AUDIT magazine

Magazine voor internal en operational auditors

nummer 5 december 2008

thema:

Continuous auditing

Continuous auditing en de (veranderde) rol van de IAD

Meer managementaandacht voor continuous assurance gewenst

Continuous control monitoring nader beschouwd

Instituut van Internal Auditors Nederland

SVRO Stichting Verenigde Operational Auditors

CCH® TeamMate
Audit Management System

CCH is helping build intelligent businesses.

With added and more varied responsibilities, the role of the auditor is expanding. Thankfully, so are our world-class product offerings.

Already the industry leader in audit management systems, CCH® TeamMate now offers expanded assets for your business, including AuditNet's global resources.

Access to AuditNet standard and premium content is FREE and simple for TeamMate users, who can supplement their audit planning by searching across thousands of audit steps and programs in TeamMate-compatible format.

What business challenge can we help you address?

Visit **www.CCHTeamMate.com** for more information or contact one of the following regional representatives for the Benelux:

Cuno de Witte +31 20 568 6392 cuno.de.witte@nl.pwc.com

Wim Mandemakers +31 20 568 7374 wim.mandemakers@nl.pwc.com

Carolien Kapel +31 20 568 5124 carolien.kapel@nl.pwc.com

CCH
a Wolters Kluwer business

STRATEGIC BUSINESS PARTNER

AuditNet®
The Global Resource for Auditors

Continuous auditing en de kredietcrisis

Continuous auditing, een onderwerp dat op de agenda van vele auditdiensten staat. Een onderwerp dat tegelijkertijd ook veel vragen oproept. Wat is het nu eigenlijk, is het hetzelfde als continuous monitoring en continuous assurance? Kunnen wij er als auditdienst wat mee en zo ja, hoe dan? Betekent dit dat we voortaan rapporteren in een 'realtime'-omgeving op basis van analyse van alle relevante gegevens uit een database in plaats van op basis van een beperkte steekproef? Is dit droom of werkelijkheid?
In dit nummer wordt vanuit verschillende invalshoeken op dit onderwerp ingegaan. Niet alleen komen diverse definities en tools aan de orde, maar ook de wijze van implementatie en uiteraard de rol van de auditor ten aanzien van dit onderwerp. Kortom, een onderwerp waar verschillende opvattingen over bestaan en waar binnen organisaties op verschillende manieren invulling aan wordt gegeven.

Een onderwerp dat mogelijk nog hoger op de agenda staat, is uiteraard de kredietcrisis. Welke rol vervulden de auditors in dit kader? Of, misschien beter gezegd, welke rol hadden de auditors moeten vervullen? Een andere veel gehoorde opmerking in het licht van de kredietcrisis: waar waren de auditors en waarom is het zo stil in auditland? Kan de conclusie worden getrokken dat zowel externe als interne auditors onvoldoende kennis hadden van de ingewikkelde financiële producten die onderwerp waren van de audits? Enkele columns in dit nummer gaan hierop in. Naast deze thema-artikelen treft u uiteraard nog vele andere artikelen over onderwerpen die ons als auditor in de dagelijkse praktijk bezighouden.

Karin Laker is na een aantal jaren inzet teruggetreden uit de redactie van *Audit Magazine*. Wij bedanken Karin voor haar inzet. Om de positie van Karin in te vullen roepen wij u op om u aan te melden als redactielid. Hebt u interesse? Stuur dan een mail aan Jansen.Ronald2@kpmg.nl.

2009 In een notendop
Inmiddels wordt alweer hard gewerkt aan het eerste nummer van 2009. De thema's van de vier nummers die in 2009 uitkomen zijn: (1) Sustainability, (2) Leiderschapstijlen, (3) Bijzondere audits en (4) Soft controls. Raakt u geïnspireerd door een van deze thema's en wilt u een artikel schrijven over een van deze of andere auditgerelateerde onderwerpen, neem dan contact op met de redactie van *Audit Magazine* en wij laten u weten wanneer uw kopij moet worden aangeleverd. Uw bijdragen zijn van harte welkom!

Wij wensen u veel leesplezier en al het beste voor het nieuwe jaar!

De redactie van *Audit Magazine*

INTERNAL AUDIT SOFTWARE

- ☑ Streamline the audit process
- ☑ Improve audit visibility
- ☑ Increase audit efficiency & productivity
- ☑ Leverage assessments by other GRC groups
- ■ **SAVE TIME, CONDUCT BETTER AUDITS**

INTERNAL AUDIT SOFTWARE • THINK PAISLEY

Internal audit software from Paisley includes features for risk assessment, planning, scheduling, workpapers, reporting, issue tracking, time and expenses, quality assurance and personnel records. It is part of a comprehensive governance, risk and compliance solution that also includes functionality for financial controls management, compliance, risk management and IT governance.

Join over 1,300 leading organizations that utilize software from Paisley to increase efficiencies, reduce costs and improve the overall quality of financial, IT and operational audits.

PAISLEY | *Software for Governance, Risk & Compliance*

PAISLEY *ENTERPRISE GRC*™ AND **GRC** ON **DEMAND**™ — Software for integrated audit, operational risk management, financial controls management, IT governance, and compliance. **Call 888-288-0283 or visit www.paisley.com**

inhoud

thema Continuous auditing

Continuous auditing en de (veranderde) rol van de IAD

Meer managementaandacht voor continuous assurance gewenst

Continuous control monitoring nader beschouwd

Verder in dit thema

"Ik ben zeer bedacht voor internal auditors die een eigen imperium proberen op te bouwen"

Soft controls relatief meetbaar

Cultuur en gedrag: onderbelichte IT-aspecten

rubrieken

COLOFON *Audit Magazine* wordt uitgebracht namens Het Instituut van Internal Auditors Nederland (IIA Nederland), tevens eigenaar van het magazine, en de Stichting Verenigde Operational Auditors (SVRO). De redactie nodigt lezers uit een bijdrage te leveren aan Audit Magazine. Bijdragen kunnen worden gemaild aan: Jansen.Ronald2@kpmg.nl **Redactieraad:** F. Steenwinkel (voorzitter), Th. Smit RA CIA, G.M. van Gameren RA RO **Redactie:** drs. R.H.J.W. Jansen RO (voorzitter), drs J.F. Breedveld, drs. R. Kamstra, drs. H.A. Mulders RA RC, drs. L.Z. Nagy RO EMIA, drs. R. de Ruiter RE RA RO CISA, drs. D.L. Stabel RE CIA **Nieuws van de Opleidingen:** drs J.F. Breedveld en drs. R. Kamstra **Verenigingsnieuws IIA Nederland:** drs. S. Bantwal Rao **IIA Nederland:** Postbus 5135, 1410 AC Naarden, tel.: 088-0037100, fax: 088-0037101, e-mail: iia@iia.nl, internet: www.iia.nl **SVRO:** Postbus 5135, 1410 AC Naarden, e-mail: iia@iia.nl, internet: www.iia.nl **Bureauredactie:** R. Harmelink, info@vm-uitgevers.nl **Uitgever:** drs. J.Y. Groenink, jeannette@vm-uitgevers.nl **Vormgeving:** M. Maarleveld **Druk:** Senefelder Misset, Doetinchem **Advertenties:** voor informatie over tarieven kunt u terecht bij Bureau IIA Nederland, tel.: 088-0037100, e-mail: iia@iia.nl. **Abonnementen:** IIA Nederland, Postbus 5135, 1410 AC Naarden, tel.: 088-0037100, fax: 088-0037101, e-mail: iia@iia.nl (zie ook de website: www.iia.nl). Abonnementen kosten € 85 per jaar, losse nummers € 25. Leden van IIA ontvangen Audit Magazine uit hoofde van hun lidmaatschap gratis. Abonnementen hebben telkens een looptijd van een jaar en gelden tot wederopzegging tenzij anders overeengekomen. Partijen kunnen ieder schriftelijk opzeggen tegen het einde van de abonnementsperiode, met inachtneming van een opzegtermijn van twee maanden. Audit Magazine verschijnt vijfmaal per jaar.

ISSN: 1570-856X
VM UITGEVERS

Continuous auditing en de (veranderde) rol van de IAD

Over continuous auditing wordt veel gezegd en geschreven. Maar wat is het nu eigenlijk? Hoe verhoudt het zich tot begrippen als continuous risk assessment en continuous monitoring? Wat is de rol van de internal auditor met betrekking tot continuous auditing? En de relatie met de externe accountant? Hoe kun je continuous auditing in de praktijk vorm geven? Deze en andere vragen komen in dit artikel aan de orde.

Drs B.F. van Meegeren RA RO CIA

Financiële en operationele transacties zijn de laatste jaren in aantal en complexiteit toegenomen. Wellicht keert de kredietcrisis het tij en nemen we afscheid van hedgefunds, CDO's (Collateralized Debt Obligations) en andere ondoorzichtige constructies. Toch blijven grote stromen transacties bestaan. Organisaties worstelen voortdurend om de minimaal vereiste beheersmaatregelen te treffen in een steeds meer gereguleerd ondernemingsklimaat. Het traditionele auditproces is ingericht om de zekerheid te verschaffen dat het geheel van deze beheersmaatregelen adequaat is ingericht en dat het, binnen een afgegrensd tijdvak, ook effectief werkt. Echter, dit auditproces vindt plaats nadat de transacties zijn afgerond en is slechts zelden in staat om alle transacties te beoordelen. Dat leidt tot een significant risico dat bij veel organisaties fouten en fraude voorkomen én niet tijdig opgemerkt worden. Het gevolg hiervan kan gepaard gaan met een zeer negatieve impact voor de organisatie. De praktijkvoorbeelden hiervan zijn al zo vaak beschreven dat een nadere toelichting overbodig is.

In het licht van al deze gebeurtenissen valt ook het onderwerp continuous auditing te plaatsen. De oorsprong van het begrip is technologisch van aard: voortdurende auditing door middel van gebruik van geautomatiseerde systemen. Continuous auditing kan als gevolg van het huidige niveau van geautomatiseerde toepassingen een welkome aanvulling zijn op de noodzakelijke verbeteringen op het gebied van beheersing van risico's. Al in 1999 voerde het American Institute for Certified Public Accountants (AICPA) samen met het Canadian Institute of Chartered Accountants (CICA) een onderzoek uit naar continuous auditing.[1] Eén van de vragen die resteerde na dit onderzoek luidde: 'how can the knowledge, expertise and work of internal auditors be used most effectively in setting up a continuous audit process?' Mede op grond van de uitkomsten van dit rapport staat continuous auditing in de Verenigde Staten sinds 1999 op de agenda van het IIA. Vanuit het IIA startte in de Verenigde Staten het onderzoek naar de relatie met de internal auditor. In 2005 leidde dit tot de publicatie van GTAG 3 over continuous auditing.[2] Ook in Nederland raakt het begrip meer en meer bekend, maar er bestaat ook nog steeds veel onduidelijkheid over. Wat is het nu precies en hoe kun je het in een organisatie invoeren?

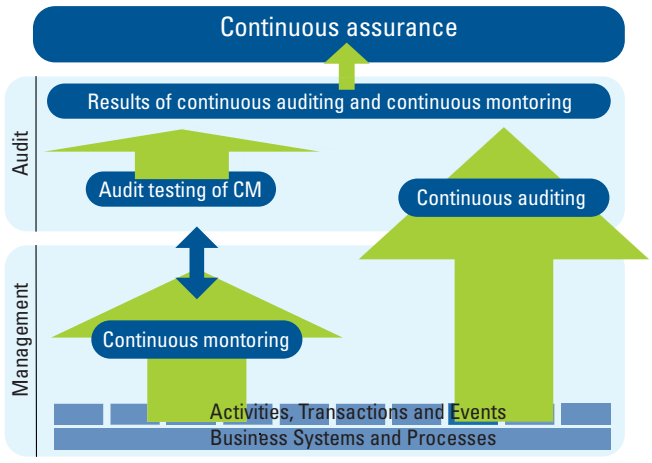
Wat is continuous auditing?

Er zijn verschillende definities van continuous auditing te vinden in de literatuur, vaak passend in het tijdsbeeld. Volgens de GTAG 3 is continuous auditing 'any method used by auditors to perform audit-related activities on a more continuous or continual basis'. Daarnaast is het onderdeel van een meer overkoepelend begrip: alles wat de internal auditor en het management doen, variërend van continuous monitoring en continuous auditing tot het continu beoordelen van risico's. Dit wordt continuous assurance genoemd (zie *figuur 1*).

In dit conceptuele model worden twee pilaren onderscheiden: continuous monitoring en continuous auditing. Het grote verschil

met continuous auditing is dat continuous monitoring een activiteit is die door het management (of door door het management aangewezen lijnfunctionarissen) wordt uitgevoerd. Continuous monitoring is een managementgedreven proces. Bij continuous monitoring worden computertechnieken gebruikt om op een continue basis uitzonderlijke situaties of problemen te identificeren. Continuous monitoring wordt dus door de eigenaar van de data uitgevoerd en is erop gericht om resultaten te rapporteren, data voor operationele beslissingen te analyseren en om specifieke acties te verrichten.
Continuous monitoring wordt vervolgens door de IAD getoetst, het management kan namelijk een belang hebben om resultaten gunstiger voor te stellen dan dat de werkelijkheid is. Dit heet 'audit testing of continuous monitoring'.
Als al deze continuousbegrippen tezamen in een onderneming goed worden toegepast, ontstaat continuous assurance.

Continuous risk assessment
Een nieuwe begrip dat elders in de GTAG 3 voorkomt maar (nog) niet expliciet in het conceptuele model, is continuous risk assessment. Dit sluit nauw aan op de visie die Pricewaterhouse-Coopers heeft beschreven in haar studierapport *Internal Audit in 2012**[3], een lezenswaardig stuk over de verandering die de IAD moet doormaken wil het 'overleven'. Het slechts assurance geven over control monitoring en eigen control assessments is hiervoor onvoldoende. Wil de IAD een goede plaats binnen de organisatie behouden door toegevoegde waarde te bieden aan haar stakeholders, dan zal ze zich tevens moeten gaan richten op het meer op continue basis evalueren en zelf uitvoeren van risk assessments. Het model kan uitgebreid worden met een derde pijler: op de managementlaag het enterprise risk management en op auditniveau het continuous risk assessment.
Door continu risico's te beoordelen en beheersmaatregelen te auditen kan de auditor zijn onafhankelijke oordeel over de interne beheersing aan zijn belangrijkste stakeholders rapporteren.



Figuur 1. Continuous assurance

Overigens lenen niet alle processen zich voor deze aanpak, het is een vereiste dat de auditor de onderliggende processen goed kent, inclusief de techniek. Er moet toegang zijn tot alle relevante data, die met behulp van de juiste softwaretools benaderd kunnen worden.

Continuous auditing is een welkome aanvulling op de noodzakelijke verbeteringen op het gebied van beheersing van risico's

De relatie tussen externe accountant en internal auditor
Bij het uitvoeren van zijn normale auditwerkzaamheden bepaalt de externe accountant onder meer in welke mate hij kan steunen op de werkzaamheden van de internal auditor. Hij stelt vast wat de invloed is van de internal auditor op de controleomgeving en op de controlemaatregelen.
Of de accountant inderdaad kan steunen op deze werkzaamheden hangt af van de mate van onafhankelijkheid van de internal auditafdeling, de scope van de IAD, de kennis en competenties en of de werkzaamheden zorgvuldig zijn uitgevoerd. In een onlangs verschenen artikel in *Internal Auditor*[4] staan de belangrijkste stappen genoemd voor de implementatie van continuous auditing:
- vaststellen van aandachtsgebieden die onderworpen worden aan continuous auditing (op basis van kritieke processen, beschikbaarheid van data, kosten/baten, snelle resultaten/demonstratie-project);
- vaststellen van de regels voor queries;
- bepalen van de frequentie;
- configuratie van parameters;
- follow-up;
- communiceren van resultaten.

In het kader van continuous auditing heeft de internal auditor een andere rol dan de externe accountant. De toegevoegde waarde van de internal auditor ligt in de kennis van de 'te auditen' organisatie, de processen, en vooral in de gehanteerde informatiesystemen. Enerzijds kan de internal auditor werkzaamheden verrichten waar de externe accountant op kan steunen met betrekking tot zijn werkzaamheden. Anderzijds kan de internal auditor een 'interne consultant'-rol krijgen. Vanuit de kennis van IT-systemen, risicobeheersingssystemen en performance-indicatoren kan de internal auditor adviezen geven aan het lijnmanagement over het inrichten en de werking van continuous monitoringsystemen. Hierbij is wel van belang om de consequenties voor de onafhankelijkheid van de IAD in acht te nemen.

Continuous auditing in de praktijk

Bij BinckBank is de IAD bezig met het implementeren van continuous monitoring en continuous auditing als onderdeel van het interne risicobeheersingssysteem. Er is een software tool aangeschaft om het control framework zoveel mogelijk te automatiseren. Alle processen zijn geïnventariseerd, inclusief de risico's en de bestaande beheersmaatregelen, ofwel de controls. Deze structuur, het procesrisicocontrol, is afgestemd met de proceseigenaren, het zijn tenslotte de controls van het lijnmanagement. De structuur ligt vast in de tool en per control wordt een controleschema aangemaakt. Dit schema bestaat uit een tweetal reviewmomenten.

BinckBank heeft ervoor gekozen om het lijnmanagement qua vastlegging in de tool geen actieve rol te geven. De eerste review wordt uitgevoerd door Interne Controle namens het lijnmanagement. Deze afdeling voert dus de eerder genoemde continuous monitoring uit. De tweede review is eenzelfde actie, namelijk door middel van zelfstandige waarneming beoordelen of een control goed heeft gewerkt, maar omvat tevens een beoordeling van de door Interne Controle uitgevoerde monitoringactiviteiten. Deze tweede review wordt uitgevoerd door de onafhankelijke IAD, ofwel audit testing of continuous monitoring (ook wel continuous control assessments genoemd).

Ook de controles die door de zogeheten 'second line of defence' worden verricht, kunnen opgenomen worden in het raamwerk. Zeker bij financiële instellingen zijn compliance, risicomanagement en IT-security belangrijke aandachtsgebieden. Door bijvoorbeeld compliance als 'proces' op te voeren in de tool met als (generiek) risico 'het niet voldoen aan wet- en regelgeving XYZ', kunnen als laatste stap de controles worden opgevoerd die compliance uitvoert bij het toetsen of de organisatie voldoet aan wet- en regelgeving. Ook hier vervult de IAD de functie van 'third line of defence' om vast te stellen dat deze werkzaamheden juist en volledig zijn uitgevoerd.

Bas van Meegeren is sinds 2007 manager IAD bij BinckBank nv in Amsterdam. Hiervoor werkte hij onder meer bij Kas Bank, Euronext en Van der Moolen.

Van continuous monitoring en control assessments…

Door deze opzet worden dus continuous monitoring en control assessments gecombineerd in een tool. Hiermee dekken we de linker pilaar uit *figuur 1* af. De frequentie van het reviewschema wordt afgestemd op het risico en het type control en daarnaast op de richtlijnen van de externe accountant. Een application control wordt bijvoorbeeld jaarlijks of na een nieuwe release getest. Het vaststellen van de aanwezigheid van beleidsdocumenten vindt ook jaarlijks plaats. Bij grote operationele risico's is een hogere frequentie gewenst.

Bij het uitvoeren van de reviewwerkzaamheden bestaat de mogelijkheid om het bewijs toe te voegen aan de beheersmaatregelen en dit vast te leggen in de tool. Dit geldt ook voor opmerkingen ten aanzien van de geldigheid van het bewijs. Bijvoorbeeld door een opmerking vast te leggen dat de deelwaarneming uitgebreid moet worden. De externe accountant heeft (read-only) toegang tot de tool en kan zich aldus een beeld vormen van de interne beheersing, inclusief het onafhankelijke oordeel van de IAD. Door middel van rapportages uit de tool worden het bestuur en de auditcommissie geïnformeerd over de resultaten van de reviewwerkzaamheden. Het oordeel van de business wordt dus altijd gestaafd door de IAD, wat tot uitdrukking komt in een kleurcode per control (van groen, geel, oranje tot rood). Bij groen zijn zowel de business als de IAD het eens over de effectiviteit van de control. Geel als een controle ineffectief is, maar er tevens een effectieve mitigerende controle aanwezig is. Oranje als de IAD het oordeel van Interne Controle bijstelt van effectief naar ineffectief. Bij rood zijn beide het eens over de ineffectiviteit van de control. In dit geval kan de IAD in de tool een zogeheten 'issue' aanmaken en deze toekennen aan de proceseigenaar. Bijvoorbeeld: 'uit reviewactiviteiten op control XYZ over de maand november 2008 is gebleken dat de controleactiviteit ABC niet heeft plaatsgevonden. De IAD adviseert om met ingang van december 2008 deze controle weer uit te voeren.'

Het onderdeel issue management wordt ook gebruikt om de aanbevelingen uit reguliere audits vast te leggen (IAD, externe accountant, toezichthouder). De issues worden inclusief een deadline toegekend aan de proceseigenaar. Zodra de issues zijn opgelost wordt de IAD geïnformeerd door de proceseigenaar en na de follow-up (het vaststellen dat het issue adequaat is opgelost), wordt het issue op gereed gezet en gearchiveerd in de tool. Dit raamwerk kan voor zowel de traditionele controls als voor de meer geautomatiseerde controls gebruikt worden. Beide zijn vertegenwoordigd in dit raamwerk.

…via continuous auditing…

De in dit artikel eerder beschreven vorm van continuous auditing richt zich echter ook op het geven van een oordeel over alle transacties en niet over slechts een deelwaarneming. Dit kan bij processen die zich hier voor lenen. Denk hierbij aan processen als berekening van rente, bewaarloon en provisie. Deze controls zijn ook opgenomen in de tool, maar worden uitgevoerd door gebruik te maken van een audit query tool. Hier komt continuous auditing terug zoals de meesten het kennen: het op frequente basis uitvoeren van controls op de volledige populatie, in dit voorbeeld de rente, bewaarloon en provisieboekingen. In de audit query tool hoeft deze query slechts eenmaal opgevoerd te worden, om vervolgens met de gewenste frequentie uitgevoerd te worden. Van cruciaal belang is dat deze query de juiste data benadert. Hiertoe is een grondige kennis van de onderliggende

databases nodig. Na het periodiek draaien van de query beoordeelt de auditor de uitkomsten. Vreemde uitkomsten worden nader onderzocht en afgestemd met het lijnmanagement. Waar mogelijk worden relaties gelegd met andere bronnen zodat verbandcontroles gelegd kunnen worden, bijvoorbeeld de afrekening van de clearing member die het aantal transacties registreert. Hiermee wordt een oordeel mogelijk over de volledigheid van het aantal transacties.

Er zijn echter ook verstoringen in het proces, in sommige gevallen is er sprake van een korting. Bijvoorbeeld: als gevolg van een 'member-get-member'-actie krijgt een klant een aantal transacties gratis. Deze controle op juistheid vindt vervolgens plaats door afstemming met de brondocumenten voor de opvoer van deze korting. Het voordeel voor de IAD is dat de werkzaamheden veel dieper kunnen ingaan op de processen en de aanwezige beheersmaatregelen en er efficiënter onregelmatigheden worden geïdentificeerd. Hiermee dekken we de rechter pilaar uit *figuur 1* af.

De IAD heeft nu een behoorlijk aantal controles in kaart gebracht (die uiteraard door het lijnmanagement zijn vastgesteld) die continu worden beoordeeld. De frequentie van 'continu' zou ver doorgevoerd kunnen worden, zelfs tot dagelijks. De keuze hiervoor is afhankelijk van het risico en zal per onderneming en proces verschillen. Bij BinckBank is de praktijk dat een maandelijkse toets door de IAD de hoogste frequentie is. Voor de review door de business kan deze frequentie in feite nog hoger liggen, bijvoorbeeld bij de dagelijkse reconciliatie. Ook hier is echter gekozen voor een maandelijkse review door de business, bijvoorbeeld vaststellen of de reconciliatie per maandeinde is uitgevoerd en of alle verschillen verklaard zijn en niet ouder zijn dan dertig dagen. Verder wordt van een drietal ad random geselecteerde dagen vastgesteld of de reconciliatie door het lijnmanagement correct is uitgevoerd.

…naar continuous assurance

Door het invoeren van dit controleraamwerk is de rol van de IAD gewijzigd. De reguliere onderzoeken waar processen eenmaal in een periode van drie jaar werden getoetst, vervallen grotendeels. Er is namelijk al een continu oordeel over de mate van beheersing per proces. De reguliere audits zijn veranderd in het beoordelen van de opzet van de beheersmaatregelen en of deze in voldoende mate de inherente risico's afdekken zonder dat de werking getoetst wordt, aangezien dit deel in het raamwerk wordt opgevoerd. De IAD kan zich hierdoor meer richten op de ontwikkelingen op het gebied van risico's in processen en kan daardoor sneller inspelen op de realiteit.

Binnen de software bestaat ook een module 'risk assessment'. Hierin kunnen proceseigenaren periodiek gevraagd worden om de risico's van hun proces op kans en waarschijnlijkheid in te schatten. Afhankelijk van de volwassenheid van de organisatie kan de IAD hierbij een faciliterende rol spelen. Zoals al eerder aangegeven ligt hier de toekomstige waarde van de IAD: enerzijds het continu assurance geven over de effectiviteit van de controls, anderzijds het continu betrokken zijn bij het identificeren en inschatten van de risico's die de organisatie loopt (let wel, het management is hiervoor verantwoordelijk). De IAD zal vervolgens toetsen hoe deze risico's beheerst worden. Door hierover op een tijdige basis te rapporteren aan het bestuur en de auditcommissie is het doel bereikt: continuous assurance.

Het conceptuele continuous assurancemodel kent verschillende continuousbegrippen met elk hun eigen toepassing in de internal auditpraktijk. Door middel van geautomatiseerde oplossingen en uiteraard medewerking van de business, is een succesvolle implementatie van een dergelijk raamwerk mogelijk. Als de IAD zich bewust is van de mogelijkheden die haar positie, kennis van de processen en de techniek biedt en van de toegevoegde waarde die zo voor de organisatie gecreëerd kan worden, ligt er een mooie toekomst voor continuous auditing.

Literatuur

1 *Continuous Auditing, Research Report*, CICA/AICPA, 1999.
2 'Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment', *Global Technology Audit Guide* (GTAG 3), IIA, 2005.
3 *Internal Audit 2012* 'A study examining the future of internal auditing and the potential decline of a controls-centric approach'*, PricewaterhouseCoopers, 2007.
4 'Moving towards continuous auditing', *Internal Auditor*, IIA, augustus 2008.

