

# Een positieve blik op modellen voor risicomanagement

Er zijn de afgelopen jaren nieuwe normen op het gebied van risicomanagement ontstaan. Welke handvatten geven deze normen – COSO, ISO 31000 en M\_o\_R – voor verankering van risicomanagement binnen de organisatie? Hoe groot is de invloed van deze normen ten opzichte van de cultuur en de daadwerkelijk door het bestuur gewenste transparantie?

Robert 't Hart

Tijdens en na elke crisis, grote fraude (Ahold, Enron) of ramp (zoals bij BP: driemaal menselijk falen op een rij), verschijnen onderzoeksrapporten, waarin steeds nadrukkelijker de bestuurders verantwoordelijk worden gehouden voor onder meer de veiligheidscultuur binnen het bedrijf. Op de rapporten volgen vaak wijzigingen in de regelgeving en governancecodes, omdat de bestaande codes kennelijk in de praktijk niet de gewenste gevolgen hebben gehad. In de wijzigingen in de regelgeving rondom governance zijn twee trends te herkennen:

- een sterke focus op de interne beheersing, naast de al langer beschreven externe verantwoording;
- bij die beschrijving van aantoonbare interne beheersing (control) wordt steeds vaker de aanwezigheid van een integraal risicomanagementsysteem gevraagd.

Hoog tijd dus om eens aandacht te besteden aan modellen voor integraal risicomanagement.

## De modellen en de praktijk

Er bestaan vele risicomanagementmodellen die handvatten geven om individuele risicoanalyses uit te voeren. Er zijn echter minder normen beschikbaar die gericht zijn op borging van integraal risicomanagement in organisaties. Dit artikel beperkt zich tot de modellen COSO 2 (2004), ISO 31000 (2009) en M\_o\_R (2009), drie normen die wel aandacht besteden aan borging van integraal risicomanagement. De kern van de drie genoemde normen is dat ze uitgaan van een directe koppeling tussen doelstelling en risico's, van recente datum zijn en generiek toepasbaar. Aangezien er vele boeken en artikelen over

Het management van overheidsorganisaties zit in toenemende mate in de spagaat tussen risicomanagement en risicoverantwoording. Naast COSO zijn er twee nieuwe best practice-modellen (ISO 31000/ M\_o\_R), die handvatten bieden risicomanagement vorm te geven.

Voordeel om bij een risicomanagementstandaard aan te haken is, dat alle gebruikers ervan dezelfde 'risicomanagementtaal' spreken. Maar er is meer nodig voor een succesvolle verankering van risicomanagement in organisaties: de juiste positionering in de organisatie, de juiste *tone at the top* en aandacht voor de individuele manager.

het risicomanagementproces (globaal: identificeren – wegen – beheersen) zijn geschreven en ook de modellen min of meer in vergelijkbare stappen hebben omschreven, wordt hierop in dit artikel niet ingegaan. Interessanter is wat je aan de verschillende normen hebt. In dit artikel worden dan ook de positieve punten van de verschillende modellen belicht.

Echter, met het toepassen van een integraal risicomanagementmodel alleen ben je er nog niet.

Daarom wordt in het tweede deel van dit artikel ook ingegaan op water in de praktijk mis kan gaan bij de implementatie van integraal risicomanagement.

## De modellen

### COSO 2 (2004)

#### Geschiedenis

Het raamwerk voor COSO 1 ontstond in 1992 na een reeks boekhoudfraudes bij Amerikaanse bedrijven eind jaren '80, onder druk van accountants. Voor externe controle was het noodzakelijk het interne beheersmodel op zijn werking te kunnen beoordelen. In 2004 publiceerde COSO in nauwe samenwerking met een grote accountant het nieuwe raamwerk 'Enterprise Risk Management'. In deze versie is het bereiken van de strategische doelstellingen als extra doelstelling opgenomen.

