Crisislessen voor interne audit

Hoe functioneren afdelingen internal audit en governance, risk & compliance (GRC) bij niet-financiële sector. Een onderzoek en discussie in de slagschaduw van de financiële crisis.

TEKST **BERT BAKKER** | BEELD **MARJA BROUWER**

'Het glas is per saldo meer half vol dan half leeg.' Dat concludeerde San Croonenburg, projectleider van het NIVRA-onderzoek naar het functioneren van afdelingen internal audit en GRC (governance, risk & compliance) bij niet-financiële ondernemingen dat 25 mei 2010 werd gepresenteerd tijdens een discussiebijeenkomst georganiseerd door NIVRA en IIA.
Achtergrond van dat relatieve positivisme – ondanks de niet weg te poetsen inschattingsfouten die de afgelopen jaren in bijna alle organisaties zijn gemaakt – was dat de 53 hoofden van internal audit- en GRC-afdelingen die aan een enquête meededen, kennelijk het gevoel hebben dat hun werk door de top van hun ondernemingen redelijk goed wordt gezien en gehoord. Uit deze enquête bleek dat ongeveer driekwart van die afdelingen rechtstreeks aan een ceo rapporteren en de overige aan de cfo. En ondanks de obstakels die er soms zijn, vindt men ook dat de communicatie tussen de afdelingen internal audit en GRC – die samen met het lijnmanagement onderdeel vormen van het *three lines of defence-model* dat ondernemingen moet beschermen tegen ongewenste risico's – redelijk verloopt. Ondervraagden lieten overigens wel weten dat ze (te) weinig aanwezig konden zijn bij vergaderingen van de raden van bestuur en commissarissen. En – opmerkelijk – een derde van de ondervraagden vindt zichzelf beperkt geëquipeerd om de onderlinge samenhang van risico's te beoordelen.
De bijeenkomst was onder meer belegd om reacties op de enquêteresultaten te registreren van mensen uit het vak. Samen met een literatuuronderzoek worden die gebundeld in een eindverslag dat deze zomer moet uitkomen.

'TE MILD'

Maar tijdens de discussie die zich met NIVRA's directeur Public Trust Robert Mul als moderator ontspon na de presentaties tussen inleiders, panelleden en deelnemers in de zaal bleek wel dat menigeen de indruk had dat de geënquêteerden toch een wat te mild oordeel over zichzelf hadden.
Panellid Jan van de Poel, emeritus-hoogleraar risk management in Maastricht, auteur van een boek over het Ahold-boekhoudschandaal: "Ik kan niet geloven dat tweederde van de internal auditors en GRC-managers tevreden zijn over de onderlinge informatie-uitwisseling, zoals de enquête suggereert."
Maar nog veel kritischer over de prestatie en positionering van het gecombineerde vakgebied was Leen Paape, hoogleraar en dean aan de Nyenrode School of Accounting & Control.
"Wat moeten wij ervan denken dat de functie van de interne auditor in het rapport van de commissie De Wit onlangs maar één keer werd genoemd? En dat de commissie Maas pas na verschijning van zijn rapport iets zei over het belang van goede rapportage van een internal auditafdeling? Betekent dit niet dat GRC en internal audit zich moeten herdefiniëren?"

Jan van de Poel: 'Liever een slager die zijn eigen vlees keurt, dan eentje die meer interesse heeft in compliance dan in wat ie verkoopt.' ▶

RISICO-REGEL-REFLEX

Mede gevoed door een nogal ontnuchterend Amerikaans onderzoek waarin wordt gepoogd te inventariseren wat bepaalt hoe volwassen een afdeling enterprise risk management in een organisatie is en hoe effectief, vroeg Paape zich hardop af of raden van bestuur en commissarissen wel echt begrijpen wat internal audit en GRC beogen en wat ze vermogen. "Is er niet sprake van een hype, aangejaagd door een risico-regel-reflex?", vroeg hij zijn gehoor. "Zijn we wel op de goede weg door na elke crisis nieuwe regels te willen introduceren? Zou het niet beter zijn om waar mogelijk regels juist at te schaffen, zodat niemand zich meer daarachter kan verschuilen? En moeten we niet ophouden meer te pretenderen dan we kunnen waarmaken door te zeggen: 'incidenten gebeuren nu eenmaal dus wen er maar aan'?"

