Drs. Urjan Claassen RA RE CIA

HANDBOEK

Risico-management

Integratie van risico- en prestatie-management

2e HERZIENE DRUK

Management IMPACT

Handboek risicomanagement

Drs. Urjan Claassen RA RE CIA

Handboek risicomanagement

Integratie van risico- en prestatiemanagement

Tweede, herziene druk

MANAGEMENT IMPACT

Samensteller(s) en de uitgever zijn zich volledig bewust van hun taak een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kunnen zij geen aansprakelijkheid aanvaarden voor onjuistheden die eventueel in deze uitgave voorkomen.

Management Impact is een onderdeel Boom uitgevers Amsterdam.

Redactie: Nettie Dekker, www.kortwegdekker.nl
Vormgeving en opmaak: Bottenheft
Foto op omslag: Shutterstock

ISBN 978 94 6276 317 3
NUR 801

Eerste druk, eerste oplage 2009 (Kluwer, Deventer)
Eerste druk, tweede oplage 2015 (Vakmedianet, Deventer)
Tweede, herziene druk 2019 (Management Impact, Deventer)

Voorwoord

Volgens het woordenboek is het Nederlands sinds 1525 verrijkt met het woord 'risico'. Hoewel er twijfel bestaat of het woord 'risico' is afgeleid van het Latijnse 'resecare' (snoeien, afsnijden) of het Arabische 'rizq' (lot, fortuin, zegening) bestaat er wel overeenstemming over de betekenis hiervan: gevaar voor schade of verlies of kansen die zich bij een gebeurtenis voordoen. En waar gevaar is, bestaat de neiging dit te willen bezweren, negeren of te beheersen. Voor veel directies en managementteams vormt het onderwerp 'risico' of risicomanagement dan ook, impliciet of expliciet, een vast terugkerend onderdeel van de bestuurlijke agenda. De reden hiervoor is gelegen in de aantoonbare toegevoegde waarde die risicomanagement heeft. Adequaat risicomanagement kan een wezenlijke bijdrage leveren aan het daadwerkelijk realiseren van organisatiedoelstellingen, adequate rapportage hierover en het inrichten van een efficiënte bedrijfsvoering.

Wereldwijd vormt het COSO ERM-model verreweg het meest door directies van organisaties als toezichthouders en auditors gebruikte raamwerk voor het inrichten en beoordelen van risicomanagement. Dit model is in 2004 uitgevaardigd en vernieuwd in 2017 door de Committee of Sponsoring Organizations of the Treadway Commission (COSO) en heeft tot doel organisaties te helpen waarde te creëren voor aandeelhouders en andere belanghebbenden door risicomanagement en prestatiemanagement met elkaar te verbinden.

Ondanks het gegeven dat het COSO ERM-model wereldwijd veelvoudig wordt toegepast, bestaat er ook kritiek op. Zo wordt het model vaak theoretisch en conceptueel genoemd, ontbreekt er een eenduidig normenkader voor de beoordeling van de toepassing van COSO ERM en voorziet het niet in een duidelijk stappenplan voor de implementatie.

In dit boek beoog ik deze bezwaren zoveel mogelijk weg te nemen en de praktische toepasbaarheid van het COSO ERM-model voor operationele medewerkers, managers, adviseurs en auditors te vergroten door de verschillende componenten van het model verder uit te diepen en handvatten te bieden voor de toepassing ervan. Om dit te bereiken heb ik de principes en uitgangspunten van het COSO ERM-model doorvertaald naar een meer pragmatische en gestructureerde routekaart.

Inhoud

1 Inleiding

1.1 Waarom risicomanagement?

Van bestuurders, collega's of studenten krijg ik met enige regelmaat de vraag wat de feitelijke toegevoegde waarde is van risicomanagement voor een organisatie. Waarom moeten we aan risicomanagement doen?

Veelgehoorde opmerkingen in dit kader zijn: 'We doen dit voor de accountant of de financiële controller', 'Risicomanagement betekent extra werk en checklists' en 'Risicomanagement is toch gewoon je werk goed doen?' Hieruit leid ik af dat bij bepaalde groepen het beeld bestaat dat risicomanagement vooral toegevoegde waarde betekent voor anderen en niet voor de organisatie zelf. Dit is zorgelijk. Zonder een duidelijk antwoord te hebben op de vraag waarom een organisatie aan risicomanagement moet doen, is de kans groot dat elk initiatief op dit terrein mislukt. Kortom: we zullen eerst onszelf moeten overtuigen van het nut en de noodzaak van risicomanagement alvorens we verdere organisatorische of inhoudelijke stappen kunnen zetten.

1.1.1 CONFORMANCE- EN PERFORMANCE-MOTIEF

Het nut en de noodzaak voor risicomanagement zijn gelegen in een tweetal basisprincipes die het bestaansrecht van elke organisatie bepalen: het conformance- en performance-motief.

Conformance-motief
Het eerste basisprincipe heeft betrekking op het voldoen aan wet- en regelgeving, zoals fiscale en operationele wetgeving of corporate-governancecodes. Organisaties zullen zich moeten confirmeren aan wet- en regelgeving. Ingeval een organisatie zich niet houdt aan wet- en regelgeving kan dit leiden tot sancties, zoals boetes of het kwijtraken van vergunningen. Ook kunnen meer schades in termen van tijd en geld het gevolg zijn van 'non-conformance'. Denk hierbij bijvoorbeeld aan vertragingen van bouwprojecten of onverwachte juridische kosten. Feitelijk biedt het voldoen aan wet- en regelgeving een 'licence to operate', ofwel een licentie om de bedrijfsvoering te kunnen uitoefenen. Het voldoen aan wet- en regelgeving wordt ook aangeduid met de term conformance-motief.

