de interne accountant

Dynamisch risicomanagement

Schieten op

Roel van Rijsewijk (links), Robert Willemse (midden) en Pascal Looij: "Het is meer regel dan uitzondering dat er na een forse inspanning niet veel meer overblijft dan een indrukwekkend pak papier."

FOTO: SIMONE VAN ES

bewegend doel

Aandacht voor risicomanagement is er volop, maar concrete resultaten blijven vooralsnog uit. Tijd voor een dynamischer aanpak.

ROBERT WILLEMSE, ROEL VAN RIJSEWIJK EN PASCAL LOOIJ*

Over risicomanagement wordt veel geschreven. Nieuwe methoden en strategieën hebben het gemaakt tot een vaak geïntegreerd onderdeel van de bedrijfsvoering. Maar in hoeverre zijn we daadwerkelijk geslaagd in het beter managen van risico's? En hoe verloopt de wisselwerking met internal audit?
Het is niet eenvoudig daarover een algemene conclusie te trekken. Praktijkstudies laten verschillende resultaten zien, vaak veroorzaakt door het niet eenduidig uitoefenen van risicomanagement. In grote lijnen kunnen we wel stellen dat risicomanagement:

- een gevestigde bedrijfsactiviteit is geworden;
- het risicobewustzijn in de organisatie verbetert;
- communicatie over risico's verbetert;
- op de directie agenda is geplaatst.

Daarmee is een essentiële eerste stap gezet, maar veel verder is men tot nu toe nog niet gekomen. Het ontbreekt nog aan échte resultaten. Alle aandacht tot nu toe heeft niet geresulteerd in risicoreductie, heeft niet bijgedragen aan een beter risicomanagement, heeft de bedrijfsvoering niet verbeterd. In wat krassere bewoordingen: het is grotendeels irrelevant en is een techniek 'door consultants voor consultants'.

'Magere' resultaten tot nu toe

Concreet bestaat de output van risicomanagement nu doorgaans uit vier onderdelen:

- een database waarin alle geïdentificeerde risico's zijn opgeslagen, soms resulterend in een soort risicobijbel;
- een kwalitatieve analyse van de verwachte combinatie van kosten/impact en waarschijnlijkheid van al deze risico's;
- een kwalitatieve analyse van de mate van beheersing (hoeveel 'restrisico' is over?);
- identificatie van restrisico's die niet acceptabel zijn.

En daar houdt het (te) vaak op. Hoe goed de methodiek ook is uitgevoerd en wat de kwaliteit van deze output ook moge zijn, er kan niet worden beweerd dat de organisatie nu beter presteert en dat de kans op onaangename verrassingen hiermee is gereduceerd. De beloften die aan het begin van het proces worden gedaan, worden over het algemeen niet nagekomen. Helaas is het meer regel dan uitzondering dat er na een forse inspanning van de 'facilitators' én de organisatie, niet veel meer overblijft dan een indrukwekkend pak papier. Welke tekortkomingen zijn verantwoordelijk voor deze magere resultaten?

Huidige tekortkomingen

Op hoofdlijnen ontlopen de verschillende methoden en gebruikte technieken (in praktijk en theorie) elkaar niet. Er is hoogstens sprake van enige nuanceverschillen, al naar gelang de cultuur en omvang van de organisatie en de aard van de processen. En in de meeste gevallen zijn de resultaten ronduit mager. De belangrijkste oorzaken hiervan zijn de volgende:

Het leidt tot een vermindering van eigen initiatief
Ondanks dat de meeste technieken zijn gebaseerd op self assessment en geen 'facilitator' het zal nalaten het management te wijzen op de *eigen* verantwoordelijkheid, leidt de implementatie van een gestructureerd risicomanagementproces vaak tot een vermindering van eigen initiatief. Het bewustzijn van risico's en het begrip van risicomanagement neemt weliswaar toe, maar het aantal concrete acties om iets met die risico's te gaan doen, neemt merkwaardig genoeg af. Met de komst van ▶

'We hebben een techniek nodig die mee verandert met de organisatie.'

risicomanagement wordt een deel van die verantwoordelijkheid overgedragen aan een onpersoonlijk en organisatiebreed proces. Een logisch en concreet verband tussen waargenomen risico's, mate van beheersing, en benodigde actieplannen en probleemeigenaren ontbreekt vaak.

Het wordt verpletterd onder zijn eigen gewicht
Als we alle risico's van elk proces in de organisatie willen identificeren, daar vervolgens per risico en per proces een kwalitatieve analyse op uitvoeren (impact en waarschijnlijkheid) én daarnaast ook nog eens naar de mate van beheersing per risico per proces willen kijken, dan is het duidelijk dat er voor grote en complexe organisaties een langdurig en nauwelijks beheersbaar project ontstaat.