DE BESTE BANEN VOOR FINANCIALS

ROBERT HALF - JE CARRIÈRE LANG

WWW.ROBERTHALF.NL

Robert Half®

Meer managementaandacht voor continuous assurance gewenst

Organisaties en hun internal auditdiensten zijn actief op zoek naar innovatieve wegen om op adequate wijze de risico's en controlomgeving te managen. Leidinggevenden moeten hun stakeholders op continue basis kunnen informeren over het realiseren van hun doelstellingen. Continuous assurance is zo'n innovatie.

Dr. J.R. van Kuijck RA RC

De afgelopen twee decennia hebben de ontwikkelingen in de IT een significante invloed gehad op organisaties. Als gevolg hiervan is de bedrijfsomgeving sterk gewijzigd. Allereerst hebben de IT-ontwikkelingen geleid tot veranderingen in operationele systemen en de aansturing daarvan binnen organisaties. Er zijn mogelijkheden gecreëerd om accountinginformatie en andere data in digitale vorm te genereren. Tegenwoordig kunnen grote hoeveelheden transactie- en procesgegevens worden vastgelegd en vervolgens automatisch worden geanalyseerd. Deze informatie kan het management gebruiken om geïntegreerde bedrijfsprocessen te monitoren en meer direct bij te sturen. Sterker nog, het management is theoretisch in staat om bedrijfsprocessen continu te monitoren.

In tegenstelling tot het verleden hebben organisaties ook meer en meer tijdige data beschikbaar om informatie te verstrekken aan verschillende partijen binnen en buiten de organisatie. Elliot (1997)[1] stelt dat 'online reporting based on databases updated in real time will be less wedded to current protocols for periodicity, creating a parallel evolution towards continuous auditing. Continuous auditing may lead to continuous reporting that supplements and eventually replaces the annual audit report. To audit effectively in these environments, auditors will use electronic sensors, software agents and computerized audit programming models.' Kortom, organisaties zijn in staat om meer informatie te verstrekken als gevolg van de ontwikkelingen op IT-gebied.

Behoefte aan continuous assurance

Vanuit verschillende partijen in de ontwikkelde financiële markten is behoefte ontstaan aan meer diverse, frequente en betrouwbare (financiële) informatie. Naar aanleiding van de verschillende financiële schandalen de afgelopen decennia is de aandacht verschoven van zuiver financiële informatie naar informatie over risico- en beheerssystemen. Bovendien is er behoefte aan continue zekerheid (assurance) over periodieke financiële informatie en de werking van risicomanagement en internal controls. Dit betekent dat een jaarlijkse beoordeling van de internal controls niet langer voldoende is. Om in staat te zijn om continuous assurance te leveren aan partijen in de financiële markt zou het management de internal controls op een meer continue basis moeten monitoren.

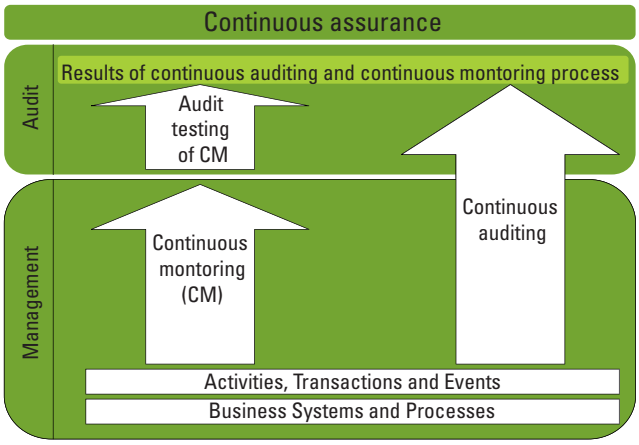
Bob van Kuijck geniet van een sabbatical. Tot 1 september 2008 was hij CAE bij de VION Food Group. Hij is verbonden aan de Vrije Universiteit Amsterdam voor onderzoek op het gebied van continuous assurance.

Hoe kan dit op een efficiënte manier worden georganiseerd? De Sarbanes-Oxley Act heeft de compliancelasten van veel organisaties vergroot. Recente ontwikkelingen laten zien dat de rationaliteit terugkomt en het management en auditors met oplossingen komen om deze corporate governancekosten te reduceren. De oplossingen zullen erop gericht zijn om beoordelingsmechanismen in te bakken in de processen zelf in plaats van een keer per jaar een 'on-top'-review te laten uitvoeren door externe auditors. In de praktijk zal worden gezocht naar een gezonde mix van continuous monitoring en continuous auditing; een oplossing die zal worden ondersteund door IT.

Hierna wordt het landschap geschetst waarin continuous monitoring, auditing en assurance een rol spelen.

Continuous monitoring en auditing

Continuous monitoring kan worden gedefinieerd als een proces waarbij Real Time/On Line-systemen (RT/OL) worden gebruikt om de performance van bedrijfsprocessen ook daadwerkelijk op een meer RT/OL-wijze te volgen. De monitoring ondersteunt het management om continu significante afwijkingen van verwachte uitkomsten te signaleren en voorts tijdig bij te sturen.
Continuous auditing wordt in GTAG 3[2] omschreven als een werkwijze gebruikt door auditors om auditgerelateerde activiteiten op een meer continue basis uit te voeren. Via continuous auditing verschuift het auditparadigma van een periodieke steekproefsgewijze test van transacties naar het continu testen van transacties.
In feite wordt de afstand tussen feitelijke transacties en audit kleiner of verdwijnt deze zelfs. Het onderscheid tussen audit en monitoring wordt minder eenduidig. De GTAG 3 laat zien dat de lijn tussen continuous monitoring en auditing erg dun is. Bovendien worden in dit rapport beide begrippen door elkaar gebruikt. Het belangrijkste verschil is dat continuous monitoring wordt verricht door het management en continuous auditing door auditors. Vanuit eigen invalshoeken trachten zowel het management als auditors zekerheid te krijgen over het bestaan en de werking van de bedrijfsprocessen in de organisatie.



Figuur 1. Het landschap van continuous monitoring, auditing and assurance (Bron: GTAG 3)

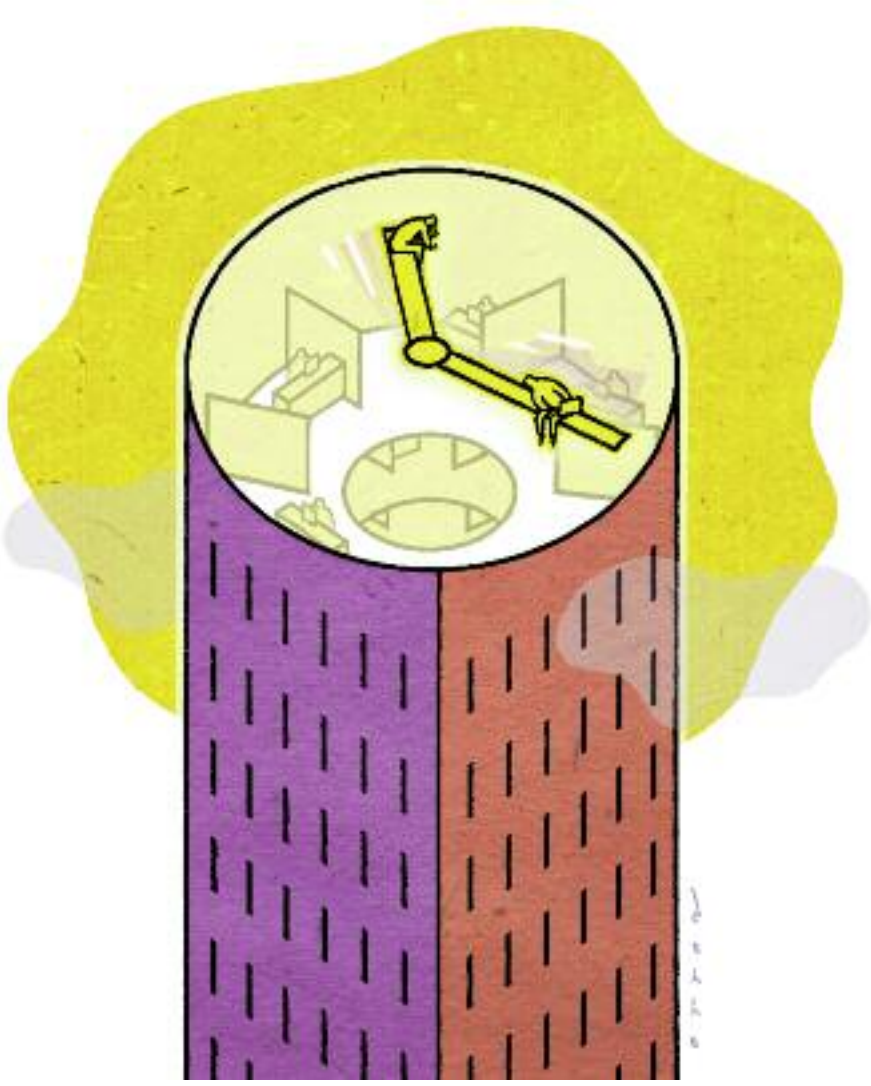
Het landschap

GTAG 3 geeft een helder conceptueel raamwerk dat de relatie beschrijft tussen continuous monitoring, auditing en assurance. *Figuur 1* geeft op een begrijpelijke wijze weer op welke verschillende manieren continuous assurance kan worden gerealiseerd. Continuous assurance moet natuurlijk worden gerealiseerd tegen zo laag mogelijke kosten. Om als auditor efficiënt te opereren tracht deze uiteraard te steunen op het bestaande systeem van beheersmaatregelen binnen de organisatie. Dit betekent dat de auditor de aanwezige continuous monitoring moet beoordelen en testen. Op terreinen waar niet of nauwelijks sprake is van continuous monitoring zal de internal/external auditor meer assurance verkrijgen door zelf – al dan niet continu – te auditen.
Continuous auditing zal de eindgebruikers van informatie meer tijdige zekerheid geven dat de door systemen verstrekte informatie correct is. Uiteindelijk stelt continuous assurance de organisatie in staat om naar aanleiding van gebeurtenissen meer accurate, meer frequente en snellere updates van (financiële) informatie te verstrekken.
De GTAG 3 geeft aan dat een gecombineerde strategie van continuous auditing en continuous monitoring ideaal is. Echter, in mijn visie is een dergelijke strategie juist een randvoorwaarde om continuous assurance op een efficiënte manier te realiseren. Om de auditinspanningen te optimaliseren zouden internal en external auditors moeten bouwen op de reeds aanwezige continuous monitoringactiviteiten van het management. Zo zal de organisatie continuous assurance op een optimale wijze realiseren. Dit betekent dat de strategie van de organisatie zich zou moeten richten op het zoveel als mogelijk inbedden van continuous auditingactiviteiten in de organisatie. Daarmee verwordt continuous auditing uiteindelijk tot continuous monitoring. Uiteraard is daarbij intensieve samenwerking vereist met de IT-organisatie en -infrastructuur. Deze organisatiefunctie moet ervoor zorgen dat de aanwezige kennis bij zowel internal als external auditors wordt vertaald naar IT-specifieke oplossingen om inbedding in de monitoringsystemen te realiseren.

Weinig progressie in het realiseren van continuous assurance

Tot dusver richtte dit artikel zich op de noodzaak en het belang van investeringen in continuous auditing en monitoring om continuous assurance te realiseren. Maar wat is de stand van zaken in de hedendaagse praktijk? Laten we de VS eens als voorbeeld nemen. Hier blijkt men niet echt bezig te zijn met het investeren in deze nieuwe omgeving. Een van de wortels van de problemen is de claimcultuur die de VS karakteriseert. Deze omgeving maakt organisaties minder enthousiast en bereidwillig om nieuwe rapporteringsformats alsmede onbeproefde werkwijzen te omarmen. Bovendien hebben veel organisaties zich de afgelopen jaren gefocust op de implementatie van de Sarbanes-Oxley Act. Hierdoor was er weinig aandacht voor de ontwikkeling van continuous monitoring en continuous auditing.
Los van de bovenstaande specifieke omstandigheden geldt voor veel organisaties wereldwijd dat dit thema ook niet hoog op de prioriteitenlijst van het management staat. Het is dan ook logisch

dat het management niet de rol van pionier speelt in het opstellen van een strategie voor – laat staan het implementeren van – continuous assurance. Toch is een actieve rol gewenst en kan het mede helpen om het in de kredietcrisis van 2008 verloren vertrouwen te herwinnen.
Naast het management zijn ook de external auditors verantwoordelijk voor de traagheid op dit terrein. In de praktijk lijken external auditors veelal geïnteresseerd te zijn in een toenemende interactie van IT met het auditproces. Daarmee worden hun controlebenaderingen meer efficiënt, wat ook goed is voor de cliënt. Ook softwarebedrijven als SAP, ACL, Caseware en Approva investeren in de ontwikkelingen van tools die continuous auditing mogelijk maken. Echter, accountantskantoren zijn urenfabrieken waar het resultaat wordt bepaald door de hoeveelheid gedeclareerde uren. Dit gegeven beperkt – uitzonderingen daargelaten – de motivatie om proactief mee te werken aan een minder arbeidsintensieve, meer technologiegedreven benadering om continuous assurance binnen de organisatie te verkrijgen. Ofschoon IT-auditors en -adviseurs onder de paraplu van audit firms een pioniersrol vervullen, hebben zij niet of nauwelijks invloed op de controlebenadering van de external auditor.



Illustratie: Roel Ottow

De rol van Internal Audit

Op grond van het voorgaande kan worden gesteld dat de kans niet groot is dat het management en accountantskantoren de rol van pionier zullen spelen om continuous assurance op een efficiënte manier te realiseren. Toch is er sprake van een ‘sense of urgency’ en zal het management uit de startblokken moeten komen. Met de komst van XBRL zal een organisatie niet alleen informatie moeten leveren, maar additioneel ook assurance. Dit alles moet op een efficiënte manier gebeuren. Het ligt voor de hand dat de oplossing vanuit de organisatie zelf komt. Daarbij zou de internal auditfunctie een voortrekkersrol kunnen spelen. Deze organisatiefunctie kan bij uitstek de organisatie helpen om zich geleidelijk aan te passen aan een nieuwe manier om assurance over bedrijfsprocessen te realiseren. De onafhankelijke positie van de internal auditfunctie zal externe partijen stimuleren om vertrouwen te hebben in de geleverde continuous assurance.
Internal auditors zouden een actieve rol moeten spelen in het inventariseren van de bestaande continuous monitoringsystemen en de bestaande continuous auditingbenadering van de external auditor. Daarnaast zouden zij continuous auditing zelf kunnen toepassen vanuit het oogpunt de opgedane kennis en ervaring door de IT-organisatie in te laten bedden in de monitoringsystemen. Op deze wijze kunnen – in lijn met de visie van COSO – auditinspanningen worden getransformeerd naar monitoringactiviteiten. Het stelt het management in staat om op termijn op continuous monitoring te steunen. Als gevolg hiervan zal het landschap van continuous assurance zich geleidelijk vormen en zal de organisatie in staat zijn om continuous assurance over de bedrijfssystemen en processen te geven. Bovendien zullen de kosten van corporate governance worden gereduceerd als gevolg van de manier waarop men zekerheid over de bedrijfsprocessen realiseert.

Randvoorwaarden

Om een adviserende en ondersteunende rol te kunnen spelen moet de organisatie enkele randvoorwaarden creëren. Zoals hiervoor besproken zullen de aard en timing van auditprocedures significant veranderen. Bovendien moeten de competenties en vaardigheden worden aangepast om aan te sluiten bij de vereisten van continuous auditing. De GTAG 3 noemt de volgende noodzakelijke randvoorwaarden om de rol van de internal auditfunctie tot een succes te maken:

- De Chief Audit Executive (CAE) moet de steun van het senior management en het audit committee hebben om continuous auditing te kunnen implementeren.
- De competenties van internal auditors moeten op niveau worden gebracht om continuous audits te kunnen uitvoeren.
- Investeringen in tools en technieken om data-analyses te kunnen uitvoeren die zullen worden gebruikt in het continuous auditproces.

- De CAE moet de toepassing van continuous monitoring door het management stimuleren en ondersteunen.
- De CAE moet de aanpassing in het nieuwe landschap beoordelen en het effect daarvan op de overall auditplanning vaststellen.
- De CAE ondersteunt het management door continuous auditing uit te voeren.

Echter, de GTAG 3 noemt niet expliciet een belangrijke speler in het totale corporate governancespectrum, namelijk de external auditor. Om optimale audit coverage te realiseren moet de Chief Audit Executive naast het senior management en het audit committee ook de externe accountant in het proces betrekken. Hiervoor zijn twee redenen te noemen. Ten eerste zorgt de betrokkenheid van de externe auditor ervoor dat optimale audit coverage wordt gerealiseerd. Het implementeren van continuous auditing – dat wellicht in de toekomst wordt getransformeerd in continuous monitoring – versterkt het systeem van beheersmaatregelen waarover de externe accountant zekerheid moet geven. Dit beïnvloedt de scope en diepte van het werk van de external auditor. Bouwen op een systeem van continuous monitoring reduceert zeker de auditinspanningen en, als gevolg daarvan, de kosten van de external auditor.
Ten tweede zal de betrokkenheid van de external auditor in het proces buitenstaanders meer comfort geven over het niveau van continuous assurance. Immers, zij steunen op de continuous assurance zoals verstrekt door de organisatie. Men zal zeker meer vertrouwen hebben in een benadering waarin een external auditor participeert. Samengevat: bij het realiseren van continuous assurance zal de organisatie de genoemde voordelen behalen door de external auditor erbij te betrekken. Bovendien zal het de positie van de internal auditfunctie verstevigen.

Conclusie

Het fenomeen van continuous assurance is niet nieuw. Ondanks de inzet van vele pioniers is continuous assurance in de praktijk van veel organisaties nog geen gemeengoed. Het management moet continuous auditing en continuous monitoring hoger op de prioriteitenlijst zetten. Dit is namelijk de sleutel om te voldoen aan de toenemende behoefte aan continuous assurance en om daarnaast de kosten van corporate governance te optimaliseren.
In dit artikel wordt gesteld dat het management een strategie moet ontwikkelen om continuous monitoring te intensiveren om uiteindelijk continuous assurance te realiseren. Daarbij is een prominente rol weggelegd voor de internal auditfunctie. De internal auditfunctie zou een meer actieve rol moeten spelen in het transformeren van hedendaagse auditpraktijken en het adopteren van nieuwe benaderingen. Internal auditors moeten daarbij hun verworven kennis bij continuous auditing overdragen aan de IT-organisatie, die belast is met de inbedding in de monitoringsystemen. Als gevolg hiervan zal het management continuous assurance over de bedrijfsprocessen op een meer effectieve en efficiënte manier kunnen realiseren. Door de onafhankelijke rol van Internal Audit neemt de acceptatiegraad van de wijze waarop organisaties continuous assurance verschaffen toe. Ik ben ervan overtuigd dat door een actieve rol van de internal auditfunctie het nieuwe landschap van continuous assurance geleidelijk zal ontstaan en de totale kosten van corporate governance worden gereduceerd.

Noten

1. 'Assurance service opportunities: implications for academia', *Accounting Horizons*, 11 (4), pp.61-74.
2. 'Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment' *Global Technology Audit Guide 3*, IIA, 2005.

Continuous control monitoring nader beschouwd

Met continuous control monitoring (CCM) kunnen organisaties zorgdragen voor een effectieve naleving van beleid, richtlijnen en procedures. CCM betreft het op continue basis toetsen van instellingen of transacties van een business proces aan vooraf gedefinieerde beslissingsregels. In dit artikel wordt ingegaan op de te onderkennen categorieën van CCM-tools. Vervolgens komen achtereenvolgens de randvoorwaarden en de voordelen van de inzet van CCM aan de orde. Tot slot worden de implementatie en de toekomst van CCM besproken.

Drs. A.Th.J. Buffing RE RA en drs. M.F. van der Meijden RE

De laatste jaren is CCM volop in de belangstelling komen te staan, mede door de hoge kosten van de invoering van de Sarbanes-Oxley-wetgeving (SOx) bij organisaties die onder het toezicht van de Security Exchange Commission vallen. Nu SOx alweer enige tijd is ingevoerd, staat het terugdringen van de jaarlijks terugkerende kosten van het testen van de controls voorop. Behalve dat organisaties nog eens kritisch zullen kijken naar de gedefinieerde controls en de hoeveelheid daarvan, zal ook de inzet van geautomatiseerde tools steeds meer uitkomst bieden. Door tools voor CCM in te zetten kan het testen van controls efficiënter verlopen.
Naast Internal Audit zijn meer afdelingen betrokken bij de invoering en het gebruik van CCM. Als 'bewaker' van het internal control framework is Internal Audit wel de afdeling die als een van de eerste zal worden gevraagd een visie hierop te hebben. Bij organisaties met een beperkt aantal informatiesystemen en organisaties die gebruikmaken van een integraal Enterprise Resource Planning informatiesysteem (ERP) is invoering van CCM relatief eenvoudig. Invoering van CCM kan in omgevingen met een grote diversiteit aan systemen echter een behoorlijke uitdaging vormen.

Categorieën van CCM-tools

Daar waar traditionele tools zich voornamelijk richten op controle achteraf, verschijnen er op de markt steeds meer tools die zich richten op het voorkomen c.q. eerder signaleren van onvolkomenheden. Deze CCM-tools zijn in verschillende categorieën in te delen:

- *Financiële transactie monitoring.* Deze tools zijn erop gericht om permanent alle transacties te kunnen bekijken en de transacties te identificeren die niet in lijn zijn met vooraf bepaalde kaders (normen). De focus ligt veelal op de beperking van het aantal fouten, fraude en operationele onvolkomenheden.
- *Beveiliging en IT-controls.* Deze tools worden vooral gebruikt voor IT-management. Hierbij kan gedacht worden aan monitoring van de door de geautomatiseerde systemen afgedwongen functiescheidingen, het detecteren van potentiële beveiligingsinbreuken en de 'three way match', waarbij gebruikgemaakt wordt van een verondersteld verband tussen de geaccepteerde order, goederenontvangst en inkoopfactuur. Ook monitoring van changemanagement en versiebeheer kunnen met deze categorie tools worden ingeregeld.
- *Audittools.* Deze tools zijn gericht op het inzichtelijk maken of het internal control framework adequaat heeft gefunctioneerd. Dergelijke tools worden gebruikt voor monitoring van transacties nadat die al door de organisatie verwerkt zijn. De monitoring wordt vaak op steekproefbasis uitgevoerd in plaats van dat het een integrale verificatie betreft.
- *Compliance managementtools.* Deze tools ondersteunen bij het managen van het auditproces en verzorgen tegelijkertijd de noodzakelijke documentatie.

Voor de eerste twee categorieën is sprake van een toenemende belangstelling, mede ingegeven door het integrale en het preventieve karakter van de hiermee uitgevoerde controles, dat wil zeggen dat signalering plaatsvindt voordat daadwerkelijk schade wordt geleden. Deze tools dragen ook bij aan de verbetering van de mogelijkheden van fraudedetectie en inperking van business-risico's.
De toepassingsgebieden van deze CCM-tools liggen veelal op het gebied van:

- het grootboek, waarbij bijvoorbeeld monitoring plaatsvindt op afwijkingen als dubbele journaalposten, ongeautoriseerde boekingen, tijdigheid van boekingen en gehanteerde wisselkoersen;
- het proces van verkooporder tot incasso, waarbij bijvoorbeeld monitoring plaatsvindt op gehanteerde prijzen, speciale kortingen en betalingscondities;
- het proces van inkooporder tot betaling, waarbij bijvoorbeeld vastgesteld wordt dat betalingen uitsluitend plaatsvinden op bankrekeningen die voorkomen in de stambestanden, waarvan natuurlijk eveneens is nagegaan of deze niet overeenkomen met bankrekeningnummers uit de salarisadministratie.

Randvoorwaarden

Het gebruikmaken van de mogelijkheden die CCM-tools bieden is geen vanzelfsprekendheid. De informatiesystemen en data waarop de CCM-tools worden toegepast dienen hiervoor aan een aantal eisen te voldoen. De belangrijkste randvoorwaarden met betrekking tot de toepassing van CCM-tools die gesteld worden aan de informatiesystemen en data betreffen een gewaarborgde data-integriteit, een afdoende audittrail, en accountability met betrekking tot de uitgevoerde handelingen binnen het informatiesysteem en de data.
Voor de toepassing van CCM-tools kan enerzijds gekozen worden voor het rechtstreeks toepassen van de tool op het informatiesysteem door de databasebestanden rechtstreeks toegankelijk te maken. Anderzijds kan toepassing van de CCM-tool plaatsvinden op geïsoleerde transactie- en mutatiebestanden. In beide gevallen geldt de voorwaarde dat de integriteit van de transactiebestanden en de mutatiebestanden met een redelijke mate van zekerheid dienen te zijn gewaarborgd. Hiertoe is een adequaat stelsel van controls in en rondom het informatiesysteem gericht op de integriteit van de gehanteerde data, een belangrijke vereiste. Daarnaast is een goed werkend stelsel van general IT-controls van groot belang. Zo is er behoefte aan goede en toegankelijke back-ups van de bestanden, dienen de toegangsrechten tot de betreffende data adequaat te worden beheerd, en dient de mogelijkheid om buiten het informatiesysteem om wijzigingen in de bestanden aan te brengen, afgeschermd te zijn.
Bij het gebruik van geïsoleerde transactie- en mutatiebestanden dient getoetst te worden of de bestanden nog integer zijn. Hiertoe worden veelal eerder gebruikte en bewaarde controletotalen zoals batch- en hashtotals ingezet.
Een audittrail is een functionele eis die gesteld wordt aan de aanleverende informatiesystemen. Bij elke uitgevoerde actie dient in het systeem te worden vastgelegd welke gebruiker wat en op welk moment heeft uitgevoerd. Steeds meer informatiesystemen bieden de mogelijkheid om aan deze voorwaarde te voldoen. Voor de historie van de mutaties op stamgegevens en de integriteit van de interfaces tussen de verschillende deelsystemen is dit echter nog vaak een punt van aandacht. Indien een volledige audittrail, van details naar totalen en andersom, beschikbaar is, dan is aan deze randvoorwaarde voldaan.
De toepassing van CCM is niet uitsluitend gericht op het detecteren van fouten, maar ook op het corrigeren en kunnen leren van deze fouten. Om het lerend effect te kunnen realiseren moeten de vastgelegde gebruikersgegevens correct zijn ingevoerd en correct blijven. Het dient derhalve onomstotelijk vast te staan dat de user-id die bij een actie in het systeem staat vermeld ook daadwerkelijk toebehoort aan de persoon die de actie heeft uitgevoerd. Kortom, de accountability van de gegevens dient niet ter discussie te staan. Ultieme voorwaarden hierbij zijn de aanwezigheid van IT-security-awareness binnen een organisatie en het gebruik van unieke en persoonsgebonden user-id's.