BRANDBLUSSER

Inleider Wim Eysink, partner bij Deloitte *Enterprise Risk Services*, legde er in zijn betoog nadruk op dat de drie verdedigginglijnen – uitvoerend management, risk management en internal audit – niet alleen naar boven moeten rapporteren, maar dat de drie lagen en ook de top van de onderneming elkaar relevante feedback moet terugsturen. "Ik vraag me af of we niet moeten vaststellen dat dit model ons te veel bezig laat zijn met verantwoording afleggen en te weinig met wat je met de ingewonnen informatie kunt doen qua sturing. En als althans internal audit zo compliance-gericht is, moeten we daar dan niet aan verwachtingsmanagement doen?" Eysink zei daarmee impliciet dat de buitenwereld veronderstelt dat als een internal auditor een vuur ziet, hij wel een brandblusser zal grijpen, maar feitelijk geeft hij slechts een brandmelding door.

'THIS TIME IS DIFFERENT'

Ten slotte legde Eysink zijn toehoorders ook de hamvraag voor: Bewees de laatste crisis niet dat de risico- en controlesystemen in de financiële sector hebben gefaald? Het antwoord dat panellid Jim Emanuels, hoogleraar bestuurlijke informatieverzorging aan de Rijksuniversiteit Groningen daarop gaf, weerspiegelt waarschijnlijk precies wat er in het vakgebied wordt gedacht en waarom het zelfbeeld tamelijk ongeschonden bleef. Maar ook waarom de wereld daarbuiten dat zo moeilijk snapt. "In academische zin", zei Emanuels, "hebben de systemen niet gefaald. Ze faalden alleen in praktische zin". Van de Poel, hoe kritisch ook over zijn eigen vak, steunde die paradoxale vaststelling door te verwijzen naar het boek *This Time Is Different* van Carmen Reinhart en Kenneth Rogoff. Daarin wordt aannemelijk gemaakt dat nooit zoveel tijd en geld in risicomonitoring, -beheersing en -rapportage is gestoken als in de vijftien jaar, maar dat wanneer een mondiaal vertakt financieel systeem ineens instort, een probleem ontstaat dat simpelweg te groot is voor risk managers van individuele bedrijven. Van de Poel: "Strikt genomen was de geleverde inspanning inderdaad voldoende."

Opmerkelijkste resultaten uit interviews

Meest gehoorde opmerkingen uit 28 interviews bij 22 (middel)grote organisaties in de niet-financiële sector, samengevat in suggesties voor internal auditors en gecombineerde IA-GRC-afdelingen

Do's voor internal audit sec:

- Zorgen voor transparant en goedgekeurd auditproces.
- Continue verbeteren auditproces.
- Verbeteren integratie kennis over de onderneming bij internal audit.

Do's voor Internal Audit en GRC:

Risicomanagement afstemmen op organisatie.

- Bewustworden samenspel en cumulatie van risico's.
- Hanteren van één GRC-begrippenstelsel.
- Bewustworden invloed kredietcrises en recessie.
- Versterking verschillende GRC-relaties.
- Bouwen en onderhouden GRC-beheersingskader.
- Evalueren positionering internal audit en GRC.

Het onderzoek is uitgevoerd door San Croonenberg, projectleider en coördinator internal audit Koninklijk NIVRA.

▼ Jim Emanuels (RUG): 'In academische zin hebben de systemen niet gefaald. Ze faalden alleen in praktische zin.'

◀ Wim Eysink (Deloitte): 'Als internal audit zo compliance-gericht is, moeten we dan niet aan verwachtingsmanagement doen?'

▲ Marnix den Heijer (Aercap): 'Het gevaar van een separate risk managementafdeling is dat het tot schijnzekerheid kan leiden.'

◀ Leen Paape (Nyenrode): 'Zou het niet beter zijn om waar mogelijk regels juist af te schaffen, zodat niemand zich meer daarachter kan verschuilen?'

