Koninklijk Actuarieel Genootschap

Leidraad Enterprise Risk Management (ERM)

Auteurs: drs. Jurriaan Borst AAG, drs. Annemieke Ooteman Actuarieel Analist AG, Jasper Hoogenstraaten MSc en MSc Loes de Boer AAG CERA

Hoofdindeling: Beroepsreglementering
Categorie: Leidraden
Opgesteld door: AG-Werkgroep ERM
Datum (laatste wijziging): oktober 2016

Inhoudsopgave

Introductie

Belang van ERM

Het nemen van risico is een inherent onderdeel van ondernemen. Organisaties hebben bestaansrecht, en voegen waarde toe, door het nemen van risico's. Hoe meer inzicht in de risico's die de organisatie loopt, hoe meer waarde kan worden toegevoegd. ERM helpt organisaties haar (strategische) doelstellingen te behalen, ook in tijden dat het economisch minder goed gaat.

De traditionele meer silo-gedreven aanpak voor elk afzonderlijk risico voldoet niet meer, door onder andere de volgende ontwikkelingen:

de toegenomen focus op een passende vergoeding voor kapitaalverschaffers, in combinatie met de snelheid waarmee kapitaal, vanwege de globalisering, wereldwijd wordt ingezet;

de toegenomen complexiteit in de financiële wereld waarbij deze in sterke mate internationaal verweven is, wat een belangrijke oorzaak is van financiële en economische crises;

als reactie hierop de invoering van de Basel kapitaalregimes bij banken en Solvency II bij (her)verzekeraars. Het toezicht geeft hiermee richtlijnen ten aanzien van de nadere invulling van de ERM raamwerken met specifieke vereisten zoals ICAAP (Basel), ORSA en use test (Solvency II).

In deze leidraad behandelen we ERM vanuit het perspectief van de verzekeraar. De gepresenteerde concepten zijn echter ook makkelijk door te vertalen naar andere organisaties.

Doel ERM

Door toepassing van ERM wordt de kans vergroot dat de doelstellingen van de organisatie worden gerealiseerd, door een inschatting te maken van de risico's, in termen van kans en impact, met als doel om beheersmaatregelen te treffen, binnen de grenzen van de risicobereidheid.

Het succes van een verzekeraar wordt in grote mate bepaald door het vinden van de optimale balans tussen rendement, risico en kapitaalsbeslag, waarbij het klantbelang centraal wordt gesteld.

Doel van de leidraad ERM

Het doel van de leidraad ERM (Leidraad) is om de leden van het Koninklijk Actuarieel Genootschap (AG) te informeren over de mogelijke opzet en werking van een ERM-systeem. De gepresenteerde informatie geeft de actuariële en andere ERM-professionals een handvat voor de uitvoering van haar taken en inzicht in haar rol binnen een ERM-systeem. De leidraad geeft verder inzicht in de rollen voor de actuariële professional

binnen de bredere context van het ERM-systeem. Daarnaast bevordert het discussies binnen en buiten het AG, onder andere door het creëren van een gemeenschappelijke taal met betrekking tot ERM.

Doelgroep

De primaire doelgroep van de leidraad zijn actuariële en andere ERM-professionals die werkzaam zijn voor Nederlandse verzekeraars. Ook buiten het AG geeft deze leidraad nuttige inzichten.

De leidraad is als volgt opgebouwd:

in hoofdstuk 1 wordt allereerst een aantal kernbegrippen behandeld;

in hoofdstuk 2 wordt de opzet van een ERM-systeem gepresenteerd, aan de hand van relevante uitgangspunten en een voorbeeld ERM raamwerk;

in hoofdstuk 3 worden de bouwstenen van het voorbeeld ERM raamwerk uitgewerkt;

in hoofdstuk 4 staat de monitoring en beoordeling van het ERM-systeem centraal; en

in hoofdstuk 5 wordt ten slotte stil gestaan bij de mogelijke rollen van de actuaris binnen het ERM-systeem.

In deze leidraad worden de belangrijkste bouwstenen waaruit een ERM-systeem is opgebouwd behandeld, zonder teveel in detail te treden. Voor wie meer wil lezen over ERM, is naast de bijlage met definities (Bijlage I) en een voorbeeld risicodashboard (Bijlage II), ook een bijlage opgenomen met relevante verwijzingen naar andere documenten (Bijlage III).

1 Kernbegrippen ERM

In dit hoofdstuk is een aantal kernbegrippen uitgewerkt, zodat in het vervolg van deze leidraad helder is wat precies met de kernbegrippen wordt bedoeld.

De Committee of Sponsoring Organizations of the Treadway Commission (COSO) definieert ERM als:

"a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives".

De Casualty Actuarial Society (CAS) hanteert een andere definitie van ERM:

"the discipline by which an organization in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders".

Met deze definitie benadrukt de CAS dat ERM bedoeld is om waarde toe te voegen aan de organisatie.

Naast de definitie van COSO en CAS bestaan nog vele andere definities van ERM. De definities zijn niet allemaal hetzelfde, maar weerspiegelen wel een aantal fundamentele uitgangspunten van ERM. Deze uitgangspunten zijn opgenomen in paragraaf 1 van hoofdstuk 2. In deze leidraad wordt niet één definitie van ERM gehanteerd, maar worden de uitgangspunten voor ERM als basis gehanteerd voor de uitwerking van de opzet en werking van een ERM-systeem in hoofdstuk 2 en 3.

ERM-systeem

In deze leidraad wordt de volgende definitie van een 'systeem' gehanteerd:

Een verzameling van op elkaar afgestemde (zelfstandige) bouwstenen, die elk een functie hebben, maar als één geheel functioneren in het bereiken van een gemeenschappelijk doel.

Het ERM-systeem beslaat daarmee de verzameling van alle risicomanagementprocessen door de gehele organisatie heen.

Solvency II[1] omschrijft een risicomanagementsysteem of ERM-systeem als:

"de strategieën, processen en rapportageprocedures die nodig zijn om op individueel en geaggregeerd niveau de risico's waaraan de organisatie blootstaat of blootgesteld zou kunnen worden, alsook de onderlinge afhankelijkheden en relaties daartussen voortdurend te onderkennen, te meten, te bewaken, te beheren en te rapporteren".

[1] Richtlijn Solvency II, artikel 44, lid 1.