De voordelen van de inzet van CCM

De doelstellingen van CCM zijn niet wezenlijk anders dan die van interne controle. CCM ondersteunt het management ook bij de handhaving van interne policies, richtlijnen en procedures. Uiteindelijk is CCM gericht op:

1. het terugdringen van de interne controlerisico's binnen een organisatie;
2. de controle zo goedkoop mogelijk uit te voeren;
3. het vergroten van het vertrouwen in de (financiële) informatie binnen een organisatie;
4. de verbetering van (financiële) operaties door verlaging van de foutkans en de kans op fraude;
5. de verbetering van de winstgevendheid van een organisatie door betere sturing en het terugdringen van operationele fouten.

CCM biedt ook directe voordelen voor de toegevoegde waarde van de internal auditor. Zo kan met CCM een integrale beoordeling van alle mutaties op stambestanden of parameterbestanden en op transacties plaatsvinden. Hierbij zijn in het geval van afwijkingen meteen concrete voorbeelden voorhanden waardoor de (internal) auditor zich niet hoeft te beperken tot het niveau van potentiële risico's, maar direct de daadwerkelijke praktijkcases met het management kan bespreken. Enkele voorbeelden hiervan zijn:

- Een functionaris heeft ten onrechte een autorisatie voor het fiatteren van de betaling van een inkoopfactuur, maar er kan niet worden aangetoond dat deze persoon hier daadwerkelijk gebruik van heeft gemaakt. Met CCM kan relatief eenvoudig worden aangegeven welke facturen door de betreffende functionaris zijn gefiatteerd en welke bedragen hiermee gemoeid waren.
- Geconstateerd kan worden dat een funcionaris tien facturen heeft geaccordeerd binnen een halve minuut. Met deze wetenschap kunnen vraagtekens worden gezet bij de kwaliteit van de door hem verrichte controlewerkzaamheden.

Ook bij het testen van IT-general controls krijgt een internal auditor door CCM meer mogelijkheden. Voorbeelden van uit te voeren controles zijn:

- een relatie leggen tussen de user-id's zoals deze gedefinieerd zijn in een mailsysteem en de user-id's uit het financiële administratiesysteem om inzicht te verkijgen of persoonsgebonden user-id's worden gehanteerd en of het user managementproces effectief functioneert;
- een analyse maken van de relaties tussen de (software)sources van de programmatuur en de gecompileerde objecten om waardevolle informatie te krijgen over de werking van de software change managementprocedures.

Naast het uitvoeren van gerichte controles op de effectieve werking van controls kan de internal auditor CCM ook gebruiken om input voor positieve feedback te verkrijgen, bijvoorbeeld:

- vaststellen dat het moment waarop de periodeafsluiting is afgerond aanzienlijk is vervroegd ten opzichte van eerdere perioden;
- vaststellen of bij vreemde valutatransacties de gehanteerde koersen correct waren.

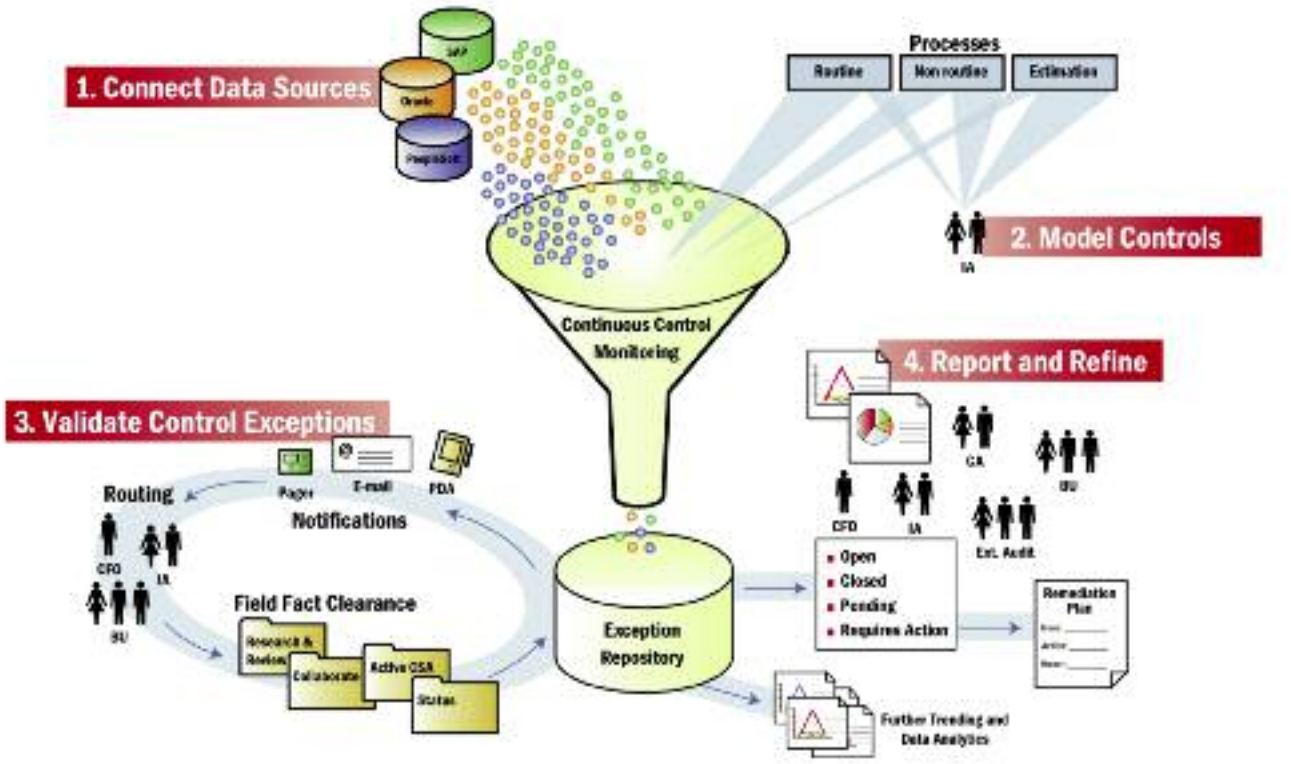
Kortom, juist het spreken over concrete gevallen maakt de communicatie een stuk plezieriger voor de betreffende auditor. Bevindingen kunnen niet meer worden afgedaan met de opmerking dat er weliswaar een risico is, maar dat deze gevallen zich toch niet zullen voordoen. De concrete voorbeelden kunnen gegeven worden, zowel in situaties waar het niet goed gaat als in situaties waar het wel goed gaat. Op deze manier toont de auditor aan dat de dagelijkse praktijk van de organisatie niet uit het oog wordt verloren en levert CCM een belangrijke bijdrage aan de toegevoegde waarde van de internal auditfunctie voor het management van een organisatie.

Implementatie van CCM

De wijze van implementatie van CCM is vergelijkbaar met de implementatie van een internal control framework. In beide gevallen is betrokkenheid en commitment van het management een zeer belangrijke voorwaarde. Ook is kennis van de business nodig en dienen de juiste risicoafwegingen te worden gemaakt. Tot slot dienen de reikwijdte en de frequentie van testen te worden bepaald.

De belangrijkste verschillen met een internal control framework zijn dat CCM ingrijpt op de activiteiten van vandaag en ook op de geplande activiteiten van morgen. Deze tijdigheid is dan ook meteen de grote meerwaarde van CCM. De interne beheersing wordt zo ingericht dat de organisatie er 'bovenop zit', opdat onregelmatigheden voorkomen worden. Overigens blijft CCM gericht op het monitoren van het functioneren van de controls en zal CCM nooit een vervanging zijn van de ingerichte business controls. De lijnorganisatie behoudt hiervoor te allen tijde de primaire verantwoordelijkheid en dient overeenkomstig daarmee de noodzakelijke maatregelen te nemen. Hierbij kan de lijnorganisatie overigens gebruikmaken van CCM-tools om haar business controls in te richten. Of deze controls hebben gewerkt wordt vervolgens door de internal auditor vastgesteld met zijn set van de in CCM opgenomen controls.

De implementatie van CCM heeft ten opzichte van het reguliere managementinformatiesysteem als belangrijkste voordeel dat voor data/informatie geput kan worden uit verschillende bronsys-



temen. Dit levert uiteraard meteen ook uitdagingen op voor de implementatie van CCM op het gebied van:
- data- en begripsdefinities (wat is de definitie van kosten, winst, opleidingskosten, et cetera);
- synchroniteit tussen de verschillende systemen, in termen van tijdsperiode, hoeveelheden, valuta's.
- de koppelgegevens (sleutels) tussen de verschillende systemen.

Het kan voor een organisatie verleidelijk zijn direct over te gaan tot het definitief inbouwen van alle noodzakelijke signaleringen in de bestaande bedrijfsprocessen. Dit gaat echter voorbij aan het gegeven dat de implementatie van CCM een zoekproces is naar een balans tussen de (data)mogelijkheden van de diverse systemen en hetgeen de organisatie wil bereiken om de interne controle te verbeteren. Hierbij dient rekening gehouden te worden met de daarmee samenhangende kosten. Dit alles vereist een iteratie in het implementatieproces en de gebruikte ontwikkelingsmethodiek waarbij tevens de volgende onderwerpen in het implementatieproces dienen te worden meegenomen:
- toegankelijkheid data, dat wil zeggen het kunnen benaderen, selecteren, verwerken van data uit verschillende systemen uit de gehele IT-organisatie;
- functionaliteit ter ondersteuning van tests, bijvoorbeeld voor sampling, sequence testing;
- aanpassingsmogelijkheden voor de uit te voeren tests (parameters, scripting, logging);
- capaciteit om omvangrijke datasets te kunnen verwerken zonder de dagelijkse IT-operaties te verstoren.

De relevante data zullen bij een organisatie veelal decentraal benaderd, geselecteerd en beschikbaar gesteld worden. De stappen verwerken, verrijken, controleren integriteit, uitvoeren analyses en rapporteren worden meestal centraal uitgevoerd of gecoördineerd.

Ton Buffing is directeur Advisory bij Ernst & Young. Zijn aandachtsgebieden zijn onder meer data-analyse, business intelligence en datawarehousing, zowel voor de (jaarrekening)controle als op het gebied van advisering.
✉ ton.Buffing@nl.ey.com

Martijn van der Meijden RE, is senior manager Advisory bij Ernst & Young. Zijn aandachtsgebieden zijn data-analyse en business intelligence. Voor diverse sectoren en cliënten voert hij zowel adviesopdrachten als opdrachten in het kader van de jaarrekeningcontrole uit.
✉ martijn.van.der.meijden@nl.ey.com

De implementatie van CCM kan als een succes worden beschouwd als daarmee het niveau van de interne controle verbeterd wordt terwijl de kosten van interne controle gereduceerd worden. Hierbij geldt dat het totaal van de kosten van de implementatie en het onderhoud van CCM moeten worden terugverdiend met de besparing op de kosten van de uitvoering en monitoring van de controls.

Toekomst van CCM

Gezien het iteratieve en exploratieve karakter kunnen met CCM belangrijke stappen gezet worden in de verdere verbetering van het internal control framework. Techniek, beschikbare tools en datasets vormen steeds minder een beperkende factor, terwijl tal van voorbeelden te geven zijn waar CCM aantoonbaar een goede bijdrage kan leveren.
De invoering van CCM is echter een strategische keuze waarbij de implementatie van CCM een proces is dat niet onderschat mag worden. Een realistische kijk op de aanwezige mogelijkheden om CCM toe te passen is vereist. Vervolgens dienen bij de toepassing van CCM belangrijke afwegingen gemaakt te worden over welke controles in welke perioden moeten worden uitgevoerd, alsook over keuzen over het tijdsframe waarbinnen gewerkt moet worden, aangezien niet alle informatie beschikbaar is op het moment dat beslissingen worden genomen.
Tot slot zal een succesvol CCM niet alleen op het verleden en het heden gericht moeten zijn, maar vooral ook op de toekomst. Met de beschikbare gegevens uit het verleden en het voortschrijdende inzicht uit het heden kunnen de effecten van genomen beslissingen immers nog beter worden geanalyseerd en aangewend worden voor de toekomst. ❑

Getting you there.

FORTIS

Fortis is een internationale financiële dienstverlener op het gebied van bankieren en verzekeren. Wij bieden onze particuliere, zakelijke en institutionele klanten een breed pakket van producten en diensten via de eigen kanalen, in samenwerking met het verzekeringsintermediair en via andere distributiepartners. Fortis behoort tot de twintig grootste financiële instellingen van Europa.

Fortis Audit Services geeft als corporate department "assurance" aan het management van Fortis omtrent beheersingsvraagstukken op het gebied van corporate governance, risk management en internal control. FAS voert integrated audits uit, die bestaan uit een combinatie van operational, ICT en financial audit werkzaamheden.

Ben jij de **senior auditor / assistant audit manager** die assurance kan geven aan top management van Fortis?

Je functie
Binnen FAS doe je in teamverband onderzoek naar de effectiviteit en efficiëntie van (financiële) bedrijfsprocessen, de kwaliteit van de informatieverstrekking en risicobeheersing binnen de organisatorische eenheden en je rapporteert hierover (regelmatig in het Engels). Daarnaast wordt van je verwacht auditors te begeleiden, op te leiden en aan te sturen. Je standplaats wordt Rotterdam, Utrecht of Amsterdam.

Wij bieden
Je vindt bij FAS een plezierige werkomgeving die hoge eisen stelt, maar waarin je kwaliteiten en initiatieven goed tot hun recht komen. Daarnaast bieden wij je een uitdagende omgeving waarin professionaliteit centraal staat. Bij Fortis zijn voldoende mogelijkheden om door te stromen. Dit ondersteunen wij door de vele opleidingen die we bieden. De arbeidsvoorwaarden worden vastgesteld op basis van de Fortis Bank CAO met een aantrekkelijke honorering en een uitstekend pakket aan secundaire en tertiaire arbeidsvoorwaarden.

Je profiel
HEAO RA/AC of BE of universitair bedrijfseconomie. Werkervaring bij een van de grote accountantskantoren, een audit afdeling van een financiële instelling of in een relevant aandachtsgebied bij een financiële instelling. Sterk analytisch vermogen, uitstekende communicatieve vaardigheden en een goede beheersing van het Engels. Bezig met het volgen van een opleiding RO, RE of RA, CIA, of bereidheid om een van deze opleidingen te (ver)volgen.

Interesse?
Roelie Haasbroek (030-226 3780) kan je meer informatie verstrekken. Een schriftelijke reactie kun je sturen aan Roelie Haasbroek, Fortis Audit Services (U01.07.15), Postbus 2049, 3500 GA, Utrecht.
E-mail: roelie.haasbroek@nl.fortis.com.

Dagelijks beheersen, efficiënt auditen!

De registratie van bedrijfsactiviteiten is van evident belang. Of het nu gaat om interne managementinformatie of externe rapportageverplichtingen, betrouwbaarheid van informatie is cruciaal. Er is een tendens dat in toenemende mate over die betrouwbaarheid gerapporteerd moet worden of dat deze moet worden aangetoond. Dit leidt tot hernieuwde aandacht voor interne beheersing. Continuous monitoring heeft hierbij, ondanks de soms overduidelijke efficiënctie- en effectiviteitvoordelen, helaas geen prominente plek gekregen.

Ing. M. Hill RE en drs. J. Joppe RA

Dit artikel gaat kort in op de voordelen van continuous monitoring (CM) voor de lijnorganisatie en de auditor. Daarna wordt een pragmatische aanpak voor de implementatie van CM behandeld. Door zich bewust te zijn van de benodigde stappen in een dergelijk traject kan de auditor bij de implementatie gericht adviseren over de totstandkoming van de CM-toepassing en de eisen waaraan deze vanuit auditperspectief dient te voldoen.

Dagelijkse grip op processen en verantwoording

CM behandelt vragen die dicht bij de uitvoering van het proces liggen. Hierbij kan gedacht worden aan zaken als: maak ik voldoende rendement op mijn contracten? Worden er geen ongeoorloofde kortingen gegeven? En: gaan er geen ongeautoriseerde betalingen de deur uit? Vragen die dicht aanzitten tegen de risico's die een auditor zou kunnen onderkennen. CM helpt de manager en de auditor deze vragen op terugkerende basis te beantwoorden. De verantwoordelijk manager is hierdoor beter in staat zijn processen aan te sturen door gegevens te analyseren op het niveau van transactiestromen.

De uitdaging voor de auditor ligt in het gebruik van de resultaten van de toepassing van CM

Tevens kan hij aantonen dat de processen in control zijn. Dit kan op twee manieren. Enerzijds door CM in te zetten als controlemaatregel, bijvoorbeeld door met behulp van data-analyse integraal aan te tonen dat alle kortingen onder de gestelde limiet liggen. Anderzijds kan CM gebruikt worden om aan te tonen dat bestaande controlemaatregelen effectief zijn. In beide gevallen ligt voor de auditor de uitdaging in het gebruik van de resultaten van de toepassing van CM.

Met de hernieuwde aandacht voor interne beheersing de afgelopen jaren is veelal teruggevallen op de vertrouwde controlemethoden en -technieken. Met arbeidsintensieve steekproeven (of liever gezegd deelwaarnemingen) wordt getracht de betrouwbaarheid van processen aan te tonen. Afhankelijk van de doelstellingen kan CM een goedkoper en vele malen effectievere oplossing zijn, zowel voor de auditor als voor de verantwoordelijke manager. Een ander belangrijk voordeel van CM-oplossingen is dat de analyses altijd goed controleerbaar en reproduceerbaar zijn. Dit is van evident belang op het moment dat analyses gebruikt worden door de auditor of voor externe rapportagedoeleinden.

Als laatste, we hebben het al genoemd, worden de transactiestromen gebruikt als basis voor CM. Deze transacties vormen tevens

de basis voor de financiële verantwoording. Aldus is er geen ruimte voor interpretatieverschillen, omdat vanuit een verantwoordingsperspectief en vanuit een perspectief van control effectiveness naar dezelfde basisgegevens wordt gekeken.

Een pragmatische aanpak voor de implementatie

De toepassing van CM biedt de auditor de mogelijkheid de audit efficiënter en effectiever in te richten. Om gebruik te kunnen maken van de resultaten van CM is het van belang dat de auditor reeds bij de implementatie van de CM-toepassing betrokken is. Zo kan worden bewaakt dat voldaan wordt aan de eisen waaraan de CM-toepassing vanuit auditperspectief moet voldoen. Hiertoe is het van belang dat de auditor begrijpt hoe de implementatie van een CM-toepassing verloopt.

Het implementatietraject van een CM-toepassing wordt gekenmerkt door het iteratieve karakter. In feite gaat het om het nemen van kleine stappen op weg naar de juiste oplossing, waarbij het van groot belang is een helder einddoel voor ogen te hebben. De volgende stappen moeten mimimaal onderkend worden in een CM-traject:

1. bepaal de visie op interne controle;
2. inventariseer de omgeving;
3. haal gegevens op;
4. analyseer transacties en transactiestromen;
5. rapporteer;
6. realiseer de CM-omgeving.

De eerste vijf stappen hebben betrekking op het realiseren van een ad-hocrapportage op basis van beschikbare gegevens. In stap zes wordt van de ad-hocrapportage een draaiende CM-omgeving gemaakt. De stappen worden hierna kort uitgewerkt.

Visie op en doelstelling van interne controle

Een van de ontbrekende elementen is veelal het concreet maken van de doelstellingen. Een visie op interne controle waarin de doelstelling expliciet is opgenomen, moet duidelijk maken wat de belangrijkste elementen zijn voor het interne controleraamwerk, met welke periodiciteit gedemonstreerd moet worden dat de controls werken en op welke wijze hierbij technologie ingezet kan worden. De visie moet bijdragen aan een beeld over de mate waarin gegevens uit bestaande processen en systemen moeten worden hergebruikt.

Inventariseer de omgeving

De omgeving is een belangrijk onderdeel van de uiteindelijke oplossing. Het gaat om het snappen welke processen belangrijk zijn, het snappen hoe die processen aan elkaar gelinkt zijn en het in kaart brengen van systemen die een rol spelen binnen deze processen. Op basis van deze informatie kan doelgericht gekeken worden naar de beschikbare data door in kaart te brengen in welke databases de transacties worden vastgelegd en hoe er wordt omgegaan met geaggregeerde informatie. Het resultaat van deze stap is een proces- en systeemschets. Op hoofdlijnen is het door deze stap mogelijk aan te duiden welke criteria worden gehanteerd om gegevens op te halen en uit welke tabellen deze gegevens afkomstig moeten zijn. Tevens moet helder worden over welke periode gegevens moeten worden opgehaald.

Prototype

In het traject richting een goed draaiende oplossing is het nuttig eerst een prototype te realiseren. Er zijn twee belangrijke voordelen van een dergelijke benadering: a) de mensen in de organisatie doorlopen een steile leercurve en zijn daarom steeds beter in staat om doelstellingen te formuleren omdat ze grip hebben op de transactiestromen en b) inzicht in de transactiestromen helpt enorm bij het verfijnen van resultaten. Overigens is het zaak om het prototype niet direct als definitieve CM-oplossing in te zetten. Immers, een robuuste oplossing vereist een bepaalde mate van beheersing van de oplossing zelf, iets dat bij een prototype veelal achterwege gelaten wordt.

Integrated control

Een actuele ontwikkeling in de markt is integrated control. CM kan goed geïmplementeerd worden in relatie tot integrated control. De combinatie met integrated control biedt voordelen omdat er in een integrated controltraject vanuit een risicoanalyse wordt gebouwd aan een controleraamwerk. Afhankelijk van de interne en externe eisen zal een aantal controlemaatregelen in het raamwerk periodiek beoordeeld moeten worden op effectiviteit. Een CM-oplossing kan hierbij een zeer efficiënte oplossing bieden.

Haal gegevens op

De voorgaande stap maakt het mogelijk om aan de IT-organisatie uit te leggen welke gegevens ontsloten moeten worden. Tevens biedt het mogelijkheden om via de proceseigenaar specifieke

Een praktijkvoorbeeld: regelgeving en CM bij de zorgverzekeraar

'Om de zorgverzekering uit te mogen voeren, moeten zorgverzekeraars een vergunning hebben van De Nederlandsche Bank (DNB) en zich voor de uitvoering van de Zorgverzekeringswet hebben aangemeld bij de Nederlandse Zorgautoriteit (NZa). De Nederlandse Mededingingsautoriteit (NMa), de NZa en DNB houden toezicht op de uitvoering van de Zorgverzekeringswet en de Algemene Wet Bijzondere Ziektekosten.'

Dit kleine stukje tekst is afkomstig van de website van Zorgverzekeraars Nederland. Een klein stukje tekst met grote gevolgen. Er zijn nogal wat regeltjes waaraan een zorgverzekeraar zich moet houden. Alle toezichthouders wensen een bepaald niveau van inzicht. Het integreren van de vraagstukken en zoveel mogelijk vanuit één model rapporteren schept ruimte voor CM.

In dit kader wordt bij een van de grote zorgverzekeraars gewerkt aan het implementeren van een CM-oplossing. Het doel is om op terugkerende basis te kunnen rapporteren over de effectiviteit van de maatregelen die genomen zijn om het proces conform regelgeving te laten verlopen. Hiervoor is allereerst een risicoanalyse uitgevoerd waarin de operationele risico's in kaart zijn gebracht. Vervolgens is beoordeeld welke maatregelen reeds genomen zijn en is voor zover nodig, gestart met het nemen van aanvullende maatregelen. Parallel is gestart met het bekijken op welke wijze het best over de effectiviteit van controlemaatregelen gerapporteerd zou kunnen worden en hoe de controlevragen het best beantwoord zouden kunnen worden. Een deel van de controlevragen is beantwoord door middel van data-analyse. Voorbeelden zijn 'het aantal huisartsendeclaraties voor dezelfde verzekerde op een dag', en 'het beoordelen of normen voor vergoedingen niet worden overschreden'. De analyseresultaten worden gerapporteerd als onderdeel van het totale controlevraagstuk en worden tevens gebruikt ten behoeve van mogelijke verbeteringen in processen. Uiteraard is de risico-analyse hierbij leidend: eerst de belangrijkste risico's! De data-analysescripts worden vervolgens geplaatst in een continu draaiende rapportagetool dat in dit geval maandelijks resultaten genereert.

verwerkingrapportages op te vragen. Doorgaans worden door middel van een aantal queries gegevens opgehaald uit de databases. Deze gegevens worden ingelezen in de te gebruiken data-analysetools waarna een controleaansluiting met de brongegevens noodzakelijk is. Denk aan een aansluiting tussen saldi per grootboekrekening in Exact en de ontvangen download uit Exact. Immers, in de loop van het traject worden conclusies verbonden aan de gegevens en de integriteit van die gegevens is dus van cruciaal belang.

Analyseer transacties en transactiestromen

Het is nuttig eerst een aantal basale analyses uit te voeren om de plausibiliteit van de ontvangen gegevens vast te stellen. Voorbeelden zijn een verdeling van alle producten naar omzet of een berekening van marge per klant. Het analysetraject is een iteratief proces, de focus ligt immers op het proces maar de kennis in organisaties is veelal versplinterd over afdelingen. Afhankelijk van de doelstelling is het zaak antwoorden op controlevragen op te leveren door de gewenste aansluitingen tussen systemen te realiseren of door de integriteit van transactiestromen te beoordelen. Voor ieder doel kan een specifiek aantal analyses worden gemaakt. Conclusies trekken op basis van analyseresultaten wordt beter naarmate er meer challenge op het niveau van processen plaatsvindt. Challenge vanuit de hoek van proceseigenaar en vanuit auditperspectief is een noodzakelijke en kwaliteitsverhogende factor. De data-analyse eindigt met het documenteren van de opzet en het bevriezen van de manier waarop het resultaat bereikt is. Veelal is dit het vastleggen van queries in scripts zodat de analyses periodiek gedraaid kunnen worden. De basis is nu gelegd voor het realiseren van een draaiende CM-omgeving.

Rapporteer

Afhankelijk van de aard van de opdracht kunnen in deze stap de afgestemde resultaten gerapporteerd worden, respectievelijk kan een plan gepresenteerd worden om op basis van de resultaten naar de draaiende CM-omgeving te komen.

Realiseer de CM-omgeving

Na de stappen 1 tot en met 5 is het realiseren van een draaiende CM-omgeving een stuk eenvoudiger geworden. De belangrijkste redenen hiervoor zijn: a) er is een draaiend prototype van de gewenste rapportages, b) er is in scripts en documentatie vastgelegd welke systemen, tabellen en velden nodig zijn en c) er is een uitgebreide challenge geweest om de bruikbaarheid van de rapportages te beoordelen. Het is nu zaak om de rapportages om te vormen naar dashboards per proces, om vervolgens de dashboards per proces op te hangen in een compliance cockpit en om de ontsluiting van gegevens op structurele basis te realiseren. Voor deze laatste stap kan veelal aangesloten worden bij bestaande business intelligence-oplossingen.

