt uiteen in vier subprocessen:
1. idee vormen;
2. concept ontwikkelen;
3. haalbaarheid toetsen;
4. realiseren/implementeren.

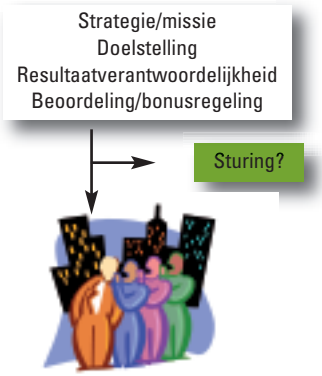
Auditvariabelen vanuit deze optiek zijn voor deze processen niet anders dan voor andere procesaudits: zijn deze processen onderkend, toegewezen (taken, verantwoordelijkheden en bevoegdheden), in werking en zijn er toereikende beheersmaatregelen? (zie *figuur 3*).



Figuur 1. Het auditmodel



Figuur 3. Auditvariabelen voor het innovatieproces



Figuur 4. Auditvariabelen voor sturing

Toch zijn er enkele specifieke aandachtspunten:

- De betrokkenheid van verschillende disciplines en externe partijen is bij de ideevorming en de conceptontwikkeling essentieel zodat niet alleen ideeën worden gevormd en ontwikkeld in het kader van procesinnovatie, maar ook in de vorm van product- en marktinnovatie.
- Voor het toetsen van de haalbaarheid van ontwikkelde ideeën is een brede visie eveneens een randvoorwaarde. Niet uitsluitend financiële criteria maar ook criteria op het vlak van imagoeffect, kennisverrijking en marktontwikkeling dienen bij de toetsing betrokken te worden. Een voorbeeld daarvan is de aanwezigheid van bedrijven in virtuele werelden als Second Life. De opbrengsten van deze investering zijn onzeker omdat in een virtuele wereld bijvoorbeeld niets kapot gaat en producten dus een oneindige levenscyclus hebben. Echter, aanwezigheid op dit soort platforms heeft wel een uitstraling op de markt. Bovendien wordt kennis opgedaan van deze gamingwereld die een mogelijk toekomstig concurrentievoordeel oplevert die te vergelijken is met de eerste bedrijven die internet toepasten in hun bedrijfsprocessen.

Sturing van innovatie

De laatste invalshoek voor een audit op innovatie die in dit artikel wordt besproken is het sturen op innovatie (zie *figuur 4*). Die sturing begint bij het opnemen van innovatie in de missie en strategie van de onderneming die vervolgens vertaald wordt naar tactische doelstellingen met concrete targets en dus wordt opgenomen in de PDCA-cyclus.[4] Het toewijzen van resultaatverantwoordelijkheid voor het behalen van deze doelstellingen en het onderdeel laten zijn van de jaarlijkse beoordeling en/of bonusregeling, versterkt deze sturing.

Conclusie

In dit artikel is getracht een lans te breken om innovatie op de auditplanning te zetten door de relatie te leggen met beheersing van het bedrijfsrisico. Er is een aantal invalshoeken voor een audit op innovatie genoemd. Per invalshoek is een aantal mogelijke auditvariabelen aangereikt waarvoor eerst normstelling aanwezig moet zijn alvorens deze in een audit te kunnen betrekken. Ik roep de lezers van dit artikel op te reageren op de titel van dit artikel en daarbij aan te geven wat de invalshoeken en auditvariabelen waren om daarmee een aanzet tot discussie te geven.

Noten

1. Messemaeckers van de Graaff, C., 'Topprioriteiten voor internal audit in een veranderende omgeving', *Audit Magazine*, 4-2006.
2. Het auditmodel is een middel om een overzicht te krijgen van de verschillende stappen die gezet moeten worden om de auditdoelstelling, in dit geval 'een oordeel geven over de inbedding van innovatie in de organisatie', te bereiken. Vanuit een korte omschrijving van het doel van de audit moet worden bepaald met welke invalshoek (bril) de organisatie beschouwd zal worden en dus met welke bril het onderzoek zal worden uitgevoerd. Deze invalshoek levert met behulp van literatuur, theorieën, (control)modellen, et cetera de auditvragen en bijbehorende auditvariabelen c.q. beoordelingscriteria.
3. Vries, B.A.C., de, 'Managementcontrolmodellen en medewerkers: een kwestie van vertrouwen', *Audit Magazine*, 4-2006.
4. Plan-Do-Check-Act.