Analyse blijkt achteraf vaak verkeerd te zijn
Risicomanagement wordt veelal 'statisch' bedreven. Het zijn vaak grote en eenmalige projecten die niet echt zijn geïntegreerd in de dagelijkse werkzaamheden van de lijn. De oorspronkelijke statische analyse van de risico's blijkt vaak achterhaald tegen de tijd dat er actie wordt ondernomen. Risico's die niet beheerst zouden zijn, blijken toch redelijk 'in control' en risico's die niet waarschijnlijk zouden zijn, doen zich plotseling wel voor. De verklaring: risico's die als onbeheerst worden geschat, staan blijkbaar op het netvlies van het management, en *daar zijn ze dus al mee bezig*. De risico's waarvan het management zich ten tijde van de analyse blijkbaar niet goed bewust was, hebben uiteraard een hoge waarschijnlijkheid van optreden.

Het sluit niet aan met het nieuwe COSO Enterprise Risk Management-model.
In de meeste gevallen voldoet de huidige statische benadering aan het bekende COSO Internal Control Framework met name op de onderdelen risk assessment en controls & procedures. Echter, het nieuwe COSO Enterprise Risk Management-model kent ook de onderdelen 'objective setting' (waarin risicobeleid is opgenomen!), 'event identification' en 'risk response'. De statische benadering gaat hier meestal niet op in (zie kader).

Wat moet er veranderen?

Het draait veelal allemaal om techniek (de 'hoevraag'). Techniek die wordt afgestemd op een organisatie die per definitie in een continue staat van verandering verkeert. We hebben een techniek nodig die mee verandert met de organisatie of kan inspelen op de veranderingen daarbinnen. De definitie van risicomanagement kan nog steeds worden gehandhaafd, maar de praktische invulling verandert. Om iets aan de huidige tekortkomingen te doen, moeten de volgende aspecten veranderen:

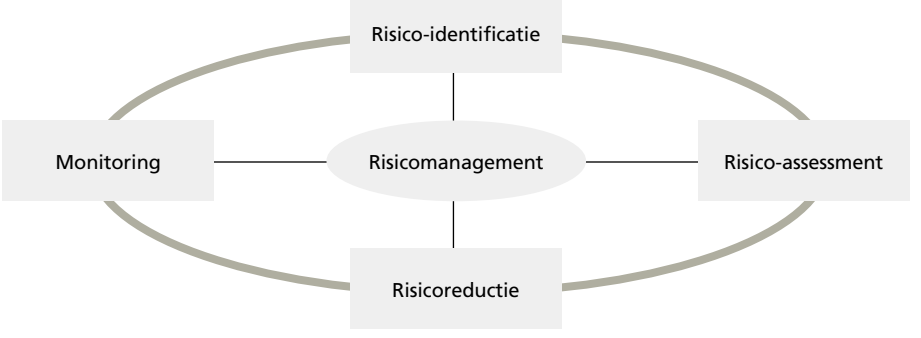
- de tijd tussen analyse en acties moet sterk worden verkort;
- de frequentie van analyse moet 'vele malen' hoger;
- het volume van de analyse moet 'vele malen' lager;
- de betrokkenheid van lijnmanagement moet hoger.

Implementatie van deze drie verbeteringen leidt tot wat wij zijn gaan noemen *dynamic risk management*.

Dynamic risk management

Dynamic risk management identificeert uitsluitend de *veranderingen* in het systeem van interne beheersing en omgevingsfactoren. Vervolgens worden de mogelijke risico's en effecten hiervan beoordeeld. Daarna wordt bepaald wie hier binnen de organisatie acties op onderneemt. Naar audit reviews, assessments en mogelijke risico's en gebeurtenissen in het verleden wordt niet meer gekeken.
Het principiële en vernieuwende uitgangspunt van dynamisch risicomanagement is dat *het systeem van interne beheersing op dit moment effectief is*. We kijken niet meer terug naar het verleden en naar de eventuele negatieve scores van toen. We beginnen met een schone (en lege) lei, nemen alleen die zaken die veranderen in ogenschouw, en daaraan besteden we vervolgens onze aandacht in het vervolg van het risicomanagementproces. Een en ander is opgebouwd uit vier stappen:

Stap 1 Risico-identificatie
Periodiek, bij voorkeur maandelijks, worden alle significante veranderingen binnen en buiten de organisatie geïdentificeerd, gewogen en beoordeeld. Het risicodomein moet aldus worden uitgebreid. Voorbeelden van veranderingen binnen de organisatie zijn nieuwe projecten, de levenscyclus en innovatie van



Het risicomanagementproces

producten en diensten, veranderende operationele en ICT-processen, nieuwe medewerkers etc. Buiten de organisatie zijn eveneens allerlei veranderingen denkbaar in de wet- en regelgeving, ontwikkelingen in de markt, onderzoeken door externe bureaus, concurrenten en binnen de economie in het algemeen. Identificatie en agendering aan de hand van COSO, de value chain van Porter, een business analysis framework of een ander referentiemodel kan handig zijn. Centrale vraag is hoe en wanneer gebeurtenissen van buitenaf een invloed hebben op de eigen operationele, administratieve en ICT-processen. *Al met al zoeken we naar nieuwe risico's en veranderde risico's.*

Stap 2 Risico-assessment
Hiermee worden de effecten van de nieuwe en veranderde risico's beoordeeld: wat zijn de effecten en gevolgen, wat is de kans dat ze zich voordoen, de afweging van de inherente en residuele risico's.