HOUD HET SIMPEL

Dat de professie desondanks piekert over welke lessen er uit de recente crisis moeten worden getrokken en welke alternatieven er zijn te bedenken voor het op papier mooie maar in de praktijk toch haperende *three lines of defense*-model, bleek uit de uitnodiging aan Marnix den Heyer, hoofd internal audit en *corporate council* bij de Nederlandse vestiging van het vliegtuigleasebedrijf Aercap, om te vertellen hoe GRC en internal audit daar zijn georganiseerd. Zijn boodschap: hou het simpel en overzichtelijk. Leg de verantwoordelijkheid voor risk management en compliance bij het lijnmanagement en je hebt geen aparte GRC-afdeling nodig.
Reden om voor deze oplossing te kiezen was volgens Den Heijer: "Vrees voor bureaucratie en vinkgedrag. Het gevaar van een separate risk managementafdeling is dat het tot schijnzekerheid kan leiden."

SLAGER

In de wereld van internal audit, risk management en compliance loopt al enige tijd de discussie of de functies niet effectiever uitgevoerd zouden worden als ze werden samengevoegd. Governance-technisch kent dat bezwaren, maar een motief er vóór (zie 'de Accountant' januari/februari 2010), is dat een combinatie van de taken het werk interessanter en verantwoordelijker maakt. Daardoor zouden makkelijker ambitieuze mensen met sterkere communicatieve vaardigheden voor de functie kunnen worden aangetrokken. En dat alleen al zou de effectiviteit van IA-GRC vergroten.
Kennelijk bestond er op dat vlak wel consensus tussen Paape, Eysink en ook Van de Poel: met alleen regeltjes naleven red je het niet.
Op de voorgelegde stelling: Een interne auditor die risk management adviseert én er *assurance* over verschaft, is als een slager die zijn eigen vlees keurt, reageerde Van de Poel met: "Nou ik ga liever naar zo'n slager dan naar eentje die meer interesse heeft in compliance dan in wat ie zijn klanten verkoopt." □

Opmerkelijkste resultaten uit de enquête

Positie GRC en IA ten opzichte van bestuur en commissarissen onderneming
- Eindverantwoordelijkheid voor GRC ligt meestal bij raad van bestuur (79 procent).
- GRC-onderwerpen vaak op agenda raad van bestuur, raad van commissarissen en commissies, maar GRC-functies niet altijd aanwezig.
- Het lijkt het makkelijkst aanschuiven bij commissies.
- 47 procent van de internal auditors zowel betrokken bij inrichting als beoordeling GRC.

Rapporteringslijnen:
- 67 procent van de hoofden internal audit rapporteren aan de ceo (29 van 43).
- 64 procent van de gecombineerde hoofden internal audit, risico management en compliance rapporteren aan de CEO (zes van tien).
- Twintig procent van beiden groepen rapporteren aan de cfo (twaalf van 53).

Informatie-uitwisseling internal audit en GRC-functies:
- Informatie-uitwisseling zowel formeel als informeel (procent gelijk) en frequentie heel divers.
- 67 procent tevreden met huidige informatie-uitwisseling.

GRC-verantwoordelijkheid en begrippen:
- 73 procent vindt GRC-verantwoordelijkheden eenduidig belegd.
- 65 procent vindt GRC-begrippenstelsel eenduidig belegd in dezelfde taal.

Wie kijkt naar onderlinge verband van risico's?
- 69 procent antwoordt: internal audit.
- 72 procent antwoordt: risicomanagement.
- Dertig procent antwoordt: compliance.

Voldoende of onvoldoende geëquipeerd?
- 33 procent vindt internal audit en GRC-functies beperkt geëquipeerd om onderlinge samenhang risico's te beoordelen.

Ruimte voor verbetering?
- Informatie-uitwisseling (67 procent).
- Eenduidigheid GRC-verantwoordelijkheden (73 procent).
- Eenduidigheid GRC-begrippen (65 procent).
- Beoordelen onderlinge risicoverbanden (67 procent).