Drs. U.P.W.L.M. Claassen RA RE CIA

Controlling & auditing in de praktijk 102

Risicomanagement in de praktijk

Kluwer, 2012

De CAIP-reeks wordt uitgegeven in samenwerking met Tijdschrift Controlling

Eindredactie: Frieda Crince Le Roy
Redactie: Drs. J. Gieskens AC CCM QT en A. Molenkamp RO

Ontwerp omslag en binnenwerk: Bottenheft

NUR 782-220
ISBN 978 90 13 11143 9

Inhoud

1 Inleiding

Ondernemerschap en het nemen van risico's zijn onlosmakelijk met elkaar verbonden. Welvaart en werkgelegenheid worden enkel mogelijk dankzij investeringen en innovaties, waarvan de mate van succes bij aanvang vermoed maar qua samenstelling en omvang vaak onbekend is. Kortom: zonder risico's geen rendement en zonder rendement geen bestaansrecht. Dit logische verband doet verwachten dat risicomanagement dan ook bij alle organisaties hoog op de bestuurlijke agenda staat. De praktijk wijst echter uit dat dit in veel gevallen niet het geval is. Onder bestuurders en managers rijst met enige regelmaat de vraag wat de feitelijke toegevoegde waarde is van integraal risicomanagement voor een organisatie. Waarom moeten we aan integraal risicomanagement doen?

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

Nut en noodzaak van risicomanagement kunnen worden geduid door middel van een tweetal fundamentele basisprincipes die het bestaansrecht van elke organisatie bepalen: het 'conformance-' en het 'performance'-motief.

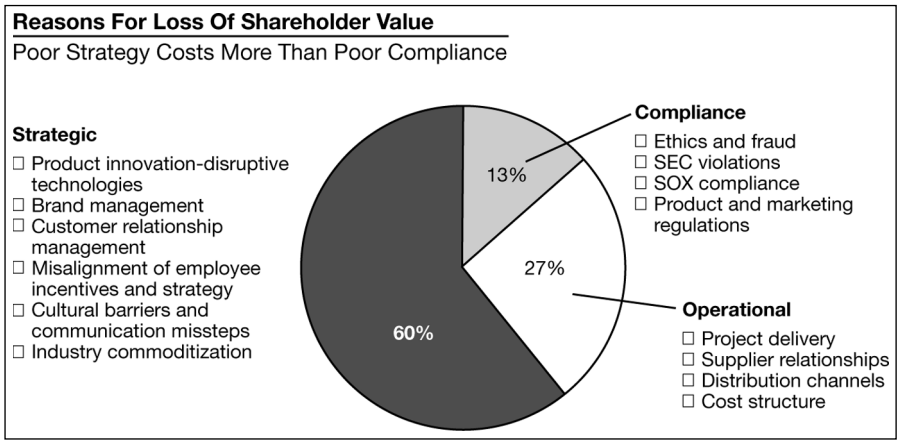
Het 'conformance'-motief
Het eerste basisprincipe heeft betrekking op het voldoen aan wet- en regelgeving, zoals fiscale en operationele wetgeving of corporate-governancecodes. Organisaties zullen zich moeten conformeren aan deze wet- en regelgeving. Ingeval een organisatie zich niet houdt aan wet- en regelgeving, kan dit leiden tot sancties, zoals boetes of het verlies van vergunningen. Ook kunnen meer schades in termen van tijd en geld het gevolg zijn van 'non-conformance'. Denk hierbij bijvoorbeeld aan vertragingen in 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.

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

Het 'performance'-motief
Het tweede basisprincipe heeft betrekking op het creëren van toegevoegde waarde voor cliënten en burgers. In het bedrijfsleven zal dit vooral betrekking hebben op het creëren van aandeelhouderswaarde. In de publieke sector zal het performancemotief 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 performancemotief is dan ook gericht op het waarborgen van het (commerciële) bestaansrecht van de organisatie, ofwel een 'licence to survive'.

Interessant in dit kader is een onderzoek van Booz Allen Hamilton uit 2004 naar de belangrijkste redenen voor het verlies van aandeelhouderswaarde. Dit onderzoek toonde aan dat in slechts 13 procent 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 procent was te wijten aan operationele en strategische blunders.