In deze leidraad zijn in hoofdstuk 2 en 3 bovenstaande definities van ‘systeem’ en ‘ERM-systeem’ als basis gehanteerd voor de uitwerking van de opzet en werking van een ERM-systeem.

Risicomanagementproces

De internationale norm ISO 31000:2009 van de International Organization for Standardization (ISO) bevat principes en algemene richtlijnen voor risicomanagement en in het bijzonder ‘het’ risicomanagementproces. De norm kan worden toegepast op een breed scala aan activiteiten, zoals strategie- en besluitvorming, processen, projecten, en producten. Het risicomanagementproces wordt door de norm gedefinieerd als:

“de systematische toepassing van beleidslijnen, procedures en werkwijzen op de activiteiten met betrekking tot communicatie, overleg, vaststelling van de context, en het identificeren, analyseren, evalueren, behandelen, monitoren en beoordelen van risico’s”.

In deze leidraad wordt deze definitie van risicomanagementproces als basis gehanteerd voor de uitwerking van de risicomanagementprocessen op strategisch, tactisch, en operationeel niveau in hoofdstuk 3.

Strategie

De strategie van een organisatie is de manier waarop strategische doelstellingen worden gerealiseerd. De volgende elementen zijn relevant bij het bepalen van de strategie:

- Aansluiting bij missie, visie en kernactiviteiten. Hoe ondersteunt de strategie het realiseren van de missie en visie en in welke mate sluit het aan bij de kernactiviteiten van de organisatie?
- Verdienmodel. Op welke manier creëert de strategie (lange termijn) waarde voor de organisatie?
- Propositie. Welke producten en diensten voorzien in welke markt- of klantbehoeften?
- Distributiekanalen. Door middel van welke kanalen en partners worden de proposities naar de markt gebracht?
- Markt- en marktpotentieel. Is er een koopkrachtige vraag, en zo ja, in welke omvang en hoe zal deze zich ontwikkelen?
- Concurrentieveld. Wie begeeft zich verder nog in deze markt en hoe wordt geconcurreerd?
- Differentiatie. Hoe leidt de strategie tot een houdbaar onderscheidend vermogen?
- Benodigde investeringen. Welk beroep doet de strategie op de financiering en heeft de organisatie die mogelijkheden?
- Samenwerking. Zijn allianties of overnames nodig voor de realisatie van de strategie?
- Globale indicatie van de interne consequenties voor de organisatie. Wat betekent de strategie voor de personele formatie, IT-infrastructuur, interne processen en besturing?

- Risico's. Welke risico's brengt de strategie met zich mee en is de organisatie in staat deze risico's te dragen?
- Risicostrategie. Op welke manier worden de geïdentificeerde risico's beheerst en kansen benut, binnen de grenzen van de risicobereidheid?
- Globale business case met een financiële doorrekening van risico, rendement en kapitaal. Wat levert de strategie op in termen van rendement versus risico/kapitaal en benodigde investeringen?
- Iedere organisatie bepaalt zelf haar definitie van strategie.

Het strategievormingsproces bestaat in het algemeen uit de volgende stappen, die niet noodzakelijkerwijs in chronologische volgorde worden uitgevoerd:

- Formuleren missie, visie en kernwaarden;
- Formuleren ambities of strategische doelstellingen;
- Uitvoeren strategische analyse. De strategische analyse bestaat bijvoorbeeld uit een sterkte-zwakteanalyse en strategische risicoanalyse;
- Vertalen van de strategische analyse naar strategische opties;
- Analyseren van de strategische opties en strategiekeuze (onder andere met behulp van de ORSA).

Risicostrategie

Een risicostrategie omvat in het algemeen de volgende componenten:

- De strategische doelstellingen en uitgangspunten waarmee de risico's beheerst worden;
- De risicobereidheid; en
- Wie waarvoor verantwoordelijk is (i.e. risicogovernance), rekening houdend met de bestaande interne governance- en organisatiestructuur en bijbehorende verdeling van taken en verantwoordelijkheden.

Iedere organisatie bepaalt zelf haar definitie van risicostrategie.

Solvency II stelt in dit verband, dat een welomschreven risicomanagementstrategie aanwezig moet zijn die in overeenstemming is met de algemene bedrijfsstrategie van de onderneming.[2] De doelstellingen en grondbeginselen van de strategie, de goedgekeurde risicotolerantie-limieten en de toewijzing van verantwoordelijkheden voor alle activiteiten van de onderneming moeten hierbij schriftelijk zijn vastgelegd.

Verder wordt in Solvency II gesteld dat voor de implementatie van de risicostrategie schriftelijke beleidslijnen voor de materiële risico's en de goedgekeurde risico-tolerantielimieten per risicocategorie aanwezig moeten zijn.[3]

[2] Gedelegeerde Verordening Solvency II, artikel 259.
[3] Gedelegeerde Verordening Solvency II, artikel 259.

Risicobereidheid

Risicobereidheid ('risk appetite') wordt in deze leidraad gedefinieerd als:

"de hoeveelheid en het soort risico's dat een organisatie kan en bereid is te accepteren bij het nastreven van haar doelstellingen".

Deze definitie wordt gehanteerd als basis voor de uitwerking van de risicobereidheid.

ORSA

De ORSA betreft een interne beoordeling van de eigen risico- en solvabiliteitspositie. Solvency II stelt dat de beoordeling van het eigen risico en de solvabiliteit integraal deel uitmaakt van de bedrijfsstrategie en steeds in aanmerking wordt genomen bij de strategische beslissingen van de organisatie.[4] Bij het toepassen van de ORSA kan inzicht worden verkregen in het huidige en toekomstige risicoprofiel van de organisatie. Hiermee wordt getoetst of de kapitaalspositie toereikend is om de strategische plannen, ook in ongunstige scenario's, te realiseren. De ORSA kan tevens worden gebruikt als middel om verschillende strategische opties te onderzoeken, ter ondersteuning van strategische besluitvorming.

Strategische risicoanalyse

Strategische risicoanalyse houdt in dat de belangrijkste risico's, die het verwezenlijken van strategische doelstellingen op een negatieve of positieve manier kunnen beïnvloeden, worden geïdentificeerd, geanalyseerd, en geëvalueerd. De uitkomsten kunnen aanleiding zijn tot herijking van de strategie en/of strategische doelstellingen.