#### Uitleg model

Kerngedachte is dat als een organisatie haar doelstellingen wil bereiken, ze met risico's moet leren omgaan en deze moet proberen te beheersen. COSO beschrijft en definieert in dit kader de elementen van een intern beheersingssysteem. Het model geeft in de COSO-kubus de directe relatie weer tussen:

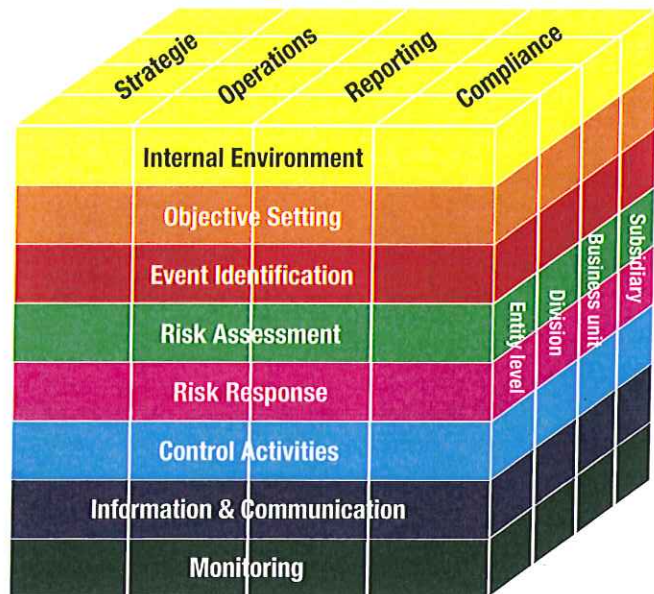
- doelstellingen (bovenvlak);
- organisatorische dimensie (zijvlak); de activiteiten/eenheden waarvoor de interne controle benodigd is;
- componenten van model (voorvlak); de stappen van een risicoanalyse.

#### Sterke punten

Het voordeel van een COSO-aanpak is dat het een internationaal geaccepteerde standaard is, die in Nederland met name door de beursgenoteerde bedrijven gebruikt wordt. Het feit dat in de governancecodes (Sarbanes Oxley en Tabaksblat) expliciet naar COSO wordt verwezen, maakt het model algemeen en, ook door accountants, geaccepteerd. Door aan te haken bij COSO geeft een organisatie een helder signaal dat zij risicomanagement serieus neemt. Zeer sterk is de beschrijving van de eerste stap van het proces, het vaststellen van de interne control. De componenten zijn goed uitgelegd.

COSO 2 maakt een helder onderscheid tussen de verschillende doelstellingen, door vele organisaties gebruikt om risico's te clusteren.

- Strategisch: betreft globale doelen en is afgestemd op de missie;
- Operationeel: betreft effectief en efficiënt gebruik van de middelen;



Figuur 1. De COSO-kubus

- Rapportage: betreft betrouwbaarheid van verslaggeving;
- Toezicht: betreft naleving van wet- en regelgeving.

De eerste twee doelstellingen gaan meer uit van ondernemingsrisico's, waarbij externe risico's die niet altijd beïnvloedbaar zijn door de organisatie op een efficiënte en effectieve wijze moeten worden gemanaged. Van belang is