Figuur 1. Redenen voor het verlies aan aandeelhouderswaarde (bron: Booz Allen Hamilton, 2004)



Modellen voor risicomanagement

Wereldwijd hebben verschillende instanties standaarden ontwikkeld voor de vormgeving van (integraal) risicomanagement. We noemen bijvoorbeeld Australian/New Zealand Risk Management Standard 4360, Basel II en Solvency II. Wereldwijd vormt het COSO ERM-model verreweg het meest gebruikte raamwerk voor de beoordeling en inrichting van risicomanagement. Zowel door directies van organisaties als toezichthouders en auditors. Dit model, uitgevaardigd in 2004 door de Committee of Sponsoring Organizations of the Treadway Commission (COSO), heeft tot doel organisaties te helpen met de beoordeling en verbetering van de interne beheersingssystemen. De afkorting ERM heeft betrekking op de internationale, Engelstalige titel van het model: 'Enterprise Risk Management – Integrated Framework'.

Enterprise Risk Management volgens het COSO ERM-model bestaat uit acht componenten die met elkaar verband houden. Deze componenten zijn afgeleid van de wijze waarop het management een onderneming runt en zijn verbonden met het managementproces. De componenten zijn:

- *interne omgeving*: de interne omgeving omvat de toon van een organisatie en legt de basis voor de manier waarop risico's worden beschouwd en geadresseerd door de mensen van de organisatie, inclusief risicomanagementbeleid en risicoacceptatiegraad, integriteit, ethische normen en waarden en de omgeving waarin zij opereren;
- *formuleren van doelstellingen*: doelstellingen moeten bestaan voordat het management potentiële gebeurtenissen die invloed hebben op het behalen van deze doelen kan erkennen. Ondernemingsrisicomanagement zorgt ervoor dat het management een proces heeft dat doelstellingen vastlegt en dat gekozen doelstellingen afgestemd zijn op de missie, deze ondersteunen en consistent zijn met de risicoacceptatiegraad;
- *identificeren van gebeurtenissen*: interne en externe gebeurtenissen die invloed hebben op het behalen van de doelstellingen van de onderneming moeten worden geïdentificeerd. Daarbij moet men onderscheid maken tussen risico's en kansen. Kansen worden teruggekoppeld naar het strategie- en/of doelstellingenformuleringsproces;
- *risicobeoordeling*: risico's worden geanalyseerd, waarbij men de waarschijnlijkheid en de impact in overweging neemt, als basis voor de vaststelling hoe men deze zou moeten managen. De inherente en restrisico's worden ingeschat;
- *reactie op risico*: het management selecteert de reacties op risico's – vermijden, accepteren, verminderen of delen van risico – waarbij een set acties

wordt ontwikkeld om risico's af te stemmen op de risicotolerantie en risicoacceptatiegraad;
- *beheersingsactiviteiten*: richtlijnen en procedures worden geformuleerd en geïmplementeerd om te waarborgen dat de reacties op risico effectief worden uitgevoerd;
- *informatie en communicatie*: relevante informatie wordt geïdentificeerd, verzameld en gecommuniceerd in een vorm die en tijdsbestek dat mensen mogelijk maakt hun verantwoordelijkheden uit te voeren. Effectieve communicatie vindt ook in ruimere zin, horizontaal, verticaal en bilateraal, plaats binnen een onderneming;
- *bewaking*: de totaliteit van ondernemingsrisicomanagement wordt bewaakt en waar nodig worden wijzigingen aangebracht. Bewaking wordt mogelijk gemaakt door voortdurende managementactiviteiten, afzonderlijke evaluaties of beide.

Ondanks het gegeven dat COSO ERM wereldwijd veelvoudig wordt toegepast, is er ook kritiek op het model. Zo hoort men vaak dat het model theoretisch en conceptueel van aard is, dat het hierdoor geen eenduidig normenkader vormt en niet voorziet in een duidelijk stappenplan voor de implementatie van dit raamwerk.