Risicogovernance

Risicogovernance is de manier waarop gestuurd wordt op basis van risico's en risicoposities, en bijbehorende taken en verantwoordelijkheden. Een risico-overlegstructuur speelt hierbij een belangrijke rol (zie paragraaf 3.5). Een goed ingerichte risicogovernance waarborgt dat risico's worden meegenomen in de besluitvormingsprocessen van de organisatie en verantwoording over deze risico's, en de beheersing ervan, wordt afgelegd door de risico-eigenaar.

Planning- en controlcyclus

De uitwerking, implementatie en monitoring van de strategie en risicostrategie van een organisatie, vindt in het algemeen plaats via een planning- en controlcyclus. Het doel van de planning- en controlcyclus is het management te informeren en te rapporteren over of de gekozen (risico)strategie op strategisch, tactisch en operationeel niveau het gewenste resultaat oplevert en indien nodig bij te sturen. De planning- en controlcyclus is veelal gebaseerd op het PDCA-principe.

[4] Richtlijn Solvency II, artikel 45, lid 4.

PDCA is een afkorting die staat voor: Plan – maak een plan met de resultaten die je wilt bereiken, Do – voer het plan uit, Check – vergelijk de resultaten met wat je had willen bereiken, en Act – stuur indien nodig bij om de resultaten alsnog te bereiken.

Datakwaliteit

Datakwaliteit kan gedefinieerd worden als de toetsing van informatie op vooraf vastgestelde criteria. Belangrijke criteria onder Solvency II zijn: volledigheid, adequaatheid, juistheid en tijdigheid (zie paragraaf 3.7).[5]

[5] Richtlijn Solvency II, Artikel 82.

2 Opzet ERM-systeem

In dit hoofdstuk wordt de opzet van een ERM-systeem beschreven, aan de hand van relevante uitgangspunten (paragraaf 2.1) en een voorbeeld ERM-raamwerk (paragraaf 2.2).

2.1 Uitgangspunten

ERM

- Betreft een geïntegreerde aanpak voor de risico's waaraan een organisatie is of in de toekomst kan worden blootgesteld. Dit houdt tevens in dat rekening wordt gehouden met de onderlinge samenhang tussen de risico's;
- Is volledig geïntegreerd in de bedrijfsvoering en besluitvormingsprocessen van de organisatie;
- Wordt uitgevoerd op zowel het strategische, als tactische en operationele niveau binnen de organisatie;
- Is van toepassing op:
    - alle werknemers binnen een organisatie;
    - alle korte en langere termijn risico's waaraan de organisatie is of in de toekomst kan worden blootgesteld;
- Gaat zowel over het managen van blootstellingen aan operationele risico's als het optimaal benutten van niet-operationele of financiële risico's. Bij het laatste spelt de afweging tussen risico, rendement en kapitaal een belangrijke rol.

Een ERM-systeem kan beschreven worden aan de hand van:

- de processen en onderliggende activiteiten waaruit het systeem is opgebouwd;
- de input/output van de processen;
- de manier waarop de processen worden aangestuurd, inclusief taken en verantwoordelijkheden (risicogovernance);
- de mensen die de processen uitvoeren (kennis, kunde, vaardigheden, ervaring, houding, gedrag);
- de middelen waarmee de uitvoering van de processen mogelijk wordt gemaakt; en
- criteria en randvoorwaarden waaraan de processen, input/output, mensen en middelen moeten voldoen.

Ieder ERM-systeem is uniek, want:

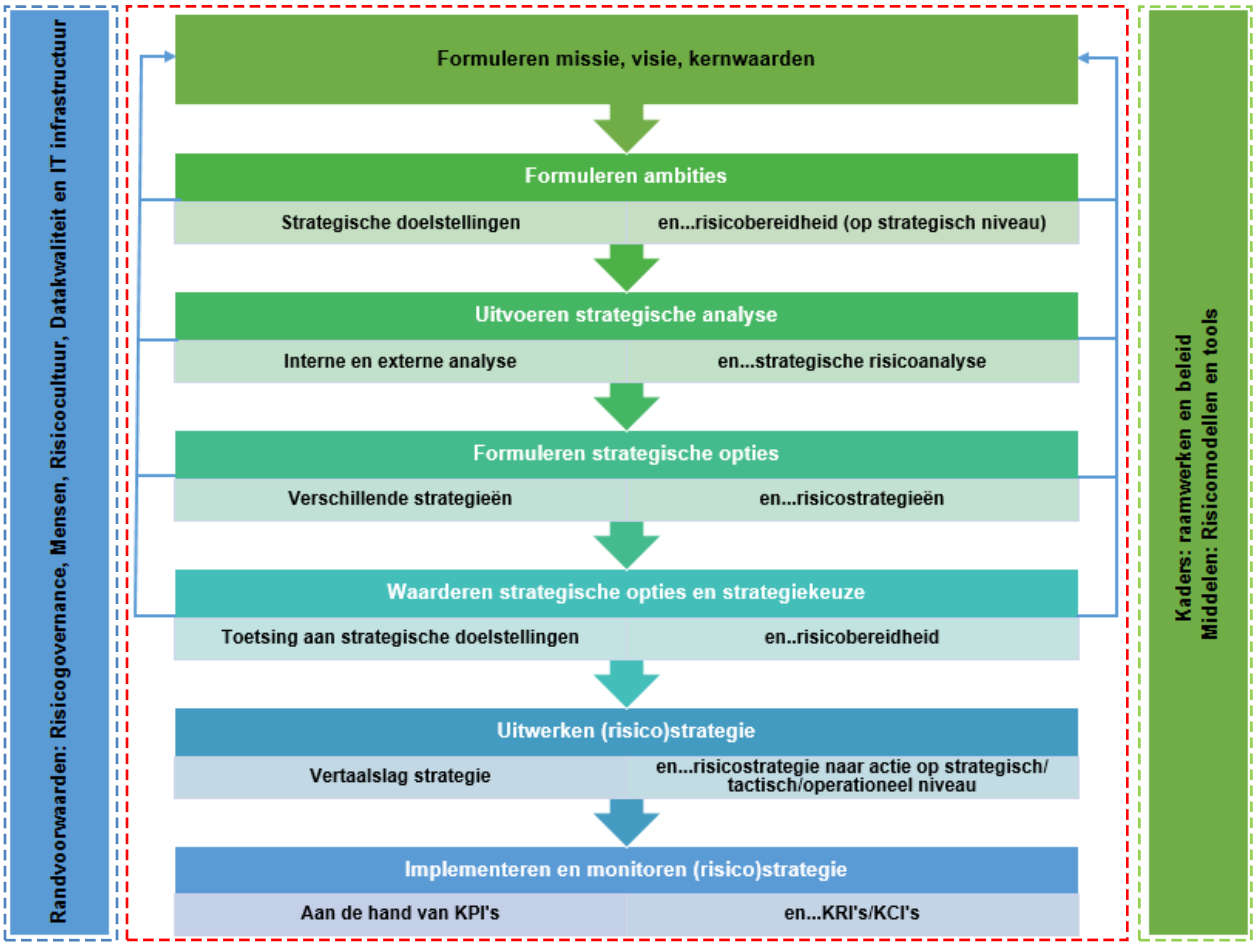
Iedere organisatie hanteert haar eigen definitie van ERM en bijbehorend doel. Daarnaast kent iedere organisatie haar eigen governance-, organisatie- en processtructuur. Afhankelijk van de gehanteerde definitie van ERM en de inrichting van de organisatie kan de opzet en werking van het gewenste ERM-systeem worden vastgesteld. Dit betekent dat de opzet en werking van een ERM-systeem niet voor iedere organisatie exact hetzelfde kan en hoeft te zijn.