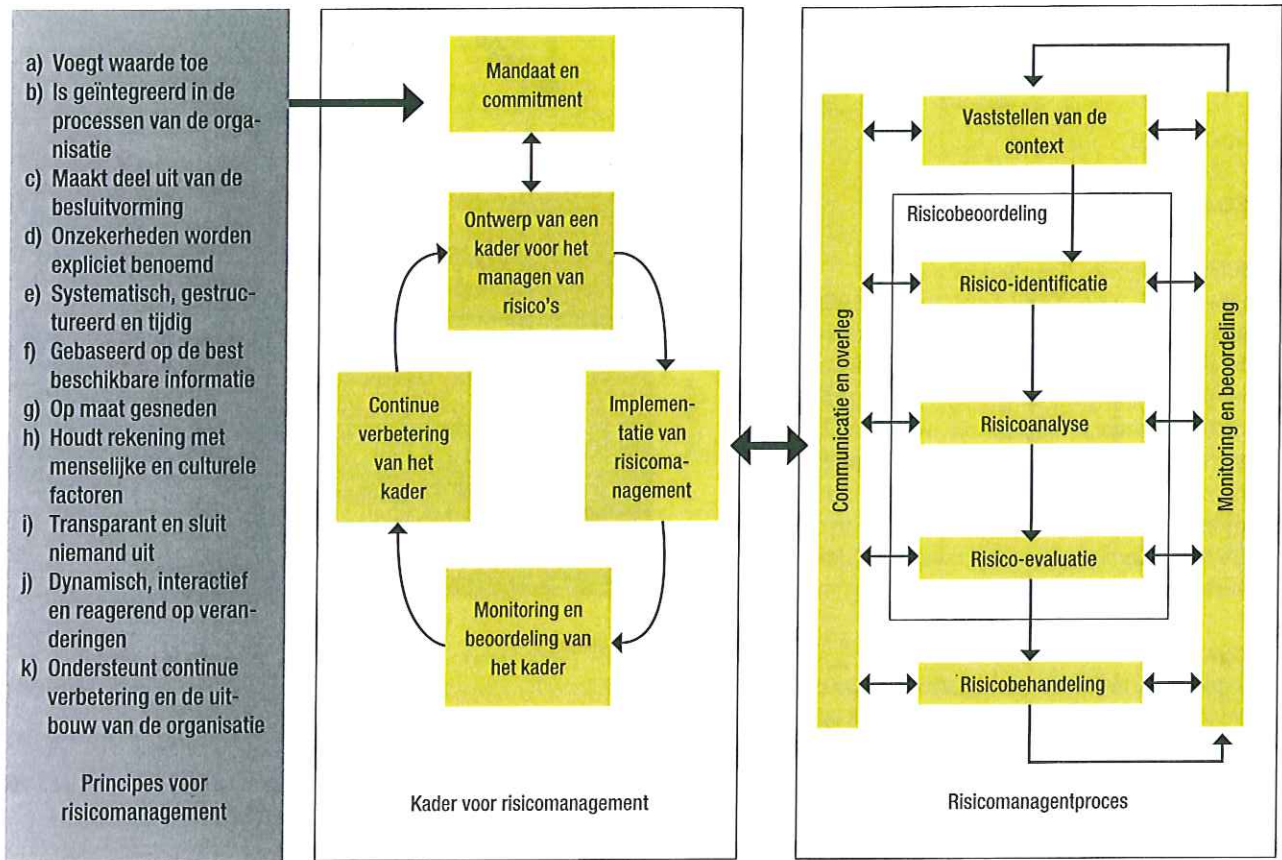
- a) transparantie naar bestuur en toezichthouders over in welke mate men met deze risico's omgaat, en
- b) in welke mate de organisatie zich beweegt richting het realiseren van de doelstellingen.

De laatste doelstellingen rondom toezicht en rapportage zijn de verplichte nummers, hieraan moet de organisatie gewoon voldoen. Het hoofdstuk 'taken en verantwoordelijkheden' is bruikbaar om de juiste rolverdeling te bepalen, met name omdat de rollen van externe partijen – accountant, toeleveranciers en zelfs de financieel analisten en de media – worden omschreven. Al met al is COSO een prima model om vast te stellen wat er van een organisatie verwacht wordt ten aanzien van risicomanagement.

### ISO 31000 (2009)

#### Geschiedenis

In 2005 stelden Japan en Australië samen voor om een algemene ISO-richtlijn voor de principes en implementatie van risicomanagement te ontwikkelen. Bij gebrek aan beter bleken veel organisaties hun toevlucht te nemen tot de Australisch-Nieuw-Zeelandse norm AZ/NZS 4360. De doelstelling die men met de nieuwe norm wilde bereiken, was tweeledig. Ten eerste een algemeen kader (best-practice-model) bieden voor organisaties die risicomanagement in de meest brede zin in de praktijk willen brengen. Ten tweede als paraplu dienen voor allerlei sector- en onderwerpspecifieke ISO-normen op het gebied van risicomanagement.



Figuur 2. De drie hoofdonderdelen van ISO 31000

**Uitleg model**

ISO 31000 bestaat uit drie hoofdonderdelen:

- **Principes voor risicomanagement**  
De principes vormen het fundament waarop risicomanagement moet zijn gebaseerd, wil het een positieve bijdrage leveren aan het functioneren van een organisatie.
- **Raamwerk**  
Dit omvat de beleidscyclus (draagvlak, risicobeleid, contextanalyse, implementatie, monitoring, review en verbetering), waarin de bekende PDCA-cyclus is te herkennen. Het raamwerk vormt het kader voor aansturing van alle risicomanagementprocessen in de organisatie. Die processen moeten passen in het risicobeleid en leiden tot relevante informatie die besluitvorming binnen de organisatie voor allerlei onderwerpen en op allerlei niveaus ondersteunt.
- **Proces**  
De bekende stappen van identificatie, analyse, evaluatie en beheersing van risico's, met daarnaast aandacht voor consultatie & communicatie (rapportages) en monitoring & review. Die aanvullende elementen zorgen voor de link met het raamwerk.