Literatuur

- Bijvoet, drs. C.C., 'Succesvol ondernemen met personeel', *MKB-special 2007*, Economisch buro ING, Amsterdam.
- Chan Kim, W. en Renée Mauborgne, *De blauwe oceaan*, Business Contact, Amsterdam, 2005.
- Doff, René, *Risicomanagement bij verzekeraars*, NIBE-SVV, Amsterdam, 2007.
- *Het Financieele Dagblad* (18 juni 2007), 'PwC: farma moet het roer snel omgooien – Innovatie speelt niet in op de vraag'.
- Jong, J.P.J. de en E. Brouwer, *Determinants of the innovative ability of SMEs: literature review*, Zoetermeer, EIM, 1999.
- Jong, J.P.J. de, R. Kemp en C. Snel, *Research Report 0010/A-Determinants of innovative ability – an empirical test of a causal model*, Zoetermeer, EIM, 2001.
- Lonkhuyzen, Peter, 'Manager wordt creativiteitsdelver', *Management Team*, nr. 5, 23-3-2007.
- Pickford, J., *Mastering Innovatie*, Business Contact, Amsterdam, 2006.
- Prahalad, C.K. en Venkat Ramaswamy, *The future of competition*, Harvard Business School Press, 2004.
- Voort, P. van der, *Innoveren van droom tot daad*, SDU, Den Haag, 2006.

Brigitte de Vries is senior auditor bij Allianz Nederland Groep nv. Dit artikel is op persoonlijke titel geschreven. E-mail: brigitte.de.vries@planet.nl

Kwantificering van niet-financiële risico's

Drs. H. Malaihollo CIA*

De afgelopen jaren hebben ondernemingen aanzienlijk geïnvesteerd in het optuigen van hun risicomanagementorganisatie. Nu lijkt de tijd gekomen om de verschillende activiteiten en initiatieven op het gebied van risicomanagement te integreren. Met andere woorden: slimmer aanpakken. Daarnaast wordt gezocht naar mogelijkheden om meer relevante informatie te genereren uit de nieuwe risicomanagementprocessen.

De onlangs uitgebrachte adviezen van de Commissie-Frijns en Eumedion gaan hier nader op in. De monitoringcommissie Corporate Governance adviseert in haar derde rapport over de naleving van de Nederlandse corporate governance-code (december 2007) dat ondernemingen in hun jaarverslag explicieter moeten aangeven welke risico's zij bereid zijn te nemen om hun doelstellingen te realiseren. Hierbij moeten zij de kwalitatieve impact van de risico's beschrijven en daar waar mogelijk de risico's door middel van een gevoeligheidsanalyse kwantificeren. Ook Eumedion, het corporate governance-platform voor institutionele beleggers, constateert in haar jaarlijkse speerpuntenbrief aan de 75 grootste Nederlandse beursgenoteerde ondernemingen (november 2007) dat risico's slechts in een beperkt aantal gevallen worden gekwantificeerd.

Het belang van het kwantificeren van risico's wordt dus nadrukkelijk onderschreven in beide adviezen. Er wordt echter geen concreet normenkader aangereikt om hier daadwerkelijk invulling aan te geven. Vooral het kwantificeren van niet-financiële risico's zoals operationele en compliancerisico's, leidt tot de nodige 'hoofdbrekens'. Daar waar financiële risico's zoals krediet- en verzekeringsrisico met behulp van historische data en modellering berekend kunnen worden, is deze aanpak voor niet-financiële risico's niet een-op-een toepasbaar. Enkele financiële instellingen zijn inmiddels gestart met het verzamelen en documenteren van niet-financiële incidenten en verliezen, maar de tijdsperiode waarover dit plaatsvond en de hoeveelheid vergaarde data is nog verre van toereikend.