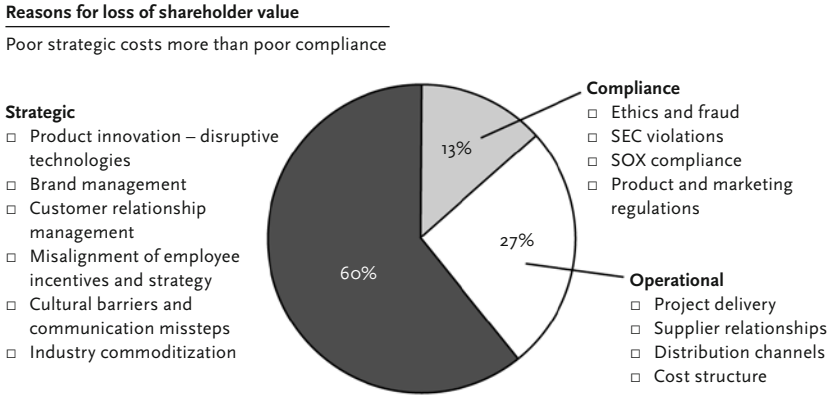
Door risico's te inventariseren ten aanzien van relevante wet- en regelgeving en hiertoe een stelsel van beheersingsmaatregelen in te richten kan op efficiënte en effectieve wijze worden voldaan aan wet- en regelgeving. Risicomanagement is hierbij een nuttig hulpmiddel. Risicomanagement kent echter wel een sterk defensief karakter, 'het moet', en het heeft daardoor mogelijk een 'check the box-mentaliteit' tot gevolg.

Performance-motief

Het tweede basisprincipe heeft betrekking op het creëren van toegevoegde waarde voor klanten en burgers. In het bedrijfsleven zal dit met name betrekking hebben op het creëren van aandeelhouderswaarde. In de publieke sector zal het performance-motief betrekking hebben op het realiseren van maatschappelijke doelstellingen. Hierbij kent risicomanagement een offensief karakter, het is gericht op bedreigingen die het bereiken van deze doelstellingen in de weg kunnen staan. Het performance-motief is dan ook gericht op het waarborgen van het (commerciële) bestaansrecht van de organisatie, of wel het is een 'licence to survive'.

Interessant in dit kader is een onderzoek van Booz Allen Hamilton uit 2006, dat onderzocht wat de belangrijkste redenen voor het verlies van aandeelhouderswaarde zijn (zie figuur 1.1). Dit onderzoek toonde aan dat in slechts 13% van de onderzochte ondernemingen het verlies aan aandeelhouderswaarde, of breder geformuleerd 'maatschappelijk nut', te wijten was aan het niet voldoen aan wet- en regelgeving. De overige 87% was te wijten aan operationele en strategische blunders.

Figuur 1.1 Redenen voor het verlies aan aandeelhouderswaarde (bron: Booz Allen Hamilton, 2004)



1.1.2 VAN RISICOMANAGEMENT NAAR INTEGRAAL RISICOMANAGEMENT

Zoals uit het onderzoek van Booz Allen Hamilton blijkt, wordt het bestaansrecht van organisaties in hoge mate bedreigd door andere soorten risico's dan waar ze traditioneel gewend zijn om naar te kijken. Als uw medewerkers of collega's aangeven dat risicomanagement 'moet van de wetgever of van de accountant' bedoelen ze veelal compliance-risico's. In dat geval wordt risicomanagement ervaren vanuit het conformance-motief: het moet, maar we zien er zelf niet de toegevoegde waarde van, met als gevolg dat het draagvlak binnen de organisatie zeer beperkt is.

Inmiddels weten we dat het niet bereiken van ambities en het niet nakomen van beloftes aan aandeelhouders in belangrijke mate samengaan met het goed beheersen van strategische en operationele risico's. Het is dus zaak om risicomanagement in een breder perspectief te bezien en het meer integraal te benaderen.

Integraal risicomanagement betekent in de eerste plaats dat risico's van verschillende risicogebieden in onderlinge samenhang worden bezien en gemanaged. In de tweede plaats betekent integraal risicomanagement dat risicomanagementprocessen op verschillende hiërarchische niveaus binnen de organisatie worden ingericht en dat de verschillende niveaus interactief met elkaar samenwerken bij het identificeren, analyseren en beheersen van risico's. Door risico's in samenhang te bezien wordt het voor organisaties eenvoudiger om risicomanagement vanuit een performance-motief te beleven in plaats van vanuit een conformance-motief.

1.2 Risicomanagementmodellen

Er zijn vele risicomanagementmodellen en -standaarden in omloop die allemaal hun eigen specifieke achtergrond en kenmerken hebben. Sommige modellen en standaarden houden verband met een specifiek vakgebied, zoals de wettelijk verplichte risico-inventarisatie en -evaluatie (RI&E) voor arbo-veiligheid of Solvency II voor de verzekeringsbranche. Andere modellen zijn meer algemeen van aard, zoals COSO ERM, ISO 31000, Management_of_Risk en RISMAN. Dit boek gaat in op de twee risicomanagementmodellen die al langere tijd wereldwijd het meest gebruikt worden: COSO ERM en ISO 31000.

Hoewel deze risicomanagementmodellen in aard en opzet van elkaar verschillen, zijn de basiscomponenten in essentie hetzelfde. Hierdoor is de essentie van risicomanagement terug te brengen tot de volgende zes basisstappen:

1. het formuleren van strategie en doelstellingen;

2. het inventariseren van risico's;
3. het beoordelen van risico's;
4. een keuze maken in hoe om te gaan met de risico's (risicostrategie);
5. het beheersen van risico;
6. communicatie en monitoren.

