



## Wat iedere bestuurder over ERM moet weten

**Enterprise Risk Management (ERM) oftewel organisatiebreed risicomangement vindt niet vanzelf plaats. Negen kritische vragen en antwoorden die iedere bestuurder zou moeten overwegen als hij een goed ERM-beleid nastreeft voor zijn bedrijf.**

*Door Joost Spoel*

### 1 WAAROM IS ERM RELEVANT?

Sinds 2004 moeten alle (Nederlandse) beursgenoteerde ondernemingen voldoen aan de code-Tabaksblat. Volgens deze code moet het management verslag doen van alle risico's die materiële invloed kunnen hebben op het realiseren van de doelstellingen van de onderneming. Dit betreft zowel de financiële en operationele als de strategische risico's.

De Monitoring Commissie (in de wandelgang de commissie-Frijns) heeft bepaald dat er ten aanzien van de 'in control'-verklaring onderscheid dient te worden gemaakt tussen de financiële verslaggevingsrisico's en de operationele en strategische risico's. De ondernemingsleiding dient te verklaren dat de interne risicobeheersings- en controlesystemen ten aanzien van de financiële risico's adequaat en effectief zijn. Dat wil zeggen dat er zich redelijkerwijs geen onjuistheden van materieel belang hebben voorgedaan, c.q. zullen voordoen. Met betrekking tot het verslagjaar 2004 verklaarden echter maar weinig bestuurders dat de interne risicobeheersings- en controlesystemen in hun onderneming inderdaad adequaat en effectief waren.

Dat dit niet alleen een Nederlands verschijnsel is, blijkt uit onderzoek van Protiviti USA ([www.protiviti.com](http://www.protiviti.com)), waarin

60 procent van het senior management aangeeft niet het vertrouwen te hebben dat alle risico's die serieuze impact kunnen hebben op de onderneming dankzij de huidige riskmanagementactiviteiten voldoende bekend zijn en/of effectief worden gemanaged.

Een andere reden waarom ERM relevant is, is dat het als integrale benadering de verschillende regelgevingen en de daarmee verbonden compliancebehoeften prioriteert voor management en proceseigenaren. Deze groepen worden overladen met instructies vanuit verschillende wetgeving en komen nauwelijks toe aan hun eigenlijke taken. Control dient op efficiënte en effectieve wijze integraal onderdeel uit te maken van de dagelijkse werkzaamheden. De integrale benadering komt tot stand via ERM.

### 2 WAT BETEKENT ERM VOOR MIJN ORGANISATIE?

ERM is geen nieuwe managementmethode. ERM richt zich op het vormen van een integraal risicomangementbeleid en een eenduidige toepassing van risicomangement door de gehele organisatie. Zoals de term ERM al zegt, beoogt het een organisatiebrede aanpak en ligt de nadruk op operationele, financiële en strategische risico's.

Overigens bestaat er geen generieke ERM-aanpak, omdat het risicomangement onder andere sterk samenhangt

met de organisatiestructuur, het type bedrijfsprocessen, de markten waarin men opereert en ook de organisatiecultuur. De terugkerende essentie van ERM is echter dat elk organisatieonderdeel verantwoordelijk is voor het managen van zijn eigen risico's. In het algemeen kan men binnen grotere dan wel internationale organisaties doorgaans op drie niveaus risicomanagementprocessen onderscheiden.

Van onder naar boven zien we eerst het operationele niveau, waar het het doel is inzicht te krijgen in de belangrijkste organisatieprocessen en hun risico's, de mate van control en potentiële verbetermogelijkheden. Dit wordt ook wel Operational Risk Management (ORM) genoemd en is een wezenlijk onderdeel van de ERM-filosofie.

Tactisch riskmanagement richt zich op zelfstandige entiteiten en projecten binnen de onderneming (inclusief investeringen en overnames) en dient de belangrijkste organisatie- (of entiteits-) risico's expliciet te maken, zodanig dat het management deze systematisch kan mitigeren. Afgeleid van het COSO-model kunnen hiervoor vier riskmanagementstrategieën worden gehanteerd: 'Take, Treat, Transfer of Terminate'. Vrij vertaald: accepteren, actie ondernemen, afwentelen of afkappen.