CM versus business intelligence?

De oplettende lezer zal zich afvragen wat het verschil is met business intelligencetoepassingen. Voorbeelden hiervan zijn toepassingen op basis van Business Objects of SAP Business Warehouse. Technisch en functioneel is er weinig verschil. Business intelligence (BI) wordt veelal toegepast vanuit bredere operationele doelstellingen. Zo kan een doelstelling zijn dat de logistieke processen beoordeeld worden om te zien of leveringen aan dezelfde cliënt mogelijk gebundeld kunnen worden om kosten te besparen. Dezelfde technische faciliteiten van een dergelijke toepassing kunnen ook gebruikt worden voor het realiseren van een CM-toepassing.

Het eerste verschil is dan ook de doelstelling. In tegenstelling tot BI gaat het bij CM om het aantonen van het in control zijn. In het kader van het beoordelen van controls rond logistieke processen zou dan bijvoorbeeld gemonitord kunnen worden of afleverkosten per order correct vastgesteld worden en vervolgens ook of deze daadwerkelijk in rekening worden gebracht en correct geboekt worden.

Marco Hill en Joris Joppe zijn als partner verbonden aan Coney. Coney koppelt vraagstukken rond interne beheersing aan innovatieve technologische oplossingen. Het doel is om interne controle efficiënt te laten verlopen.
✉ marco.hill@coney.nl en joris.joppe@coney.nl.

Een ander verschil is de toegevoegde waarde van BI-oplossingen. Dat is potentieel groter naarmate dit breder (en dus duurder) opgezet wordt. CM-oplossingen zijn over het algemeen juist eng gedefinieerd en gericht op het eenvoudig verkrijgen van data om te analyseren en te rapporteren. Om die reden is er dan ook een aantal tools specifiek geschikt voor het toepassen van CM. Met deze tools is data snel te benaderen en kunnen scripts eenvoudig worden gemaakt. Deze scripts kunnen vervolgens op elk moment op nieuwe data gedraaid worden omdat resultaten onafhankelijk van bronsystemen gedraaid kunnen worden. De ACL AX-suite is een voorbeeld van een dergelijke toepassing.

Proceseigenaar en auditor hand in hand

De doelstelling van CM is het identificeren en monitoren van interne controlemaatregelen die niet alleen overwegend financiële risico's afdekken, maar ook breder kunnen worden ingezet om andere typen risico's af te dekken. Het inzetten van CM om direct te 'kijken' in de systemen stelt de verantwoordelijk manager beter in staat zijn processen aan te sturen én om aan te tonen dat de processen in control zijn. Voor de auditor geldt dat de toepassing van CM door de organisatie de mogelijkheid biedt de audit efficiënter en effectiever in te richten. Daarbij geldt dat de uitgevoerde management controls goed controleerbaar en reproduceerbaar zijn en dat een directe link kan worden gelegd met de gegevens die gebruikt worden voor de financiële verantwoording. Als belangrijke randvoorwaarde geldt dat de auditor dient vast te stellen dat voldaan is/wordt aan de eisen die gesteld worden aan het implementatietraject.

Continuous auditing: de impact op assurance,

Onder de naam Global Technology Audit Guides (GTAG) brengt The Institute of Internal Auditors leidraden uit over auditonderwerpen die samenhangen met de automatisering van bedrijfsprocessen. Al in 2005 publiceerde IIA Inc. een derde leidraad met als titel 'Continuous Auditing: Implications for Assurance, Monitoring and Risk Assessment'. Naar aanleiding van het thema van dit nummer, Continuous auditing, heeft de redactie van *Audit Magazine* een aantal collega's om een reactie gevraagd. Twee ervan zijn in deze bijdrage verwerkt.

Continuous auditing als uitdaging

Drs. R. de Ruiter RE RA RO CISA

In de derde leidraad van het IIA is beschreven op welke wijze het concept continuous auditing (CA) kan worden geïmplementeerd in geautomatiseerde omgevingen. CA omvat alle methoden en technieken die door auditors worden gebruikt voor het uitvoeren van controlewerkzaamheden (inclusief beheersings- en risicobeoordeling) op transacties op een meer continue basis.

Randvoorwaarde

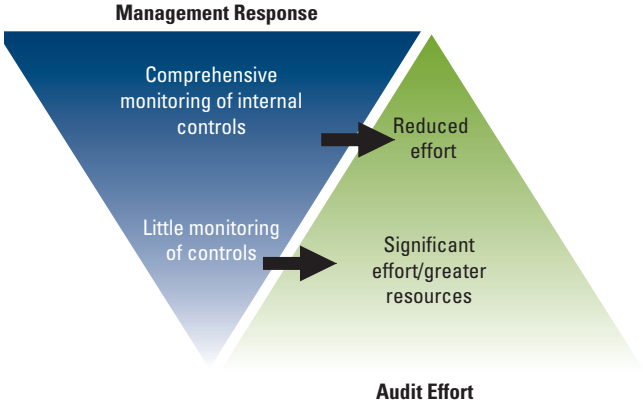
Door het volgen van het beschreven stappenplan maakt de internal auditor optimaal gebruik van de mogelijkheden die juist in geautomatiseerde omgevingen door IT worden geboden. Wel moet hiervoor aan een belangrijke randvoorwaarde zijn voldaan in de vorm van sponsorship door het management. Dit is niet alleen nodig omdat het toepassen van het CA-concept kan noodzaken tot het doen van aanvullende investeringen in IT, maar juist ook voor het verkrijgen van directe toegang tot de geautomatiseerde systemen met de daarin vastgelegde transactiegegevens. Het management is primair verantwoordelijk voor de blijvend goede werking van het interne beheersingssysteem. Idealiter richt zij voor het kunnen dragen van deze verantwoordelijkheid een proces in van continuous monitoring (CM), waarbij voor alle transacties wordt vastgesteld of deze voldoen aan de interne controledoelstellingen. Het management verkrijgt op deze wijze de zekerheid dat het interne beheersingssysteem goed functioneert en dat in het geval van afwijkingen escalatie kan worden voorkomen door in te grijpen.

Omgekeerd evenredige relatie

Tussen CM en CA bestaat een omgekeerd evenredige relatie. Wanneer het proces van CM door het management op een adequate wijze is ingericht en naar behoren functioneert dan hoeft het proces van CA niet met eenzelfde diepgang te worden uitgevoerd door internal audit. Volstaan kan worden met een review van het proces van monitoring en de behandeling van de gesignaleerde afwijkingen.

Indien het management zelf de bedrijfsprocessen nauwelijks monitort wordt de controle-inspanning van de internal auditor evenredig groter, zoals gevisualiseerd is in *figuur 1* uit de leidraad. Deze redenering past binnen de huidige opvattingen omtrent de taakverdeling tussen het management en Internal Audit en de daarop gebaseerde systeemgerichte controlebenaderingen.

Het toepassen van het CA-concept is geen gemakkelijke opgave. De leidraad spreekt over uitdagingen en over overige condities waaraan moet worden voldaan. Een voorbeeld hiervan is dat het bedrijfsproces in voldoende mate moet worden begrepen voor



Figuur 1. De controle-inspanning van de internal auditor

monitoring en risk assessment

het kunnen opstellen van de benodigde analyses en het identificeren van de risico's en kritische beheersingsmaatregelen.
Het CA-concept is een zeer krachtig instrument dat de procesbeheersing door het management positief beïnvloedt, wat op haar beurt een bijdrage kan leveren aan het verbeteren van het bedrijfsresultaat.

Stapsgewijze inwijding
Al met al is de leidraad een lezenswaardig document dat de geïnteresseerde stapsgewijs in het CA-onderwerp inwijdt om het in de eigen beroepsuitoefening toe te kunnen passen. De leidraad bevat ook nog een continuous auditing self assessment voor het vaststellen van de mate waarin Internal Audit CA heeft geïmplementeerd. De leidraad is echter ook interessant voor degenen die niet direct met het CA-concept aan de slag willen, maar die wel hun gedachten willen aanscherpen over controlemethoden en technieken in het algemeen.

Ronald de Ruiter is redactielid van *Audit Magazine* en auditmanager bij de Rijksauditdienst dat ressorteert onder het ministerie van Financiën.

Continuous auditing is onvermijdelijk

Drs. H. van Gils RE RA

In de jaren zeventig en tachtig van de vorige eeuw was het gebruik van auditsoftware populair, mede ingegeven door de toen nog gegevensgerichte controles. Veel indruk maakte toen een presentatie van een Canadese collega die voorspelde hoe accountant Kees in het toen nog ver wegliggende magische jaar 2000 de controle zou doen. Hij zocht met zijn auditcomputer verbinding met de computer van de klant (er was nog geen internet) en startte het auditprogramma op. Aangezien alle data en procedures en autorisaties in het systeem zouden zitten (er was nog geen ERP-software) kon het programma alle data analyseren en waar nodig nog geautomatiseerd wat analyses uitvoeren met de data van vorig jaar en externe bronnen (als de bank). Aan het eind van de ochtend was het programma klaar en rolde de conceptverklaring uit de printer. Met ambities in de accountancy en IT-auditing sprak me dit erg aan. Daarna is het snel bergafwaarts gegaan met auditsoftware. We moesten wachten tot na het millennium voordat er weer iets van het voorgaande aan de horizon begon te gloren.

Realisatie
In 2005 publiceerde de IIA de 'Global Technology Audit Guide nummer 3: Continuous Auditing'. Het concept continuous monitoring, met in het verlengde daarvan continuous auditing en uiteindelijk continuous assurance, spreekt aan. Zoals de guide terecht aangeeft is de realisatie sterk afhankelijk van technology ofwel van de moderne versie van auditsoftware. De grote uitdaging zal vooral bestaan uit het efficiënt gebruik van die software en met name de te hanteren normen (rulebooks) waartegen gemonitord wordt.
Op dit moment vinden diverse pilots plaats, maar veelal nog met een beperkte scope en tamelijk afstandelijk. Het periodiek downloaden van gegevens en vervolgens analyseren met software op basis van rulebooks is een goede stap op weg, maar nog niet echt continuous. Het wachten is op geïntegreerde software in de ERP-pakketten. Dan wordt het echt integrale monitoring by exception.

Snelle ontwikkelingen
Mijn verwachting is dat de ontwikkelingen op dit gebied snel zullen gaan. Langer zal het duren voordat de continuous risk assessments zullen plaatsvinden, al is de scope daarvan in de GTAG 3 (te) beperkt tot vooral trend en performance analyses, die nu ook al plaatsvinden in KPI's, et cetera.
De voorspelling voor de auditaanpak voor het jaar 2000 is nog lang niet gerealiseerd en een volledige continuous auditingimplementatie zal nog wel twintig jaar duren, maar dan kunnen (en moeten) de financiële verantwoordingen ook 'continuous' gecertificeerd zijn.

Herman van Gils is senior manager bij KPMG IT Advisory.

Independent research firm named BWise frontrunner in overall GRC capabilities.*

Let BWise make *you* the GRC frontrunner.

BWise
PROCESS OF SUCCESS

BWise biedt uw organisatie een software oplossing van wereld formaat voor Governance, Risk en Compliance (GRC) uitdagingen. Met GRC uitdagingen bedoelen we ondermeer het voldoen aan externe wet- en regelgeving, zoals Sarbanes-Oxley en Code Tabaksblat. Ook kunt u denken aan onderwerpen zoals het krijgen van grip op Internal Control, Risk management en IT Governance.

Door onze unieke procesgerichte aanpak, bereikt u met BWise niet alleen voordelen op het gebied van procesoptimalisatie, u bespaart ook aanzienlijk op compliancekosten.

Vraag het Forrester rapport gratis aan via **www.grcfrontrunner.com**.

**The Forrester Wave™: GRC Platforms, Q4 2007*

FORRESTER®

Focus op continuïteit

De huidige economische situatie heeft de behoefte aan risico- en controlmanagement bij ondernemingen sterk vergroot. Was de drijfveer eerst de aangescherpte corporate governanceregelgeving zoals SOx of de Code Tabaksblat, nu zijn dat de economische factoren. Op dit moment kan niemand zich de reputatieschade van een control failure veroorloven. De verhoogde aandacht voor risico- en controlmanagement vergt echter niet alleen veel van het management maar ook van de auditfunctie.

Dr. T. Willems en Sj. Vredenberg

Het verder automatiseren van de risicomanagement- en controlfunctie kan voordelen opleveren en de techniek biedt de mogelijkheden daartoe. Er is nog wel eens wat begripsverwarring maar continuous monitoring en auditing zijn eenduidig bepaald. Continuous monitoring biedt ondersteuning aan het management om haar verantwoordelijkheid te kunnen nemen bij het besturen van de organisatie. Continuous auditing is de geautomatiseerde uitvoering van control tests en assessments.

Continuous monitoring, auditsupport en continuous auditing

Continuous monitoring levert KPI's en alerts, gebaseerd op operationele gegevens. Naast het monitoren van financiële risico's levert de monitoring van de operationele, strategische en commerciële risico's een grote toegevoegde waarde op. Door de implementatie van een goed control framework voor elk van deze gebieden kan op basis van de alerts en KPI's continu worden bijgestuurd. Het management kan direct actie nemen, een control deficiency remediëren en een 'foute' transactie corrigeren. De efficiency en effectiviteit van businessprocessen en hun controls wordt zo vergroot.

De auditfunctie is ingericht om de monitoring- en controlfunctie van het management te evalueren en specifiek audits uit te voeren op die processen die al dan niet door continuous monitoring zijn afgedekt. Wel moet ervoor worden gezorgd dat de grens tussen monitoring en audit niet vervaagt.[1] Momenteel is auditsupport sterk in opkomst.

Auditsupport ondersteunt de assessments binnen de audit door middel van workflowautomatisering. Verantwoordelijke medewerkers krijgen geautomatiseerd via intranet of internet assessments voorgelegd waarbij ze worden ondersteund bij het interpreteren en invullen van de vragen en het opvoeren van relevante informatie en bewijsstukken (evidence). De verzamelde data worden deels automatisch geanalyseerd en in rapportages verwerkt. Hiermee wordt het auditproces aanzienlijk efficiënter.

Continuous auditing is de geautomatiseerde uitvoering van control tests en assessments. Door het automatisch uitvoeren van business rules op transactiedata (evidence) worden uitzonderingen automatisch geïdentificeerd en als alert aan het auditteam of het management beschikbaar gesteld. Ook hier geldt dat een transparant control framework de mogelijkheid biedt direct gericht actie te nemen.

De huidige economische situatie dwingt bedrijven om continuous monitoring vesneld te verkennen

Momenteel vindt auditing nog veelal handmatig en op geplande tijden plaats waarbij de vereiste documentatie zoals evidence maar ook control- en procedurebeschrijvingen, risicomatrices, et cetera, in verschillende systemen wordt vastgelegd.[2] Vaak zijn deze assessments inefficiënt en op zijn best 'achteraf'. Door de stapsgewijze invoering van continuous auditing, ingebed in een integraal control framework van control- en risicodocumentatie, assessments en procesbeschrijving, wordt dit proces efficiënter en effectiever.

Nieuwe Generatie GRC

De in de afgelopen jaren ontwikkelde governance-, risk management- & control-software (GRC) biedt alle bovengenoemde functies geïntegreerd in één applicatie:

- continuous monitoring; automatische alerts en KPI's;
- auditsupport; geautomatiseerde assessments en evidence collection (workflow driven);
- continuous auditingfuncties;
- control frameworkdocumentatie; proces, risk & control.

Om volledige transparantie te kunnen verkrijgen moeten deze functies in een control framework worden geïntegreerd met de proces-, control- en riskdocumentatie, de relevante wet- en regelgeving en de verschillende procedures en protocollen zoals gehanteerd in de organisatie.[3] Het mag duidelijk zijn dat deze informatie samenhangend moet worden onderhouden. Dit is een dermate complexe taak dat geïntegreerde GRC-automatisering onmisbaar is. Reeds beschikbare informatie moet kunnen worden geïntegreerd of opgenomen in de GRC-omgeving.

Voor continuous monitoring en auditing in de financiële kolom kunnen we leren van business continuity management (BCM) uit de IT-kolom. Het doel van BCM is ervoor te zorgen dat de continuïteit van de organisatie wordt gewaarborgd. Hiertoe worden disaster recovery plannen opgesteld die uitgevoerd worden op het moment van een incident. Om de incidenten te onderkennen worden de IT-systemen continu gemonitord. Business rules worden ingezet om de data automatisch te evalueren. Monitoringresultaten geven soms aanleiding om een alert via e-mail of sms uit te sturen naar de verantwoordelijke manager. Deze ziet dan direct welk plan moet worden uitgevoerd om het risico te mitigeren. Binnen BCM is veel ervaring opgedaan met continuous monitoring gekoppeld aan risico's, controls en actieplannen. Er worden gestructureerd testplannen uitgevoerd die binnen de financiële kolom audits genoemd zouden worden. Er is veel ervaring met door automatisering ondersteunde assessments en met continuous auditing van risico's en controls.

Toepassen?

Het succes van continuous monitoring en auditing hangt af van gefaseerde invoering, technische integratie met bedrijfsapplicaties en van het begrip van de control/auditfunctie in de organisatie. Is duidelijk welke controls er daadwerkelijk toe doen, welke gegevens relevant zijn bij het monitoren en welke gegevens moeten worden geaudit? Wat zijn relevante business rules om schendingen van controls te identificeren, wanneer willen we een alert en wat is de gewenste rapportage?[4] Veelal kennis die wel degelijk goed voorhanden is maar die efficiënt moet worden ingezet.

In de VS maakt ruim 30 procent van de midden- en grote bedrijven gebruik van continuous monitoring/auditing. De ervaringen laten zien dat op basis van een bestaand of nieuw op te zetten control framework eenvoudig een begin gemaakt kan worden met de invoering. Een relevant controlgebied wordt geselecteerd, voor dit gebied wordt bepaald wat vereiste monitoring- en auditinginformatie is. Deze gegevens worden door middel van agents opgehaald uit beschikbare bron- of middlewaresystemen. De data worden in de GRC-omgeving opgenomen, soms gestandaardiseerd op XBRL en door middel van business rules continu geanalyseerd. Afwijkingen op de data leiden tot alerts die aan het management of de auditor worden gemaild. Uiteraard moeten

ook de 'handmatige' audits en auditsupport worden aangepast/vereenvoudigd. Deze gefaseerde benadering is relatief eenvoudig in te voeren en leidt stap voor stap tot een transparant systeem.

Voorbeelden

Hierna volgen voorbeelden van business continuity management, transaction monitoring en corporate legal compliance (CLC).

Business continuity management

Een internationale verzekeraar heeft haar BCM-documentatie volledig op orde. Alle risico's zijn beschreven en worden elk kwartaal handmatig getoetst. De bijbehorende controls worden geaudit en er zijn plannen beschreven (DRP's) die moeten worden uitgevoerd op het moment dat zich een incident voordoet. Er zijn teams geformeerd en procedures zijn beschreven.

Het beheer van het control framework en het auditen (testen in BCM-termen) van de controls was echter erg tijdsintensief. Een voorbeeld: bij verhuizing van een teamlid naar een andere vestiging was het een heel karwei om de verandering in alle documenten door te voeren. Daarom is er gekozen voor het invoeren van een continuous monitoring en auditingsysteem voor business continuity managment (Bcon-PRO). Alle documentatie is ondergebracht in één IT-platform waardoor wijzigingen die op een plaats doorgevoerd zijn direct op alle andere relevante plaatsen geëffectueerd worden. De continuous monitoringfunctie verzamelt data van onderliggende systemen (IT en niet-IT) en door middel van een set van business rules wordt op basis van deze data de performance continu gemonitord. Naast dashboards leveren de business rules ook direct alerts als er een situatie ontstaat die mogelijk de continuïteit van de bedrijfsvoering in gevaar kan brengen. Op dat moment ontvangt de verantwoordelijk manager via de mail een alert met bijbehorende risico-, control- en actieplangegevens. Alle stappen van het actieplan worden door middel van workflow aan de verantwoordelijken aangeboden met de bijbehorende procedurebeschrijving. Het systeem bouwt een audittrail om later na te kunnen gaan welke stappen van het actieplan zijn uitgevoerd. Door de invoering van de continuous monitoringfunctie is de audit op het BCM-systeem aanzienlijk vereenvoudigd.

Gelukkig komen incidenten weinig voor. De risico's, plannen en controls worden regelmatig getest. Het systeem biedt op geplande tijden aan de verantwoordelijken assessmentvragen aan en voert automatisch tests uit op verschillende controls en plannen. Hiermee krijgt het IT-management continu zicht op de beheersing van de IT-organisatie.

Transaction monitoring

Een overheidsinstelling wilde voortdurend weten of ze met haar projecten, uitbestedingen en plannen op schema en binnen budget was. Uiteraard moest ze daarbij voldoen aan wet- en regelgeving. Er was al een financiële en projectadministratie die gebruik maakten van vier bedrijfsapplicaties. Na het opzetten van een control framework is een monitoringsysteem opgezet dat data haalt uit verschillende applicaties. Deze data worden automatisch geanalyseerd en leveren dashboards en alerts aan het verantwoordelijke management. Elke actie en transactie wordt gemonitord. Daarnaast is een systeem van gestructureerde assessments ingezet om de gegevens ook te auditen. De verantwoordelijke controllers krijgen regelmatig via het systeem het verzoek om informatie aan te leveren. Deze informatie wordt gebruikt om de projecten en financiën te auditen. Uiteraard is het een volledig transparant systeem. Dat houdt in dat per control kan worden gezien welke schendingen er zijn geweest, wat de audit van deze control in de afgelopen periode heeft opgeleverd en welk project op tijd en binnen de financiële ruimte loopt. Continuous monitoring dus, gecombineerd met een stevige auditfunctie.

We hebben in Nederland een voorsprong door de jarenlange ontwikkeling van AO en risicobeheersing, we kunnen die sterke positie nu doorzetten in het continuous auditgebied

Een internationale bank wil van alle aandelentransacties monitoren of de transactie voldoet aan haar interne controls. Hierbij moet voor iedere transactie worden gecheckt of de betreffende klant deze transactie kan uitvoeren, of de financiële positie van de klant de transactie toestaat en of de transactie voldoet aan de bankspecifieke regels. Er was reeds een transactiesupportsysteem. Nu worden tijdens het invoeren van een transactie door een continuous monitoringsysteem alle relevante klant- en transactiedata opgehaald en gebruikt om te toetsen of de nieuwe transactie binnen de door de bank gestelde controls valt. In het geval van

Er wordt binnenkort een onderzoek gestart om met een aantal auditors en controllers een generieke bibliotheek van business rules, alerts, KPI-dashboards en audits samen te stellen en te publiceren. Dit proces wordt ondersteund met GRC-software waardoor de deelnemers ook direct ervaring kunnen opdoen met continuous auditing en monitoring. Indien u interesse hebt om mee te werken aan het opstellen, toetsen en publiceren van deze business rules voor continuous monitoring & audit kunt u contact opnemen met de auteurs.

een controlschending krijgt de bankmedewerker direct informatie over het gesignaleerde probleem, de klant, de control, de relevante wet- en interne regelgeving.

Corporate legal compliance (CLC)

Voor de corporate lawyer/secretary speelt compliance rondom het beheer van alle vereiste corporate gegevens: de corporate housekeeping. Gegevens van aandeelhouders, aandelen, notifications (bijvoorbeeld de 403-verklaring), bestuurders, verslaglegging, KvK-gegevens, et cetera. Het beheer van deze informatie kan worden ondersteund door gestructureerde (digitale) vastlegging. Hierbij kunnen templates worden gebruikt voor specifieke jurisdicties zodat alle bedrijfsentiteiten de gegevens op de juiste wijze presenteren en bijvoorbeeld aan de KvK beschikbaar stellen. Daarnaast bestaat op het gebied van corporate housekeeping behoefte aan een risk & control framework en zichtbaarheid van procedures en werkwijzen om zo de kans op fouten te minimaliseren. Ten slotte is het wenselijk om op allerhande legal issues continu te monitoren. Voorbeelden hiervan zijn het tijdig beschikbaar hebben van consent statements voor consolidatie onder een 403-verklaring of het tijdig aanmelden of intrekken van bankautorisaties, aansprakelijkheden en andere notificaties. In samenwerking met advocatenkantoor Boekel de Neree is hiervoor een applicatie ontwikkeld. Onderzoek heeft laten zien dat ruim 60 procent van alle in Nederland gevestigde bedrijven met een 403-verklaring een of meer problemen heeft waardoor aansprakelijkheden vaak anders liggen dan bestuurders en aandeelhouders denken.

Continuous monitoring biedt hier, zeker voor grotere internationale organisaties, enorme voordelen en beperkt juridische en daarmee samenhangende reputatierisico's in hoge mate. Koppeling aan relevante wetgeving (standaard integratie met Lexis Nexis) leidt vervolgens ook tot directe beschikbaarheid van zogenoemde rules & regulations. Wijzigingen in wetgeving of jurisdictie kunnen zo eenvoudiger worden doorgevoerd voor up to date compliance.

Conclusie

Lessen uit het verleden leren dat losstaande analyseoplossingen die continuous monitoring wel goed uitvoeren maar niet integreren in het control framework, niet het beoogde resultaat opleveren. De in dit artikel beschreven voorbeelden kunnen alle binnen één organisatie passen. Het is juist daarom dat deze samen in één geïntegreerde omgeving geplaatst moeten worden. Een primair proces (bijvoorbeeld facturatie) heeft zowel een raakvlak met BCM – het systeem moet niet uitvallen; met compliance – de omzet moet op het juiste moment worden geboekt; en met corporate legal – er moet in het facturatieproces rekening worden gehouden met de privacywetgeving.

De inrichting vindt stapsgewijs plaats, bedrijven beginnen altijd met één discipline, bijvoorbeeld financial audit & monitoring. Elke stap moet wel passen in het eenmalig opgezet raamwerk. De huidige GRC-oplossingen kunnen hier goede ondersteuning bieden. Eenmaal ingericht kunnen ze door de organisatie worden gevuld. Daarbij moet erop worden toegezien dat de dataverwerking ten behoeve van monitoring geen belasting voor het operationele systeem (bijvoorbeeld ERP) vormt en dat de gekozen oplossing voldoende flexibel is om eenvoudig te worden aangepast aan de organisatie en bestaande informatie/systemen.