Deze zes stappen noem ik in dit boek de 'risicomanagementcyclus', die in dit boek is gebruikt om een aantal hoofdstukken te structuren. In hoofdstuk 3 ga ik nader in op de risicomanagementcyclus. In dit hoofdstuk ga ik eerst verder in op de twee vaakst gebruikte risicomanagementmodellen: COSO ERM en ISO31000.

1.2.1 COSO ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is in 1985 in de Verenigde Staten opgericht door The American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) en The Institute of Management Accountants (IMA). Het COSO-platform had tot doel de Treadway-commissie te ondersteunen bij het ontwikkelen van standaarden op het gebied van interne beheersing. De Treadway-commissie was een privaat initiatief dat was opgericht in de jaren 1970 en 1980 als gevolg van diverse malversaties, en was gericht op het bestrijden van frauduleuze financiële verslaggeving.

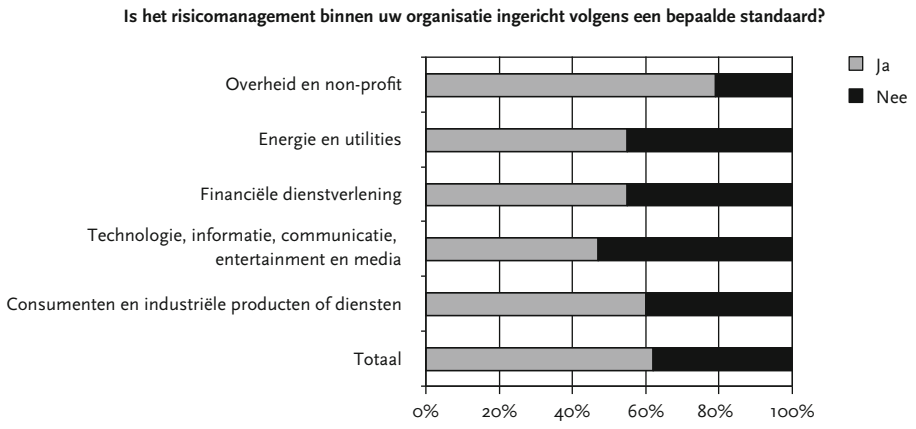
In 1992 verscheen het COSO-rapport 'Internal Control – Integrated Framework'. Dit rapport had tot doel om een algemeen aanvaard begrippenkader voor internal control te bieden. Daarnaast beoogde het rapport het management van organisaties te helpen bij het verbeteren van hun internal-controlsysteem met behulp van zeventien principes. Hierbij ligt primair de focus op betrouwbare financiële verslaggeving, de operationele bedrijfsvoering en het voldoen aan wet- en regelgeving (compliance). In 2004 publiceerde COSO een nieuw rapport, 'COSO Enterprise Risk Management (ERM) – Integrated Framework', dat een verdere verbreding was van het COSO-rapport uit 1992. In COSO ERM is internal control ook een middel voor het beheersen van strategische risico's en het bereiken van strategische doelstellingen. Binnen COSO ERM wordt ervan uitgegaan dat de organisatie al strategische keuzes en doelstellingen heeft gedefinieerd, die als basis dienen voor het formuleren van strategische risico's. In 2017 bracht COSO het rapport 'Enterprise Risk Management – Aligning Risk with Strategy and Performance' uit. Dit rapport is een update van het COSO ERM-raamwerk uit 2004.

In tegenstelling tot het COSO ERM-raamwerk uit 2004, worden risicomanagement en interne beheersing nu ook ingezet voor het formuleren van een strategie en bij de keuze van strategische doelstellingen. Strategie-keuzes werden in het COSO ERM – Integrated Framework uit 2004 als een gegeven beschouwd.

COSO meest gebruikt

Wereldwijd is COSO een van de meest gebruikte risicomanagementmodellen. Uit onderzoek van PricewaterhouseCoopers (PwC) en de Rijksuniversiteit Groningen in 2005 onder leden van het Controllers Instituut blijkt dat 63% van de respondenten gebruikmaakt van een standaardrisicomanagementmodel (zie figuur 1.2). Van deze respondenten hanteert bijna driekwart COSO.

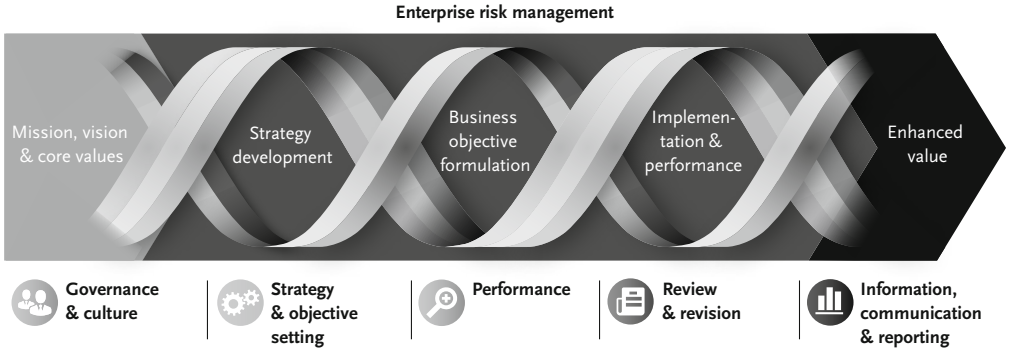
Figuur 1.2 Gebruik van risicomanagementstandaarden in Nederland (bron: PwC en Rijksuniversiteit Groningen, 2005)



Twintig principes geclusterd tot vijf basiscomponenten

Het geactualiseerde COSO ERM-raamwerk bestaat uit twintig 'principes', die geclusterd zijn tot vijf basiscomponenten. Deze vijf basiscomponenten vormen tezamen het risicomanagement'raamwerk' en hebben tot doel risicomanagement volledig te integreren binnen de bestaande bedrijfsactiviteiten en bedrijfsprocessen. Integratie wordt hierbij breed uitgelegd en wordt geacht onderdeel te zijn van alle onderdelen van beleidsformulering en beleidsexecutie. Van visie en missie tot strategie en beleid, van het formuleren van doelstellingen tot het meten en evalueren van prestaties. In figuur 1.3 worden de vijf basiscomponenten van het vernieuwde COSO ERM-raamwerk uitgelegd.

