ISO-norm risicomanagem

Dit jaar wordt richtlijn ISO 31000 voor risico-management internationaal gelanceerd. Het NIVRA is bij dit project betrokken.

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

Tot nu toe waren het gescheiden werelden: de beheersing van kwaliteit en veiligheid rond fysieke, technische operaties enerzijds, en anderzijds het risicomanagement van financiële en *governance*-processen. Maar dat moet binnenkort verleden tijd zijn. Want met de lancering van richtlijn ISO 31000 voor risk management wordt voor het eerst een serieuze poging gedaan om organisaties in een integrale benadering een systematiek aan te bieden waarin ze alle risico's in kaart kunnen brengen en beheersen. En het ligt voor de hand dat accountants - primair interne accountants, maar ook controlerend accountants - met deze nieuwe, op vrijwillige basis in te voeren richtlijn te maken krijgen. Management consultants zullen in hun dienstenpakket wellicht ondersteuning bij implementatie van de norm opnemen.

AARDBEVING JAPAN

In oktober van dit jaar hoopt NEN, het Nederlands Normalisatie-instituut in Delft, samen met vergelijkbare instellingen over de hele wereld, de nieuwe ISO-richtlijn te lanceren.
Het lijkt een goed getimede reactie op de kredietcrisis, om juist nu te komen met een norm voor risicobeheersing, waarbij milieu, veiligheid op de werkvloer, de kwaliteit van industriële producten en financiële en bestuurlijke risicobeheersing in één kader worden geplaatst. Maar dat is schijn.
Dick Hortensius, seniorconsultant bij NEN-Managementsystemen, en nauw betrokken bij de totstandkoming van ISO 31000, maakt meteen duidelijk dat er geen enkel oorzakelijk verband met de financiële crisis bestaat. "Het initiatief om te komen tot een norm voor een alomvattende risk managementaanpak, is veel ouder. Het ontstond in Japan in 1995 na die enorme aardbeving in Kobe. Men merkte daar hoezeer kwaliteits- en risicobeheersingssystemen uit diverse disciplines onderling samenhangen."

Dick Hortensius (NEN): 'Na die enorme aardbeving in Kobe merkte men hoezeer risicobeheersingssystemen uit diverse disciplines onderling samenhangen.'

NEUTRAAL BEGRIP

Dat het nog zo lang moest duren voordat het tot een norm of richtlijn kwam, had te maken met de angst bij het bedrijfsleven dat zulke normen tot ongewenste - want kostbare en bureaucratiebevorderende - certificatieactiviteit zou leiden. Voorzichtig werd daarom eerst begonnen met het ontwikkelen van een soort vocabulaire waarin termen en definities op het gebied van risk management werden vastgelegd. Hortensius: "Als partijen uit zoveel verschillende landen het erover eens zijn wat ze met bepaalde woorden precies bedoelen, dan kun je pas verder."
Onder meer werd er gediscussieerd over hoe het begrip 'risico' überhaupt te definieren. Hortensius: "Als Nederlandse delegatie bepleitten wij risico als een neutraal begrip op te vatten. Als risico een onverwachte ontwikkeling is, dan kunnen daarin bedreigingen zitten maar ook kansen. Dat idee is geaccepteerd."
Dat de werking van een ISO-norm zich uitstrekt tot de niet-technische wereld is relatief nieuw. NEN en vergelijkbare instituten in het buitenland worden traditioneel bevolkt door ingenieurs. Ze legden vast aan welke eisen een spoorbrug moest voldoen of hoe je een zaagmachine veilig maakt. Financieel risicomanagement of normen voor behoorlijk bestuur lagen buiten hun schootsveld.

ent

Johan Scheffe (NIVRA): 'De interne accountant zal moeten certificeren. En dat geeft later de externe accountant weer een bodem om op te bouwen.'