Nu het verleden voorlopig geen oplossing lijkt te bieden voor het probleem, zullen we ons moeten wenden tot het heden en de toekomst. Vragen die hierbij passen zijn: welke gebeurtenissen of scenario's kunnen zich in de toekomst voordoen die de onderneming daadwerkelijk kunnen schaden? En: hoe kwetsbaar is de onderneming hiervoor? Voor de eerste vraag kan gebruikgemaakt worden van diverse scenarioanalysebenaderingen.
Voor de tweede vraag lijkt de traditionele risicoanalyse op basis van 'impact' en 'waarschijnlijkheid' een logische keuze. Hierbij past echter één kanttekening: in de praktijk blijkt 'waarschijnlijkheid' geen goede voorspeller, vooral niet als het gaat om onverwachte of extreme gebeurtenissen. Ter illustratie, wanneer we in 2000 gevraagd hadden: hoe groot acht u de kans op een gebeurtenis als 9/11, Enron of de orkaan Catharina?, dan waren er maar weinigen geweest die deze kans als groter dan nul hadden ingeschat. Het zijn juist deze gebeurtenissen waarvan aandeelhouders willen weten of ondernemingen hiertegen gewapend zijn. Het zijn dan factoren als controleffectiviteit, snelheid van reageren op gebeurtenissen, complexiteit van activiteiten en alertheid op signalen, die de kwetsbaarheid van de onderneming bepalen.

Tot slot. Ofschoon scenarioanalyse in combinatie met een impact en kwetsbaarheidanalyse, niet direct leidt tot het kwantificeren van niet-financiële risico's, helpt het aandeelhouders en beleggers wel om beter onderscheid te kunnen maken tussen kwetsbare en minder kwetsbare ondernemingen. Het verdient dan ook de aanbeveling om bij het ontwikkelen van de optimale kwantificeringsaanpak voort te bouwen op de fundamenten van de kwalitatieve analyse en daarbij het doel, het verbeteren van de kwaliteit van de besluitvormingsinformatie, niet uit het oog te verliezen.

* Harold Malaihollo CIA, senior manager Deloitte ERS

Deloitte.

Een luisterend oor

Ben Tiggelaar • Dromen Durven Doen • Spectrum • ISBN 90 274 2672 4

R.J. Klamer

Hoe moet je een multimedia-uitgave eigenlijk recenseren? Even naslaan hoe het ook al weer gezegd werd, is nagenoeg onmogelijk. Even een aanhaling overnemen is wel mogelijk, maar terwijl je op zoek bent naar die ene quote hoor je al weer een heleboel andere mededelingen en ervaar je opnieuw dat gedetailleerd luisteren lastig is.

Toch wil ik mij er een keer aan wagen. Omdat ik denk dat het een nieuwe manier van kennisoverdracht is die iedereen een keer uitgeprobeerd moet hebben. Recent onderzoek in Amerika leert dat een gemiddelde manager 1,5 managementboek per vijf jaar (!) leest. Het moet ook wat sneller en eenvoudiger kunnen.
Nu wonen wij in een land waar te veel auto's of te weinig wegen zijn. Het gemiddeld verblijf in onze auto's wordt langer en langer. En natuurlijk is er altijd nieuws te beluisteren. Maar als je nu met simpel naar een cd te luisteren op een moment dat je toch niet zo heel veel te doen hebt de tijd zowel nuttig als aangenaam kunt vullen, dan is zo'n luisterboek eigenlijk niet zo'n gek idee. En kunnen we tegelijkertijd ook nog wat leren en ons gemiddeld aantal 'verwerkte' boeken wat verhogen.

Dromen Durven Doen is een monoloog van ongeveer drie uur, verdeeld over drie cd's. Er zit ook een dvd bij waarop Tiggelaar het gestelde in een videoboodschap in 25 minuten nog eens samenvat, maar die reken ik even niet mee. Tenslotte hebben nog niet veel mensen plasmaschermen in hun auto's. De drie uren lijken lang en zijn het ook. Gelukkig duurt zelfs een filerit gemiddeld niet langer dan een uur en kan het geheel in brokken worden beluisterd. Tiggelaar adviseert zelfs om wat tijd te nemen voor het verwerkingsproces.
Je krijgt nogal wat te horen. Dat 95 procent van ons handelen automatische gedragingen zijn, is voor een oppassend en nadenkend mens soms moeilijk te bevatten. Maar ook ik betrap me er regelmatig op dat ik wel thuisgekomen ben, maar geen idee heb wat er onderweg is gebeurd. En autorijden is inspannend…
Het betoog van Tiggelaar dat juist door die 95 procent automatismen onze veranderwensen mislukken, is dan ook zeer begrijpelijk en goed voor te stellen. Zijn oplossing is niet: houd vol en wees sterk, maar veel meer: denk na voordat je begint.
Bedenk wat echt belangrijk is en wat je echt leuk vindt, of waar je goed in bent. Overweeg van daaruit wat de keuzen zijn die je gaat maken en vooral wat de gevolgen van die keuzen zijn en meet en beloon vervolgens je veranderde gedrag.
Hoewel het allemaal een hoog 'nogal wiedes'-gehalte heeft, ben ik me er ook wel van bewust dat alles wat mensen en menselijk gedrag beschrijft vaak heel herkenbaar en alleen ogenschijnlijk eenvoudig te begrijpen is.