**Sterke punten**

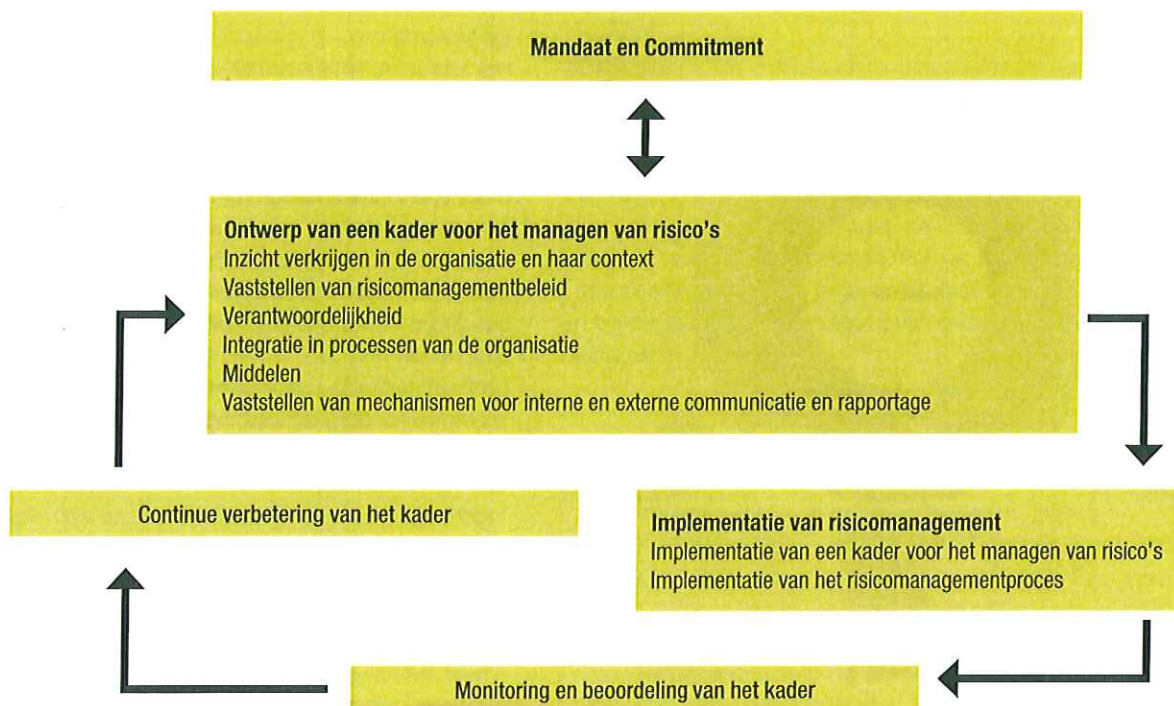
Van ISO 31000 is het prettig dat hij minder dan dertig pagina's telt en dat de hoofdstructuur zeer helder is. Daarnaast is sterk dat principes expliciet worden gepositioneerd en dat er een link is met stap één

uit het raamwerk; het verkrijgen van mandaat en draagvlak.

Door het gebruik van de juiste principes is de kans groter dat risicomanagement uit de puur financiële- / controlhoek wordt gehaald en iets van de individuele manager wordt. De principes ('tegeltjes wijsheden') moeten zo concreet mogelijk gemaakt worden en aansluiten bij de organisatie.

Daarnaast geeft het raamwerk de basis voor het verankeren van risicomanagement in de organisatie, op alle niveaus. Dit raamwerk vormt het beleidskader en daarmee het mandaat voor de aansturing van alle risicomanagementprocessen in de organisatie (zie figuur 3).

Het raamwerk is ontwikkeld om risicomanagement te integreren in bestaande managementsystemen van organisaties en te vermijden dat er een systeem wordt ingevoerd dat los staat van de gewone bedrijfsvoering. Daarom is het als organisatie noodzakelijk om de onderdelen van het raamwerk aan te passen aan de bestaande procedures en richtlijnen.



