de interne accountant

Onder invloed van de corporate governance-regelgeving doen steeds meer organisaties serieus aan risicomanagement. Van een formeel beleid is echter meestal nog geen sprake. Van de grote bedrijven legt zestien procent de risico-managementfunctie in handen van de interne audit-afdeling. Opvallenderwijs hebben institutionele beleggers - die er juist van profiteren - weinig aandacht voor risicomanagement. Een onderzoek.

DENNIS FRERIKSEN, DANIËL GOUDEKET, LEEN PAAPE EN DIRK SWAGERMAN*

Risico's in be

Eind 2004 hielden PricewaterhouseCoopers en de Rijksuniversiteit Groningen een enquête onder de leden van het Controllers Instituut over de toepassing van risicomanagement in hun organisatie. De enquête leverde 283 reacties op**.

De toepassing van risicomanagement heeft in Nederland in de afgelopen jaren een vlucht genomen, zo blijkt uit de resultaten.

Voerde drie jaar geleden nog slechts negentien procent van de organisaties in Nederland integrale risicoanalyses uit, begin 2005 was dat al 66 procent en nog eens 26 procent geeft aan dat in de toekomst te willen gaan doen.

In de meeste organisaties waar risicoanalyses worden uitgevoerd gebeurt dit jaarlijks (34 procent), maar ook per kwartaal komt regelmatig voor (26 procent). Halfjaarlijks is een stuk minder gebruikelijk (zeven procent).

Hierbij kan natuurlijk de vraag worden gesteld wanneer er sprake is van een echte risicoanalyse en wanneer het slechts een update van een eerder opgebouwd risicoprofiel betreft.

Grote projecten

Een in de praktijk veel voorkomende en goed werkbare vorm is een jaarlijkse diepgaande risicoanalyse, gekoppeld aan het opstellen van het jaarplan en budget. Gedurende het jaar, meestal per kwartaal, wordt vervolgens het risicoprofiel nog eens tegen het licht gehouden om te kijken of er significante wijzigingen zijn opgetreden. Deze minder diepgaande analyse wordt vaak gekoppeld aan het opstellen en bespreken van de kwartaalrapportage.

Bij grote projecten en investeringsbeslissingen worden blijkens de enquête nog slechts in beperkte mate risicoanalyses uitgevoerd.

Opvallend, omdat juist in deze situaties, met hun onzekerheid en grote belangen, een gedegen risicoanalyse zeer waardevol kan zijn.

Planning & controlcyclus

Risicomanagement is een continu proces dat op diverse plekken in de organisatie wordt doorlopen. Vijf basisstappen maken (impliciet) onderdeel uit van elk risicomanagementproces: identificeren, analyseren, reageren, monitoren en rapporteren.
Een praktische manier om de continue werking van dit proces te waarborgen is door het te koppelen aan de verschillende stappen van de planning & controlcyclus. Uit de enquête blijkt dan ook dat 77 procent van de ondervraagde organisaties het risicomanagement daar volledig (25 procent) of gedeeltelijk (52 procent) in heeft geïntegreerd.

Zoals kon worden verwacht is dit in grotere organisaties al vaker het geval dan in kleinere. In 89 procent van de organisaties met meer dan één miljard omzet is risicomanagement (deels) in de planning & control geïntegreerd.

Formeel beleid

Ondanks dat risicomanagement redelijk gemeengoed begint te worden, is de toepassing ervan vaak nog niet verankerd in een formeel beleid. In slechts 39 procent van de gevallen heeft het topmanagement een risicomanagementbeleid geformuleerd en gecommuniceerd. Ook bij de beursgenoteerde ondernemingen, waar gezien de wettelijke eisen een aanzienlijk hoger percentage mag worden verwacht, heeft nog slechts 56 procent een formeel risicomanagementbeleid.

FOTO'S: MARJA BROUWER

De financiële sector springt er met 61 procent nog relatief hoog uit, gevolgd door de energie- en *utilities*-bedrijven met 53 procent.
Overheid en non-profit blijven duidelijk ver achter met elf procent.