Door 'dromen' te benaderen vanuit het antwoord op de aan jezelf gerichte vragen: 'Kan ik mij een moment of situatie herinneren dat alles ging zoals ik het eigenlijk altijd zou willen?' en: 'Wat deed ik zelf toen het heel goed ging?', wordt het mogelijk om een vage veranderwens om te zetten in een concrete beschrijving van echt gewenst gedrag.
In de 'durven'-fase bedenk je vooraf wat je gaat doen met de crisismomenten die zeker zullen komen. Door ook hier concreet gedrag in te zetten, voorkom je terugval in en door het automatisme.
De situatie vervolgens gaan uitvoeren in de 'doen'-fase heeft een veel grotere slagingskans (70-80 procent) als je niet het resultaat meet, maar je concrete gedrag. Je ziet immers pas na enige tijd het resultaat van de sportschool. Het gedrag nu: gaan sporten, wordt sneller opgenomen in het automatische repertoire als je jezelf in het begin regelmatig beloont voor de gang naar de sportschool. Al is het maar door jezelf een complimentje te geven.

Meerdere malen in zijn betoog beschrijft Tiggelaar dat hij alles zelf ook meegemaakt, gedaan en geprobeerd heeft. Daarin faalde ook hijzelf regelmatig. Juist daardoor wordt hij geloofwaardig. Daardoor wordt hij die personal coach die veel vertelt, eigenlijk constant aan het woord is terwijl je (paradoxaal) steeds het gevoel hebt gehad dat er naar jou geluisterd is. Je ervaart al luisterend een luisterend oor.

Tiggelaar heeft een leerzaam boek gemaakt voor luisterende oren waar je vooral zelf mee aan het werk moet. Maar veranderen willen we allemaal en de kans op succes van die verandering vergroten is de investering van drie uur luisteren waard.

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

Voor **Mark Jongejan** is het nieuwe jaar begonnen met een nieuwe baan. Daarnaast werd hij bestuurslid van IIA Nederland. In De Overstap vertelt hij over zijn eerste ervaringen als manager Internal Audit bij Heineken Nederland.

Hoewel Mark eigenlijk nog niet bezig was met een overstap, heeft hij het er uiteindelijk toch op gewaagd. Door de krapte op de arbeidsmarkt worden auditors regelmatig benaderd voor een eventuele overstap. Mark had het nog prima naar zijn zin bij Connexxion. “De raad van bestuur en leden van het audit committee hebben mij veel ruimte en vertrouwen gegeven om de auditfunctie goed neer te zetten in de organisatie. Het werken aan een goede werkrelatie met de business vond ik plezierig en belangrijk. Daarnaast had ik het voorrecht om sturing te mogen geven aan een leuk en goed audit team.”
Ondanks het feit dat hij niet actief op zoek was naar een andere baan is Mark toch op gesprek gegaan voor de functie van manager Internal Audit bij Heineken Nederland en maakte hij uiteindelijk de overstap.

Kleine IAD

De overeenkomst tussen zijn oude en huidige functie is dat beide IAD’s qua bezetting relatief klein zijn. “Een efficiënte inzet van middelen krijgt daarmee extra de nadruk. Dit maakt dat het elke keer een creatief proces is om de audits te focussen op de belangrijkste, actuele risico’s. Een goede voorbereiding van de audit moet leiden tot een effectieve, maar met name ook efficiënte uitvoering van het veldwerk. Dit stelt overigens wel hoge eisen aan de individuele auditors, aangezien er op zo’n kleine afdeling geen verregaande hiërarchie aanwezig is.
Bij een kleine IAD (en dit geldt waarschijnlijk ook voor grote IAD’s) zijn prestaties niet zozeer aan één individu toe te wijzen. Een prestatie is per definitie een teamprestatie. Het werken in een klein team met professionals geeft mij veel voldoening. Dat vind ik ook het leuke van een kleine IAD. Continu met elkaar in gesprek zijn om uiteindelijk de klant een goed product aan te kunnen bieden.”