Deze leidraad schetst een voor iedere organisatie toepasbaar, generiek voorbeeld voor de opzet en werking van een ERM-systeem.

2.2 ERM-raamwerk

Een ERM-raamwerk laat zien uit welke bouwstenen een ERM-systeem is opgebouwd. Bij de inrichting van een ERM-systeem dient rekening te worden gehouden met alle gedefinieerde bouwstenen. Hierbij is met name ook de samenhang tussen de bouwstenen van belang; zonder randvoorwaardelijke elementen en/of kaders en middelen werkt het systeem niet, of minder effectief. Een belangrijk kenmerk is verder dat een ERM-systeem bestaat uit cyclische risicomanagementprocessen (Plan-Do-Check-Act) op strategisch, tactisch en operationeel niveau.

Figuur 1 omvat een voorbeeld ERM-raamwerk. In het raamwerk wordt onderscheid gemaakt tussen 'processen' (rode stippellijn), 'randvoorwaarden' (blauwe stippellijn), en 'kaders' en 'middelen' (groene stippellijn). De verdeling van de gedefinieerde bouwstenen over deze onderwerpen in het voorbeeld raamwerk is subjectief. Deze verdeling kan door iedere organisatie anders worden benaderd. Uitgangspunt is dat een ERM-systeem beschreven kan worden aan de hand van de genoemde punten in paragraaf 2.1.



Figuur 1: Voorbeeld ERM-raamwerk

Door de processtappen, zoals geformuleerd in Figuur 1 (rode stippellijn), te doorlopen, worden risico's achtereenvolgend geïdentificeerd (strategische analyse), geanalyseerd, geëvalueerd (formuleren strategische opties en waarderen strategische opties en strategiekeuze) en behandeld (uitwerken risicostrategie en implementatie). Als onderdeel van de implementatie van de risicostrategie, worden risicomanagementprocessen op tactisch en operationeel niveau doorlopen. Om de risicomanagementprocessen op strategisch, tactisch en operationeel niveau effectief te laten verlopen, is het van belang voldoende aandacht te besteden aan randvoorwaardelijke[6] elementen (blauwe stippellijn) als risicogovernance, mensen, risicocultuur, en datakwaliteit en IT infrastructuur. Daarnaast zijn kaders (groene stippellijn) nodig om sturing en richting te geven aan de uit te voeren risicomanagementprocessen en implementatie van de risicostrategie. En ten slotte zijn middelen (groene stippellijn) als risicomodellen en tools nodig ter ondersteuning van de uitvoering van de risicomanagementprocessen. De hoofdonderdelen van het raamwerk (i.e. risicomanagementprocessen, randvoorwaardelijke elementen, kaders en middelen) worden hieronder beknopt toegelicht, waarbij de belangrijkste bouwstenen zijn onderstreept.

Risicomanagementprocessen (rode stippellijn)

De kern van het voorbeeld ERM-systeem bestaat uit op elkaar aansluitende cyclische risicomanagementprocessen op strategisch, tactisch en operationeel niveau. Zoals aangegeven in hoofdstuk 1 bestaat dit proces op alle niveaus uit de volgende stappen: identificeren, analyseren, evalueren, behandelen, monitoren en beoordelen van risico's. De stappen van het risicomanagementproces op strategisch niveau staan uitgewerkt binnen de rode stippellijn in Figuur 1 en worden nader toegelicht in paragraaf 3.1.1. De risicomanagementprocessen op tactisch en operationeel niveau maken onderdeel uit van de laatste stap van het risicomanagementproces op strategisch niveau: het "implementeren en monitoren van de (risico)strategie" en worden nader toegelicht in paragraaf 3.1.2. Het risicomanagementproces op strategisch niveau vormt de zogenaamde 'context' voor de risicomanagementprocessen op tactisch en operationeel niveau.[7]

Belangrijke input/output van de risicomanagementprocessen zijn:

- Risicostrategie en risicobereidheid;
- Risicoclassificatie en risicoprofiel;
- Risicorapportages.

Randvoorwaardelijke elementen (blauwe stippellijn)

Om het ERM-systeem te laten 'werken' moet het systeem aan een aantal randvoorwaarden voldoen:

[6] Randvoorwaardelijk voor de effectieve werking van het ERM-systeem.
[7] Zie bijvoorbeeld Robert J. Chapman, Simple tools and techniques for enterprise risk management, hoofdstuk 8.