De huidige economische situatie samen met de reeds sterk toegenomen wet- en regelgeving, maakt dat continuous monitoring en continuous auditing een logische stap zijn. Het management wenst risicobeheersing en de auditfunctie moet worden ontlast. De beschikbare technologie maakt een goede, integrale benadering mogelijk waarbij risk & control framework, dashboarding en alerting, business rules en auditsupport hand in hand gaan. Hiermee zijn onmiddellijk efficiëncyvoordelen te halen. Hergebruik van bestaande informatie is uiteraard een randvoorwaarde.

Tim Willems is mede-oprichter van BWise en heeft in 2006 Ba-PRO opgericht. Ba-PRO levert integrale GRC-applicaties. Naast het ontwikkelen van softwareconcepten werkt Willems veel samen met mensen uit verschillende disciplines (legal, financial, audit, IT, social reporting) om een bijdrage te kunnen leveren aan de integratie van de verschillende GRC-gebieden.

Sjoerd Vredenberg is mede oprichter van Bcon-PRO. Bcon-PRO richt zich op het samenhangend inrichten van het business continuity managementproces. Daarbij wordt de BCM-applicatie van Ba-PRO ingezet. Vredenburg beschikt als voormalig directeur van CIAD over ruime ervaring op het gebied van risk management en hij heeft als interimmanager in verschillende omgevingen organisaties geholpen in-controlprocessen te verbeteren.

Literatuur

1. Krass, P., 'The Never-Ending Audit. Can software prevent future Enrons?', *CFO Magazine*, november, 2002.
2. Taub, S., 'Continuous Auditing Not Yet Automatic', *CFO.com*, juni, 2006.
3. Meyer, B., 'GRC: Governance, Risk and Compliance belong together', Audit Committee Institute KPMG Belgium, *Audit Committee Quarterly*, issue 10, 2008.
4. Coderre, D., *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, Guide 3 , The Institute of Internal Auditors.

In de rubriek ‘de estafettecolumn’ schrijft een auditprofessional op persoonlijke titel een stuk over een onderwerp dat hem of haar bezighoudt, irriteert of verbaast. Dit op uitnodiging van de columnist uit een vorig nummer van *Audit Magazine*, om daarna zelf het stokje weer door te geven. Dit keer **Hans Nieuwlands**, algemeen directeur van IIA Nederland.

De nieuwe kleren van de Keizer

Tijdens mijn eerste honderd dagen als werknemer van het IIA werd het nieuws vooral beheerst door de kredietcrisis, die zo zoetjes aan een bodemloze put lijkt te worden. Ik vraag mij dan ook af in hoeverre internal auditors, risicomanagers, corporate governancecodes, Sarbanes Oxley en COSO-ERM effectief zijn. Naar mijn mening communiceren internal auditors en risk managers onvoldoende over de echte risico’s naar de top van de organisatie. Misschien begrijpen we het zelf niet meer, maar durven we dat niet te zeggen. Het doet me denken aan het spookje *De nieuwe kleren van de keizer* van Hans Christian Andersen. Dat ging zo.

Er was eens een keizer die zo veel van mooie nieuwe kleren hield, dat hij al zijn geld eraan uitgaf. Hij was zo druk met het uitzoeken, passen en tonen van zijn kleding dat hij aan regeren niet meer toe kwam. Op een dag kwamen er twee bedriegers naar het paleis die beweerden dat ze de allermooiste stoffen konden weven voor de keizer. De stoffen hadden de wonderbaarlijke eigenschap dat ze onzichtbaar waren voor iedereen die niet voor zijn werk deugde of onvergeeflijk dom was. Dit sprak de keizer aan omdat hij zo eenvoudig te weten kon komen wie onbekwaam of oliedom was.
Hij moest de wevers fors betalen, maar het doel heiligt de middelen. De wevers gingen direct aan de slag op lege weefgetouwen. De keizer was erg benieuwd naar de voortgang, maar durfde zelf niet te gaan kijken omdat hij bang was als onbekwaam te worden ontmaskerd. Daarom stuurde hij zijn eerste minister. Uiteraard zag deze helemaal geen stoffen, maar de wevers beschreven hem het materiaal en de patronen. Met deze kennis ging de minister terug naar de keizer. Deze kon niet wachten om zijn nieuwe kleren aan de bevolking te laten zien.
De keizer organiseerde een optocht door de stad om zijn nieuwe kleren te tonen. Tot zijn schrik kon hijzelf de kleding niet zien, maar alle ministers bevestigden dat het bijzonder fraai was. Gesterkt door deze woorden begon de keizer vol zelfvertrouwen aan de wandeltocht. De bevolking wist inmiddels van de bijzondere eigenschappen van het weefsel en iedereen beaamde dan ook de pracht van de kleding. Plotseling riep een klein meisje: ‘maar de keizer heeft helemaal geen kleren aan!’ De rest van het volk begon dit nu ook te roepen. De keizer voltooide zijn wandeltocht terug naar zijn paleis. De wevers waren inmiddels met de noorderzon vertrokken.

Tot zover dit sprookje. Durven wij als auditors of risk managers toe te geven dat de risico’s inmiddels zo complex zijn geworden dat niemand ze meer kan begrijpen? En durven we dit dan ook te zeggen tegen de raad van bestuur en de auditcommissie? En kunnen we dat ook eens in begrijpelijke taal doen, zoals het meisje in het sprookje?

Graag draag ik het stokje over aan Peter Hartog van ACS.

Hans en Daniela Nieuwlands wachten op de uitreiking van de Victor Z. Brink Award. Een Award die wordt uitgereikt ter erkenning van bijzondere bijdragen van individuen aan het Institute of Internal Auditors.

Interview met commissaris Gilles Izeboud:

“Ik ben zeer beducht voor internal auditors die een eigen imperium proberen op te bouwen”

Gilles Izeboud is commissaris bij tal van bedrijven, waaronder Corporate Express, ENDEX en Robeco Groep. Zijn naam is onlosmakelijk verbonden met de commissie-Izeboud (voorheen commissie-Peters), die adviseerde over de beloningsnormen voor corporatiedirecteuren. Bovendien was Izeboud als lid van de commissie-Tabaksblat mede-auteur van een eigentijdse code voor goed ondernemingsbestuur. Een gesprek met deze deskundige bij uitstek over de verschuivende rol en positie van de internal auditor.

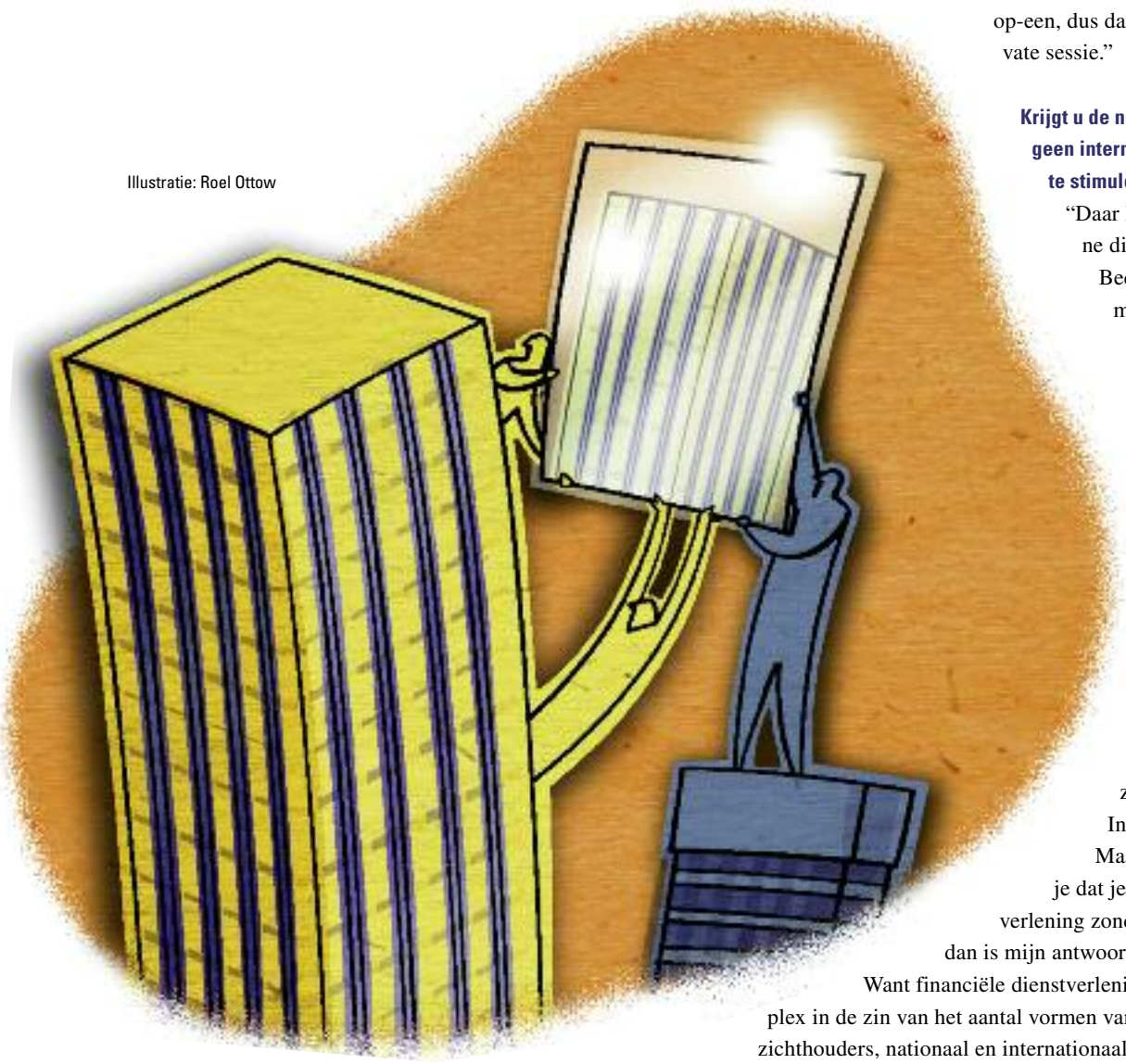
Interview: drs. D.L. Stabel RE CIA en C. Klumper RA CIA
Tekst: A. Gras

Kenmerkend van Gilles Izeboud als het gaat om de benadering van het thema, is dat hij er geen doekjes om windt. Als in de aanloop naar het gesprek de complexe structuur ter sprake komt waarin de internal auditor zijn werk doet en de openingsvraag is of het de afgelopen periode niet veel lastiger is geworden voor de internal auditor, dan liegt zijn reactie er niet om. “Als mij die vraag gesteld wordt dan geef ik daar steevast een tweeledig antwoord op. Ten eerste, door wat er nu allemaal speelt is het beroep inderdaad relevanter en interessanter geworden, maar niet lastiger. En ten tweede, als je dat wél vindt dan zit je in het verkeerde métier.”
De vraag wordt daarom aangepast.

Er vanuit gaande dat we te maken hebben met de juiste man, wat is dan zijn juiste plaats?
Izeboud: “In de gevallen waar ik mee te maken heb – dat zijn er twee – zit de internal auditor rechtstreeks onder de CEO. De chief internal audit woont alle vergaderingen van de auditcommissie uit de raad van commissarissen bij, standaard en volledig, behalve natuurlijk de private sessies met de external auditors of met de CEO/CFO. En er zijn dus ook private sessies met de internal auditors waarbij vragen gesteld kunnen worden en dingen gezegd.”

Zijn het dan standaard geplande private sessies met de internal auditors?
“Private sessies vinden minimaal een keer per jaar plaats, maar vaker als daar redenen voor zijn. Met de external auditors doe ik het altijd zo – dat vind ik wel prettig – dat elke vergadering van de auditcommissie begint met een private sessie. Als je daarin iets hoort, heb je die vergadering van de auditcommissie als manier om er iets mee te doen. Private sessies zijn niet voor de lol. Er kunnen zakelijke dingen aan de orde komen waarop zakelijk actie moet worden ondernomen en dan kun je dat maar beter direct doen.

Drs. Gilles Izeboud RA CPA
- Voormalig partner en lid van de raad van bestuur van Coopers & Lybrand.
- Voormalig lid van de commissie-Tabaksblat.
- Commissaris en voorzitter van de auditcommissie bij Corporate Express, ENDEX (Energy Derivates Exchange) en Robeco Groep.
- Commissaris bij Robeco, Rolinco en Rorento.



Illustratie: Roel Ottow

Met internal auditors is het eenmaal per jaar. De dingen die we moeten doen hebben we in de agenda staan om te bewaken dat ze ook gebeuren. Het komt echter wel voor dat er in de vergaderingen van de auditcommissie zoveel onderwerpen aan de orde komen dat je sommige agendapunten niet haalt. Dan kiezen we er wel eens voor dat de voorzitter apart praat met degene die een onderwerp heeft aangedragen." Glimlachend: "Dat is dan een-op-een, dus dat is dan wel een zeer private sessie."

Krijgt u de neiging organisaties die geen internal auditafdeling hebben te stimuleren er een op te zetten?

"Daar kan ik moeilijk algemene dingen over zeggen. Bedrijven zijn op die manier onderling niet vergelijkbaar. De ene organisatie opereert lokaal, de andere wereldwijd. Het is dus niet zo dat zodra je een bepaalde grens overschrijdt van complexiteit of omvang, je automatisch naar een Internal Audit moet. Ik heb ondernemingen goed zien functioneren, ook in control, zonder dat ze een Internal Audit hadden. Maar als je me vraagt, denk je dat je in de financiële dienstverlening zonder Internal Audit kan, dan is mijn antwoord: vermoedelijk niet. Want financiële dienstverlening is ontzettend complex in de zin van het aantal vormen van regelgeving en toezichthouders, nationaal en internationaal, de diverse mogelijkheden van middelpuntvliedende krachten – dan moet je dus zeker een gedifferentieerde entiteit hebben, of je die nu Internal Audit of financial control noemt, of wat dan ook.

Er is ook een andere kant. Ik ben zeer bedacht voor internal auditors die te veel silo-gedachten hebben en die te veel van die imperiummakers zijn, zo van: Internal Audit moet dit en Internal Audit moet dat. Ik heb internal auditafdelingen gezien van zeer grote ondernemingen waarvan ik het idee had dat ze totaal verkeerd bezig waren omdat ze te veel cyclische audits deden. Elk jaar weer, langer of korter, volgens een standaardmodel, een jaar later een samenvatting van die dingen voor de raad van commissarissen – geen hond die het las! Als je in zo'n situatie zit, zou ik zeggen: schaf de hele boel maar af. Maak een centrum van financiële talenten dat dicht onder de CEO zit. Laat die rondkijken en dingen rapporteren aan

Als je me vraagt of ik denk dat je in de sfeer van de financiële dienstverlening zonder internal audit kan, dan is mijn antwoord: vermoedelijk niet

de CEO zodat de stijl wat verandert. Dat heeft dan meer relevantie."

In wezen betreft het organiseren van de internal auditfunctie dus het vinden van de juiste balans?

"Een van de mooiste voorbeelden van hoe het zou moeten werken heb ik meer dan twintig jaar geleden gezien bij Monsanto. Daar had je een Internal Audit die voor een kwart bestond uit beroeps internal auditors en voor driekwart uit andere personeelsleden, tijdelijk in het kader van hun management developmenttraject. Daardoor bereikte je twee dingen, a. de Internal Audit verkokerde niet, hield zich niet met zelfbevrediging bezig, en b. de auditappreciatie bij de rest van het management nam toe. Allebei elementen om het goed te doen. Of het nu Internal Audit heet of iets anders, of je certificaten hebt of dat je drie, vier titels achter je naam zet – van het imperium opbouwen word ik altijd een beetje kriegel. Essentieel is dat je toegevoegde waarde hebt in controlesituaties. Idealiter, afhankelijk van de situatie, denk ik dat er een bepaalde balans moet zijn tussen cyclische en adhocaudits, in de zin van kortetermijnverzoeken van het management of anderszins naar iets speciaals."

Wat vindt u van de verschuiving tussen operational en financial audit?

"Als financial audit niet meer aanwezig is, dan is het niet goed. Er moeten financial audit skills binnen Internal Audit zijn omdat je de taal van de financiële rapportage moet kunnen verstaan, anders loop je het risico om te veel in de silo te komen. Door SOx zie je de weg terug. Een beweging van operational naar financial audit. En terecht! Het gaat ook om de balans tussen operational en financial audit. Ik ben bang voor al die te veel gemoduleerde, te veel apart optredende clubs. Je hebt een veel sterkere compliance-afdeling dan tien jaar geleden. Je hebt een aparte operation risk managementclub – ook in verband met Basel II – je hebt een financiële administratie en de controle die daar bij past en je hebt een internal auditteam. Als die gezelschappen niet op de een of andere manier samenwerken of dingen afstemmen of soms dingen samen doen, dan krijg je een gedrocht van een organisatie. Maar alsjeblieft geen aparte lijnen zoals in de medische wereld waar specialisten god zijn in hun eigen koninkrijk, want dan loop je grote risico's als de patiënt meerdere problemen heeft, de een geeft je dit, de ander iets dat daar averechts op werkt... Daar word je niet beter van."

Wat is de rol van de commissaris in het sturen van de internal auditfunctie?

"Ik hoor altijd hetzelfde verhaal, dat de auditcommissie de baas van de internal auditors moet zijn omdat ze in de hele organisatie zitten. Onzin! In de situaties waar ik mee te maken heb zijn auditcommissies en voorzitters daarvan niet de baas van de internal auditors. Het feit dat de internal auditor bij de auditcommissie zit betekent natuurlijk toch dat de auditcommissie meebepaalt hoe hij werkt en wat er met hem gebeurt. Kwartaalverslagen van internal audits die toegepast zijn, resultaten daarvan, het jaarplan, de risicogebieden waarnaar gekeken wordt, soms suggesties die opkomen naar aanleiding van ad hoc internal audits – het is allemaal in de auditcommissie aan de orde. Overigens zit wat mij betreft de CEO ook altijd bij de auditcommissie, tenzij er conflicterende dingen zijn."

Hoe kan voorkomen worden dat onduidelijkheid ontstaat over het opdrachtgeverschap van de internal auditfunctie?

"Er is eenheid van leiding in de organisatie nodig en dat betekent dat internal auditors geen twee bazen moeten hebben. Dus je moet ook als commissaris je plaats weten. Maar de manier waarop je dan functioneert hoeft niet te betekenen dat je als auditcommissie geen invloed hebt. Ik vind dat je de zaken niet altijd te principieel of te orthodox moet benaderen. Als je bijvoorbeeld in de vergadering van de auditcommissie constateert dat een aantal dingen niet zo lekker gelopen is – in een acquisitie bijvoorbeeld – dan moet daar iets aan gebeuren. Een van de potentiële instrumenten die je hebt is de internal auditor erop af sturen. Een ander voorbeeld. Je weet van een meerjarig IT-project waarvan je in de loop der jaren al hebt gezien dat het meer kost en potentieel minder oplevert dan geraamd. Laat dan de internal auditor ernaar kijken: hoe zit dat in elkaar? Welke vragen er ook zijn ten aanzien van een bepaald project, ik vind het niet verkeerd om de internal auditor te vragen om daar iemand bij te zetten die via een bepaalde monitoring scant: is dat in control, wat is de governance van dat project, hoe is het ingebed, wat gebeurt er met de producten die er uitkomen, et cetera."

> **Het feit dat de internal auditor bij de auditcommissie zit betekent natuurlijk toch dat de auditcommissie meebepaalt hoe hij werkt en wat er met hem gebeurt**

Kunnen internal auditors ook nog wat leren van de manier van werken van de auditcommissie?

"Zeker, een goed element van de praktijk van de auditcommissie is dat 'we' daar allemaal *samen* om tafel zitten en dat je gewoon praat over de problemen en wat daar aan te doen is. Dat maakt dat een deel van die oude gebiedenstrijd verdwijnt. Niemand aan tafel, ook de internal auditor niet, kan het zich nog permitteren om te weigeren om samen te werken. Ontsnappen kan niet meer."

Soft controls relatief meetbaar

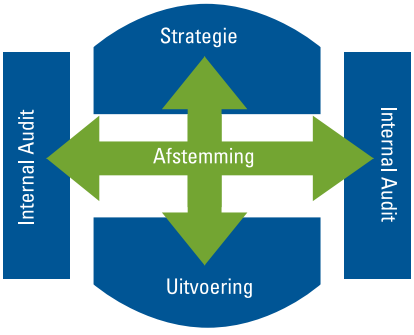
Risicomanagement is niet meer uit de bedrijfsvoering weg te denken. Langzamerhand ontstaat er steeds meer consensus dat het succes van risicomanagement sterk afhangt van het gedrag van mensen. Soft controls zijn de beheersmaatregelen die zich richten op het gedrag van mensen. De vraag voor de internal auditor is welke rol hij hierin kan vervullen en hoe gedrag getoetst kan worden.

J. Bisseling EMIA RO en J. van Harskamp MSc

In de literatuur is veel geschreven over de beantwoording van één vraag: gedraagt het personeel zich passend? Veel managers beantwoorden deze vraag met 'ja'. De vraag is echter of dit altijd terecht is. Uit diverse onderzoeken blijkt namelijk dat de grootste problemen zich niet voordoen bij het definiëren van een strategie, de rol die het management graag op zich neemt, maar bij het implementeren van strategie (managementcontrolvraagstuk). De schandalen uit het recente verleden tonen eens te meer aan dat een goede implementatie van een controlstructuur moeilijk is. Ze tonen ook aan dat het probleem niet alleen de inrichting van de beheersmaatregelen betreft, maar juist dat er niet adequaat wordt gereageerd op de signalen vanuit de organisatie. Mensen gedragen zich dus niet altijd volgens het boekje.
Risicomanagement kan goed van pas komen bij de definiëring en implementatie van strategie. Het succesvol implementeren van risicomanagement komt feitelijk neer op twee dingen heel goed doen:
1. zorgen voor het juiste proces;
2. zorgen voor de juiste inhoud.

Het juiste proces
Voor het proces dient er een afstemming te zijn over de beoogde strategie en het uitvoeren van deze strategie in de tactische en operationele processen. De internal auditor kan vanuit zijn toetsende verantwoordelijkheid, zoals de managementcyclus beschrijft, de rol van procesbegeleider oppakken en het risicomanagementproces faciliteren. Een belangrijk onderdeel daarvan vormt de assessment over de afstemming tussen strategie en uitvoering (zie *figuur 1*). Lachotzki en Noteboom (2005) beschrijven dit helder in *Managing Beyond Control.* Bij deze afstemming dienen drie partijen aanwezig te zijn:
1. management;
2. uitvoerenden;
3. Internal Audit.

De taak van de internal auditor is het begeleiden van de afstemming (die overigens kan plaatsvinden in verschillende lagen van de organisatie) tussen 'wat' er moet gebeuren, 'hoe' het moet gebeuren, 'wie' het gaat uitvoeren, 'wanneer' de activiteiten plaatsvinden en 'hoe' er verantwoording afgelegd wordt over deze activiteiten. Het faciliteren van deze afstemming heeft als voordeel dat er veel transparanter gewerkt wordt. Wel is het aan te bevelen dat de internal auditor in de rol van procesbegeleider blijft en niet op de spreekwoordelijke stoel van het management gaat zitten. Hierdoor blijft de onafhankelijke positie van de inter-



Figuur 1. Afstemming tussen strategie en uitvoering

nal auditor gewaarborgd. Afstemming tussen deze drie partijen heeft de volgende voordelen:
- de doelstellingen zijn duidelijk voor alle betrokken partijen;
- de knelpunten bij het uitvoeren van de beoogde strategie worden transparant en bespreekbaar;
- iedereen weet waarvoor hij accountable is.

Door de beoogde strategie en de implementatie ervan open te bespreken, worden de grootste risico's zichtbaar. Niet alleen neemt het bewustzijn over de organisatorische doelstellingen toe, maar ook het bewustzijn over de risico's. Het is van belang dat de onzekerheden die bestaan worden besproken. Transparantie over elkaars onzekerheden vergroot het oplossend vermogen van de organisatie. Het management kan ondersteuning bieden bij onzekerheden die bestaan bij de uitvoering. Uitvoerenden biedt het de gelegenheid om goede suggesties te doen betreffende de onzekerheden die bestaan bij het management. Dit samen creëert meer draagvlak voor het behalen van de organisatorische doelstellingen. Het gecreëerde draagvak voorkomt dat er doelstellingen opgelegd worden die te veel of te weinig ambitieus zijn, waardoor niet het passende gedrag op kan treden.
De internal auditor speelt een zeer belangrijke rol in deze afstemming. De internal auditor overziet het risicospectrum van de organisatie en kan helpen vaststellen wat de belangrijkste risico's zijn. Tevens is de context voor de auditor transparanter en is hij beter in staat om de afwegingen die gemaakt zijn om tot de juiste uitvoering van de strategie te komen, te integreren in het auditjaarplan. De auditor kan nu vooraf bespreken welke processen getoetst gaan worden en hoe deze processen getoetst gaan worden. Dit draagt bij aan meer draagvlak voor de uitkomsten van een audit. Hierdoor worden onnodige en tijdrovende discussies na het uitvoeren van een audit vermeden en zal de internal auditor meer toegevoegde waarde kunnen bieden aan de organisatie. Kortom, de transparantie en de accountability worden vergroot binnen de organisatie.
Door het goed faciliteren van de afstemming worden methoden zoals self assessments en embedded testing bruikbaar, waar ze zonder deze afstemming een te groot risico voor de organisatie vormen. Door een goed risicomanagementproces kan de strategie optimaal afgestemd worden met de operationele uitvoering en wordt opportunisme (in casu het niet nakomen van gemaakte afspraken) geminimaliseerd (zie *figuur 2*).

Figuur 2. Een optimale afstemming tussen strategie en uitvoering is van groot belang

De juiste inhoud
Hiervoor is toegelicht dat een juiste inrichting van het risicomanagementproces kan helpen bij het positief beïnvloeden van het gedrag van de medewerkers. Echter, net zo belangrijk is het inhoud geven aan risicomanagement. Inhoud geven kan met soft controls. Soft controls kunnen worden omschreven als beheersmaatregelen die invloed hebben op het gedrag van mensen. Er is veel geschreven over hoe managers het gedrag van de medewerkers kunnen beïnvloeden. Hierbij kan gedacht worden aan de *Four levers of control* van Simons (1995) of aan de *Result controls* en *Action controls* van Merchant & Van der Stede (2003). Echter, voor de internal auditor zijn deze theorieën lastiger bruikbaar. Gedrag is namelijk moeilijk kwantificeerbaar. Het is wel te meten, maar het is lastig om daar conclusies uit te trekken, want wat wordt er precies gemeten? Meestal blijft men steken op het benoemen van bepaalde kenmerken van bijvoorbeeld de cultuur van de organisatie. De vraag of de cultuur bijdraagt aan het optimaal uitvoeren van taken blijft vaak onbeantwoord.