Figuur 3. Risicomanagement Raamwerk

ISO is natuurlijk ook een bekende naam. Hoewel de 31000-norm een best practice-model is en niet voor certificatie is bedoeld, helpt dat wel. De aanpak van ISO 31000 sluit goed aan bij de door veel organisaties toegepaste ISO-normen voor kwaliteits- en milieumanagement.

### M\_o\_R® (2007)

#### Geschiedenis

M\_o\_R is ontstaan als reactie op het Turnbull report (1998) – de Engelse tegenhanger van de commissie Peters en Tabaksblat –, waarbij risicomanagement vanaf het begin zeer sterk aan behoorlijk bestuur werd gekoppeld. Het is ontwikkeld door dezelfde organisatie als PRINCE2®: de Office of Government Commerce (OGC).

De richtlijn is begin 2010 in het Nederlands op de markt gekomen. Het stelt organisaties in staat te voldoen aan recente regelgeving en geeft aan welke essentiële zaken ontwikkeld moeten worden om risicomanagement als bedrijfsproces in te kunnen bedden in de organisatie en de bedrijfsprocessen. Het is bewust niet verplichtend, maar een branche-onafhankelijk best practice-model. Het betreft alle medewerkers in een organisatie, vervangt niet, maar voorziet in een structuur, kaders en een communicatieomgeving.

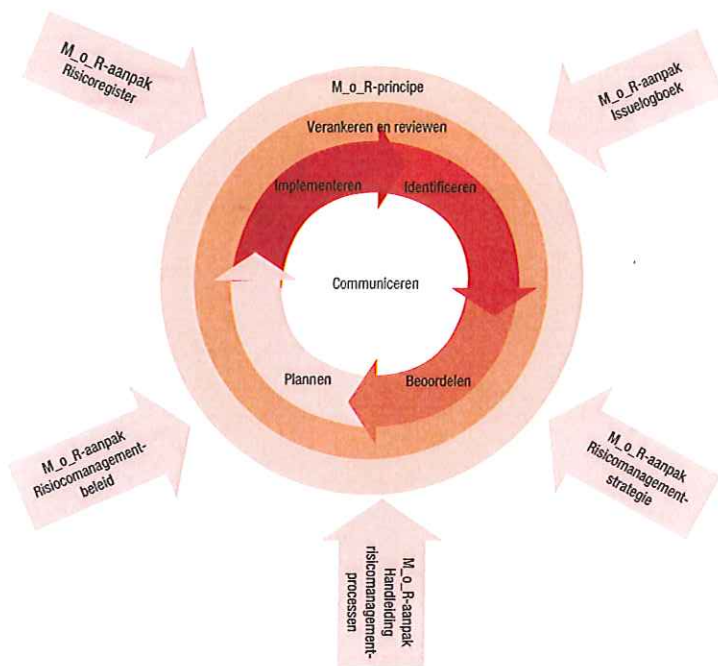
#### Uitleg model

Het doel van risicomanagement volgens M\_o\_R is het ondersteunen van besluitvorming door een goed zicht op de risico's en hun waarschijnlijke impact. Het model onderscheidt vier kernconcepten:

- **Principes**  
De principes zijn essentieel voor een ontwikkeling van volwassen risicomanagement. Zij zijn afgeleid van corporate governanceprincipes met de erkenning dat risicomanagement onderdeel is van de interne control van organisaties.
- **Aanpak**  
Elke organisatie dient de principes aan te passen en accepteren. Deze afspraken worden vervolgens vastgelegd in beleid, een proceshandleiding en strategiedocumenten en worden ondersteund door risicoregisters en incidentenregistratie.
- **Proces**  
Het risicomanagementproces onderscheidt vier hoofdstappen om risico's te identificeren, beoordelen en beheersen.
- **Verankeren en reviewen**  
Als aan bovenstaande onderdelen is voldaan, dient de organisatie ervoor te zorgen dat iedereen zich houdt aan de afspraken en dat verbeteringen worden doorgevoerd op alle niveaus.