- De taken en verantwoordelijkheden binnen het systeem dienen helder te zijn. In andere woorden: de risicogovernance moet op orde zijn, zodat sturing op basis van risico's plaats kan vinden en verantwoording wordt afgelegd over risico's en risicobeheersing door de risico-eigenaren (bijvoorbeeld door middel van een risico-overlegstructuur).
- De mensen die de risicomanagementprocessen uitvoeren, waaruit het ERM-systeem is opgebouwd, moeten beschikken over relevante kennis, kunde, vaardigheden en ervaring.
- Daarnaast speelt houding en gedrag of risicocultuur een belangrijke rol binnen het ERM-systeem. Zonder de 'juiste' risicocultuur werkt het systeem niet, of niet voldoende effectief.
- De datakwaliteit en IT infrastructuur moeten het ERM-systeem in voldoende mate (kunnen) ondersteunen. Dit betekent onder andere dat relevante informatie adequaat, juist, volledig en tijdig beschikbaar dient te zijn.

Kaders (groene stippellijn)

Raamwerken en beleid (kaders) geven sturing en richting aan de organisatie, door de strategie en risicostrategie van de organisatie te vertalen naar criteria en randvoorwaarden waaraan de (risicomanagement)processen, output, mensen en middelen moeten voldoen.

Middelen (groene stippellijn)

Om de risicomanagementprocessen uit te kunnen voeren zijn onder andere risicomodellen en tools nodig, zodat relevante methoden en technieken kunnen worden toegepast. In Tabel A is een overzicht opgenomen van de in dit hoofdstuk gedefinieerde bouwstenen (onderstreept) van een ERM-systeem.

Bouwstenen ERM-systeem
Risicomanagementprocessen
Risicostrategie en risicobereidheid
Risicoclassificatie en risicoprofiel
Risicorapportages
Risicogovernance
Mensen en risicocultuur
Datakwaliteit en IT infrastructuur
Raamwerken en beleid
Risicomodellen en tools

Tabel A: Overzicht bouwstenen ERM-systeem

De verschillende bouwstenen hebben elk een eigen functie, maar functioneren als één geheel in het bereiken van het doel van ERM.

In hoofdstuk 3 worden de bouwstenen nader besproken.

3 Werking ERM-systeem

In dit hoofdstuk wordt de werking van een ERM-systeem beschreven, aan de hand van de gedefinieerde bouwstenen in hoofdstuk 2 (Tabel A).

3.1 Risicomanagementprocessen

3.1.1 Risicomanagementprocessen op strategisch niveau

De stappen van het risicomanagementproces op strategisch niveau zijn expliciet opgenomen in het ERM-raamwerk (binnen de rode stippellijn in Figuur 1 van hoofdstuk 2). De gedefinieerde stappen worden niet noodzakelijkerwijs in chronologische volgorde uitgevoerd. Dit iteratieve karakter van het proces wordt geïllustreerd door de pijlen links en rechts in Figuur 1. Afhankelijk van het besturingsmodel van de organisatie vindt op strategisch niveau één risicomanagementproces of meerdere risicomanagementprocessen plaats (bijvoorbeeld per juridische entiteit), waarna de uitkomsten worden 'opgeteld'. Hieronder volgt een toelichting per stap van 'het' risicomanagementproces.

a. Formuleren missie, visie en kernwaarden

Een goed werkend ERM-systeem is geïntegreerd met het strategievormingsproces van de organisatie en daarom 'start' ook het risicomanagementproces op strategisch niveau met het formuleren van de missie, visie en kernwaarden van de organisatie. De missie is datgene dat de organisatie wil uitdragen naar buiten, bijvoorbeeld: kernactiviteit, bestaansrecht, betekenis voor stakeholders, intenties en idealen. Een visie vertelt meer over het beeld of de verwachting van de organisatie van de toekomst en de positie van de organisatie daarin. Kernwaarden beschrijven de normen, waarden en overtuigingen van de organisatie. Met de missie, visie en kernwaarden van de organisatie wordt sturing en richting gegeven aan zowel strategische doelstellingen als doelstellingen ten aanzien van risico's en risicoposities (de risicostrategie en risicobereidheid).

Output van deze stap:

- Beschrijving missie, visie en kernwaarden van de organisatie.

b. Formuleren ambities

Mede op basis van de missie, visie, en kernwaarden van de organisatie worden strategische doelstellingen en uitgangspunten geformuleerd. Daarnaast worden gedurende deze stap ook ambities geformuleerd ten aanzien van risico's en risicoposities. Hoeveel risico is de organisatie bereid te lopen bij het nastreven van haar strategische doelstellingen? Deze ambities ten aanzien van risico's en risicoposities kunnen afzonderlijk van de strategische doelstellingen worden geformuleerd of als onderdeel van de strategische doelstellingen. Deze keuze is onder andere afhankelijk van het ambitieniveau van de organisatie met betrekking tot de integratie van performance en risk management en de omgeving waarin de organisatie opereert, waaronder wet- en regelgeving.

Output van deze stap:

- Een samenhangende set strategische doelstellingen en uitgangspunten waarmee de risico's beheerst worden.
- Risicobereidheid op strategisch niveau, al dan niet geformuleerd als strategische doelstellingen en uitgangspunten.

c. Uitvoeren strategische analyse

Strategische analyse houdt in dat de interne en externe omgeving van de organisatie wordt onderzocht om te komen tot strategische opties. De strategische analyse kan bijvoorbeeld bestaan uit de uitvoering van een sterkte-zwakteanalyse ("SWOT-analyse") en strategische risicoanalyse. Voorbeelden van hulpmiddelen om deze analyses uit te voeren zijn: interviews, vragenlijsten, en/of enquêtes.

Output van deze stap:

- Uitkomsten SWOT-analyse.
- Risicoprofiel: een overzicht van de belangrijkste risico's waaraan de organisatie is blootgesteld en die het verwezenlijken van de strategische doelstellingen op een negatieve of positieve manier kunnen beïnvloeden. Inclusief de belangrijkste oorzaken, gevolgen, bestaande en mogelijke aanvullende beheersmaatregelen en managementacties.

d. Formuleren strategische opties

Op basis van de output van de strategische analyse worden strategische opties uitgewerkt. Met een alternatieve strategie of optie, wordt bijvoorbeeld aanpassing van het verdienmodel of propositie bedoeld. Met een alternatieve risicostrategie wordt bijvoorbeeld aanpassing van het herverzekeringsprogramma bedoeld.