Figuur 1.3 Enterprise Risk Management – Integrating with Strategy and Performance



Governance & culture	Taken en verantwoordelijkheden ten aanzien van cultuur, houding en gedrag alsmede risicotoezicht en risicobewustzijn
Strategy & objective setting	Risicomanagement is onderdeel van het strategische planningsproces. Risico's en de risicobereidheid worden meegewogen in strategische keuzes en bijbehorende doelstellingen. Doelstellingen dienen als basis voor het identificeren en beoordelen van en het reageren op risico's
Performance	Het identificeren en beoordelen van en reageren op risico's die van invloed zijn op het behalen van de strategie en bijbehorende doelstellingen. Hierbij wordt expliciet rekening gehouden met de risicobereidheid van de organisatie. Stakeholders worden op portefeuilleniveau geïnformeerd over het risicoprofiel van de organisatie
Review & revision	Beoordelen van de bedrijfsprestaties en de effectiviteit van de risicobeheersing. Waar nodig worden verbeteringen doorgevoerd
Information, communication & reporting	Het vergaren en delen van informatie binnen en buiten de organisatie en tussen de verschillende hiërarchische niveaus

Zoals eerder aangegeven, bestaat het COSO-raamwerk uit een twintigtal principes die zijn geclusterd naar vijf basiscomponenten die tezamen een raamwerk vormen. Principes dienen hierbij gelezen te worden als 'karakteristieken' of 'kenmerken' van effectief risicomanagement.

De relatie tussen de principes en het raamwerk is dat de principes beschrijven wat dient te worden bereikt. Het raamwerk biedt handvatten en een kader *hoe* deze principes kunnen worden bereikt en hoe de verschillende componenten met elkaar samenwerken.

In figuur 1.4 is een korte samenvatting opgenomen van de twintig principes achter het COSO ERM-raamwerk uit 2017.

De genoemde principes dienen te worden toegepast op de organisatie, rekening houdend met de aard, omvang en mogelijkheden van de organisatie. Zo zal een organisatie met twintigduizend medewerkers andere eisen stellen aan de inrichting van haar risicomanagementsysteem dan een organisatie met tien medewerkers. Daarnaast kan elk principe op verschillende manieren worden toegepast. Kortom: het inrichten van risicomanagement is maatwerk.

Figuur 1.4 Principes COSO ERM (2017)

Kritiek op COSO ERM

Ondanks het gegeven dat COSO ERM wereldwijd veelvoudig wordt toegepast, is er ook kritiek op het model. Kritiek die zich in belangrijke mate richt op de praktische bruikbaarheid van het model. Onderstaand volgt een overzicht van veelgehoorde punten van kritiek.

Geen eenduidig normenkader

Veelgehoorde kritiek op COSO ERM betreft het theoretische karakter van het model. COSO ERM is conceptueel van aard en beschrijft slechts een aantal aandachtspunten voor de inrichting van risicomanagement en interne beheersing. Wel zijn er voor COSO ERM ondersteunende werkdocumenten beschikbaar waarin met behulp van praktische voorbeelden de (deel)componenten nader worden uitgelegd. Echter, een concreet en eenduidig normenkader voor het beoordelen van (de effectiviteit van) risicomanagement en interne beheersingssystemen ontbreekt. Dit is jammer, omdat van veel bestuurders in navolging van corporate-governanceregelgeving een expliciete uitspraak wordt verwacht over de effectiviteit van – delen van – hun risicomanagement- en interne beheersingssystemen.

Ontbreken stappenplan

Voor het implementeren van risicomanagement is een eenduidig en concreet stappenplan van wezenlijk belang. COSO ERM voorziet niet in een dergelijk stappenplan voor implementatie. Veel organisaties worstelen dan ook met de vraag waar en hoe te beginnen. Afhankelijk van de aanleiding om met risicomanagement te beginnen en de sponsoren van de implementatie van risicomanagement leidt dit tot specifieke complicaties.

Strategische, tactische en operationele beheersing
Interne beheersing binnen het COSO ERM-raamwerk wordt in beperkte mate gespecificeerd naar de verschillende hiërarchische niveaus van een organisatie. Interne beheersing van risico's op bestuurlijk niveau kent een geheel ander instrumentarium dan de interne beheersing van risico's op operationeel niveau. Dit heeft alles te maken met het feit dat bestuurders met een ander abstractieniveau naar de organisatie kijken dan een teamleider of procesmedewerker.

1.2.2 ISO 31000

Een ander veelgebruikt risicomanagementmodel is de 31000-standaard van de International Organization for Standardization (ISO), ook wel de ISO 31000-standaard genoemd. Op initiatief van Japan en Australië stelde de ISO in 2005 een werkgroep samen om een algemene richtlijn voor risicomanagement te ontwikkelen. Aanleiding voor dit initiatief was enerzijds de groeiende belangstelling voor het onderwerp risicomanagement en anderzijds het besef dat de bestaande ISO-standaarden hier nog onvoldoende invulling aan gaven. In deze werkgroep participeerden circa 25 landen.