De kritiek van Power (2009) is hierbij onmiskenbaar. Zo stelt hij dat de risk appetite van een organisatie per project of afdeling kan variëren en dus niet is te consolideren in één overkoepelende eenheid. Andere kritiek op COSO ERM heeft betrekking op de constatering dat risicomanagement vaak erodeert tot een 'afvinkexercitie' en het ontbreken van risico's die in ketenverband bestaan. Hierdoor bestaat er te weinig aandacht voor scenarioanalyses en stress testing. In deze publicatie proberen we deze bezwaren zo veel mogelijk weg te nemen en de praktische toepasbaarheid van het COSO ERM-model te vergroten. Dat doen we door de verschillende componenten van het model verder uit te diepen en handvatten te bieden voor de toepassing van COSO ERM door operationele medewerkers, managers, adviseurs of auditors. Hiertoe hebben we de principes en uitgangspunten van COSO ERM doorvertaald in een meer pragmatische en gestructureerde routekaart. Deze routekaart heet *ERMplus*.

2 Ontwikkelingen en achtergronden

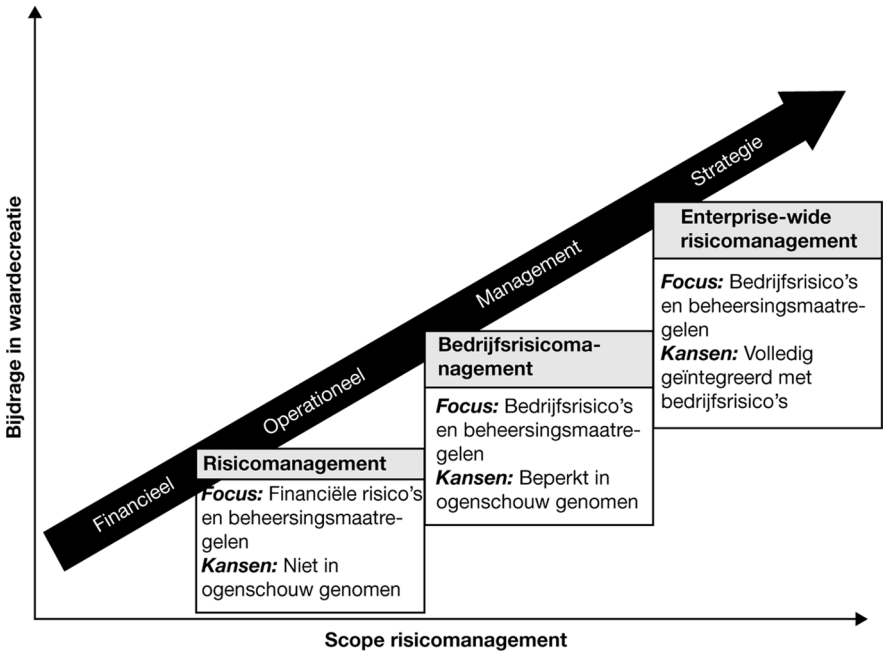
De publieke aandacht voor het realiseren van bedrijfsdoelstellingen is de afgelopen decennia steeds verder toegenomen. Dat is overduidelijk gestimuleerd door de recente kredietcrisis. Maar ook daarvóór bestond die aandacht al. Naar aanleiding van boekhoudschandalen en overdadige bonussen van bestuurders zijn stakeholders vaak bedrogen uitgekomen. Bedrijfsdoelstellingen in termen van winsten (of anderszins) werden niet gerealiseerd en de berichtgeving hieromtrent was onbetrouwbaar of te laat. In toenemende mate wensen stakeholders daarom meer transparantie rondom de bedrijfsvoering, dus transparantie over de activiteiten, doelstellingen en risico's van organisaties. Het antwoord vanuit wet- en regelgeving richt zich met name op de verantwoording rondom de beheersing van financiële verslaggevingsrisico's. Het bekendste voorbeeld hiervan is de Amerikaanse Sarbanes-Oxley Act waarbij het management een in control statement dient te verstrekken rondom financiële verslaggevingsrisico's. De informatiebehoefte van stakeholders is echter breder. Niet alleen inzake financiële verslaggevingsrisico's maar ook over andere typen risico's die waardecreatie kunnen bedreigen, respectievelijk over kansen geprojecteerd in bedrijfsplannen.