Ook in zijn functie als bestuurslid wil Mark zich sterk maken voor de kleine IAD’s. In Nederland is een behoorlijk aantal kleine IAD’s die in vergelijking met de grote auditdiensten hun eigen dynamiek hebben. “Deze kleine IAD’s verdienen grote aandacht vanuit het IIA!”
In zijn nieuwe functie bij Heineken Nederland geeft hij sturing aan een afdeling van zeven professionals die operational, financial en IT-audits uitvoeren. Daarnaast krijgt hij nog een ‘bijbaantje’ bij het Heineken Pensioenfonds en is de rol van vertrouwenspersoon in het kader van de Klokkenluiderregeling toegewezen aan de manager van de IAD.

Balans

De grootste uitdaging ziet Mark in het aanbrengen van balans in het werk van de IAD zodat in voldoende mate tegemoet kan worden gekomen aan de verwachtingen van de verschillende stakeholders. “De lokale internal auditfunctie heeft veel verschillende stakeholders met ieder zijn eigen wensen. Momenteel wordt door de lokale internal auditfunctie veel focus gelegd op de ondersteuning van de externe accountant. Dit is een aantal jaren geleden ook een bewuste keuze geweest. In mijn kennismakingsgesprekken met het management werd duidelijk dat daar meer balans in zou moeten worden aangebracht. De internal auditfunctie zal in toenemende mate moeten kijken naar risico’s die bedrijfsbrede doelstellingen bedreigen. De werkrelatie met de business zal tevens hoog op mijn agenda komen te staan. Ik verwacht dat ik daar de komende twee á drie jaar wel mee bezig zal zijn.”
Wat betreft de balans tussen werk en privé geeft Mark aan dat die voornamelijk is verbeterd als gevolg van een sterke daling van de reistijd. “Ik heb het thuisfront beloofd dit tijdvoordeel te besteden aan het gezin!”

> “Ik moet me in mijn werk kunnen uitleven, dat geeft mij energie”

Energie

Wat zijn eigen carrière betreft is Mark niet zo’n planner. Hij concentreert zich liever op het werk waar hij op dat moment verantwoordelijk voor is. “Ik vind het auditvak zeer interessant waar nog veel uit te halen valt. Ik zie mezelf voorlopig ook nog wel in dit vak functioneren. Op termijn is een overstap naar de financiële functie geen ondenkbare. Naast het feit dat ik niet zover vooruit kijk ben ik ook niet iemand die veel terugkijkt op zijn eigen successen. Ik moet me in mijn huidige werk kunnen uitleven, dat geeft mij energie. Zodra ik merk dat de energie afneemt wordt het tijd om actie te ondernemen.”

Jatten van de baas

Gijs Hiltermann en Eelco Hiltermann • Uitgeverij H&G • ISBN 97 89 07308103 1 • € 14,95

'Egels het kind van de rekening', kopte een krantenbericht in *De Telegraaf* in 2004. Wat bleek: de 57-jarige penningmeester van de Dierenbescherming, afdeling Gooiland, had 200.000 euro in eigen zak gestoken. Met vervalste jaarrekeningen en vervalste accountantsverklaringen kon hij jarenlang zijn gang gaan. Het begon pas op te vallen toen de rekeningen niet meer konden worden betaald.
De penningmeester bekende het geld van de Gooise dierenvrienden in een woning voor zichzelf te hebben gestopt. Ook kocht hij er een auto en een boot van. Met de affaire liep de opvang van zieke egeltjes in 't Gooi groot gevaar: vanwege hun financiële afhankelijkheid van de dierenbescherming werd de egelopvang in Bussum met sluiting bedreigd.
Dit boek gaat over werknemers die hun baas bestelen. Over de penningmeester die er met de kas vandoor gaat, over de boekhouder die de cijfers vervalst, over de directeur die geld van de organisatie in eigen zak steekt. Deskundigen noemen deze 'interne fraude' een groot en onderschat probleem. Nederlandse organisaties verliezen veel geld door jattend personeel; de schattingen lopen uiteen van een half miljard tot drie miljard euro per jaar.
Aan de hand van opmerkelijke, schokkende en hilarische voorbeelden uit de praktijk probeert dit boekje een antwoord te geven op de vraag waarom werknemers hun baas bestelen en wat organisaties kunnen doen om dat te voorkomen. Voor meer informatie en actualiteiten kunt u terecht op www.jattenvandebaas.nl.