Met het ontwikkelen van de 31000-standaarden beoogt de ISO twee doelstellingen te bereiken. In de eerste plaats het ontwikkelen van een algemeen kader voor het implementeren van risicomanagement en ten tweede het ontwikkelen van een overkoepelende risicomanagementkapstop voor sector- en onderwerpspecifieke ISO-standaarden. In 2009 is de eerste versie van deze risicomanagementstandaard tot stand gekomen. Deze bestaat uit drie hoofdonderdelen:
1. principes voor risicomanagement;
2. een raamwerk dat handvatten geeft voor de invulling van de risicomanagementprincipes;
3. het risicomanagementproces voor de operationele uitvoering van risicomanagement.

In 2018 heeft er een herziening plaatsgevonden van de ISO 31000-standaard. De aanleiding hiervoor was de kritiek dat de standaard uit 2009 nog onvoldoende geschikt was om risicomanagement effectief te integreren binnen een organisatie. Vereenvoudiging en meer aandacht voor leiderschap en iteratie waren noodzakelijk.

Structuur van ISO 31000
Het fundament van de ISO 31000-standaard bestaat uit acht principes, die erop gericht zijn waarde te creëren en te beschermen. Deze principes zijn:

1. *proportionaliteit*: het raamwerk en het risicomanagementproces dienen te passen bij de aard en omvang van de organisatie;
2. *aansluiting*: het risicomanagement dient aan te sluiten en in lijn te zijn met de overige activiteiten van de organisatie;
3. *diepgang*: voor effectief risicomanagement dienen risicomanagementtaken gestructureerd plaats te vinden en voldoende diepgang te hebben;
4. *integratie*: het risicomanagement dient geïntegreerd te zijn in de reguliere bedrijfsvoering;
5. *dynamisch*: het risicomanagementsysteem dient te worden verbeterd en onderhouden gezien de veranderende omgeving;
6. *beperkingen*: er wordt expliciet rekening gehouden met het gegeven dat beschikbare informatie beperkt kan zijn;
7. *cultuur en gedrag*: menselijk gedrag en cultuur beïnvloeden alle aspecten van het risicomanagement;
8. *leren*: het risicomanagement verbetert continu door te leren van opgedane ervaringen.

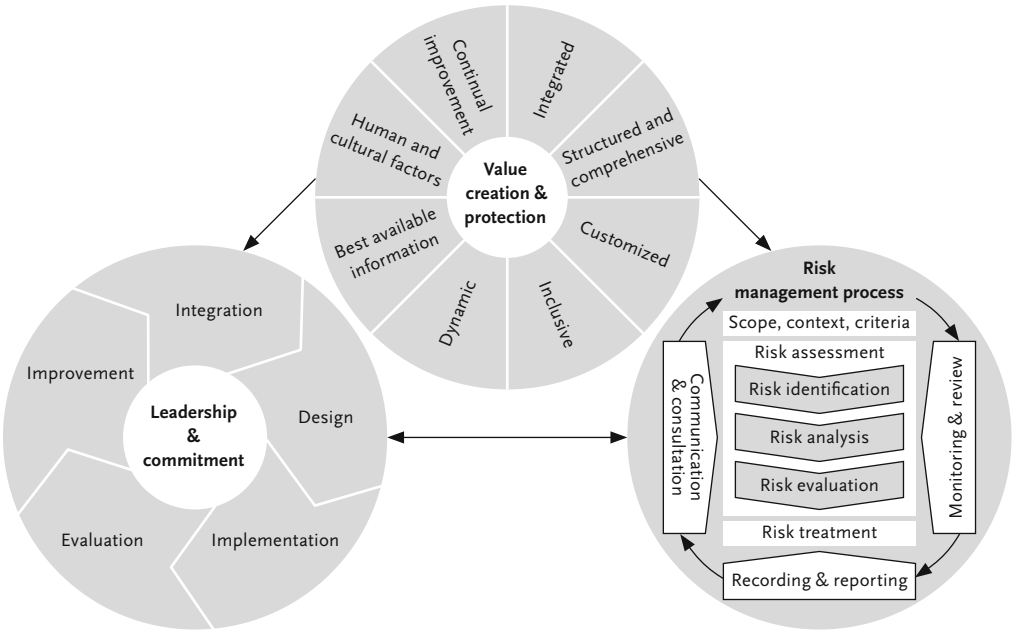
De eerste vijf principes houden verband met de wijze waarop risicomanagement binnen de organisatie wordt vormgegeven. De principes 6 tot en met 8 houden verband met de wijze waarop het risicomanagement operationeel wordt uitgevoerd.

De wijze waarop de principes kunnen worden bereikt, wordt binnen ISO 31000 (net als bij COSO ERM) vormgegeven door het aanreiken van een raamwerk. Binnen ISO 31000 bestaat dit raamwerk uit de volgende componenten:
– ontwerpen;
– implementeren;
– evalueren;
– verbeteren;
– integreren.

Het laatste, meer operationele, onderdeel is het risicomanagementproces. De onderdelen van het risicomanagementproces binnen ISO 31000 vertonen grote gelijkenis met de elementaire stappen van risicomanagement die in het begin van deze paragraaf genoemd zijn (zie figuur 1.5). Dit zijn de identificatie, analyse, evaluatie en beheersing van risico's, met daarnaast aandacht voor consultatie en communicatie (rapportages) en monitoring en review.