De ontwikkeling 'tell me, show me, prove me' is zonder meer interessant te noemen omdat dit ertoe leidt dat organisaties vaker bewijsvoering dienen te leveren over de kwaliteit van de bedrijfsvoering zelf en niet enkel over de resultaten daarvan. De kwaliteit van de bedrijfsvoering wordt hierbij tot uitdrukking gebracht in een oordeel van, bijvoorbeeld, auditors.

Deze wijziging in de informatiebehoefte van stakeholders is duidelijk waarneembaar in de ontwikkeling van het vakgebied risicomanagement. Op hoofdlijnen onderkennen we hierbij een drietal stadia, te weten traditioneel risicomanagement, bedrijfsrisicomanagement en Enterprise Risk Management.

Traditioneel risicomanagement
Onverwachte financiële tegenslagen en/of schandalen vormen voor veel organisaties (en individuen) vaak het vertrekpunt om te gaan nadenken over financiële verslaggevingsrisico's. De consequenties van financiële risico's zijn direct waarneembaar en zijn vaak verstrekkend. Het traditionele

Figuur 2. De ontwikkeling van risicomanagement (bron: DeLoach, 2000)



risicomanagement richt zich met name op de beheersing van financiële en, in beperkte mate, operationele risico's. Deze risico's worden beheersbaar gemaakt door interne controlemaatregelen binnen de bedrijfsprocessen te treffen en door gebruik te maken van specifieke producten, zoals contractuele bepalingen, verzekeringen en derivaten waarbij het risico wordt afgewenteld op een onafhankelijke derde.

Bedrijfsrisicomanagement

Het traditionele risicodenken richt zich, zoals gezegd, primair op identificatie en beheersing van financiële verslaggevingsrisico's. Door deze beperking in de reikwijdte worden andersoortige risico's mogelijk niet onderkend en beheerst. Verzekerbare, technologische, financiële, operationele, automatiserings-, milieu-, veiligheids-, kwaliteits-, integriteits- en frauderisico's enzovoort, worden hierdoor niet in ogenschouw genomen en/of onafhankelijk van elkaar beheerst vanuit gescheiden, gespecialiseerde organisatieonderdelen. Niettemin kunnen deze van wezenlijk belang zijn voor het realiseren van

bedrijfsdoelstellingen. Dit rechtvaardigt een meer geïntegreerde en bredere risicobenadering. Het bedrijfsrisicomanagement rekent behalve de financiële risico's ook de niet-financiële risico's tot zijn aandachtsgebied. Daardoor is ook het operationele management betrokken bij de identificatie en beheersing van risico's. Op die manier wordt de hokjesgeest doorbroken, zodat risicomanagement een verantwoordelijkheid is geworden van alle functionarissen van een organisatie.

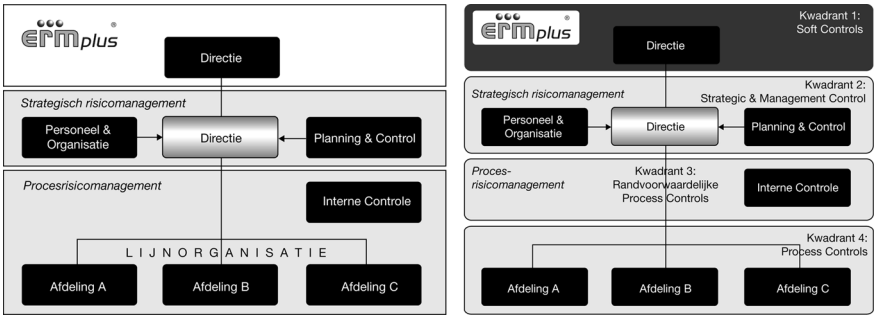
Enterprise Risk Management
Tot dusver hebben we gezien dat traditioneel risicomanagement, met een duidelijke financiële focus, evolueert naar bedrijfsrisicomanagement waarbij een breder palet aan risico's in ogenschouw wordt genomen. Aandacht voor kansen en de effecten hiervan op het creëren van waarde is echter binnen bedrijfsrisicomanagement nog beperkt. Enterprise Risk Management onderkent expliciet het belang van (en verschil tussen) risico's en kansen en werkt dit nader uit in een procesmatige aanpak voor de uitvoering van risicomanagement. Aanvullend kunnen we opmerken dat, in tegenstelling tot bedrijfsrisicomanagement, binnen Enterprise Risk Management de correlatie tussen risico's en het (gecumuleerde) effect daarvan onder de aandacht wordt gebracht. Onderlinge effecten kunnen de impact van het risico sterk beïnvloeden en deze dient men dus in ogenschouw te nemen bij de beheersing van risico's. Risico's worden hierbij geconsolideerd tot een portefeuille en als zodanig ook beoordeeld.