Output van deze stap:

- Verschillende strategische opties.

e. Waarderen strategische opties en strategiekeuze

Bij de waardering van strategische opties spelen wegingsfactoren als haalbaar, acceptabel, bruikbaar en aansluiting bij scenario's een rol.[8] De haalbaarheid van een optie is bijvoorbeeld afhankelijk van de benodigde investeringen. Voor de acceptatie van een optie speelt onder andere de houding van de stakeholders ten opzichte van de optie een rol. Voor de bruikbaarheid van een optie wordt bijvoorbeeld beoordeeld in hoeverre de optie een oplossing biedt voor de strategische aandachtspunten voortkomend uit de

[8] Zie Berenschot, Het groot strategie boek.

strategische analyse. Met behulp van een ORSA worden de strategische opties getoetst aan de strategische doelstellingen en risicobereidheid en de aansluiting bij scenario's:

- Welke strategische optie past het beste bij de geformuleerde strategische doelstellingen en risicobereidheid?
- Zorgt de strategische optie voor de gewenste financiële resultaten?
- Blijft de organisatie nu en in de toekomst binnen de grenzen van de (herijkte) risicobereidheid, ook onder scenario's en/of stress testen?
- Hoe gevoelig zijn de uitkomsten voor wijzigingen in de aannames?
- In hoeverre wijkt het risicoprofiel van de organisatie af van de aannames die ten grondslag liggen aan de berekening van het vereist vermogen onder Solvency II?[9]

Zoals in hoofdstuk 1 aangegeven maakt de ORSA, conform Solvency II, integraal deel uit van de bedrijfsstrategie en wordt steeds in aanmerking genomen bij de strategische beslissingen van de onderneming.[10] Met behulp van een ORSA worden strategische beslissingen 'getoetst' aan de strategische doelstellingen en risicobereidheid van de organisatie. Naast de toetsende rol, kan de ORSA ook een ondersteunende rol spelen in de strategievorming zelf, doordat als onderdeel van de ORSA scenario's worden bedacht en onderzocht. Hoe ziet de toekomst er voor onze klanten uit? Hoe kunnen wij daar het beste op in springen, zodat wij onze strategische doelstellingen kunnen realiseren? Op welke manier kunnen we inspringen op deze behoefte en wat zijn dan de belangrijkste risico's en vallen die binnen onze risicobereidheid?

Output van deze stap:

- Uitkomsten van onderzochte scenario's, waaronder:
    - eventuele vastgestelde aanvullende beheersmaatregelen en/of managementacties;
    - eventuele wijzigingen van de strategie en/of strategische doelstellingen.
    - Gekozen strategische optie.

f. Uitwerken (risico)strategie

Uitwerking van de (risico)strategie houdt in dat de gekozen (risico)strategie definitief wordt uitgewerkt in een strategisch plan, meerjarenplan en jaarplan, en beleid, afdelingsplannen, functieprofielen, individuele doelstellingen, etc.

Output van deze stap:

- Op strategisch niveau: strategisch plan, inclusief risicostrategie.
- Op tactisch niveau: beleid, meerjarenplan en jaarplan.
- Op operationeel niveau: afdelingsplannen, aangepaste functieprofielen en individuele doelstellingen, etc.

[9] Deze vraag is met name relevant bij gebruik van de standaardformule onder Solvency II.
[10] Richtlijn Solvency II, Artikel 45, lid 4.

De uitgewerkte (risico)strategie vormt de 'context' voor de risicomanagementprocessen op tactisch en operationeel niveau (zie paragraaf 3.1.2 en 3.1.3).

g. Implementeren en monitoren (risico)strategie

Ter monitoring van de strategie en risicostrategie wordt een samenhangende set key performance indicatoren (KPI's), key risk indicatoren (KRI's), en key control indicatoren (KCI's) vastgesteld. Met behulp van de gedefinieerde indicatoren wordt bewaakt of de strategische doelstellingen worden gerealiseerd en of de risico's, waaraan de organisatie is of in de toekomst kan worden blootgesteld, adequaat worden beheerst en/of optimaal worden benut en zich binnen de grenzen van de risicobereidheid (blijven) bevinden. Op deze manier wordt gestreefd naar het vergroten van de kans dat de strategische doelstellingen van de organisatie worden gerealiseerd.

Net als bij het realiseren van de strategie, staat bij het realiseren van de risicostrategie het PDCA-principe centraal:

- Plan: de risicostrategie is vastgesteld en uitgewerkt als onderdeel van het strategisch plan, meerjarenplan, jaarplan, beleid, afdelingsplannen, functieprofielen, individuele doelstellingen, etc.
- Do: de risicostrategie wordt uitgevoerd.
- Check: door het continu doorlopen van de risicomanagementprocessen op tactisch en operationeel niveau wordt bewaakt of de risico's waaraan de organisatie is of in de toekomst kan worden blootgesteld adequaat worden beheerst en/of optimaal worden benut. In andere woorden: er wordt bewaakt of de risicostrategie wordt gerealiseerd.
- Act: stuur bij via een ingerichte risico-overlegstructuur.

Voor de implementatie van de risicostrategie worden risicomanagementprocessen op tactisch en operationeel niveau ingericht. Deze risicomanagementprocessen dienen aan te sluiten bij de (beoogde) inrichting van de bedrijfsprocessen op tactisch en operationeel niveau ter realisatie van de strategische doelstellingen, zodat de gedefinieerde KPI's, KRI's en KCI's in samenhang kunnen worden gemonitord.

3.1.2 Risicomanagementprocessen op tactisch en operationeel niveau

De context voor de risicomanagementprocessen op het tactische (keten-) niveau en op operationeel (proces-) niveau wordt onder andere gevormd door beleid, meerjarenplannen, jaarplannen, afdelingsplannen, aangepaste functieprofielen en individuele doelstellingen. Afhankelijk van de grootte van de organisatie, kunnen de vastgestelde KPI's, KRI's en KCI's verder worden door vertaald naar onderliggende indicatoren op het tactisch en operationeel niveau ter monitoring van de strategie en risicostrategie.

Risicomanagement is de primaire verantwoordelijkheid van het management van de organisatie. Door deze verantwoordelijkheid te verwerken in afdelingsplannen, functieprofielen en individuele doelstellingen, wordt de implementatie van risicomanagement gewaarborgd. Daarnaast worden perverse prikkels voorkomen, door

het management niet alleen verantwoordelijk te maken voor realisatie van de gedefinieerde KPI's, maar ook voor de hieraan gekoppelde KRI's en KCI's.