Kritiek op ISO 31000
Natuurlijk zijn er bij ISO 31000 ook enkele kanttekeningen te plaatsen die aandacht verdienen. De kritiekpunten bij ISO 31000 overlappen met de kritiek op COSO ERM.

Figuur 1.5 ISO 31000 (2018)



Smalle definitie van interne beheersing
Beheersing richt zich binnen ISO 31000 op waarborgen dat risico's adequaat worden beheerst. Beheersing richt zich hierbij op het reduceren van (de gevolgen van) risico's. De betekenis van beheersing in relatie tot het verzilveren van kansen wordt niet nader uitgewerkt. De toegevoegde waarde van strategische planning en planning en control blijft binnen ISO 31000 dan ook onderbelicht.

Geen eenduidig normenkader
Op de tweede plaats geeft ook ISO 31000 geen inhoudelijk normenkader voor het beoordelen van de effectiviteit van risicomanagement. Er dient nog steeds een inhoudelijk normenkader te worden ontwikkeld waarmee deze beoordeling kan plaatsvinden.

1.3 Handboek risicomanagement

1.3.1 DOELSTELLING

De doelstelling van dit boek is om een meer uitgewerkte methodiek te bieden om risicomanagement binnen uw organisatie beter handen en voeten te geven.

Hierbij wordt zoveel mogelijk gebruikgemaakt van het goede van bestaande risicomanagementmodellen, in het bijzonder COSO ERM en ISO 31000, en deze worden waar mogelijk aangevuld om kritiekpunten weg te nemen.

1.3.2 UITGANGSPUNTEN

Voor het uitwerken van de aanpak van risicomanagement in dit boek is een aantal uitgangspunten gedefinieerd. Deze uitgangspunten zijn van invloed op de aard en wijze waarop risicomanagement wordt vormgegeven. Deze uitgangspunten zijn:

- Binnen dit boek wordt corporate governance bezien vanuit twee aandachtsgebieden: goed bestuur en het afleggen van verantwoording.
- Risicomanagement wordt binnen dit boek eveneens gezien als een onderdeel van goed bestuur. De toepassing van risicomanagement, als onderdeel van corporate governance, is in de praktijk veelal gericht op getrouwe (financiële) verantwoording en een deugdelijke interne beheersing.
- De kern van risicomanagement zoals beschreven in dit boek, is het bevorderen van waardecreatie en het verbeteren van prestaties. Daarbij richten we ons op strategische planning, de totstandkoming en het realiseren van bedrijfsdoelen en het afleggen van verantwoording aan stakeholders.
- Risicomanagement is een proces dat wordt uitgevoerd door mensen op elk niveau van de organisatie, dat gericht is op het herkennen en managen van potentiële gebeurtenissen die van invloed zijn op de (waarde van de) organisatie.
- Risicomanagement is erop gericht om een redelijke, maar geen absolute, mate van zekerheid te bieden aan het management dat organisatiedoelstellingen worden gerealiseerd.
- Risicomanagement en integraal risicomanagement worden in dit boek als synoniemen gebruikt. 'Integraal' heeft hierbij betrekking op enerzijds een geïntegreerde beheersing van strategische, operationele, financiële en compliance-risico's; deze risico's worden niet enkel vanuit aparte specialistische functies en afdelingen beheerst. Anderzijds heeft 'integraal' betrekking op de organisatiebrede betrokkenheid van mensen.
- Risicomanagement wordt onderverdeeld in strategisch risicomanagement en procesrisicomanagement. Dit onderscheid is van belang in verband met het instrumentarium dat voor het managen van risico's en het verbeteren van prestaties beschikbaar is.
- Verantwoording heeft binnen dit boek betrekking op het afleggen van rekenschap aan stakeholders over strategische keuzes, gerealiseerde prestaties en de effectiviteit van het interne risicomanagement- en beheersingssysteem. De verantwoording over prestaties is gekoppeld aan de (beloofde) bedrijfsdoelstellingen. De verantwoording over interne beheersing heeft betrekking op de getrouwheid van de (financiële) verantwoording en de effectiviteit van de interne beheersing.

– Risicomanagement is zowel een zaak van het (top)management, de toezichthouder, de interne en externe auditor als van de uitvoerder zelf. Het management, de auditor én de medewerker hebben een expliciete verantwoordelijkheid voor het beheersen van risico's en voor het leveren van prestaties. Dit wordt in dit boek aangeduid met de eerste tot en met de vijfde verdedigingslinie van risicomanagement.
– De raad van commissarissen en de raad van toezicht worden in dit boek als synoniemen gebruikt. Beide gaan over de rol van een toezichthoudend orgaan. Het gebruik van deze termen verschilt in de praktijk per branche.

1.4 Voor wie is dit boek geschreven?

Dit boek is geschreven voor operationele medewerkers, managers, adviseurs en auditors die in de praktijk betrokken zijn bij risicomanagement. Dit boek heeft als doel hen te voorzien van praktische handvatten en inzichten om risicomanagement te ontwerpen en te implementeren. Voor *operationele medewerkers* wordt een nadere uitleg gegeven van de betekenis van specifieke documenten en richtlijnen voor risicomanagement. Daarnaast treffen zij in dit boek handvatten aan hoe risico's en beheersingsmaatregelen kunnen worden geïdentificeerd, geanalyseerd en getest. Voor *managers* bevat het boek handreikingen om van hogerhand sturing te geven aan risicomanagement binnen hun organisatie. Aanvullend biedt het boek een kapstok voor de inrichting van een intern beheersingskader voor het laten functioneren van de interne beheersing binnen de lijnorganisatie. Voor *adviseurs* biedt het boek een passende methodiek voor het adviseren van cliënten bij het ontwerpen en inrichten van risicomanagement. *Auditors* kunnen met dit boek hun voordeel doen bij het ontwerpen en inrichten van een risicogebaseerde auditaanpak.