Mensen gedragen zich niet altijd volgens het boekje

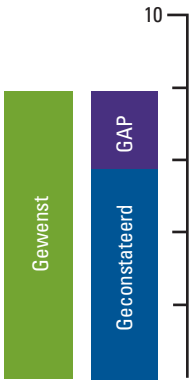
Te constateren valt wel dat er vaak een 'gap' is tussen de beleving van het management en de beleving van de medewerkers. Door middel van het hiervoor beschreven proces kan deze gap verminderd worden. De gap wordt niet alleen veroorzaakt door gebrek aan kennis over wat de organisatorische doelstellingen zijn, maar met name ook door het gebrek aan informatie over de huidige conditie van de organisatie. Is de organisatie klaar om de beoogde strategie uit te voeren? Op het gebied van gedrag is dit een moeilijke vraag om te beantwoorden. Toch willen we maar al te graag weten of het gedrag van managers en medewerkers passend is, aangezien dit essentieel is voor het kunnen behalen van de doelstellingen. Het is dus gewenst dat er inzicht verkregen wordt in hoe effectief en efficiënt de op het gedrag gerichte beheersmaatregelen (= soft controls) zijn.

Meten van de impact
Het absoluut meten van de impact van de soft controls is complex. Door relatief te meten, kunnen de uitkomsten veel beter worden geïnterpreteerd. Aan de hand van een voorbeeld met een stelling kan dit worden toegelicht.
De stelling is 'mijn manager stimuleert open en eerlijke communicatie'. Aan deze stelling moet een medewerker een waardering geven op een schaal van bijvoorbeeld een tot tien. Stel dat er een

waardering (getal) van zes (6) wordt gegeven door de medewerker. Welke conclusie kan er dan getrokken worden?
Het interpreteren van deze waardering kan vele verschillende uitkomsten geven. Met het relatief meten krijgen we veel meer informatie. Met het relatief meten willen we de delta (Δ) bepalen van de gewenste score en de geconstateerde score. Stel dat de gewenste waardering acht (8) is en de geconstateerde waardering zes (6). Nu wordt direct zichtbaar dat er een gap is van twee (2) (zie *figuur 3*). De conclusie is dan dat de medewerker vindt dat wat hij constateert niet overeenkomt met wat hij nodig acht. Gerelateerd aan de organisatorische doelstellingen geeft deze relatieve meting twee dingen weer:

1. hoe goed de huidige organisatie in staat is om de doelstellingen te behalen;
2. het ambitieniveau van de betreffende medewerker(s).

Door de soft controls relatief te meten, kunnen de uitkomsten veel beter worden geïnterpreteerd



Figuur 3. Relatief meten

Wordt er een gap geconstateerd, dan dient er een oplossing gezocht te worden om deze te verminderen of helemaal te laten verdwijnen. De oplossingsrichting kan organisatorisch van aard zijn, maar kan ook in het herijken van het ambitieniveau gezocht worden. In het voorbeeld zou de manager van de medewerker getraind kunnen worden in de wijze waarop een open en eerlijke communicatie gestimuleerd kan worden. Een andere oplossing zou kunnen zijn het ambitieniveau van de medewerker te verlagen, soms is een zes goed genoeg.

Effectiviteit van soft controls

Een organisatie is nu heel goed in staat om bijvoorbeeld door het afnemen van (anonieme) enquêtes inzicht te krijgen in de effectiviteit van de soft controls. Het relatief meten kan het inzicht in de volgende gebieden verhogen:

- integriteit van de managers en medewerkers;
- sturend vermogen van de organisatie;
- samenwerking binnen de organisatie;
- interne communicatie;
- cultuur van de organisatie;
- waarden en normen.

Het relatief meten van de soft controls geeft inhoud aan het hiervoor beschreven proces van risicomanagement. Het risicomanagementproces kan door middel van self assessments en embedded testing vormgegeven worden. Door het incorporeren (integreren) van soft controls in het risicomanagementproces worden de gaps zichtbaar. De internal auditor dient wel zorg te dragen voor afstemming over de gaps. Dit vormt het vertrekpunt voor het proces van continue verbetering. Tevens is dit een efficiënte manier om het gedrag van managers te monitoren. Als een manager geen passend gedrag vertoont, komt dat tot uiting in de beoordeling door de medewerkers. Waarschijnlijk is dit niet de oplossing tegen alle schandalen, maar is een organisatie wel beter in control. ❑

Literatuur

- Charan, R. en G. Colvin 'Why CEOs Fail', *Fortune*, 21 juni, 1999.
- Cobbold, I. en G. Lawrie, *Why do only one third of UK companies achieve strategic success?*, 2GC Ltd., mei 2001.
- Lachotzki, F. en R. Noteboom, *Managing Beyond Control: De weg naar strategie-implementatie*, Scriptum.
- Simons, R., *Four levers of control: How managers use innovative control systems to drive strategic renewal*, 1995.
- Merchant, K.A. en W.A. van der Stede, *Management control system: Performance measurement, evaluation and incentives*, Pierson Education Limited, 2003.

Jeroen Bisseling is senior consultant bij de vakgroep Audit & Risk van ConQuaestor Consulting. Hij houdt zich specifiek bezig met internal auditing en risk management in diverse branches.
Joost van Harskamp is consultant bij de vakgroep Audit & Risk van ConQuaestor Consulting. Hij houdt zich bezig met risicomanagement- en IT-controlvraagstukken.

C. Klumper RA CIA

Meer continuïteit door een dynamische auditplanning!

Continuous auditing is momenteel een buzzword. Het wordt meestal in een adem genoemd met continuous monitoring. Het IIA heeft er een Global Technology Guide aan gewijd (GTAG 3), gepubliceerd in 2005, die continuous auditing definieert als een methode om beheersmaatregelen en risico's op doorlopende in plaats van op intervalbasis te auditen. Daarbij kan de auditor gebruikmaken van dezelfde technieken en methoden die het management voor continuous monitoring kan toepassen. Continuous monitoring wordt dan gedefinieerd als een proces dat er – wederom doorlopend – voor zorgt dat beheersmaatregelen effectief zijn. Ondersteunende data-analysetools zijn, in de visie van deze GTAG, hiervoor van essentieel belang. Voorzover ik heb kunnen vaststellen is er sinds het verschijnen van de GTAG in de literatuur niet veel aan deze concepten gesleuteld: gebruik van geautomatiseerde data-analysetools zou het management en de internal auditor in staat moeten stellen om beter en actueler zicht te houden op risico's en de effectiviteit van de interne beheersing ervan.

Dat klinkt goed, maar ik zie om me heen dat de praktische toepassing van deze concepten tot nu toe relatief beperkt is gebleven. Daar zijn goede redenen voor. Ten eerste is het zo dat veel – zo niet de meerderheid – van de belangrijkste risico's zich buiten de wat ik noem 'bulkprocessen' en bijbehorende datastromen voordoen, namelijk in de handmatige controls. En die laten zich niet of nauwelijks in een geautomatiseerde data-analysetool vangen. Ten tweede vind ik dat als een nuttige geautomatiseerde check kan worden bedacht om mogelijke risico's en fouten te voorkomen of op te sporen, die check maar beter direct structureel door het management in de processen ingebouwd kan worden in plaats van als (internal) audit tool te worden gebruikt.

COSO heeft recent ook iets over continuous monitoring gezegd en wel in hun uitgebreide *Monitoring Guidance* (juni 2008). Van de ongeveer 190 pagina's die deze guidance beslaat gaan er slechts twee over het begrip continuous monitoring. Ook daarin wordt geconcludeerd dat veel van de technieken en tools die regelmatig onder de vlaggen van continuous monitoring en auditing worden genoemd, structureel worden ingebouwd als onderdeel van de reguliere beheersmaatregelen. Kortom, geautomatiseerde data-analysetools zijn zeker nuttig en dan met name als onderdeel van de set van beheersmaatregelen die in de processen aanwezig dienen te zijn, maar niet zozeer als vaandeldragers van een 'nieuw' begrip als continuous monitoring. Laat 'continuous' dan ook maar weg, en pas de nieuwe COSO *Monitoring Guidance* in de breedte, toe is mijn dringende advies.

En continuous auditing dan? Wel, mijn idee is altijd geweest dat een auditor zich niet primair moet richten op het vinden van fouten en risico's maar dat hij moet toetsen of het *management* daar adequaat mee bezig is. Waarom zou internal audit doorlopend uitgebreide data-analysetools in willen zetten als dat een managementtaak is?
Wel kunnen internal auditors nadenken over hoe ze het internal audit*proces* veel meer kunnen dynamiseren, bijvoorbeeld hoe te komen tot een doorlopende risicoanalyse in plaats van een periodieke (soms alleen jaarlijkse!) en hoe te komen tot een dynamische auditplanning, waarbij continu bijvoorbeeld zes maanden vooruit wordt gepland in plaats van te werken met statische jaarplannen? Die vorm van continuous auditing spreekt mij in elk geval een stuk meer aan. En internal audit kan natuurlijk het management helpen bij het inregelen van de juiste monitoringactiviteiten, inclusief het gebruik van de juiste data-analysetools.

Cultuur en gedrag: onderbelichte IT-aspecten

Hoewel in de markt diverse frameworks beschikbaar zijn die organisaties kunnen helpen bij het opzetten, uitvoeren en monitoren van projecten, blijken in de praktijk toch nog veel IT-projecten te 'mislukken', dat wil zeggen dat ze te laat, te duur en/of niet de gewenste kwaliteit hebben. Hierbij nemen de factoren cultuur en gedrag een prominente plaats in. In dit artikel wordt het kader beschreven waarbinnen de beoordeling van IT-projecten plaats kan vinden.

Drs. I. Kouters en drs. J. de Vries

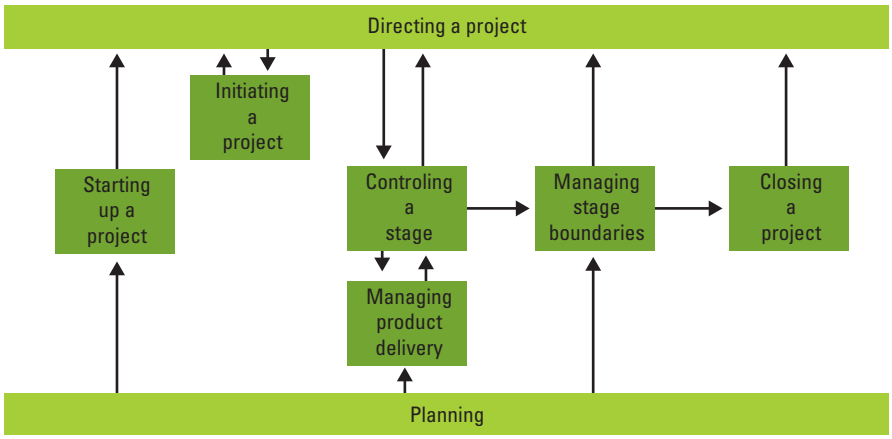
De reden voor het mislukken van IT-projecten is dat veel zogenaamde IT-projecten geen IT-projecten zijn, maar wel als zodanig beschouwd worden. Zij raken vaak een groot deel van de gehele organisatie en moeten daarom niet alleen tot het domein van IT gerekend worden. Als zulke zogenaamde IT-projecten falen hebben de oorzaken dan ook vaak niet alleen maar met IT te maken. De oorzaken moeten gezocht worden in de volledige IT-keten die begint bij de formulering van de strategische doelstellingen van een organisatie en eindigt bij de operationele IT-processen. Zoals genoemd blijken de factoren cultuur en gedrag hierbij een prominente plaats in te nemen.

Projectgovernance

IT-projecten spelen zich veelal af in dynamische en complexe omgevingen waardoor het succesvol afronden een forse inspanning vergt. In de praktijk blijkt echter dat in veel gevallen de geleverde inspanning niet leidt tot het bereiken van het oorspronkelijke doel. Hierbij is vaak sprake van tekortkomingen in de gehanteerde projectaanpak en de besturing van projecten, de zogenaamde projectgovernance. Een adequaat ingerichte projectgovernance omvat de inrichting van processen en beheersmaatregelen gericht op het succesvol afronden van projecten. Een van de meest bekende en gebruikte geformaliseerde methodieken voor projectgovernance is Prince2 (zie *figuur 1*). Een standaard projectmethodiek als Prince2 is geschikt voor projectbesturing, maar biedt *alleen* geen waarborg voor succesvolle IT-projecten. De aandacht moet ook uitgaan naar het beheersen van de volledige IT-keten.

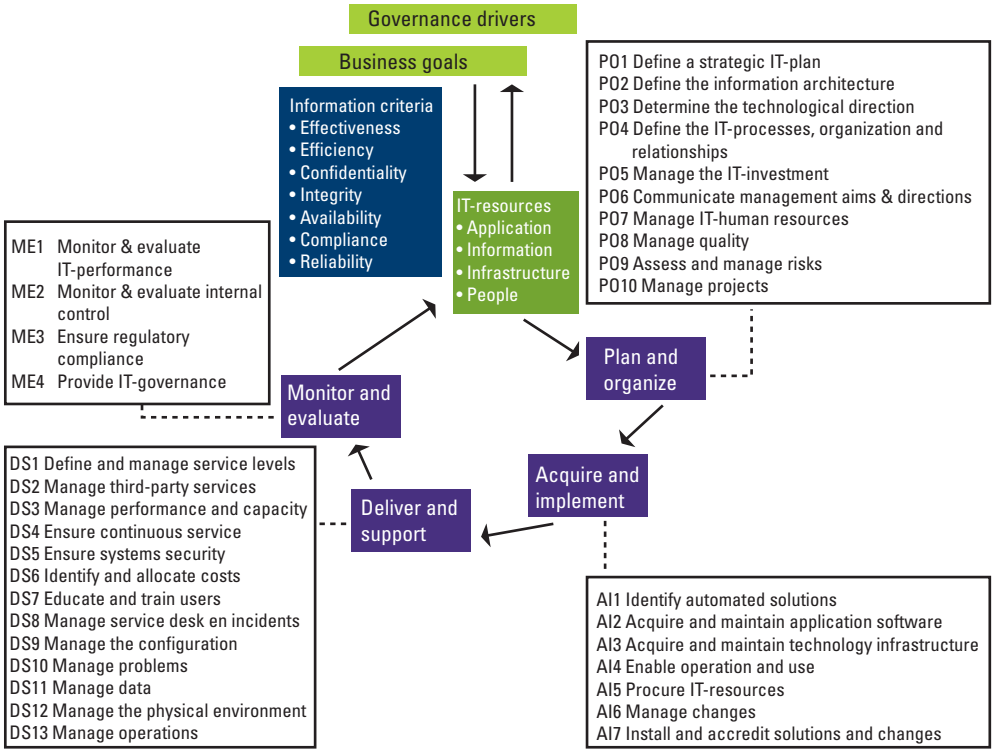
IT-Governance

Het in de greep hebben en houden van de volledige IT-keten, die begint bij de formulering van de strategische doelstellingen van een organisatie en eindigt bij de operationele IT processen,



Figuur 1. Het Prince2 procesmodel

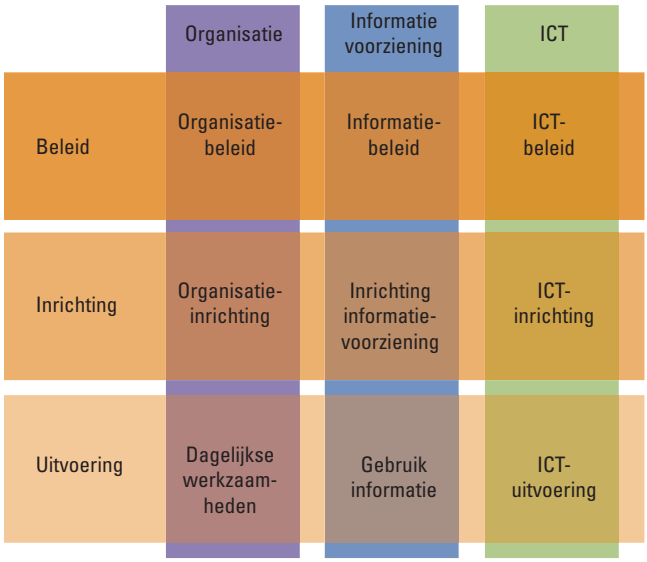
Prince2 (PRojects IN Controlled Environments) is een gestructureerde projectmanagementmethode, ontwikkeld en geïntroduceerd in 1989 door het Britse Office of Government Commerce. De methodiek is gebaseerd op bestaande methoden voor projectmanagement en een groot aantal casestudies in Groot-Brittannië. Prince2 is daardoor een integrale en universeel bruikbare bundeling van best practices voor het managen van zowel IT-projecten als niet-IT-projecten. Prince2 hanteert een procesgeoriënteerde benadering, waarbij elk proces is gedefinieerd op basis van input en output, gecombineerd met de specifiek te behalen doelen en activiteiten die moeten worden uitgevoerd om deze doelen te bereiken. De methode beschrijft hoe een project is verdeeld in beheersbare fasen, waardoor efficiënt gebruik van middelen en regelmatige monitoring van de voortgang gedurende het project mogelijk is.



Figuur 2. Het CobiT-framework

Het IT-governance framework CobiT (Control Objectives for Information and related Technology) is een internationaal gehanteerde standaard voor het gestructureerd inrichten en beoordelen van de geautomatiseerde informatievoorziening. CobiT is vanaf 1992 ontwikkeld door de Information Systems Audit and Control Association (ISACA) en het IT Governance Institute. In de huidige vierde versie van het CobiT-raamwerk worden 318 beheersdoelstellingen onderscheiden die zijn gerangschikt naar vier beheerdomeinen (die weer zijn onderverdeeld in 34 aandachtsgebieden): Plan and Organise, Acquire and Implement, Deliver and Support en Monitor and Evaluate. In december 2005 is een nieuwe versie (4.0) uitgebracht, waarin de overlap met ITIL (Information Technology Infrastructure Library) is weggenomen door aan te sluiten bij de ITIL-uitgangspunten. Ook is voor de aspecten op het gebied van informatiebeveiliging aansluiting gevonden bij de Code voor Informatiebeveiliging. ITIL wordt in Nederland veruit het meest gebruikt als methode voor exploitatie van IT-voorzieningen (IT-management).

wordt IT-governance genoemd. Cruciaal daarbij is business alignment: de aansluiting tussen enerzijds de wensen van de business en anderzijds de IT-operatie binnen een organisatie. Het CobiT framework (zie *figuur 2*) en het 9-vlaksmodel (zie *figuur 3*) zijn handige hulpmiddelen bij het realiseren en beoordelen van IT-governancevraagstukken. Het CobiT framework wordt gezien als IT-specifieke invulling van het COSO framework (corporate governancemodel) en is een doemodel. Het 9-vlaksmodel of het Amsterdams Informatiemanagement Model is een praktisch toepasbaar en kaderscheppend model. In tegenstelling tot CobiT is dit een denkmodel. Gelet op het complementaire karakter van beide modellen hanteren wij deze in de praktijk op een gecombineerde wijze.



Figuur 3. Het 9-vlaksmodel

Het 9-vlaksmodel (ook wel het Amsterdamse Informatiemanagement Model, van prof. ir. Rik Maes van de Universiteit van Amsterdam) is een praktisch hulpmiddel om verantwoordelijkheden, rollen, processen en relaties tussen vraag en aanbod in de IT-keten in ruime zin in kaart te brengen. Het model zoals wij het nu hanteren stamt uit 2003 (Abcouwer, Gels en Truijens, 2006). In ruime zin wil in dit verband zeggen dat het hele domein vanaf bedrijfsstrategie via de verbindende informatiemanagementfunctie tot en met operationele IT-processen wordt afgedekt.
Het model onderscheidt drie besturingsdomeinen (dit zijn de kolommen in het model): organisatie, informatievoorziening en ICT. Verder onderscheidt het model drie besturingsniveaus (dit zijn de rijen in het model): strategisch (beleid), tactisch (inrichting) en operationeel (uitvoering). Door deze rijen en kolommen in een matrix te plaatsen ontstaan negen vlakken. Het 9-vlaksmodel maakt duidelijk dat veranderingen in de bedrijfsstrategie vaak veranderingen in de informatiebehoefte teweeg brengen en dat hierdoor veranderingen noodzakelijk kunnen zijn in de inrichting van de IT. Nadrukkelijk wordt aandacht geschonken aan de zogenaamde koppelvlakken. Dit betekent dat tussen aangrenzende afdelingen goede afspraken moeten worden gemaakt over de afbakening van taken en verantwoordelijkheden.

Succesfactoren in de theorie

De vraag die nu rijst is welke succesfactoren onderkend worden voor het slagen van IT-projecten. Uit de literatuur blijkt dat in diverse onderzoeken een drietal succesfactoren worden onderkend, te weten: planning en fasering, projectorganisatie en besturing, cultuur en gedrag. De succesfactor planning en fasering is gericht op de projectinrichting en een voorwaarde voor adequate besturing en beheersing van projecten. De succesfactor projectorganisatie en besturing betreft het eenduidig definiëren van rol-

len in het project en het toewijzen van taken en beleggen van verantwoordelijkheden. De succesfactor cultuur en gedrag is van belang omdat de (informele) machtsstructuur, het leiderschapspatroon en de samenwerking, al dan niet versterkt door externe medewerkers, van invloed kunnen zijn op het al dan niet behalen van de uiteindelijke projectdoelen.

Faalfactoren in de praktijk

Naast succesfactoren is tevens aandacht vereist voor risico's en aandachtsgebieden (hierna faalfactoren genoemd). Vanuit onze ervaring met het beoordelen van IT-projecten is de volgende top twintig van meest voorkomende faalfactoren samengesteld.

1. Onvoldoende overeenstemming over het doel van het project en het ontbreken van een breed gedragen plan van aanpak met voldoende diepgang.
2. Het uit handen geven van het opdrachtgeverschap zodra het project begint en te veel externen op cruciale posities in het project.
3. Optimisme over het aantal veranderingen dat de organisatie in een periode kan adopteren.
4. Onderschatting van weerstand tegen verandering.
5. Softwareontwikkeling op basis van documenten die niet overeenkomen met de wensen van de business vanwege een geringe betrokkenheid van de business.
6. Niet sturen door de stuurgroep door het ontberen van 'gereedschap'.
7. Het niet werken van werkgroepen door te veel overleg en te weinig sturing hierop.
8. Onderschatting van de tegengestelde belangen, resulterend in een slechte samenwerking.
9. Een zwakke onderbouwing van de kwantitatieve inschattingen.
10. Onvoldoende communicatie binnen het project.
11. Het slecht beleggen van taken, bevoegdheden en verantwoordelijkheden binnen het project.
12. Te weinig tijd beschikbaar voor projectmedewerkers, het moet er even bij.
13. Te veel optimisme over de voortgang door het inbouwen van te weinig 'slack'.
14. Het onvoldoende uitvoeren van risicoanalyses op het gewenste procesverloop van key processen.
15. Het ontbreken van een doecultuur om het project tot goed einde te brengen.
16. Onvoldoende aanwezigheid van kennis en ervaring in de organisatie om IT-projecten goed uit te voeren.
17. Verstoring van projecten door aanvullende wensen zonder dat de consequenties goed worden overzien.
18. Projectleiders blijken projectmedewerkers te zijn.
19. Contracten met leveranciers die een inspanningsverplichting in plaats van een resultaatverplichting inhouden.
20. Door een informele sfeer en vage besluiten elkaar onvoldoende aanspreken op gedrag.

Het Cultuur en Gedragmodel

In de loop der jaren is het steeds duidelijker geworden dat veel faalfactoren te maken hebben met de cultuur en het gedrag binnen de organisatie. Iets waarvan het management van de organisatie en het projectmanagement zich vaak onvoldoende bewust blijken te zijn.

Daarnaast reiken projectmanagementmethodieken en IT-governancemodellen vooral handvatten aan voor het beïnvloeden van de succesfactoren planning en fasering en projectorganisatie en besturing. Ten aanzien van de succesfactor cultuur en gedrag worden vanuit de genoemde modellen echter geen of weinig handreikingen gedaan om de faalfactoren die bij deze factor behoren, in voldoende mate te kunnen beheersen. De factor cultuur en gedrag blijkt dus onderbelicht te zijn. Een nieuw door ons op basis van praktijkervaring ontwikkeld model dat zich richt op de aspecten cultuur en gedrag vult deze leemte op (zie *figuur 4*).

In de praktijk worden IT-auditors vaak betrokken bij IT-projecten die niet goed verlopen. Zij hanteren bij het in kaart brengen van de oorzaken gereedschappen die normatief van karakter zijn. Menselijk gedrag is echter een niet-tastbaar fenomeen en is daarom niet in normen te vervatten en met genoemde gereedschappen te ondervangen. Hier wordt het gebied van de gedragswetenschappen zoals sociologie, psychologie, en sociale psychologie (andragogie) betreden.

Gebleken is dat veel van wat misgaat in (project)organisaties veroorzaakt wordt doordat individuen contraproductief gedrag

Het Cultuur en Gedragmodel is door de auteurs van dit artikel ontwikkeld en is net als het 9-vlaksmodel een denkmodel. In het model wordt een achttal aandachtsgebieden onderkend binnen een organisatie die bepalend zijn voor de organisatiecultuur en het gedrag van mensen, zowel individueel als in groepen. Ze komen voort uit de onderkende factoren die in de praktijk ten grondslag liggen aan het falen van projecten.

Figuur 4. Het Cultuur en Gedragmodel

vertonen en dat de heersende cultuur binnen een organisatie een klimaat schept waardoor de kans op het succesvol kunnen afronden van projecten klein is. Zo kunnen verschillen bestaan tussen de doelstellingen van het individu en die van de (project)organisatie. Deze verschillen leiden uiteindelijk tot voor de (project)organisatie ongewenst gedrag.

Bij het implementeren van een nieuw systeem speelt bijvoorbeeld mee dat mensen vaak niet willen veranderen. Men ontbeert een *professionele attitude* en laat zich leiden door het eigen gevoel. *Acceptatie* van verandering is hierbij ook een belangrijke factor. Andere aandachtsgebieden betreffen de vaak slechte *communicatie* en *samenwerking* onderling waardoor onduidelijkheden en interpretatieverschillen kunnen ontstaan. Weinig efficiënt en het heeft tot gevolg dat het project gevaar loopt.

Een ander veel voorkomend fenomeen is dat de organisatie bij aanvang van een project zeer enthousiast is en zich bij de definitie van het project voornamelijk door dit enthousiasme laat leiden in plaats van door *realisme*. Overschatting van bijvoorbeeld het aantal veranderingen dat de organisatie in een bepaalde periode aan kan en een te breed georiënteerde *focus* en scope van het project, dragen bij aan het creëren van een situatie waarin het succesvol afronden van het project moeizaam zal zijn. Effectief *leiderschap* van zowel de projectleiding als het management van de organisatie, onder andere goed opdrachtgeverschap, is van groot belang en randvoorwaardelijk voor het adequaat kunnen sturen van projecten.