Het door The Committee of Sponsoring Organizations of the Treadway Commission (COSO) gepubliceerde raamwerk *COSO Enterprise Risk Management – Integrated Framework* uit 2004 biedt een integraal raamwerk voor de inrichting van risicomanagement bij strategische, operationele, financiële en niet-financiële verslaggevings- en compliancerisico's. Zoals eerder gezegd, is dit wereldwijd het meest gebruikte raamwerk. Om de praktische toepasbaarheid van het model te vergroten en bezwaren tegen het model weg te nemen wordt in deze publicatie een nadere, praktischer uitwerking beschreven. Deze uitwerking duiden we aan als *ERMplus*.

ERMplus kent twee verschillende dimensies: een risicodimensie en een beheersingsdimensie. De risicodimensie heeft betrekking op het 'risiconiveau', waarbij onderscheid wordt gemaakt in strategische risico's en procesrisico's. Naar analogie van COSO ERM hebben strategische risico's betrekking op de strategische doelstellingen, de globale doelen, en zijn ze afgestemd op de visie en missie van de organisatie. Procesrisico's hebben betrekking op de overige doelstellingen uit het COSO ERM-model, te weten operationeel, rapportage en toezicht op naleving van wet- en regelgeving. Het onderscheid van enerzijds

strategische risico's en anderzijds procesrisico's wordt binnen deze methodiek relevant geacht, omdat deze risico's ieder een eigen wijze van beheersing vergen. Zo zijn procesrisico's vaak gerelateerd aan transacties of stromen die binnen een bedrijfsproces worden afgehandeld. Beheersing van deze risico's vindt dan ook met name plaats door middel van handmatige beheersingsmaatregelen of applicatiecontroles. Strategische risico's hebben meer betrekking op strategische, organisatiebrede doelstellingen. Beheersing van strategische risico's vindt daarom plaats door middel van management control op hoger hiërarchisch niveau.

Figuur 3. ERMplus: risicodimensie (links) en beheersingsdimensie (rechts) (bron: Clascon, 2009)



De beheersingsdimensie heeft betrekking op de verschillende hiërarchische niveaus die betrokken zijn in het risicomanagementproces. In de literatuur wordt dit ook wel aangeduid als 'lines of defense'. Binnen de ERMPlus-methodiek wordt een vijftal 'lines of defense' onderkend. De eerste verdedigingslinie heeft betrekking op de primaire bedrijfsvoering van een organisatie. Het zijn de mensen op de werkvloer en het management op tactisch en strategisch niveau die de dagelijkse bedrijfsrisico's moeten identificeren en daadwerkelijk beheersen. De eerste verdedigingslinie wordt ook wel de 'business frontline' genoemd. De tweede verdedigingslinie heeft betrekking op de ondersteunende staffuncties die, vanuit een specifieke materie- of risicomanagementdeskundigheid, het overzicht bewaren en over specifieke risicogebieden rapporteren aan de directie. Voorbeeld hiervan zijn functies als compliance, health & safety en human resource management. De derde verdedigingslinie is de internal auditfunctie, die verantwoordelijk is voor een oordeel over

het ontwerp en de effectiviteit van risicomanagement en het interne beheersingssysteem. De vierde verdedigingslinie is de rol van de externe accountant, die vanuit de jaarrekeningcontrole een onafhankelijk oordeel geeft over de interne beheersing. De vijfde en laatste verdedigingslinie heeft betrekking op het houden van toezicht. We spreken hierbij over bijvoorbeeld een raad van commissarissen, raden van toezicht, maar ook over toezichthouders binnen een specifieke branche.

De relatie tussen COSO ERM en ERMplus is schematisch weergegeven in figuur 4.

Figuur 4. De relatie tussen COSO ERM en ERMplus