De stappen van het risicomanagementproces worden hierbij geïntegreerd in de operationele en tactische processen binnen de organisatie.

Risico-identificatie

Risico-identificatie vindt primair plaats op het operationele niveau binnen de organisatie; dit is het niveau waar risico's 'ontstaan' en in het geval van verzekeringstechnische risico's letterlijk worden binnengehaald. Er zijn verschillende manieren ter identificatie van risico's, waaronder bijvoorbeeld workshops en analyse van relevante rapportages, issue logs, en/of benchmark informatie.

Geïdentificeerde risico's op het operationele niveau, worden besproken op tactisch niveau, als een afdelings-overstijgende aanpak benodigd dan wel gewenst is. Dit is ook het niveau waarop risico's, voortkomend uit de processen binnen de keten, in samenhang worden beschouwd. Op deze manier vindt identificatie van afhankelijkheden en relaties tussen (oorzaken van) risico's plaats. Een risico kan op zichzelf staand misschien niet erg belangrijk lijken, in termen van kans of impact, maar 'opgeteld' bij andere geïdentificeerde risico's wellicht heel vervelend uitpakken. Op tactisch niveau wordt vastgesteld welke risico's, of groep van risico's, op strategisch niveau besproken dient te worden.

Risicoanalyse

Risicoanalyse houdt in dat inzicht wordt verkregen in de geïdentificeerde risico's, waaronder:

- de kans dat het risico zich voordoet en de mogelijke impact als het risico zich voordoet;
- de oorzaken en gevolgen (zowel positief als negatief) van het risico;
- de (effectiviteit van) bestaande beheersmaatregelen; en
- de mogelijke samenhang met andere risico's, bijvoorbeeld in de vorm van een clustering naar oorzaken.

Risicoanalyse kan zowel kwalitatief als kwantitatief plaatsvinden, afhankelijk van het type risico of de risicocategorie waartoe het risico behoort. Kwalitatieve risicoanalyse kan bijvoorbeeld inhouden dat verschillende experts hun mening geven over de oorzaken, kansen, gevolgen, beheersmaatregelen en effectiviteit van beheersmaatregelen. Kwantitatieve risicoanalyse kan bijvoorbeeld uitgevoerd worden met behulp van risicomodellen (zie paragraaf 3.9).

In principe houdt risicoanalyse op tactisch niveau hetzelfde in als op operationeel niveau, echter wordt op tactisch niveau vooral de combinatie van meerdere (afdelings-overstijgende) risico's en hun oorzaken geanalyseerd. Hierbij wordt gesteund op risicoanalyses uitgevoerd op het operationele niveau.

Risico-evaluatie en risicobehandeling

De uitkomsten van de risicoanalyse worden getoetst aan de risicostrategie en de hieruit afgeleide KRI's en KCI's. Afhankelijk van de uitkomsten van de toetsing, en bespreking van het risico met risicomanagementspecialisten, wordt vastgesteld of de bestaande beheersmaatregelen toereikend en voldoende effectief zijn. Indien hiertoe aanleiding bestaat, worden aanvullende beheersmaatregelen vastgesteld. Opties voor risicobehandeling zijn:

- vermijden van het risico door te besluiten de activiteit waardoor het risico wordt veroorzaakt niet uit te voeren of voort te zetten;
- accepteren of verhogen van het risico teneinde een kans te benutten;
- wegnemen van de oorzaken van het risico;
- veranderen van de kans dat het risico zich voordoet;
- veranderen van de gevolgen van het risico; en/of het
- delen van het risico met een of meerdere andere partijen.

Risicobehandeling gaat in het algemeen om het vinden van de balans tussen risico's en beheersmaatregelen, en de kosten en uitvoerbaarheid van deze beheersmaatregelen. Overigens kan risicobehandeling zelf nieuwe (secundaire) risico's introduceren, zoals het falen van beheersmaatregelen of het tegenpartijrisico op herverzekeraars.

De evaluatie van risico's, of groep van risico's, en risicobehandeling kan zowel plaatsvinden op het operationele als op het tactische niveau. Indien noodzakelijk of gewenst kan besluitvorming over risicobehandeling plaatsvinden op strategisch niveau.

Monitoring en beoordeling

Op basis van relevante risicorapportages vindt monitoring en beoordeling van risico's en risicobeheersing plaats. Afhankelijk van de grootte en complexiteit van de organisatie kan monitoring en beoordeling zowel op het operationele, tactische, als strategische niveau plaatsvinden. De risicomanagementinformatie kan overigens ook gecombineerd worden met relevante performance rapportages op het operationele, tactische en/of strategische niveau, waarbij de strategische doelstellingen in samenhang met de genomen risico's worden beschouwd. Risicorapportages op strategisch niveau, dienen consistent te zijn met de rapportages op het tactische en operationele niveau.

Communicatie en overleg

Communicatie en overleg over risico's en risicobeheersing vindt enerzijds binnen de afdelingen/teams plaats waarbinnen de risico's worden geïdentificeerd en beheerst. Daarnaast vindt via een risico-overlegstructuur communicatie en overleg plaats met risicomanagementspecialisten. Risicomanagementspecialisten spelen een belangrijke rol in de vaststelling van de gewenste beheersmaatregelen en vormen de brug tussen het operationele en tactische niveau, onder andere door hun inzicht in alle (oorzaken van) risico's waaraan de organisatie is blootgesteld.

Op tactisch niveau vindt afdelings-overstijgend overleg plaats over risico's en risicobeheersing. De output van communicatie en overleg op operationeel niveau is input voor communicatie en overleg op tactisch niveau. Op tactisch niveau wordt vastgesteld welke risico's, of combinatie van risico's, op strategische niveau behandeld dienen te worden. Dit betekent dat op tactisch niveau wordt vastgesteld welke risico's rechtstreeks van invloed zijn op de gedefinieerde KPI's, KRI's en KCI's op strategisch niveau.

Communicatie en overleg dragen bij aan het vergroten van inzicht in risico's en risicobeheersing, onder andere omdat verschillende percepties van risico's en risicobeheersing via de risico-overlegstructuur worden gedeeld.

3.2 Risicostrategie en risicobereidheid

Een 'goede' risicostrategie van een organisatie omvat ten minste een beschrijving van:

- de strategische doelstellingen en uitgangspunten waarmee de risico's beheerst worden (zie hieronder);
- de risicobereidheid (zie hieronder); en
- wie waarvoor verantwoordelijk is, rekening houdend met de bestaande interne governance- en organisatiestructuur en bijbehorende verdeling van verantwoordelijkheden (zie paragraaf 3.5).