#### Sterke punten

M\_o\_R (ook in het Nederlands) omschrijft zeer uitgebreid en met handige checklists alle stappen rondom risicomanagement, inclusief de mogelijke belemmeringen. Zo wordt o.a. ingegaan op het volwassenheidsmodel risicomanagement, of de selectie van risicomanagementsoftware. Het model is in combinatie met de ISO-norm goed bruikbaar.



Figuur 4. (M\_o\_R Framework)

Het M\_o\_R-model maakt helder welke informatie nodig is om risicomanagement door te voeren. De bijbehorende documenten beschrijven in eenvoudige termen hoe de invoer van risicomanagement moet worden aangepakt – en in de loop der tijd geïntegreerd kan worden in de organisatiecultuur. De activiteiten die ondernomen worden, de volgorde waarin ze worden ondernomen en de rollen en verantwoordelijkheden die nodig zijn voor deze uitvoering worden beschreven.

- Risicomanagementbeleid: communiceert hoe risicomanagement door een hele organisatie heen (of in een deel van een organisatie) wordt geïmplementeerd om het realiseren van haar strategische doelstellingen te ondersteunen.
- Handleiding risicomanagementprocessen: beschrijft de reeks stappen (van Context tot en met Implementeren) en hun respectievelijke verbonden activiteiten, die noodzakelijk zijn voor de uitvoering van risicomanagement.
- Risicomanagementstrategie: beschrijft de risicomanagementactiviteiten die voor een bepaalde organisatieactiviteit worden ondernomen.
- Risicoregister: legt vast en onderhoudt informatie over alle geïdentificeerde bedreigingen en kansen die gerelateerd zijn aan een specifieke organisatieactiviteit.
- Issuelogboek: legt informatie vast over alle geïdentificeerde issues die al hebben plaatsgevonden en actie vereisen, op een consistente en gestructureerde manier, en onderhoudt deze. Tot deze issues kunnen risico's behoren die werkelijkheid zijn geworden en zijn veranderd van mogelijke gebeurtenissen in werkelijke gebeurtenissen.

## De praktijk

Het topmanagement van organisaties zit in toenemende mate in een spagaat. Aan de ene kant wordt de wereld complexer. Er zijn ketens en systemen van vele externe risico's en kansen. De organisatie moet voortdurend kiezen hoe daarmee om te gaan. Aan de andere kant bestaat er naast risicomanagement ook risicoverantwoording: organisaties moeten gemaakte keuzes goed kunnen onderbouwen – bewijst – zodat de accountant zich hierover kan uitspreken.

Los van deze spagaat is er een fundamenteel probleem rondom de verankering van risicomanagement; de individuele mens. Kahneman toonde aan dat mensen een aversie tegen verlies hebben.<sup>1</sup> In tegenstelling tot succes praten we liever niet over mogelijk verlies (bijv. het niet behalen van je doelstelling). We nemen zelfs meer risico om het probleem of het verlies weg te werken.

*Er zijn drie goede modellen voor integraal risicomanagement. De keuze voor een bepaalde norm hangt af van wat een organisatie belangrijk vindt*

De drie modellen bieden handvatten en het voordeel dat alle gebruikers ervan dezelfde 'risicomanagementtaal' spreken. De praktijk leert echter dat er meer nodig is voor een succesvolle verankering van risicomanagement in een organisatie: de juiste positionering in de organisatie, de juiste *tone at the top*, aandacht voor de individuele manager.

### Tone en borging in de top

De directie staat in deze tijd continue voor risicovolle keuzes, voor de gemiddelde medewerker is dat niet altijd duidelijk. Om te voorkomen dat door kopieergedrag iedereen op de werkvloer spontaan risico's gaat nemen is het van belang om meer over dit soort afwegingen te communiceren.

Daarnaast is het van belang is om in woord én daad risicomanagement op de agenda te zetten. In het verleden is risicomanagement te snel gedelegeerd. In woord dient de directie het beleid, en haar visie door middel van de principes naar de organisatie te communiceren. In daad door actief naar risico's te vragen en in directieoverleg de top tien per afdeling gezamenlijk te bespreken.

### Positionering: risicomanagement of risicoverantwoording

De positionering wordt voor een belangrijk deel bepaald door waar de nadruk op komt te liggen, risicomanagement of risicoverantwoording. Ligt de nadruk meer op verantwoording dan ligt het voor de hand dat de auditafdeling/financiële afdeling /controller de aanjagers van het proces zijn, ondersteund door de externe accountant.