1.5 Verdere indeling van het boek

In dit hoofdstuk heb ik uitgelegd waarom risicomanagement nuttig is en toegevoegde waarde heeft. De reden dat we aan risicomanagement moeten doen, is het veiligstellen van het bestaansrecht van de organisatie, en wel vanuit een conformance- en performance-motief.

In het vervolg van dit handboek zal ik allereerst ingaan op de vraag wat risicomanagement inhoudt. In hoofdstuk 2 zal hiervoor een introductie worden gegeven van corporate governance en van de ontwikkelingen binnen het vakgebied risicomanagement. Deze introductie heeft tot doel de achtergrond te schetsen waarlangs belangrijke principes uit het gedachtegoed in dit boek zijn ontstaan.

De 'wat'-vraag wordt in hoofdstuk 3 gevolgd door de beschrijving van een gemeenschappelijke taal voor risicomanagement.

Op de vraag hoe risicomanagement kan worden uitgevoerd, zal worden ingegaan in de hoofdstukken 4 tot en met 11. Hoofdstuk 4 richt zich op het toepassen van risicomanagement binnen een strategische planning. Hoofdstuk 5 richt zich op de randvoorwaardelijke organisatie van risicomanagement. Het identificeren van risico's voor de organisatiedoelstellingen start in hoofdstuk 6, gevolgd door het inrichten van beheersing (hoofdstuk 7), monitoring en continu verbeteren (hoofdstuk 8), verantwoording aan de buitenwacht (hoofdstuk 9) en de implementatie van risicomanagement (hoofdstuk 10). Risicobeheersing van projecten is uitgewerkt in hoofdstuk 11.

De hoofdstukken 12 en 13 vormen tezamen een naslagwerk van een enkele specifieke onderwerpen. In hoofdstuk 12 wordt een nadere beschouwing gegeven over risicomanagement en de kredietcrisis. In hoofdstuk 13 wordt een nadere uiteenzetting gegeven van de rol van de raad van commissarissen bij risicomanagement en interne risicobeheersing.

2 Ontwikkelingen en achtergronden

2.1 Inleiding

De publieke aandacht voor continuïteit, waardecreatie en het realiseren van bedrijfsdoelstellingen is in de afgelopen decennia steeds verder toegenomen. Dit komt overduidelijk door de crisis van 2008, maar ook daarvoor stonden deze onderwerpen al in de belangstelling. Door boekhoudschandalen en overmatige bonussen voor bestuurders zijn stakeholders vaak bedrogen uitgekomen. Bedrijfsdoelstellingen in termen van winsten (of anderszins) werden niet gerealiseerd en de berichtgeving hierover was onbetrouwbaar of kwam te laat. In toenemende mate willen stakeholders daarom een grotere transparantie van de bedrijfsvoering. Als sprekende voorbeelden noem ik Enron en WorldCom, waarbij duizenden medewerkers hun banen verloren en investeerders miljarden US dollars schade leden als gevolg van een onbetrouwbare financiële verslaggeving. Als gevolg van deze schandalen werd in de Verenigde Staten in juli 2002 de Sarbanes-Oxley Act geïntroduceerd. Het doel van deze wet is het verkrijgen van meer zekerheid over de financiële verslaggeving en de totstandkoming ervan. Sectie 302 en 404 van deze wet verplichten bedrijven zich te verantwoorden over de effectiviteit van de interne beheersing van de financiële verslaggeving.

De wens van stakeholders voor transparantie beperkt zich echter niet tot de betrouwbaarheid van de financiële verslaggeving. Stakeholders willen in toenemende mate openheid over andere onderwerpen, zoals beloningen voor en verantwoordelijkheden van bestuurders en commissarissen, maatschappelijke betrokkenheid en maatschappelijk verantwoord ondernemen. Hiermee wordt de reikwijdte van risicomanagement breder. Strategische, operationele en compliance-risico's zijn vaker onderdeel van risicomanagement. De belangen van stakeholders reiken verder dan een betrouwbare jaarrekening alleen; continuïteit, waardecreatie en het realiseren van doelstellingen staan steeds vaker centraal. Deze toegenomen informatiebehoefte van stakeholders is terug te vinden in wet- en regelgeving en in diverse codes waarin van bestuurders wordt gevraagd verantwoording af te leggen over de inrichting van risicomanagement in brede zin van het woord.

De verantwoordelijkheden van organisaties ten aanzien van stakeholders worden ook wel samengevat onder de noemer 'corporate governance'. Corporate gover-

nance heeft hierbij de betekenis van deugdelijk bestuur. Als we kijken naar de toepassing van corporate governance in de praktijk, heeft ze in belangrijke mate betrekking op verantwoordelijkheden van directies, toezichthouders, externe accountants bij de verantwoording over beheersing. Waardecreatie staat hierbij centraal. De inhoud van het begrip 'waarde' wordt ingevuld door de betrokken stakeholders. Zo zullen aandeelhouders waarde vaak uitdrukken in termen van winst of een stijging van aandelenkoersen. Andere stakeholders zullen waarde beschrijven als een middel om banen te behouden (vakbonden), het zorgvuldig omgaan met flora en fauna (milieuorganisaties) of het tijdig en volledig betalen van belastingen (Belastingdienst). Het begrip waarde heeft betrekking op de verschillende (soorten) belangen van stakeholders.

Waardecreatie reikt verder dan het beheersen van risico's alleen. Ook het benutten van kansen is van belang bij het creëren van waarde. Kansen moeten hierbij zorgvuldig afgewogen worden in het licht van verwachte opbrengsten en de daaraan gekoppelde risico's.