COSO meest gebruikt

Wereldwijd hebben verschillende instanties standaarden ontwikkeld voor de vormgeving van risicomanagement. De meest recente en bekende is het *COSO Enterprise Risk Management - Integrated Framework* uit 2004, dat voortborduurt op het *COSO Internal Control - Integrated Framework* uit 1992. Andere standaarden vinden vaak hun oorsprong binnen een bepaalde branche of bepaald land *(zie kader).*
Uit de enquête blijkt dat het merendeel van de organisaties in Nederland (63 procent) een openbare standaard als uitgangspunt heeft genomen. Opvallend daarbij is dat de overheid en non-profitsector hierbij extra hoog scoren (79 procent).
Bijna driekwart van de respondenten die gebruikmaken van een standaard, hanteren COSO. Veelal is onduidelijk of zij daarmee verwijzen naar het COSO ERM Framework of het COSO Internal Control Framework.
Andere gehanteerde standaarden zijn ABIB, Bazel II, Solvency II en de Australian/New Zealand Standard. Ook enkele minder expliciet aan risicomanagement gekoppelde concepten en theorieën zoals het INK-model, CobiT, Six Sigma en de typologie van Starreveld, worden genoemd als basis voor het risicomanagement in de organisatie. Veel respondenten geven aan dat uit meer bronnen is geput, waar vervolgens een organisatiespecifieke uitwerking aan is gegeven.

Finance & control

In organisaties met bewust en expliciet risicomanagement zullen de desbetreffende activiteiten door een bepaalde afdeling of functionaris moeten worden gecoördineerd. De risicomanagementfunctie kan op verschillende plekken in een organisatie worden belegd. Ook kan worden gekozen voor het inrichten van een afzonderlijke risicomanagementafdeling.
Van de grote organisaties geeft 97 procent aan op enigerlei wijze ergens in de organisatie een risicomanagementfunctie te hebben belegd. ▶

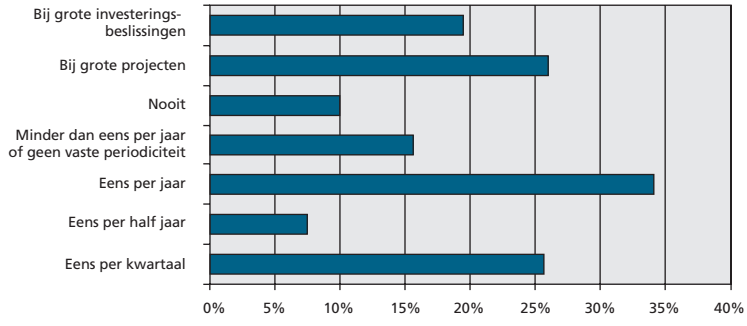
Bij grote projecten en investeringsbeslissingen worden nog slechts in beperkte mate risico-analyses uitgevoerd.

Bij middelgrote organisaties is dit 76 procent en bij kleine 59 procent.
Kleine en middelgrote organisaties beleggen de risicomanagementfunctie vooral bij de finance & control-afdeling (44 procent respectievelijk 42 procent). Ook bij grote ondernemingen is dit vaak het geval (veertig procent), maar 26 procent van de grote ondernemingen heeft een zelfstandige risicomanagementafdeling ingericht en bij zestien procent neemt de internal audit-afdeling de risicomanagementfunctie op zich.