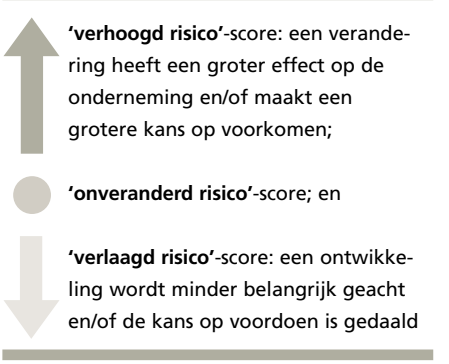
Stap 3 Risicoreductie
Na de identificatie en de beoordeling van de nieuwe en veranderde risico's worden de mogelijkheden voor het beheersen en afdekken ervan vastgesteld. Hierbij kan worden gedacht aan de vier 'T's': *take, treat, transfer en terminate.* Afhankelijk van de kans van voordoen en de mogelijke gevolgen voor de organisatie. Specifieke aandacht gaat uit naar de noodzakelijke verandering van beheersingsmaatregelen, de vraag welke veranderingen al hebben plaatsgevonden, welke nieuwe beheersmaatregelen noodzakelijk zijn, wat de gevolgen zijn voor het restrisico, en hoe uiteindelijk moet worden om gegaan met inherente en restrisico's.

Stap 4 Monitoring
Het moge duidelijk zijn dat de veranderingen van risico's en de gevolgen voor de organisatie niet meer kunnen worden gemeten met de traditionele maatstaven. Vaststelling van een hoge of lage score van een bewegend doel is immers lastig. De nieuwe monitoring-maatstaven dienen bewegende doelen te volgen: de verandering van risico's, van risicobeheersingsmaatregelen, van de risico-assessment, maar ook veranderingen buiten de eigen organisatie, waarvan het directe effect vaak niet duidelijk is vast te stellen. Voor het vaststellen van de gevolgen kan gebruik worden gemaakt van scenario-analyse, incidentonderzoek en rapportages, en van 'near miss'- en 'what if'-analyse.
In de rapportage van dynamische risico's gaan we niet uit van een statische 'hoog/medium/-laag' score, maar van een nieuwe, meer dynamische categorisering. Deze is weergegeven in de volgende figuur:

Voldoen de statische en dynamische risicomanagementmethoden aan het nieuwe COSO ERM-model?

Welke onderdelen van COSO ERM worden afgedekt?

COSO ERM-model	Statisch risicomanagement	Dynamisch risicomanagement
1. Internal environment	ja	ja
2. Objective setting (new)	soms	ja, samen met management
3. Event identification	nee	ja, met hoge frequentie
4. Risk assessment	ja, met lage frequentie	ja, met hoge frequentie
5. Risk response (new)	soms	ja, samen met management
6. Controls & procedures	ja	ja
7. Information & communication	ja	ja, met maandelijkse rapportage
8. Monitoring	ja	ja



De keuze of hier over inherente of residuele risico's wordt gesproken, maakt de betrokkenen zelf, mits er maar een duidelijke keuze wordt gemaakt.

Risk identification-groep

Het meeste profijt van deze dynamische methode is haalbaar als een *brede groep* periodiek de veranderingen in brede zin bespreekt: de risk identification-groep. Deze bestaat uit vijf tot tien personen (voornamelijk junior en senior management) en bespreekt en beoordeelt maandelijks de nieuwe ontwikkelingen. Deze discussie kan gestructureerd verlopen met een vooraf vastgestelde agenda, maar een 'brainstorm-sessie' kan zeker in het begin goed werken. De groep besluit ook over de te nemen acties en de verdeling hiervan over de verantwoordelijke personen (lijnmanagement en internal audit). Het kan dus heel goed voorkomen dat 'traditionele' internal audit-werkzaamheden door het lijnmanagement worden opgepakt, en andersom. De planning van internal audit en risicomanagement sluit hierdoor naadloos aan op de managementbehoeften van dat moment.
De resultaten van de besprekingen in de risk identification-groep kunnen door middel van een *bulletin board* aan de rest van de onderneming kenbaar worden gemaakt.

Dynamic risk management met risk identification groups biedt een concrete mogelijkheid tot verbetering van de nu vaak afstandelijke en eenzijdige risico-analyses. Het is veel makkelijker, intuïtiever en praktischer, en door de betrokkenheid van diverse lagen en functies binnen de organisatie, wordt risicomanagement meer preventief en pro-actief. Internal audit en risicomanagement helpen zo pro-actief mee de organisatie te verbeteren. ■

Noot

* Robert Willemse, Roel van Rijsewijk en Pascal Looij zijn werkzaam bij Deloitte & Touche afdeling Enterprise Risk Services. Dit artikel is op persoonlijke titel geschreven.