Ingeval bedrijven op grote schaal producten ontwikkelen die niet succesvol zijn op de markt, kan dit ernstige financiële consequenties hebben. Hierdoor komt een belangrijke doelstelling van aandeelhouders, te weten winstgevendheid, ernstig in het gedrang. Wanneer deze verliezen op betrouwbaar wijze worden gerapporteerd, is wel voldaan aan bijvoorbeeld de vereisten van de Sarbanes-Oxley Act, maar is de doelstelling 'winstgevendheid' voor de aandeelhouder nog niet ingelost. Een betrouwbare jaarrekening vormt in mijn optiek dan ook een noodzakelijke randvoorwaarde om aandeelhouders goed te informeren, maar ze is geen garantie voor duurzaam succes. De geplande acties om verliesgevendheid om te buigen in winstgevendheid zijn minstens zo relevant. Het onderkennen van kansen en het verzilveren van deze kansen is van wezenlijk belang om de doelstelling 'winstgevendheid' voor de aandeelhouder te kunnen realiseren.

Ten aanzien van het managen van bedreigingen en kansen zien we belangrijke verschillen. Bedreigingen kunnen veelal direct worden gerelateerd aan beheersingsmaatregelen die door het management dienen te worden gemanaged. Kansen daarentegen, kunnen niet worden gerelateerd aan beheersingsmaatregelen. Kansen dienen te worden uitgewerkt in scenario's, strategieën en bedrijfsplannen, en moeten worden gemonitord.

Dit boek bevat een praktische handreiking voor het inrichten van management control bij waardecreatie. Kenmerkend voor de wijze waarop is het integraal managen van risico's én kansen.

Dit hoofdstuk begint met een nadere uiteenzetting van de betekenis van corporate governance, gevolgd door een beschouwing van de ontwikkeling van risico-

Over de auteur

DRS. URJAN CLAASSEN RA RE CIA (1973) studeerde bedrijfseconomie en accountancy aan de Universiteit van Tilburg, Erasmus Universiteit Rotterdam en het Roskilde Universitetscenter te Denemarken. Na zijn studie is hij lange tijd werkzaam geweest als registeraccountant en IT-auditor bij Arthur Andersen en later KPMG.

Sinds 2005 is Urjan als partner verbonden aan C-Profile en actief op de gebieden audit, (organisatie)advies en innovatie. Vanuit zijn rol adviseert hij menige directie rondom risicomanagement, governance en strategische vraagstukken. Verder is hij intensief betrokken bij het realiseren van nieuwe bedieningsconcepten (en verdienmodellen) voor advieskantoren en overheden. C-Profile is een zeer innovatief advies- en softwarebedrijf binnen de adviesbranche en heeft tot doelstelling advies significant goedkoper en kwalitatief beter aan te bieden. Verder is Urjan een veel gevraagd spreker op congressen en is hij docent aan de Vrije Universiteit van Amsterdam en Nyenrode Business Universiteit.

C-Profile
C-Profile ondersteunt organisaties op het gebied van risicomanagement, organisatieadvies en audit. Verder ondersteunt C-Profile advieskantoren in diverse sectoren en overheidsinstanties met het realiseren van omnichannel adviesconcepten via een adviesplatform. Het adviseren van cliënten wordt hierdoor uiterst efficiënt en effectief vormgegeven dankzij een gecombineerde inzet van meerdere, op elkaar afgestemde communicatiekanalen zoals chat, messaging, e-mail, webcam, call en face. Dit leidt tot significante besparingen in de bedrijfsvoering en rendementsverbeteringen. Verder bevat het C-Profile adviesplatform uitgebreide functionaliteiten en dataverzamelingen voor het geven van data-driven advies. Consultants van C-Profile ondersteunen advieskantoren en overheidsinstanties bij het implementeren en gebruik van het platform binnen hun praktijk. Voor meer informatie over C-Profile en het C-Profile adviesplatform verwijzen we u naar de website www.c-profile.nl.

Het beheersen van risico en het verzilveren van kansen houden veel organisaties bezig. Soms gedreven door ambities en soms door complianceverplichtingen. Echter, de implementatie van risicomanagement is geen sinecure. Veel toezichthouders, directeuren en controllers worstelen met de vraag hoe dit het beste kan worden aangepakt. Dit boek beschrijft een praktische aanpak om risicomanagement effectief en efficiënt te implementeren. Hierbij vormen de principes van het COSO ERM-model, wereldwijd het meest gebruikte model voor risicomanagement, het fundament. De risicomanagementaanpak richt zich op alle functies binnen een organisatie: van toezichthouder tot teamleider en van controllers tot risicomanagers. Het biedt een uniforme gemeenschappelijke taal en geeft alle betrokkenen concrete handvatten voor het identificeren en beheersen van risico's (en kansen). Zowel op strategisch, tactisch als operationeel niveau. In deze herziene druk is in het bijzonder aandacht besteed aan de integratie van risicomanagement en prestatiemanagement. Het management wordt ondersteund bij het maken van de juiste keuzes en het bereiken van doelstellingen door aandacht te besteden aan relevante risico's. Dit boek is een 'must have' voor elke organisatie met ambitie!

Drs. Urjan Claassen RA RE CIA is CEO van C-Profile. C-Profile is gespecialiseerd in risicomanagement en bedienings-concepten (www.cprofile.nl). Daarnaast is hij als docent verbonden aan de Nyenrode Business Universiteit en de Vrije Universiteit Amsterdam.

C Profile
ADVIESPORTALEN

Management IMPACT

www.managementimpact.nl

9 789462 763173