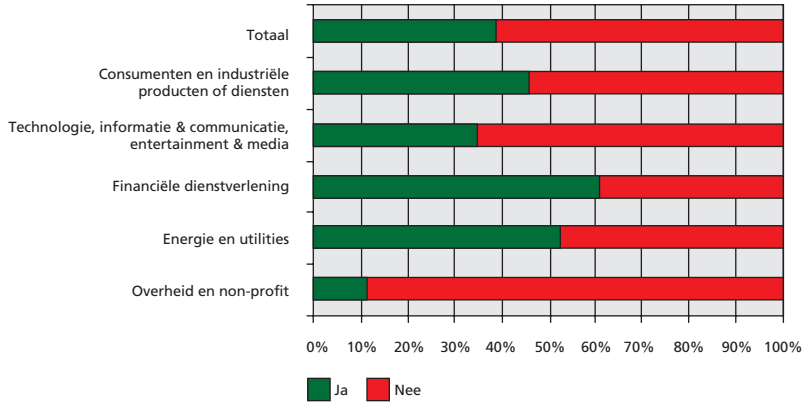
Internal audit

Risicomanagement is een integrale verantwoordelijkheid van elke manager. In de ideale situatie zou er dan ook geen aparte risicomanagementondersteunende functie nodig moeten zijn. Deze situatie zal echter niet snel worden bereikt, en daarom is het goed dat deze functie ergens in een organisatie expliciet wordt belegd. De meest geschikte plek verschilt per organisatie. De omvang van het takenpakket zal afhangen van de grootte van de organisatie. Zoals gezien kiezen grote organisaties soms voor een aparte afdeling. In kleinere organisaties is dit veelal niet kostenefficiënt en wordt deze risicomanagementfunctie gecombineerd met andere functies. Elke oplossing heeft voor- en nadelen.
Met name aan het beleggen van de risico-

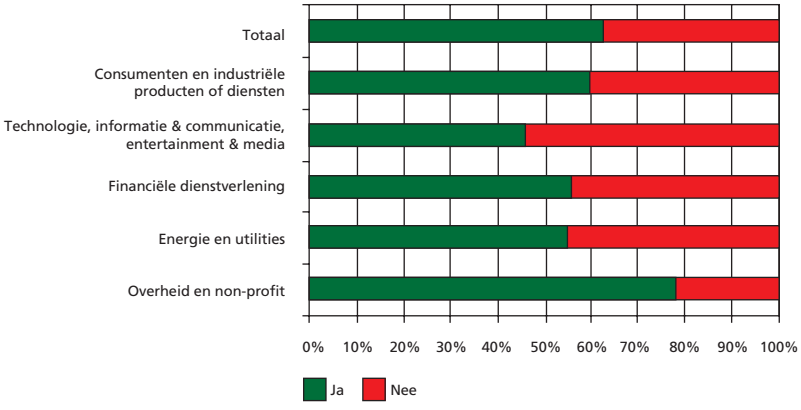
Hoe vaak dient het management een risico-inventarisatie en-analyse uit te (laten) voeren en hierover te rapporteren?



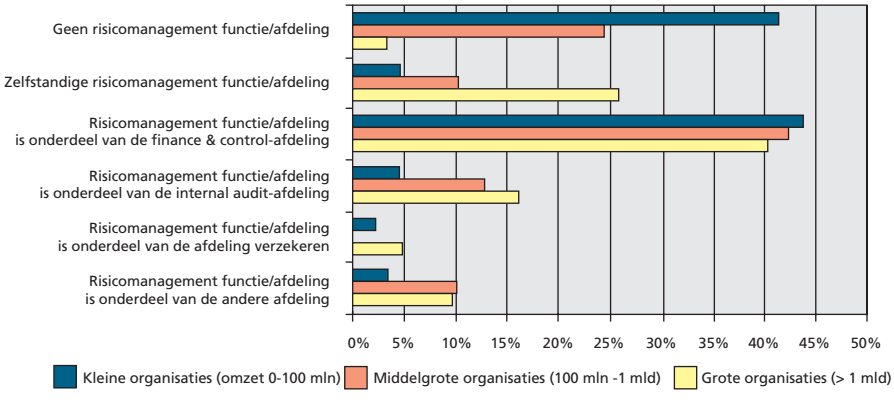
Heeft het topmanagement een risicomanagementbeleid geformuleerd en gecommuniceerd?



Is het risicomanagementbeleid ingericht volgens een bepaalde risicomanagement standaard?



Hoe is de risicomanagement (ondersteunende) functie belegd?



Standaarden voor risicomanagement

Andere standaarden dan het bekende COSO-model vinden vaak hun oorsprong binnen een bepaalde branche of bepaald land.
Zo is er de *Australian/New Zealand Risk Management Standard 4360* waarvan reeds in 1995 de eerste versie werd uitgegeven door de *Council of Standards* van beide landen. In 1999 en in 2004 verscheen een geactualiseerde versie van deze standaard.
Voorbeelden van branchespecifieke risicomanagementstandaarden zijn Bazel II voor het bankwezen en Solvency II voor de verzekeringsbranche. Ook de Internationale Organisatie voor Standaardisatie (ISO) heeft inmiddels van zich laten horen op het terrein van risicomanagement: in 2002 verscheen een richtlijn voor het gebruik van risicomanagementtermen in standaarden (ISO/IEC Guide 73).