Bestuurlijke informatieverzorging deel 2 B

R. W. Starreveld, O.C. van Leeuwen en H. B. de Mare • Wolters-Noordhoff • ISBN 97 8902073310 5 • € 55,95

Bestuurlijke Informatieverzorging deel 2B. Typologie van de bedrijfshuishoudingen maakt deel uit van hét standaardwerk op het gebied van bestuurlijke informatieverzorging voor controllers, bedrijfseconomen, bedrijfskundigen, bestuurskundigen, organisatieadviseurs, informatiemanagers, automatiseringsdeskundigen, systeemontwikkelaars en iedereen die daarvoor wordt opgeleid.
In dit ten opzichte van de vierde druk geheel herziene deel, wordt een tweetal typologieën op het gebied van bestuurlijke informatievoorziening behandeld. Het gaat om de typologie gebaseerd op doelgerichtheid (beheersbaarheid) van bestuurlijke informatie en de typologie gericht op betrouwbaarheid van informatie. De typologie op het gebied van beheersbaarheid van bestuurlijke informatie ofwel de toltypologie, is nieuw in deze uitgave van deel 2B.
Alle hoofdstukken zijn gemoderniseerd. Het hoofdstuk overheidsbedrijven is grondig herzien en uitgebreid met 'provincies en gemeenten' en 'organisaties op afstand'. De dienstverlenende bedrijven zijn uitgebreid met de typologie 'bedrijven die informatiegoederen of informatiediensten leveren'.

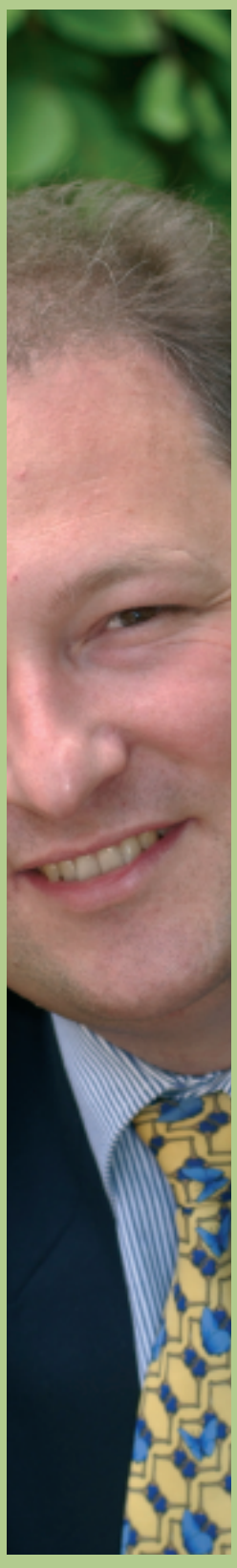
Good to Great (Nederlandstalig)

Jim Collins • Business Contact • ISBN 97 8902542510 4 • € 32,50

Dit boek wordt in bijna alle managementliteratuur aangehaald als de meest grondige, inzichtelijke en vernieuwende studie van de afgelopen decennia. Inmiddels geldt ook de Nederlandstalige editie als een klassieker.
Uit een langdurig onderzoek van honderden Fortune 500-bedrijven kwamen elf bedrijven naar voren die in een periode van vijftien jaar explosief groeiden: een tijdlang presteerden ze even 'good' als hun concurrenten in dezelfde branche, maar plotseling accelereerden ze en werden 'great'.
Wat onderscheidt deze succesvolle bedrijven nu van hun concurrenten en wat kunnen anderen daarvan leren? Collins heeft zijn inzichten in een aantal principes geformuleerd. Het zijn tijdloze factoren voor succes – geen hypes. Voor al deze bedrijven geldt:

1. Het leiderschap bevindt zich op niveau vijf (dienstbaar).
2. Ze werven de juiste mensen.
3. Ze zien de harde feiten onder ogen, maar blijven vertrouwen op succes.
4. Ze vinden een antwoord op drie afbakeningsvragen: wat kunt u het best, waar gelooft u het meest in en wat is cruciaal voor uw economisch voortbestaan?
5. Ze zorgen voor een gedisciplineerde organisatiecultuur.
6. Ze hechten groot belang aan technologie, maar zijn daarin selectief.
7. Ze werken gestaag en zijn volhardend, zonder revolutionaire doorbraken.