Ten slotte zal een raad van bestuur en raad van commissarissen op strategisch niveau inzicht willen hebben in het geconsolideerde risicoprofiel van de organisatie en de kwaliteit van de beheersing ervan. Een ander aspect van strategisch riskmanagement is het verband tussen het ondernemingsrisicoprofiel en de extern gepercipieerde (aandeelhouders-) waarde van de onderneming. (Zie vraag 7.) Kortom, ERM betekent een systematisch en expliciet risicomanagementproces op drie niveaus. Dit alles wordt ondersteund door één risicomanagementraamwerk waarin de spelregels voor ieder worden uitgelegd. Een dergelijk raamwerk kan bestaan uit een risicomanagementhandboek & -beleid, vastgelegde risicorapportages, rollen en verantwoordelijkheden etc.

De hamvraag mag uiteraard niet ontbreken, namelijk wat levert ERM op? De volgende zaken kunnen worden genoemd:



Elk organisatieonderdeel is verantwoordelijk voor het managen van zijn eigen risico's

- aantoonbaar risicomanagement als onderdeel van het interne-controleraamwerk
- verbetering van de 'level of control'
- betere (risicogebaseerde) besluitvorming inzake investeringen en substantiële organisatieveranderingen
- verhoogd risicobewustzijn door de gehele organisatie
- potentiële verbetering van de (operationele) prestaties van de organisatie
- eenduidige risicomanagementprocessen
- transparantie door inzicht in alle risicoprofielen van de organisatie
- gemoedsrust voor interne en externe stakeholders.

Het kwantificeren van de genoemde voordelen is geen sinecure en een investering in ERM is dan ook, net als investeringen in ICT, eerder een 'politieke' dan een puur financieel-economische zaak.

### 3 HOE ZIJN DE ROLLEN EN VERANTWOORDELIJKHEDEN BINNEN HET ERM-SPEL VERDEELD?

De belangrijkste 'spelers' zijn de raad van bestuur, de raad van commissarissen, de auditcommissie, internal audit, het corporate-riskmanagement en niet te vergeten de 'business' zelf. Zonder in te gaan op een lijst van taken kan het interessant zijn de volgende rolomschrijvingen in overweging te nemen.

**CORPORATE-RISKMANAGEMENT** Afhankelijk van de grootte en het type van de organisatie kan deze rol op zichzelf staand, mogelijk in samenhang met specialistische riskmanagementfuncties, een toegevoegde waarde hebben. De corporate-riskmanager is de bewaker van de spelregels, faciliteert, reikt methoden en technieken aan, ‘challenge’ senior management en steunt de business bij het identificeren en managen van operationele en financiële risico’s. Deze functie brengt tevens diverse relevante disciplines bij elkaar, zoals legal, investor relations, en accounting en control.

**INTERNAL AUDIT** bewaakt het riskmanagementproces en rapporteert over onvolkomenheden.

**DE ‘BUSINESS’** ten slotte is eigenaar van de risico’s en heeft tot taak de belangrijkste risico’s te managen en inzicht te geven in de voortgang van de risicomangementactiviteiten.

## 4 WAT IS HET VERBAND TUSSEN ERM EN SOX?

Een relatief nieuw onderwerp is het linken van SOX met ERM. Menige onderneming heeft veel tijd en geld in SOX gestoken, maar de toegevoegde waarde moet er nog uit komen, is de overheersende opinie. Na twee jaar SOX-veldervaring is op dit moment de belangrijkste vraag hoe SOX gerationaliseerd kan worden. Enkele aanbevelingen uit recent onderzoek luiden als volgt.

- Minimaliseer het aantal key controls en gebruik zo veel mogelijk geautomatiseerde controls.
- Key controls en de mate van detail zouden bepaald moeten worden door de organisatie en niet door de externe auditor.
- Maak meer gebruik van self assessment door het management in plaats van onafhankelijk testen.
- Verander van een complianceproject naar een risicomangementproces.

Overigens dient te worden opgemerkt dat SOX primair een financiële inslag heeft, terwijl in de brede opzet van ERM ook en met name operationele en strategische risico’s van belang zijn. In dit opzicht sluit de code-Tabaksblat beter aan op ERM dan SOX.