Het laatste aandachtsgebied is het hebben van een doecultuur binnen de organisatie. Veelal komt men met grootse plannen maar ontbreekt het vermogen om tot *executie* van deze plannen over te gaan. ❑

Conclusie

Onderzoek naar de oorzaak van het falen van zogenaamde IT-projecten wordt veelal gedaan door te kijken naar IT. Het blijkt echter dat het mislukken vaak niet alleen maar met IT te maken heeft, maar een veel breder karakter heeft. Om IT-projecten met succes uit te kunnen voeren is het van belang de volledige IT-keten te beheersen en daarbij aandacht te besteden aan de succesfactor cultuur en gedrag. Ervaring met organisatievraagstukken is derhalve onmisbaar om de volledige IT-keten te beheersen.

Ten aanzien van het slagen van IT-projecten worden de succesfactoren planning en fasering, projectorganisatie en besturing, en cultuur en gedrag onderkend. Vanuit traditionele governancemodellen als Prince2 en CobiT worden handvatten aangereikt om te voorkomen dat de faalfactoren gerelateerd aan de succesfactor planning en fasering en projectorganisatie en besturing, zich manifesteren. Voor de succesfactor cultuur en gedrag worden vanuit de genoemde modellen echter geen of onvoldoende handreikingen gedaan om te voorkomen dat de faalfactoren die samenhangen met deze succesfactor manifest worden.

Ten aanzien van de succesfactor cultuur en gedrag kunnen IT-auditors vanuit een IT-perspectief nauwelijks een constructieve bijdrage leveren. Waar het gaat om gedrag van individuen, zowel zelfstandig als in groepen, wordt het terrein betreden van de gedragswetenschappen. Het is bij governance van IT-projecten dan ook noodzakelijk kennis van gedragswetenschappen en ervaring met organisatievraagstukken, waarbij de succesfactor cultuur en gedrag een centrale rol speelt, te betrekken.

Het ontwikkelde Cultuur en Gedragmodel kan een bijdrage leveren aan het beheersen van het totale spectrum van faalfactoren die zich in de praktijk bij IT-projecten kunnen voordoen.

Literatuur

- Abcouwer, T., H. Gels en J. Truijens, *Informatiemanagement en beleid*, Academic Service, 2006.
- Anthony, R. en V. Govindarajan, *Management Control Systems*, McGraw-Hill, 1995.
- Grembergen, W. van en S. de Haes, *IT Governance mechanismen*, Kluwer, 2004.
- Horn, L.A. ten, *Psychologische aspecten van de organisatie*, Samsom Bedrijfsinformatie, 1994.
- Onna, M. van en A. Koning, *De Kleine Prince2*, Academic Service, 2007.

Ivo Kouters (l) en Jasper de Vries zijn beiden werkzaam bij Ernst & Young Advisory en houden zich voornamelijk bezig met IT-governance- en program assurancevraagstukken.

✉ ivo.kouters@nl.ey.com

✉ jasper.de.vries@nl.ey.com.

APM TERMINALS

INTERNAL AUDITOR
THE HAGUE, THE NETHERLANDS

APM Terminals, a world leader in container terminal development and operations, and a division of global energy and transportation conglomerate A.P. Moller–Maersk Group, is seeking an experienced Internal Audit professional. The position reports to the Director, Business Audit and is located at the company headquarters in The Hague, Netherlands.

Responsibilities include:

- Planning and coordination of business audits of the 50+ facilities in the APM Terminals Global Terminal Network.
- Development and maintenance of standardized procedures, guidelines, manuals, reporting templates, and other facets of audit and accounting reporting.
- Participation in developing APM Terminals' internal audit strategy.

Requirements:

- 5-10 years of external/internal audit experience.
- Relevant degree in Accounting or Finance.
- Strong analytical skills.
- Fluency in both written and spoken English.

The successful candidate will possess empathy, personal tact, multicultural sensitivity and the strong interpersonal skills required for effective leadership and communication in a large, dynamic and rapidly expanding international business environment.

The position involves approximately 75 days of international travel per year.

For immediate consideration, please e-mail your CV to Rex.Jackson@apmterminals.com

Continuous auditing: science fiction?

Drs. A. Lucassen RE CISA*

Iemand heeft het bankrekeningnummer van een van uw leveranciers aangepast en heeft vervolgens enkele facturen voor deze leverancier ingevoerd en betaalbaar gesteld. Natuurlijk wilt u hier als management of als internal auditor meer van weten, dit kan immers duiden op het doorbreken van de in de organisatie ingebouwde functiescheiding. En het liefst zo snel mogelijk, zodat kordaat opgetreden kan worden. Echter, de huidige (interne) controle(aanpak) is meestal nog niet (in)gericht op het tijdig signaleren van dit soort situaties. Het antwoord hierop: continuous monitoring.

Met continuous monitoring wordt een bedrijf in staat gesteld de werking van het systeem van interne controle continu te verifiëren. Indien een control niet effectief werkt wordt onmiddellijk een signaal afgegeven aan het management. Hierbij dient te worden opgemerkt dat het bij continuous monitoring niet alleen gaat om het beperken van financiële risico's, maar natuurlijk ook om operationele en strategische risico's.
Doordat bij continuous monitoring het verifiëren geautomatiseerd gebeurt, is er niet alleen sprake van een efficiënte en effectieve aanpak, maar ook van een diepgaande en uitgebreide aanpak, aangezien men zich niet hoeft te beperken tot deelwaarnemingen en steekproeven en aldus gehele populaties onder de loep genomen kunnen worden.
Een dergelijke aanpak leidt ertoe dat op ieder moment van de dag vastgesteld kan worden hoe het interne controlesysteem ervoor staat. Voeg daaraan toe een (internal) auditor die vaststelt dat dit nieuwe interne beheersingsinstrument goed werkt en je hebt continuous auditing en continuous assurance. Maar om een dergelijk intern beheersingsinstrument te kunnen gebruiken zijn er wel enkele randvoorwaarden. Evident is natuurlijk dat om risico's te kunnen beheersen, je deze geïdentificeerd moet hebben en periodiek moet evalueren. Dus een goed risicomanagementproces en borging hiervan in de organisatie is essentieel.
Voor een deel van de bedrijven is dit al het geval, omdat zij moeten voldoen aan allerlei wet- en regelgeving. Daarnaast is continuous monitoring alleen mogelijk als de bedrijfsprocessen die hierin worden betrokken in hoge mate geautomatiseerd zijn, dan kunnen de analyses op continue basis worden uitgevoerd zonder menselijke tussenkomst. Ook dit geldt al voor het merendeel van de bedrijven aangezien veel bedrijven vaak geïntegreerde oplossingen gebruiken zoals ERP-systemen.

Is continuous monitoring en continuous auditing (i.e. assurance) science fiction? Nee, zeker niet nu de technologie die dit moet ondersteunen meer en meer volwassen wordt. Zijn bedrijven hier op korte termijn al klaar voor? Nee, waarschijnlijk nog niet voor alle bedrijfsprocessen, aangezien er nog veel handelingen handmatig en buiten de geautomatiseerde systemen om worden uitgevoerd, maar voor bepaalde processen en onderdelen liggen hier wel degelijk kansen.
Moet je dit als internal auditor omarmen? Absoluut! Natuurlijk moet er een vinger aan de pols gehouden worden hoe continuous monitoring wordt ingericht, maar eenmaal ingericht geeft het de internal auditor dezelfde zekerheid als voorheen. Zelfs nog meer, omdat geen gebruik wordt gemaakt van deelwaarnemingen. En doordat het geautomatiseerd gebeurt heb je als internal auditor nog meer ruimte en aandacht voor andere, minder structurele onderwerpen en kun je nog meer waarde toevoegen.
Dus continuous monitoring en continuous auditing zijn zeker geen bedreigingen maar juist welkome aanvullingen op het 'arsenaal' van een internal auditor.

* Antoine Lucassen is director Deloitte ERS

Deloitte.

En daar wandel je dan…

Bart Verkuijl en Arnold van Emmerik • Omgaan met stress en burnout • Bohn Stafleu van Loghum • ISBN 978903143911

R.J. Klamer

Opeens is het zover. Dan wandel je op een doordeweekse dinsdagmorgen door een park. Zonder je schuldig te voelen. Zonder je blij te voelen. Je voelt eigenlijk niks. Alleen een totaal onvermogen. Niet in staat te werken, niet in staat thuis te zitten. Leeg.

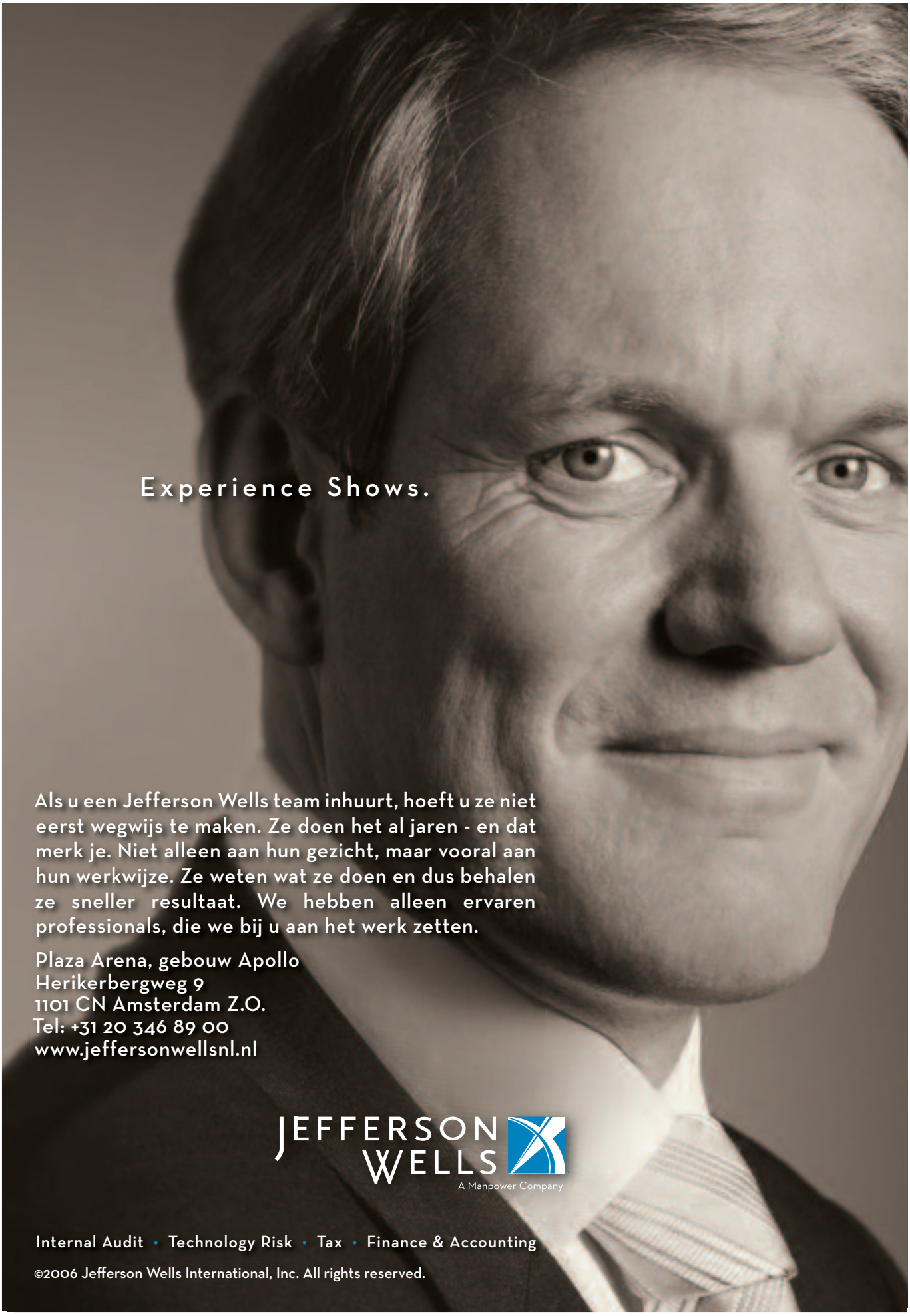
Ik ken een paar mensen die dit hebben meegemaakt. En het lijkt erop of steeds meer mensen het op een of andere manier ervaren. Een burn-out. Natuurlijk, achteraf kun je het best aanwijzen. Te veel werk, te veel dingen tegelijk, te veel moeite, maar eigenlijk kon alles best wel. Bovendien wist je het toch zelf het allerbest. Uitleggen en overdragen zou wel kunnen, maar dan doen ze het toch niet helemaal goed en voor jou… ach, het was niet zo moeilijk. Nog even dit en dan meteen maar even dat doen. Even eten koken, even voorbereiden voor de vergadering, even naar de vergadering, even napraten en jij kon dat toch wel even doen. Straks neem je wel even een beetje rust, even een glaasje wijn erbij...
Opvallend is dat het woordje 'even' ongelooflijk vaak terugkomt in het vocabulaire van iemand op de rand van een burn-out. Tenslotte zijn de meeste dingen die we doen niet zo moeilijk en lijken ze maar korte tijd de aandacht te vragen.

In een recente training over omgaan met stress heb ik de deelnemers gevraagd een brief aan zichzelf te schrijven waarin ze zichzelf aanmoedigen om het geleerde (opnieuw, na zes weken) in de praktijk te brengen. Wat mij opviel in die brieven – ik mocht ze ook lezen – is dat de schrijvers zichzelf meer rust toewensen. Meer tijd en gelegenheid om zaken af te maken. En dat ze zichzelf toewensen wat vaker een afgewogen 'nee' te kunnen laten horen. Ontroerende brieven die, naar ik hoop, echt een functie hebben voor de deelnemers.

Het boek *Omgaan met stress en burnout* is een dun boek: 126 pagina's. Qua omvang ideaal om in huis te hebben en eens door te lezen. Om te leren hoe dat nu ontstaat, zo'n burn-out. Om mee te denken over potentiële oplossingen. Als leidinggevende van iemand die dreigt om te vallen. Maar wellicht ook voor jezelf als je in de afgelopen week wel erg vaak een lege wijnfles hebt opgeruimd.
Een van de leukste tips die iedereen kan gebruiken is het instellen van een piekerhalfuur. Per dag een half uur in te ruimen om lekker te piekeren. Daardoor kun je het piekeren op andere momenten kanaliseren naar dat piekerhalfuur. Neem er een vaste rustige plek in huis voor (je piekerplek) op een vaste tijd. Daarmee wordt de rest van het huis piekervrij. Plan het niet vlak voor het naar bed gaan...
Zoals op ieder boek is ook op dit boek wel wat aan te merken. Ik merkte dat ik bij bepaalde onderwerpen eigenlijk wel meer wilde weten. Wat meer tegengas verwachtte of een wat diepere uitwerking. Dat is soms een gemis. Uiteraard wordt in de paragraaf over doelen stellen de SMART-regel opgevoerd. Dat deze regel op zichzelf al een reden voor veel stress kan zijn ('Hoe bedoel je dat ik een realistisch doel moet opschrijven, ik bak er toch niks van', is een vaak voorkomende belemmerende overtuiging) wordt niet genoemd. Een dergelijke nuancering kun je wel opzoeken in de bijgeleverde literatuurlijst en website-adressen.

Toen ik het boek las moest ik sterk denken aan een zakelijke relatie die mij uitvoerig verslag deed van hoe de relatie tussen hem en zijn beste medewerkster binnen een paar maanden volledig was verwoest. De medewerkster was emotioneel geknakt door enorme drukte op het werk gecombineerd met een sterfgeval, relatieproblematiek en nog zo wat onvolkomenheden. En hij had daar begrip voor, stelde hij. Maar ze moest na drie maanden toch wel een keer terugkomen... Uiteraard probeerde ze het. Maar het mislukte compleet, want er was nog niets verbeterd. Behalve wandelen in het park had ze nauwelijks professionele ondersteuning gehad.
Deze baas had er veel aan gehad als hij dit boekje had gelezen. Hij zou echt begrip hebben kunnen tonen, hebben aangedrongen op echte hulp en hij had beter begrepen dat de emotionele uitspraken een andere oorzaak hadden. Bovendien had het hem een ellendige en kostbare ontslagprocedure bespaard.
Want een ding is zeker. Je wenst je ergste vijand geen burn-out toe. De gevolgen zijn altijd schadelijk en zo levensveranderend dat je maar beter een boekje van 126 bladzijden kunt lezen. Dan kun je daarna tenminste gewoon wandelen in het park. Op zaterdag of zondag.

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


Experience Shows.
Als u een Jefferson Wells team inhuurt, hoeft u ze niet eerst wegwijs te maken. Ze doen het al jaren - en dat merk je. Niet alleen aan hun gezicht, maar vooral aan hun werkwijze. Ze weten wat ze doen en dus behalen ze sneller resultaat. We hebben alleen ervaren professionals, die we bij u aan het werk zetten.
Plaza Arena, gebouw Apollo
Herikerbergweg 9
1101 CN Amsterdam Z.O.
Tel: +31 20 346 89 00
www.jeffersonwellsnl.nl
JEFFERSON WELLS
A Manpower Company
Internal Audit • Technology Risk • Tax • Finance & Accounting
©2006 Jefferson Wells International, Inc. All rights reserved.

Jurgen Schaerlaeckens vertelt dit keer in de rubriek De Overstap over zijn carrièreswitch naar het vak van internal auditor. Na vijf jaar als accountmanager bij ING gewerkt te hebben is hij nu internal auditor bij Interpolis/Achmea.

"Ik heb een nieuwe uitdaging gevonden en daar ben ik nog wel even zoet mee"

Als accountmanager bij ING bestonden de werkzaamheden van Jurgen onder meer uit het beheren van kredietportefeuilles, het beoordelen van kredietaanvragen en het opstellen van kredietvoorstellen voor de zakelijke markt. In het begin vond Jurgen deze functie zeer uitdagend en afwisselend, maar de functie werd steeds commerciëler. Daardoor bleef er minder ruimte over voor de inhoudelijke kant van het vak. Dat stond hem steeds meer tegen.
Zijn herinneringen aan zijn tijd bij ING beschrijft hij als volgt: "Het eerste jaar was erg zwaar. Veel zieken en afwezigen waardoor ik nauwelijks ben ingewerkt. Ik zat vaak alleen en de targets liepen gewoon door. Uiteindelijk is het toch een goed jaar geworden. Daarnaast ben ik trots op een hele grote deal die we hebben gesloten. Met het team – de relatiemanager, de assistent en ik – zijn we mede daarvoor genomineerd voor het beste verkoopteam van de maand (van het land)."

Geen uitdaging meer

Omdat hij toe was aan een nieuwe uitdaging ging hij op zoek naar een andere baan. Over zijn keuze voor het vakgebied internal auditing zegt hij: "De voornaamste reden was het gevoel geen echte uitdaging meer te zien. Het vak werd steeds commerciëler en een volgende stap zou buitendienstmedewerker zijn (relatiemanager). Dat zag ik absoluut niet zitten. Ik heb goed nagedacht over wat ik leuk zou vinden en waar mijn sterke kanten liggen. Duidelijk was dat ik een analytische functie wilde met veel afwisseling en een brede scope. Het risicodenken bij de bank sprak me altijd al aan. Daarnaast wilde ik werkzaam zijn binnen een grote organisatie, het liefst een financiële dienstverlener, en bij voorkeur in het zuiden van het land. Zo ben ik bij de functie van internal auditor bij Achmea/Interpolis uitgekomen."

In zijn nieuwe functie als internal auditor houdt hij zich naast operational audits bezig met audits waarin financial en IT-auditaspecten naar voren komen. “Tot op heden heb ik vooral werkzaamheden uitgevoerd voor het vaststellen van de mate van beheersing van diverse processen en de uitgevoerde systeemconversies binnen mijn aandachtsgebied, de divisie Pensioenen. Daarnaast ben ik als auditor betrokken geweest bij het internal control statement dat de organisatie jaarlijks afgeeft. Ook werkzaamheden voor de vaststelling van de betrouwbaarheid van een specifiek onderdeel van de administratie heb ik het afgelopen jaar uitgevoerd.”

Verwachtingen

Over de verwachtingen die hij heeft van zijn nieuwe functie en in het bijzonder over de switch naar het vak van internal auditor, zegt hij: “Omdat ik er goed over heb nagedacht en me uitgebreid heb voorbereid, ben ik weinig verrassingen tegengekomen. Ik volg naast mijn werk de opleiding internal/operational auditing aan de Erasmus te Rotterdam. De combinatie werk/studie bevalt me goed. Vooral het herkennen van praktijksituaties in de theorie en andersom spreekt me erg aan. Daar leer je meer van dan tijdens je reguliere studie.”

Het belangrijkste verschil tussen zijn oude en huidige functie is dat een accountmanager direct met de (eind)klant te maken heeft. “Je merkt aan alles dat je in een commerciële omgeving werkzaam bent.” De belangrijkste overeenkomst betreft volgens Schaerlaeckens het in control zijn. “Als accountmanager dien je continu aan te kunnen tonen hoe en waarom je op een bepaalde wijze hebt gehandeld. Iedere keuze die je maakt dient in het dossier verantwoord te worden. Als internal auditor doe je eigenlijk niet anders, hoewel dat wel op een ander niveau is. Daarnaast zie ik als belangrijke overeenkomst het risicodenken en het analyseren. Wat kan er misgaan, wat is het maximale risico, restrisico, wat zijn specifieke dekking/controls?”

Doorontwikkelen

Schaerlaeckens wil zich de komende jaren doorontwikkelen tot ervaren auditor. Daarna ziet hij weer verder. “Ik ben opgehouden met het maken van een langetermijnplanning. Het allerbelangrijkste is dat je het naar je zin hebt, de rest komt dan vanzelf. Dat wil overigens niet zeggen dat ik niet ambitieus ben. Ik wil er het beste van maken, eruit halen wat er in zit.”

Het thuisfront ervaart de overstap als zeer positief. “Mijn vriendin vindt het ’t belangrijkste dat ik een baan heb die ik leuk vind. Daarnaast heb ik nog voldoende tijd voor onze tweeling.” Zelf beschouwt Schaerlaeckens zijn overstap nu al als een succes. “Mijn voornaamste reden voor de overstap was het vinden van een nieuwe uitdaging. Die heb ik gevonden en daar ben ik nog wel even zoet mee.”

IIA Young Professionals

ING

Op 5 november jl. bezochten we ING. Op de 37ste verdieping van het ING-pand is het thema *Getting the most out of ERM* behandeld. Centraal stond het integrale karakter van risicomanagement in het bedrijfsproces. Aan de hand van een casus ondervonden we het belang hiervan in de praktijk. De deelnemers waren na afloop enthousiast en onder het genot van een borrel en buffet werd gezellig nagepraat. Kortom, een geslaagde middag!

Vooruitblik 2009

De tot nu toe georganiseerde kick off IIA YP-bedrijfsbezoeken bij *De Telegraaf* en ING en de enthousiaste reacties op het initiatief hebben ervoor gezorgd dat commissie IIA YP voor 2009 alweer vele nieuwe ideeën heeft om het platform en netwerk voor jonge auditors te vergroten. Voor 2009 staat het volgende centraal:

- de bekendheid van IIA YP vergroten;
- de activiteiten laten aansluiten op de behoefte en wensen van de jonge auditors;
- het organiseren van activiteiten met een balans tussen netwerken en het vergroten en delen van kennis.

Op de planning staat een bedrijfsbezoek aan KPN, een kijkje in de keuken van DNB en een exclusieve Young Professionals Academy. Ook willen wij volgend jaar een aantal informele bijeenkomsten organiseren waarbij het netwerken centraal staat.

2009 Belooft een jaar te worden waarin jullie nog meer zullen horen van IIA YP. Een jaar waarvoor wij onszelf tot doel hebben gesteld om aansprekende activiteiten te organiseren zodat IIA YP het platform is waar wij voor willen staan.

Voor meer informatie: bezoek de website of stuur een ✉ naar yp@iia.nl.

Heb je zelf suggesties die aansluiten bij de centrale thema’s van IIA YP voor 2009, dan kun je ook mailen naar yp@iia.nl.

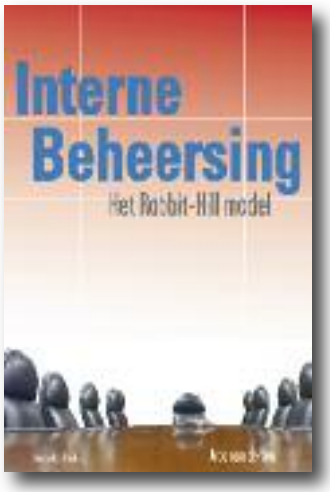
Gepast en ongepast geld

Hans Ludo van Mierlo • Scriptum • ISBN 9789055946242 • € 19,95

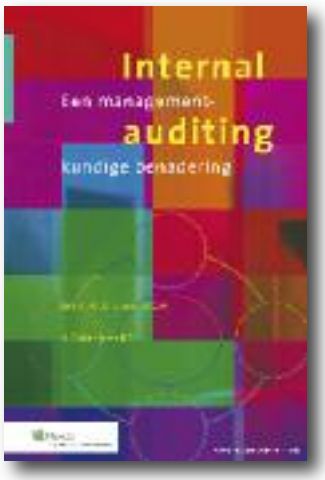
Sinds begin 2008 wordt er openlijk gesproken over een bankencrisis. Banken over de hele wereld hebben in een jaar tijd al meer dan 500 miljard euro moeten afboeken op riskante leningen en dreigden als dominostenen om te vallen. Overheden, centrale banken en Chinese staatsfondsen moesten te hulp schieten.
Maar het gaat vandaag niet meer alleen om een financiële crisis, er is tegelijk ook sprake van een morele crisis. Miljoenen mensen procederen tegen banken en verzekeraars vanwege slechte voorlichting over riskante en veel te dure producten. Financiële instellingen moeten miljarden schadevergoeding betalen aan benadeelde klanten. Maatschappelijke organisaties verwijten bankiers en beleggers gebrek aan aandacht voor de sociale en ecologische gevolgen van hun financieringen, dichtbij en ver weg. Er is ergernis over topsalarissen. Banken vertrouwen elkaar niet meer.
Wat is dat voor een industrie, die zichzelf zo in de problemen brengt? Hebben bankiers eigenlijk wel een geweten? Hoe onmaatschappelijk of maatschappelijk zijn ze? *Gepast en ongepast geld* geeft op prikkelende wijze een genuanceerd beeld van de werkelijkheid.