Continuous monitoring & auditing



Dr. J.R. van Kuijck*

Hoe zou de wereld er nu uitzien als de mensheid geen computer had uitgevonden in de vorige eeuw? We zullen het nooit weten. Toch is het nog geen zeventig jaar geleden dat een belangrijke technologische doorbraak werd gerealiseerd met de Electronic Numerical Integrator and Computer (ENIAC). De afgelopen decennia ontwikkelde de IT zich verder door de toename van opslag- en verwerkingscapaciteit van computers, de ontwikkeling van software en de toepassing van netwerken, waaronder het World Wide Web. Ook het auditen van geautomatiseerde systemen heeft zich in het kielzog hiervan ontwikkeld. Nog niet zo lang geleden spraken we van EDP-auditing in plaats van IT-auditing. Deze naamswijziging typeert de verbreding van de focus van audits van sec de Electronic Data Processing naar de relatie tussen bedrijfsprocessen en IT. In deze column sta ik stil bij het effect van de vooruitgang van de IT op de ontwikkeling van continuous monitoring en auditing.

Het concept van continuous monitoring is niet nieuw. IT maakte het mogelijk real time/online data te verzamelen en onmiddellijk te analyseren door middel van statistische methoden. In bijvoorbeeld de procesindustrie of bij milieuonderzoek zien we vele toepassingen. Ofschoon COSO al wees op het belang van continuous monitoring, is naar mijn idee de aandacht hiervoor wereldwijd pas echt toegenomen als gevolg van de Sarbanes-Oxley Act. In het verlengde van het continu monitoren ligt ook het continu auditen.
Continuous auditing wordt bijvoorbeeld door het AICPA omschreven als ‘the technologies and processes that allow an on-going review and analysis of business information on a real time basis’.
Begin jaren negentig van de vorige eeuw onderzocht Vasarhelyi – als een van de pioniers – of het mogelijk was om online technologie voor auditdoeleinden in te zetten. In de (wetenschappelijke) literatuur wordt geconcludeerd dat dit mogelijk is en worden allerlei concepten ontwikkeld om dit te faciliteren, zoals ‘process mining’ en de toepassing van allerlei statistische methoden.

Met continuous auditing is een nieuwe ontwikkeling gerealiseerd in het vakgebied auditing. Door gebruik te maken van in de systemen geïntegreerde geautomatiseerde tools kunnen processen continu worden geaudit. Dergelijke tools kosten relatief weinig menselijke auditcapaciteit en beperken zich grofweg tot de modellering van bedrijfsprocessen en de aanschaf van software. Misschien is nog wel het meest belangrijke voordeel van continuous auditing dat het mogelijk maakt dat het axiomatisch voorbehoud voor een deel niet meer hoeft te worden gemaakt. Laat ik dit uitleggen.
Het merendeel van de werkzaamheden van de auditor kenmerkt zich doordat zij worden uitgevoerd nadat de processen zijn afgewikkeld. En omdat de auditor uit kostenoverwegingen niet voortdurend aanwezig is, zal deze geen weet hebben van feiten en/of omstandigheden die zich hebben voorgedaan tijdens het proces. Denk bijvoorbeeld aan het niet werken van functiescheiding in een bepaalde periode. Continuous auditing zou in dergelijke gevallen meer zekerheid kunnen bieden dan het traditionele reviewen of testen van interne beheersmaatregelen.

Toch blijkt in de praktijk dat er nog maar weinig gebruik wordt gemaakt van continuous auditing. Wellicht is er sprake van koudwatervrees of bestaat er angst voor het idee dat de technologie een cultuur van ‘Big brother is watching you’ dichterbij brengt. Wat zouden mijn vrouw en kinderen ervan vinden als ik hun handel en wandel voortdurend zou volgen? Toch ben ik ervan overtuigd dat continuous auditing binnen nu en vijf jaar een prominentere plaats zal krijgen binnen de toolbox van auditors en de efficiëntie van audits zal verhogen. Het beroep zal blijvend veranderen, dankzij IT.

* Corporate director Internal Audit bij VION Food Group (vankuijck.bob@hetnet.nl).