Aan het beleggen van de risicomanagementfunctie bij de internal audit-afdeling kleven belangrijke nadelen.

managementfunctie bij de internal audit-afdeling kleven belangrijke nadelen. Het is immers juist deze afdeling die de kwaliteit van het risicomanagement in de organisatie voortdurend tot object van onderzoek heeft. Als deze afdeling daar echter ook zelf een verantwoordelijkheid voor draagt, kan een belangenconflict ontstaan. In voorkomende gevallen kan uit praktische overwegingen toch voor deze opzet worden gekozen, maar dan is het zaak om het belangenconflict zo veel mogelijk voor te zijn door duidelijk aan te geven waar de verantwoordelijkheid van internal audit ophoudt en die van het management begint.

Wet- en regelgeving

De belangrijkste reden waarom de toepassing van risicomanagement de afgelopen jaren een vlucht heeft genomen is waarschijnlijk de corporate governance wet- en regelgeving in diverse landen. Deze stelt strenge eisen aan het risicomanagement van beursgenoteerde ondernemingen.
Steeds luider wordt echter de vraag gesteld of wet- en regelgeving wel de juiste drijfveer is voor risicomanagement. Zo kampen bedrijven in de Verenigde Staten met de onzekerheid hoe ze aan de Sarbanes-Oxley Act moeten voldoen. Als gevolg daarvan steeg het aantal grote bedrijven (marktkapitalisatie meer dan $100 miljoen) dat zijn jaarlijkse rapport over het interne systeem voor risicomanagement en -beheersing te laat indient tussen 2003 en 2004 van 59 tot 282.

Check-the-box-mentaliteit

Ook de in eind 2003 verschenen Nederlandse code Tabaksblat lijkt wellicht niet de juiste drijfveer voor risicomanagement te zijn.
Volgens deze code moet een vennootschap als onderdeel van het 'interne risicobeheersings- en controlesysteem' onder meer risicoanalyses uitvoeren van de 'operationele en financiële doelstellingen'.
Aandacht voor risicomanagement is in beginsel een goede zaak, maar het verankeren daarvan in wetgeving, zou een *check-the-box-mentaliteit* kunnen veroorzaken. Voldoen aan regelgeving is dan het hoogst haalbare en een gedegen risicomanagement zelf zou dan bijzaak kunnen worden.
Daarom zou het goed zijn als de druk om meer werk van risicomanagement te maken ook uit een andere dan de wetgevende hoek zou komen: die van de institutionele beleggers.

Bij beursgenoteerde ondernemingen heeft nog slechts 56 procent een formeel risicomanagementbeleid.

Institutionele beleggers

Via de aandelenprijs, kredietprijzen en *ratingen* zijn institutionele beleggers in staat om adequaat risicomanagement af te dwingen bij ondernemingen. Een geïnteresseerde belegger krijgt op dit gebied meer voor elkaar dan regels.
Dat institutionele beleggers hier tot nu toe weinig aandacht voor hebben gehad blijkt uit contacten met cfo's van beursgenoteerde bedrijven. Institutionele beleggers en analisten vragen slechts zelden naar risicomanagement en interne beheersing, terwijl juist zij degenen zijn die er direct van profiteren.
Een duidelijker interesse van beleggers in het onderwerp zou een belangrijke impuls betekenen voor de ontwikkeling van risicomanagement in het bedrijfsleven. Pas als ondernemingen zich in de ogen van beleggers en analisten kunnen onderscheiden door een aantoonbaar zorgvuldige en bewuste omgang met risico's, zullen bestuurders van ondernemingen risicomanagement daadwerkelijk omarmen. Niet alleen omdat het moet, maar simpelweg omdat het hen wat oplevert. ■

Noot

* Dennis Freriksen, Daniël Goudeket en Leen Paape zijn werkzaam bij Pricewaterhouse-Coopers Advisory en Dirk Swagerman is verbonden aan de Rijksuniversiteit Groningen.

** Het onderzoeksverslag is te bestellen op de website www.pwc.com/nl/publicaties.