## 5 HOEVEEL RISICO WILLEN WE NEMEN, WAT IS ONZE RISK APPETITE?

Volgens COSO is de risk appetite van een onderneming de ‘guidepost’ bij het bepalen van de organisatiestrategie. Risk appetite is een vaak gehoorde term in risicoland en geeft simpel gezegd de risico’s aan die een organisatie te allen tijde wil vermijden. Om ERM goed te implementeren is het van fundamenteel belang om als raad van bestuur de risk appetite te definiëren. Hierbij speelt een belangrijke afweging tussen waardecreatie en waardeprotectie. Als gevolg van deze exercitie zullen bijvoorbeeld organisaties met een grotere appetite risicovolle investeringen doen in het volle bewustzijn van het vermogen dat benodigd is om dit risico te nemen (Bazel II voor de financiële sector maakt deze afweging zeer expliciet). Oftewel: wat kan men zich permitteren? Een organisatie geënt op ambitieuze groei met een zware financieringsstructuur (high leverage) en beperkt werkkapitaal zou wel eens te veel hooi op de vork kunnen nemen. Maar een organisatie die de groei financiert met cash uit eigen operationele activiteiten zal zich (ook tegenover de buitenwereld) comfortabel voelen om gestelde groei-doelstellingen te bereiken. Doorgaans wordt een op deze wijze expliciet gebruik van de risk appetite ook beloond in de vorm van een hogere waarde van het aandeel c.q. van de onderneming als geheel.

## 6 HOE KAN ERM WORDEN GEÏNTEGREERD IN HET STRATEGISCHE PLANNINGPROCES?

Risicomangement zou een onderdeel moeten zijn van besluiten over substantiële investeringen zoals overnames, sleutelprojecten en andere belangrijke veranderingen. Dit kan worden gerealiseerd door niet alleen de ‘upside’ te bestuderen, maar ook de nadruk te leggen op verschillende scenario’s en in het bijzonder een worst-

casescenario. Methoden en technieken hiervoor zijn al geruime tijd voorhanden, zoals Value at Risk (VAR) en Monte Carlo-simulaties. Tevens zal een raad van bestuur inzicht willen hebben in de voortgang van het genomen besluit, uitgedrukt in concrete performance targets en specifiek gemaakt risico's. Dit laatste aspect, het continu monitoren van de ontwikkeling van de geschetste risicoprofielen, ontbreekt echter nog vaak.



Verhoogd risicobewustzijn door de gehele organisatie

## 7 HOE COMMUNICEER IK OVER ERM NAAR DE GEÏNFORMEERDE BUITENWERELD?

De geïnformeerde buitenwereld (analisten, investeerders) geeft op basis van diverse financiële analyses (weighted average cost of capital (WACC), cashflow, EBITA) een waardeoordeel over de (beursgenoteerde) onderneming. Gericht risicomanagementactiviteiten kunnen in verband worden gebracht met de risicofactoren in de WACC en deze vervolgens gunstig beïnvloeden. Vanuit het informatieperspectief kan investor relations hierbij een sleutelrol vervullen door het opnemen van de risicomanagementcomponent in communicatie naar buiten. Voor de IR-functionaris binnen een onderneming met een laag risicoprofiel is de schone taak weggelegd om zich zo te profileren dat dit leidt tot een hogere waardering van de onderneming.

## 8 HOE HOUDEN WE ERM LEVEND?

Hoewel risicomanagement voor een belangrijk deel bij de 'business' thuishoort, wil dit nog niet zeggen dat het door managers altijd volledig wordt overgenomen. In feite is de implementatie

van ERM een changemanagementproject als elk ander. Vanuit een corporate perspectief ligt er ook een verantwoordelijkheid om ERM na een succesvolle implementatie levend te houden. Hieronder volgen enkele zaken die onontbeerlijk zijn voor succesvol ERM.

- Actief ERM-sponsorship van de CEO/CFO en medebestuurders. 'The tone at the top' bepaalt in belangrijke mate het succes van ERM.
- Een stevig budget voor interne en externe communicatie over ERM. Hierbij kan men denken aan een handzame intranetsite, nieuwsletters, maar ook begrijpelijke communicatie over wat ERM inhoudt, oplevert en wie welke verantwoordelijkheden heeft.
- Een rapportagestructuur en beloningssysteem waardoor risicomanagement op de agenda blijft staan bij de verantwoordelijken in de business, niet zijnde de raad van bestuur.

## 9 DOEN WE NIET AL LANG AAN RISICOMANAGEMENT?

Inderdaad, het senior management heeft de operationele en financiële risico's doorgaans goed op de radar staan. ERM zal dat ook niet moeten willen veranderen, maar moeten zorgdragen voor een expliciete en eenduidige manier van het managen van risico's, op alle organisatiefronten en in hun onderlinge samenhang. Geen sinecure. Maar met een pragmatische en realistische benadering kan dit de nodige interne en externe resultaten opleveren. <<

**Joost Spoel** is manager bij Protiviti Nederland (joost.spoel@protiviti.nl). Via hem kan de uitgave *Frequently Asked Questions ERM* worden besteld