Het Rabbit-Hill model

Arco van de Ven • ACN Management Consultants • ISBN 9789081084826 • € 40,00



Interne beheersing van organisaties staat volop in de belangstelling. De laatste jaren zijn veel methodieken, zoals COSO ERM, Business Balanced Scorecard, Levers of Control, INK-model, Economic Value Added en Activity Based Costing ontwikkeld om hier inhoud aan te geven. Het aanbod is echter zo groot en de uitgangspunten van de methodieken zo divers, dat de keuze voor een bij de organisatie passende methodiek van cruciaal belang is voor een adequate beheersing.
De auteur introduceert het zogenaamde Rabbit-Hill model. Het is een synthesemodel dat bestaande methoden en technieken selecteert en combineert om een optimale sturing en beheersing te creëren voor organisaties. Met de uitwerking van het Rabbit-Hill model geeft het boek een goed en up-to-date overzicht van belangrijk geachte methodieken voor interne beheersing.
Het boek wordt bij diverse opleidingen gehanteerd. Omdat het model in de praktijk zijn waarde reeds heeft bewezen, is het ook buiten de formele opleidingen zeer bruikbaar voor controllers, auditors, adviseurs en accountants.



Internal auditing. Een managementkundige benadering

A.J.G. Driessen, A. Molenkamp • Kluwer, vierde, herziene druk • ISBN 9789013055702 • € 72,50

Het vakgebied van internal auditing is constant in beweging. Vooral recente wet- en regelgeving, zoals de Sarbanes-Oxley Act, de Code Tabaksblat en VBTB, hebben een grote invloed op de wijze waarop momenteel invulling wordt gegeven aan internal auditing. Steeds nadrukkelijker wordt internal auditing gepositioneerd als waarborg voor het topmanagement dat, uitgaande van de strategie van de onderneming, de risico's adequaat worden gemanaged. Maar ook dat de set aan beheersingsmaatregelen zo is ingericht dat het management de juiste beslissingen kan nemen om de prestaties van de onderneming te optimaliseren. Ook ontwikkelingen als het toegenomen belang van internal auditing voor het audit committee, de sterke aandacht voor (de betrouwbaarheid van) in control statements en de risicogebaseerde aanpak zijn voor de auteurs belangrijke redenen geweest om het boek opnieuw geheel te herzien.
Dit vernieuwde Nederlandse handboek voor internal auditing beschrijft het vakterrein vanuit een managementkundig standpunt. Daarmee manifesteert internal auditing zich als de oren en ogen van het management. Het levert een belangrijke bijdrage aan de (continue verbetering van de) doeltreffendheid en doelmatigheid van de bedrijfsvoering. Beide auteurs doceren en doen onderzoek aan de opleiding Executive Master of Internal Auditing aan de Amsterdam Business School. Deze ervaringen én hun achtergronden (organisatiekunde en bedrijfseconomie) hebben geleid tot een boeiende en vernieuwende visie die in dit boek is vastgelegd.

Training Adding Value Using Risk-based Auditing

Op 15-16 december wordt er een training georganiseerd met als onderwerp 'Adding value using risk-based auditing'. Deze training is bedoeld voor auditdirecteuren, auditmanagers, teamleiders en interne auditors die richting willen geven aan de implementatie en uitvoering van risk-based auditing in hun organisatie en voor auditors en consultants die hun vaardigheden op het gebied van risk-based auditing willen verbeteren

Inhoud training

Onder meer aan de hand van casusmateriaal en groepsdiscussies zal deze training auditmanagers, teamleiders en andere professionals op (audit)managementniveau helpen de doelstellingen van hun organisatie in lijn te brengen met het internal auditproces. Daarnaast wordt aandacht geschonken aan het belang van corporate governance en enterprise risk management.
Meer informatie over deze training vindt u in de activiteitenkalender op onze website.

Zes nieuwe IIA Standards

Het nieuwe International Professional Practices Framework (IPPF) is vanaf 1 januari 2009 van kracht. Het bevat zes nieuwe standaarden:

- 1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the Internal Audit Charter.
- 1111 – Direct Interaction With the Board.
- 2110.A2 Assessing information technology governance.
- 2120.A2 Evaluation of the risk of fraud.
- 2120.C3 Limitation of the internal auditors role with the risk management scope.
- 2430 Use of 'conducted in conformance with the international standards for the professional practice of internal auditing'.

Een PowerPoint-presentatie met een toelichting op de wijzigingen kunt u vinden op: http://www.theiia.org/download.cfm?file=53661
De volledige standaarden, zoals deze van kracht zijn vanaf 1 januari 2009 vindt u op: http://www.theiia.org/download.cfm?file=38118

Seminar mvo: update voor internal auditors

In 2008 is een aantal belangrijke studies gedaan naar de huidige situatie en trends wat betreft maatschappelijk verantwoord ondernemen (mvo) in Nederland. Ook het kabinet heeft zijn visie bepaald en beleid neergezet voor duurzaam inkopen door de overheid. Dit alles raakt de organisaties waarvoor internal auditors werken, zowel in de private als in de publieke sector.

Actuele stand

Na het bijwonen van deze update bent u weer op de hoogte van de actuele stand van zaken inzake mvo en van de mogelijke kansen en bedreigingen voor uw organisatie. Aan de hand van een tweetal casestudies leert u hoe de internal auditdiensten van Rabobank en TNT betrokken zijn bij het verstrekken van assurance over mvo.
Het seminar vindt plaats op 17 december 2008 en is bedoeld voor hoofden van IAD's, Internal auditors die betrokken zijn bij het uitvoeren van mvo-audits, externe CSR Assurance Providers, CFO's, controllers en directeuren die verantwoordelijk zijn voor het realiseren van het mvo-beleid in hun organisatie.
Meer informatie over dit seminar vindt u in de activiteitenkalender op onze website.

SVRO Stichting Verenigde Operational Auditors

IIA Institut van Internal Auditors Nederland

Activiteitenkalender 2009

Februari

11-12	Auditen van compliance en integriteit
25-26	Skills for the new auditor in charge

Maart

3-4	COSO ERM: What's new, what's next
18-19	Fraudedetectie en onderzoek
25-26	Introduction CSA

April

6-7	Auditen van projecten
9 en 16	Creativiteit: onmisbaar voor auditors

Mei

6-8	Introductie IT-auditing
19-20	Consulting: activities, skills & attitudes
21 en 28	Basiscoachingsvaardigheden voor auditors

Juni

2-3	Tools & Techniques for the beginning auditor
9-10	Introductie SAP internal Control Auditing
16 en 23	Voortgezette coachingsvaardigheden
17-18	Introductie Operational Auditing
23-24	Tools & Techniques for the beginning auditor

Wijzigingen voorbehouden. Een actueel cursusaanbod is beschikbaar op www.iia.nl.

Internationale Conferentie 2009

Van 10 tot 13 mei 2009 zal de Internationale Conferentie van het IIA plaatsvinden in Johannesburg, Zuid-Afrika. Dit zal de eerste keer zijn dat de Internationale Conferentie op het Afrikaanse continent plaatsvindt. Tijdens de conferentie zullen sessies worden georganiseerd met prominente sprekers uit het internationale internal auditvak. Meer informatie over de conferentie is beschikbaar via www.iiasa.org.za

UNIVERSITEIT VAN AMSTERDAM

Rondetafelbijeenkomst PAS over kwaliteitstoetsing bij kleine auditafdelingen

Auditafdelingen dienen tegenwoordig eenmaal in de vijf jaar getoetst te worden aan de hand van de IIA Standards. De ervaring leert dat dit de nodige vraagtekens en onzekerheden oproept, vooral bij kleine auditafdelingen.

In hoeverre kunnen kleine auditafdelingen aan alle standards voldoen? Wat zijn de consequenties als men een of meer standards niet kan navolgen? Wat is de positie van een auditafdeling als de directie van de betreffende organisatie (of de auditafdeling zelf) niet ten volle wil meewerken aan de toetsing?
De groep PAS (Professionele Audit Solisten) heeft het onderwerp al eerder in een themabijeenkomst behandeld; een overleg waarin ook het bestuur van het IIA participeerde. Op basis van de bij dat overleg opgedane ervaringen heeft PAS, in afstemming met het CPP (de Commissie Professional Practices van het IIA), nader onderzoek gedaan naar de toepasbaarheid van de standards voor kleine auditafdelingen.
Een tweetal werkgroepjes heeft zich vervolgens over de standards gebogen. De resultaten van dat onderzoek zijn in een document uitgewerkt, waarbij per standard is aangegeven in hoeverre deze attentie- of discussiepunten voor kleine IAD's oproepen en hoe kleine IAD's hier mee om zouden moeten gaan.

Discussie
Op 16 oktober jl. vond aan de UvA een rondetafelbijeenkomst plaats waarin PAS haar opvattingen en aanbevelingen van de twee werkgroepen over de IIA Standards presenteerde aan de deelnemers, waaronder ook vertegenwoordigers van het IIA-bestuur en de Commissie Kwaliteitstoetsing. Aan de hand van de resultaten van het onderzoek en een aantal stellingen vond een discussie plaats met het doel te komen tot uitspraken over kwaliteitstoetsing bij kleine auditafdelingen en aanpalende onderwerpen als accreditatie en zelfevaluatie.
De discussie concentreerde zich onder meer op het vraagstuk van de veelzijdigheid van activiteiten die kleine of beginnende auditdiensten uitvoeren, met daarbij de vraag in hoeverre dit conflicteert met de IIA Standards. Unaniem werd herkend dat veel control-initiatieven binnen de organisatie uit de koker van beginnende IAD's komen en dat auditors, als vermeende deskundigen op het gebied van control, worden 'uitgenodigd' om werkzaamheden in dit kader uit te voeren. Deze werkzaamheden omvatten veelal het introduceren van risk management, compliance en CRSA.
Volgens de standards zouden deze activiteiten in de lijn of bij andere stafdiensten moeten worden belegd. De opvatting was dat de IAD weliswaar input kan leveren voor nieuwe initiatieven bij inrichtingsvraagstukken, maar de IAD blijft de third line of defence, waarbij ook het auditen van de second line of defence tot de scope van audit behoort.

Groeimodel
Brede steun was er voor het idee om het IIA een groeimodel te laten ontwikkelen, een model waaraan kleine IAD's getoetst kunnen worden. Vanzelfsprekend zou dat model moeten bevorderen dat de kleinere IAD binnen een periode van een aantal jaren de status 'voldoet aan de standards' zou moeten kunnen bereiken.
Een andere stellingname van het PAS was of de quality assessments wel door het IIA uitgevoerd zouden moeten worden. De opvatting daarbij is dat het IIA niet zelf moet toetsen, maar de daarvoor in aanmerking komende instanties zou dienen te accrediteren.
Bij dit onderwerp kwam naar voren of ook 'eenpitters' praktisch gezien wel aan alle standards kunnen voldoen. Een van de praktische problemen daarbij is bijvoorbeeld de interne kwaliteitstoetsing van de auditwerkzaamheden. Het laten beoordelen van de kwaliteit van uitgevoerde werkzaamheden door externen of peers werd daarbij als mogelijke oplossing naar voren gebracht.

Aan het eind van de bijeenkomst werd het resultaat van het door PAS uitgevoerde onderzoek aan het IIA-bestuur overgedragen. Verdere uitwerking daarvan zal door de Commissie Vaktechniek ter hand worden genomen.

Terugblik ESAA-symposium

'De commissaris: de zwakste schakel in corporate governance?' was het thema voor de openingsbijeenkomst van het collegejaar 2008-2009 van de Erasmus School of Accounting & Assurance. Het door meer dan vierhonderd studenten en alumni bezochte symposium vond plaats op vrijdag 5 september 2008 aan de Erasmus Universiteit Rotterdam.

Sprekers

Prof.dr. S.J. Maijoor (Autoriteit Financiële Markten) gaf zijn visie op de ontwikkelingen in corporate governance. Prof.dr. J.A. van Manen (PwC) ging in op de relatie tussen de raad van commissarissen en de externe accountant tijdens een crisissituatie. Prof.dr. M.N. Hoogendoorn RA besprak casuïstiek met betrekking tot goed bestuur zoals deze bij de Ondernemingskamer aan de orde komt. Ook de relatie tussen CFO en de commissaris (mr.drs. C.M.J.van Rijn, CFO Nutreco) en de relatie tussen private equity en de commissaris (drs, H.P.M. Stolker, kernteamlid Programma voor Commissarissen en Toezichthouders ESAA) kwamen aan de orde. De middag werd afgesloten met een levendige paneldiscussie onder leiding van prof. J.C.A. Gortemaker RA, directeur ESAA.

Module BIV/AO

In januari 2009 start weer een nieuwe serie colleges BIV/AO. De module BIV/AO maakt deel uit van het curriculum van de opleiding I/OA en IT-auditing. De module kan echter ook los worden gevolgd op vrijdag overdag.
Voor nadere informatie: www.esaa.nl of via tel.nr. 010-4082217.

ERASMUS UNIVERSITEIT ROTTERDAM

Afgestudeerd in september en oktober 2008

In september en oktober 2008 hebben de volgende studenten slotexamen afgelegd voor de opleiding I/OA:

Carlo Bavius	Eneco Energie
Gerrit Elsinga	Aegon nv
Gabriëlle ter Hart	Ernst & Young Advisory
Miranda Hesselink	ABN Amro Bank nv
Roy Jansen	Ministerie van Defensie
Arie van Krimpen	KPMG
Caroline Meun	Klaverblad Verzekeringen
Patrick Pershad	ANWB bv
Marijke van der Ploeg	Interpolis Verzekeringen nv
Erik Pothast	EDP Audit-Pool
Ashwin Ramcharan	ING Bank
Gerrit-Jan Spruijt	Quion
Reinier de Vries	Syngenta Seeds bv

Samenwerking kopjaren ESAA en NIVRA-Nyenrode

De Erasmus School of Accounting & Assurance en NIVRA-Nyenrode School of Accountancy & Controlling gaan samenwerken. Ze zijn overeengekomen om de kopjaren Executive Master in IT-Auditing en Executive Master in Internal Auditing samen aan te bieden. Dit betekent dat er voor studenten de mogelijkheid bestaat om zowel in Rotterdam als in Breukelen een van deze kopjaren te volgen. De komende tijd zal er verder vorm worden gegeven aan deze samenwerking.

Feestelijke buluitreiking

Op 28 oktober jl. vond de derde gezamenlijke buluitreiking plaats voor afgestudeerden van de postinitiële masteropleidingen Internal/Operational Auditing en IT-Auditing in hotel New York in Rotterdam.
Studenten die in de periode juni tot en met oktober 2008 zijn afgestudeerd, konden in daar hun bul in ontvangst nemen. De voorzitter van het curatorium van de beide opleidingen, Lex van der Drift, richtte namens het curatorium het woord tot de studenten en gaf onder andere het belang aan van de aandacht voor soft controls in moderne organisaties.

De feestelijke buluitreiking

De financiële crisis: door het ijs gezakt?

Dr. J.R. van Kuijck*

In de vorige column gaf ik aan dat Europa op de rand van een recessie balanceert. Maar na de ontwikkelingen in de herfst van 2008 is het duidelijk; niet alleen de VS en Europa storten zich in een recessie, ook andere delen van de wereld. Het vertrouwen in de financiële wereld is compleet zoek en dat heeft een verlammend effect op de geldstromen tussen alle marktpartijen. Als goudspuiten voor reumapatiënten worden wereldwijd geldinjecties aan grote banken en andere financiële instellingen toegediend. Ze moeten de patiënt weer op de been helpen. Maar het lijkt tevergeefs en de beurzen laten een jojo-effect met een negatieve trend zien. De afgelopen tijd is de beurswaarde van ondernemingen verdampt en dalen dekkingspercentages van pensioenfondsen. Langzaam maar zeker wordt de omvang en het effect van de crisis duidelijker. Wie had vooraf kunnen bedenken dat NINJA-hypotheken en opportunistische bankiers zouden kunnen zorgen voor het op de kop zetten van de financiële wereld en de reële economie?

Je zult net in die periode een sabbatical plannen. En ook nog eens een deel van je spaartegoed parkeren bij Icesave dat door het ijs zakt. Dom om te sparen bij Icesave? Sommigen zeggen: de spaarders waren te hebberig en hadden dit aan kunnen zien komen. Immers, zo'n hoge rente kon je bij geen enkele andere Nederlandse bank krijgen. Dat er concurrentie bestaat en de hoogte van de rente op spaartegoeden door Nederlandse banken op een structurele wijze wordt getemperd, vergeten we gemakshalve maar even. Maar gelukkig was niet alleen de individuele spaarder dom geweest. Naar later bleek waren dat ook lagere overheden zoals provincies en gemeenten. Nu zijn ineens alle Nederlandse burgers door het ijs gezakt!
Weer anderen zeggen dat IJsland financieel gezien het wilde Westen was en op omvallen stond. Maar mag je niet meer vertrouwen op garanties die een centrale bank van een geciviliseerd land afgeeft, laat staan op de overheid? Kennelijk niet meer! Waar was onze DNB eigenlijk? Hadden zij de vergunning moeten geven aan Icesave, een bijkantoor van de Landskibank? Natuurlijk, zij waren verplicht, conform Europese regelgeving, de eerste verdedigingslinie van DNB. Het bijkantoor viel keurig onder het toezicht van IJsland en er was een depositogarantie van kracht. Maar de DNB is in haar toezicht tekortgeschoten omdat de bank ook onder een aanvullende Nederlandse depositogarantie viel. Volgens econoom Sweder van Wijnbergen verschafte DNB Icesave impliciet een verklaring van goedgedrag toen de toezichthouder de vergunning verleende aan de vermeende cowboys om op de Nederlandse spaarmarkt te opereren. Kunnen we nog vertrouwen op DNB of de Staat der Nederlanden?

Managers, toezichthouders, centrale banken, rating agencies, auditors en overheden zijn de afgelopen maanden door het ijs gezakt. Mensen voelen zich bedrogen en met een kluitje in het riet gestuurd. Veel internal auditors van financiële instellingen vragen zich openlijk af of zij ook niet hebben gefaald. Dat zijn zij ook aan hun stand verplicht. Het antwoord op deze vraag zal helpen om de nieuwe toekomst te bouwen.
Laten we ook positief zijn. Wij hebben mooi ABN Amro weer terug, genationaliseerd en wel, dus wat kan er nog misgaan!? Bovendien hebben we Rijkman Groenink nog die kenbaar heeft gemaakt De Bank – en daarmee volk en vaderland – te willen dienen. Net wat we nodig hebben!? Op langere termijn komt het ook goed. Lees het boek *The Ascent of Money – a Financial History of the World* van Niall Ferguson en u zult zien dat alles goed komt. Vertrouw me!

* Geniet thans van een sabbatical. Voorheen CAE bij VION Food Group (vankuijck.bob@hetnet.nl).

THE PROTIVITI INTERNAL AUDIT PORTAL

This electronic workpaper application is the latest addition to our world-class Protiviti Governance Portal.

- Provides a central repository for your audit work
- Facilitates the audit process from risk assessment through execution
- Provides management and the audit committee with dashboards and reporting
- Improves audit efficiency, accuracy and quality through standard templates and process guidance
- Integrates seamlessly with our Sarbanes-Oxley, Operational Risk and Self Assessment modules to give a complete picture of governance

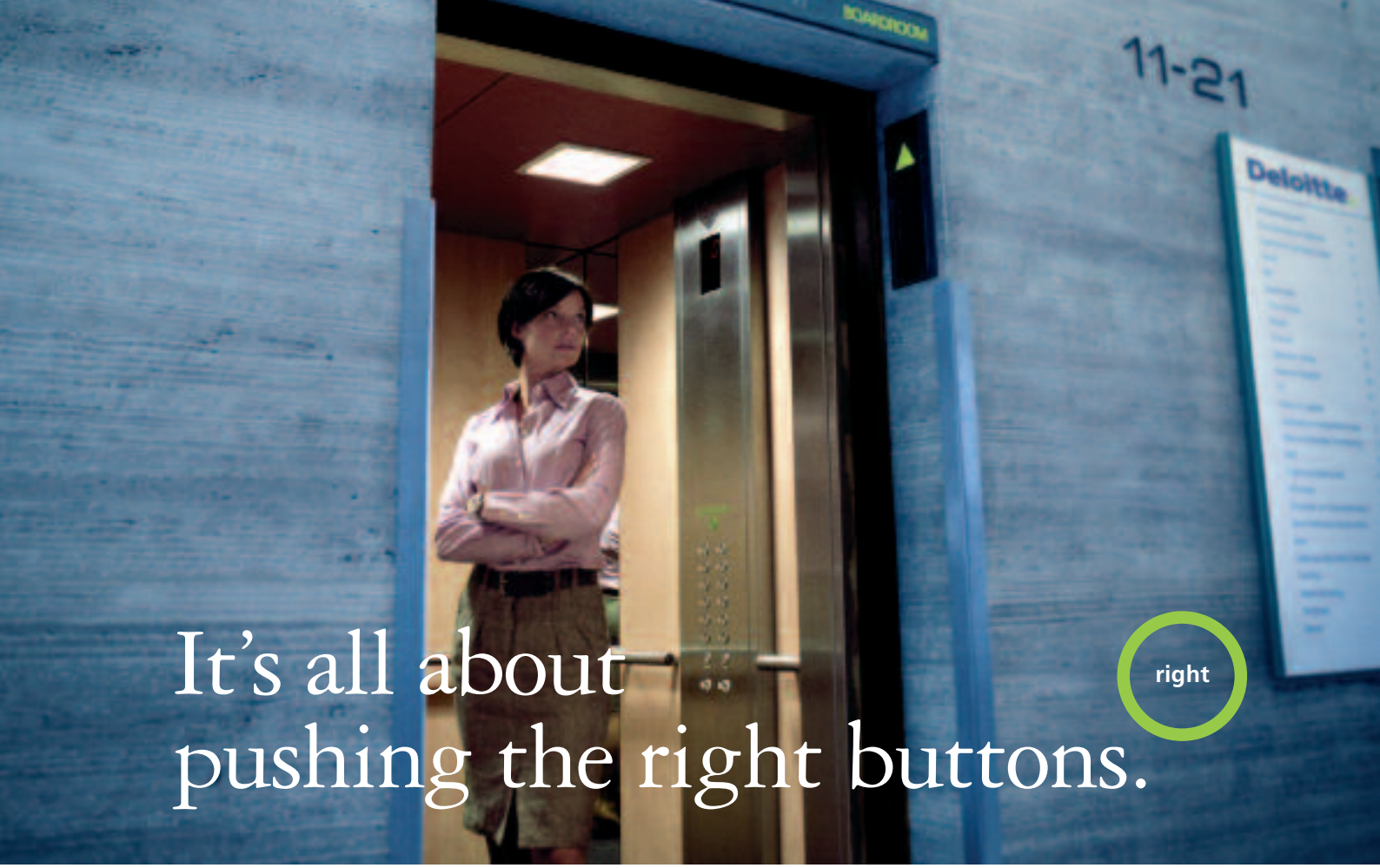
---

To learn more about our technology solutions or to schedule a demonstration, contact us at 020 346 04 00 or mail marketing@protiviti.nl.

protiviti®
Independent Risk Consulting

Know Risk. Know Reward.™

The Institute of Internal Auditors
PRINCIPAL PARTNER



It's all about pushing the right buttons.

right

Carrière maken een kwestie van een druk op de juiste knop? Niet dus, dat weet jij inmiddels ook wel. Carrière maken vergt heel wat meer. Ambitie, gedrevenheid. Vakkennis. Passie voor je vak. Sociale kwaliteiten. En natuurlijk: talent. Maar groeien, vooruit komen, jezelf ontwikkelen – het vraagt nog meer: een omgeving waarin je talenten ook werkelijk tot hun recht kunnen komen. Waarin veelbelovende professionals als jij herkend worden en de ruimte krijgen om hun knowhow, hun gevoel voor het vak en affiniteit met klanten voortdurend te scherpen. Een omgeving zoals Deloitte dus.

Deloitte is met ruim 6.000 medewerkers en kantoren in heel Nederland de grootste organisatie op het gebied van Belastingadvies, Accountancy, Consultancy en Financieel Advies. ERS houdt zich bezig met dienstverlening voor ondernemingen, gericht op de controle van de processen en de IT-architectuur achter de cijfers. Dat betekent het signaleren, analyseren, beoordelen en managen van risico's. Variërend van boardroom-risico's op strategisch niveau tot technische risico's op netwerkniveau, zowel in een adviserende als controlerende rol. Buitengewoon uitdagend en afwisselend werk voor ambitieus talent. Voor iemand als jij dus!

Voor Deloitte Enterprise Risk Services zoeken we wo-ers met een bedrijfskundige of IT-gerelateerde studie en werkervaring vanaf 3 jaar. Met interesse in een van de volgende werkgebieden:

IT-Auditors
Specialisten die zich bezighouden met onderzoek naar de kwaliteit van de beheersing van IT-risico's en vraagstukken op het gebied van Corporate en IT Governance.

Applicatiespecialisten
Consultants die betrokken zijn bij het adviseren, controleren en implementeren van control frameworks en beveiliging van ERP-applicaties (SAP, Oracle, JD Edwards, Peoplesoft).

Security-specialisten
Professionals die adviseren over complexe security-systemen en bijbehorende processen (beveiliging, netwerken, hacking, privacy) en deze controleren en implementeren.

Data-specialisten
Je richt je o.a. op fraudedetectie in databestanden; ondersteuning bij accountantscontrole m.b.v. data-analyse; econometrische modelbouw en research om specifieke klantvraagstukken op te lossen; conversie en opschoning van data in IT-systemen als SAP, Oracle, JD Edwards.

Softwarespecialisten
Je ontwerpt en bouwt internettoepassingen met de nieuwste Microsoft-technologie. En je werkt in een multidisciplinair team van specialisten aan web-oplossingen om Deloitte en haar cliënten te ondersteunen.

Riskconsultants/internal auditors
Je werkt aan opdrachten op het gebied van enterprise-wide risk management en internal audit, die je in multidisciplinaire teams uitvoert bij onze grote internationale klanten.

Deloitte biedt je een ruime mate aan afwisseling en uitstekende doorgroeimogelijkheden. Internationale trainingen, postdoctorale opleidingsmogelijkheden, een informele werksfeer: dat is typisch Deloitte. We vragen veel van je, maar geven je ook veel ruimte. Meer weten over onze vacatures binnen ERS of solliciteren? Ga dan naar onze website www.careers.deloitte.com. Je kunt ook contact opnemen met Mina Bahaj, telefoonnummer 020 - 454 74 34, e-mail: mbahaj@deloitte.nl.

Deloitte.

Audit . Tax . Consulting . Financial Advisory.

TreasuringTalent.com