Gaat het de organisatie naast verantwoording meer om het managen van de huidige onzekerheden, dan dient alles in het werk gesteld te worden om het 'iets' van de organisatie te maken. Om hier invulling aan te geven verschijnen risk committees, risicostuurgroepen die op integraal niveau het proces aanjagen en het integrale risicoprofiel beoordelen. Ook nemen topmanagers zitting in dergelijke stuurgroepen om aan te geven dat zij het onderwerp serieus nemen. De samenstelling van dit soort stuurgroepen is divers, hoewel er altijd financiële en juridische kennis aanwezig is. Los van de achtergrond zijn sociale vaardigheden (met name proactiviteit) van het team van belang. Natuurlijk horen bij de positionering ook de toewijzing van taken en verantwoordelijkheden maar bovenal van bevoegdheden.

### Aandacht voor de individuele manager.

Een grote valkuil bij het borgen van risicomanagement is de top-down benadering. Het werkt niet wanneer het topmanagement alleen algemeen beleid formuleert, tezamen met een 'risicoformat' dat individuele managers moeten invullen.

Betrokkenheid kweken en ondersteuning bieden is een must om integraal management in te bedden in de organisatie. Bij het proces van risicoverantwoording moeten medewerkers instrumenten en training krijgen die het mogelijk maken het proces zo snel en efficiënt mogelijk te doorlopen. Dan wordt het een kwestie van enkele malen per jaar de risico top tien goed door te nemen.

In het geval van nieuwe risico's die opkomen – bijvoorbeeld de te nemen keuzes rondom bezuinigingen, welke projecten kunnen we zonder risico vertragen? – moet er een pragmatische aanpak zijn die het mogelijk maakt om snel de juiste keuzes rondom risico's te maken en de juiste prioriteiten te stellen: wat is een verantwoord risico, wat niet? De manager moet ten slotte het gevoel hebben – en daarin gestimuleerd worden – dat hij expliciet kan vragen welke risico's het behalen van de doelstellingen in gevaar kunnen brengen. Regelmatig en expliciet hiernaar vragen maakt de hele organisatie risicobewuster.

### Conclusie

Er zijn drie goede modellen voor integraal risicomanagement. De keuze voor een bepaalde norm hangt af van wat een organisatie belangrijk vindt: status/bekendheid (COSO, ISO), praktische hulpmiddelen (M\_o\_R) of toegankelijkheid (ISO, M\_o\_R).

De risicomanagementmodellen bieden structuur en geven handvatten, waardoor ze zeker bijdragen aan het slagen van de implementatie van integraal risicomanagement. Echter, de sleutels tot succes zijn juiste positionering in de organisatie, expliciete steun vanuit de top en ondersteuning en stimulering van risicobewustzijn bij individuele managers.

### Risicomanagementmodel gemeente Amsterdam

De gemeente Amsterdam gebruikt de ISO 31000-structuur om risicomanagement vorm te geven binnen de gemeente. Met name de positieve formulering spreekt aan, waardoor risicomanagement hier nadrukkelijk ook de kansen in beeld brengt. Een ander pluspunt is de benadering vanuit principes en het oog voor het belang van aansluiting bij bestaande bedrijfsprocessen. De expertisegroep risicomanagement heeft conform de structuur haar eigen tegeltjes wijsheden (principes) bedacht.

### Auteur

Robert 't Hart is directeur van het Nederlands Adviesbureau voor Risicomanagement en docent bij de master Risicomanagement aan de Universiteit Twente.

### Noten

- 1 Aversie tegen verlies (Loss aversion). Daniel Kahneman (Tel Aviv, 5 maart 1934), Israëlische psycholoog, is een belangrijke pionier op het grensvlak van de economie en psychologie. Hij maakte in zijn publicaties korte metten met het idee van de rationeel calculerende mens die in zijn eigen voordeel handelt en introduceerde de menselijke psyche in de economie. In 2002 won hij de Prijs van de Zweedse Rijksbank voor economie voor "het integreren van psychologische inzichten met de economische wetenschap, in het bijzonder met betrekking tot het menselijk beoordelingsvermogen en de besluitvorming onder onzekerheid."