De elf basisprincipes van ISO 31000

1. Risk management creëert waarde
2. Het is een integraal onderdeel van organisatieprocessen
3. Het is onderdeel van besluitvorming
4. Het richt zich expliciet op onzekerheid
5. Het is systematisch, gestructureerd en tijdig
6. Het is gebaseerd op de best beschikbare informatie
7. Het is op maat gesneden
8. Het houdt rekening met menselijke en culturele factoren
9. Het is transparant en overal aanwezig
10. Het is dynamisch, iteratief en reageert op verandering
11. Het faciliteert voortdurende verbetering en versterking van de organisatie

IMAGOSCHADE

Maar bij ISO 31000 zijn dergelijke aspecten er nadrukkelijk wel betrokken. Dat de Nederlandse inbreng ook op dat vlak relatief groot is geweest, is volgens Hortensius mede te danken aan zijn nauwe samenwerking met Johan Scheffe, werkzaam op de afdeling vaktechniek van het NIVRA en gespecialiseerd in onderwerpen zoals corporate governance en interne controle. "De Amerikanen waren terughoudend. Maar dat gaf ons dus wat extra ruimte." Scheffe noemt de fusie van deze werelden logisch, omdat het type onzekerheden waarmee een bruggenbouwer en een bankier te maken hebben, punten op een continuüm zijn. "Ze beïnvloeden elkaar ook aantoonbaar. Als een bedrijf door een technische fout milieuschade veroorzaakt, dan leidt dat onder meer tot imagoschade. En uiteindelijk zal het in de financiële resultaten terug te vinden zijn."
Er bestaan overigens al wel normen op het gebied van financieel en bestuurlijk risicomanagement. COSO is een stelsel van richtlijnen voor interne controle en interne beheersing. Nogal wat bedrijven volgen die. Bovendien hebben grotere Nederlandse bedrijven te maken met de governance-code Tabaksblat, en enkele in Amerika genoteerde ondernemingen moeten ook voldoen aan Sarbanes-Oxley.
"Maar", vindt Scheffe, "ten aanzien van risk management geven die normen met name richtlijnen voor de betrouwbaarheid van de financiële rapportage; níet over hoe je risk management feitelijk breed in je organisatie implementeert. ISO 31000 biedt dat wel".

ELF PRINCIPES

ISO-normen worden geassocieerd met in absolute termen gestelde technische kwaliteitseisen die aan een product of een productieproces worden gesteld. Hortensius, wiens werk eruit bestaat zeer uiteenlopende doelgroepen te begeleiden bij het opstellen van ISO-normen, weet echter dat een ISO-norm soms niet meer is dan een genormaliseerde, dus gestandaardiseerde begrippenlijst, soms een reeks aanbevelingen en *best practices*, en soms ook een set van harde eisen.
Hortensius: "Het hangt ervan af. Bij ISO 31000 gaat het om een richtlijn, gebaseerd op elf principes die vastleggen wat risk management behelst. Daarnaast biedt ISO 31000 de elementen van het *framework*, het kader waarmee risicobewustzijn breed in de organisatie kan worden ingebed. Ook beschrijft het de hoofdlijnen van het risk managementproces: van identificatie, via analyse en beoordeling tot het beheersen van risico's."

INSPANNINGSVERPLICHTING

Scheffe verwacht overigens niet dat organisaties die straks zeggen ISO 31000 te zullen implementeren dat als een soort reclame-instrument zullen inzetten: "Deze norm heeft niet een *rule-based* maar een *principle-based* karakter. Voor een organisatie is dus het meer een inspanningsverplichting."
Daarmee is niet gezegd dat alles aan de norm zacht is. Scheffe: "Als het management besluit dat bepaalde procedures moeten worden gevolgd dan zal de interne accountant er wel op uit moeten om te zien of dat werkelijk gebeurt. Hij zal dat moeten certificeren. En dat geeft later de externe accountant weer een bodem om op te bouwen. Zo'n planmatige aanpak van risk management zal voor de interne controle onvermijdelijk en merkbaar gevolgen hebben." □