Doelstellingen

Bij strategische doelstellingen en uitgangspunten ten aanzien van risico's kan bijvoorbeeld gedacht worden aan doelstellingen ten aanzien van:

- minimale / target solvabiliteitsratio's;
- liquiditeit;
- maximale impact van risico's op resultaat, rendement, kapitaal, en/of solvabiliteitsratio;
- de toegevoegde waarde van risicomanagement voor de klant;
- de inrichting van de risicomanagementprocessen; en/of
- de benodigde (kennis)ontwikkeling en groei op het gebied van risicomanagement methoden, technieken, modellen en tools.

Risicobereidheid

Risicobereidheid ('risk appetite') kan op verschillende manieren worden uitgewerkt. In het algemeen worden de meer kwantitatieve risico's op een andere manier uitgewerkt dan kwalitatieve risico's.

Kwantitatieve uitwerking risicobereidheid

Risicobereidheid kan kwantitatief uitgedrukt worden in termen van risicobudgetten per risico of risicocategorie.[11] Dit betekent dat de impact van een risico(categorie) dat zich

[11] Een risicobudget is een gedeelte van het eigen vermogen dat wordt ingezet ter dekking van een risico of risicocategorie.

met een bepaalde kans voordoet in het komende jaar, niet groter mag zijn dan het risicobudget. Impact kan hierbij op verschillende manier uitgedrukt worden, bijvoorbeeld in termen van resultaat, rendement, solvabiliteitsratio, liquiditeitspositie, etc. In het algemeen worden verzekeringstechnische risico's, marktrisico's en tegenpartijrisico's als 'kwantificeerbaar' beschouwd.

Kwalitatieve uitwerking risicobereidheid

Voor de minder gemakkelijk kwantificeerbare risico's kan gebruik worden gemaakt van expert opinie, waaronder externe benchmarks, om de risico's te kunnen prioriteren (in termen van kans maal impact). Een andere manier om de risicobereidheid met betrekking tot minder gemakkelijk kwantificeerbare risico's uit te werken, betreft het formuleren van zogenaamde 'statements' om sturing en richting te geven aan de beheersing van het risico of de risicocategorie. In het algemeen worden niet-financiële risico's zoals strategische, operationele en compliance risico's, als minder gemakkelijk kwantificeerbaar beschouwd.

De risicobereidheid wordt vaak uitgewerkt in key risk indicatoren (KRI's) met bijbehorende tolerantieniveaus en eventuele andere beheersmaatregelen. Om binnen de grenzen van de vastgestelde risicobereidheid te acteren, dienen deze KRI's, tolerantieniveaus en andere beheersmaatregelen nader te worden vastgesteld en uitgewerkt in risicobeleid. Via de monitoring van beleid vindt bewaking van de implementatie van de risicostrategie op tactisch en operationeel niveau plaats.

3.3 Risicoclassificatie en risicoprofiel

Risico's worden vaak ingedeeld naar risicocategorieën. Voorbeelden van risicocategorieën zijn:

- verzekeringstechnisch risico;
- marktrisico;
- liquiditeitsrisico
- tegenpartijrisico;
- operationeel risico;
- compliance risico;
- strategisch risico;
- reputatierisico;
- nieuw en/of opkomend risico.

In Bijlage I is een lijst van definities opgenomen.

Een risico kan worden gedefinieerd als de onzekerheid omtrent het zich voordoen van gebeurtenissen die het realiseren van de doelstellingen van de organisatie in de weg kunnen staan. Belangrijke onderdelen bij het beschrijven van een risico zijn oorzaken (blootstellingen aan het risico), gebeurtenissen en de gevolgen van het zich voordoen van de gebeurtenis. Bovengenoemde voorbeelden zijn gebaseerd op gebeurtenissen waarbij wordt beschreven wat zich zou kunnen voordoen.

Er kan ook worden gekozen voor een risicocategorisatie op basis van de oorzaken van het risico. Voordeel hiervan is dat direct de koppeling kan worden gemaakt met de behandeling van het risico. Daarnaast kan op basis van een analyse van de oorzaken van de belangrijkste risico's waaraan de organisatie is blootgesteld, rationalisatie van risicomanagementactiviteiten plaatsvinden.

Het risicoprofiel van de organisatie bestaat uit een overzicht van de belangrijkste risico's waaraan de organisatie is blootgesteld. Met behulp van bijvoorbeeld een risicoregister worden de risico's 'bewaard' en wordt de status van risicobeheersing gemonitord. In het register kan, naast de oorzaken, gevolgen en beheersmaatregelen, worden bijgehouden wie verantwoordelijk is voor het risico, welke afspraken met de risico-eigenaar zijn gemaakt, en welke acties wanneer afgerond moeten zijn.

Eventuele nieuwe en/of opkomende risico's kunnen aan het register worden toegevoegd om doorlopend inzicht te hebben in het meest recente risicoprofiel.

3.4 Risicorapportages

Voor doeltreffend management van risico's zijn adequate risicorapportages nodig. Op basis van deze rapportages kan monitoring plaatsvinden van het meest recente risicoprofiel, in relatie tot de vastgestelde risicobereidheid, en de hierop afgestemde tolerantieniveaus, limieten en overige beheersmaatregelen.

Normen voor kwalitatief 'goede' risicomanagementinformatie zijn onder andere[12]:

- consistentie – Informatie over risico's sluit aan bij de (risico)strategie, strategische doelstellingen, en risicobereidheid;
- tijdig – Informatie over risico's wordt tijdig aangeleverd, zodat het meest recente risicoprofiel kan worden gepresenteerd. De frequentie van het rapporteren kan overigens variëren, afhankelijk van het soort risico, en de interne en externe omgeving;
- beknopt – Informatie is beknopt, maar omvat voldoende detail ter ondersteuning van besluitvorming. Op basis van de aangeleverde informatie moet besluitvorming over risicobehandeling kunnen plaatsvinden.
- consistent – Informatie is consistent met andere rapportages;
- controleerbaar – Informatie is controleerbaar en geproduceerd door middel van een traceerbaar, transparant en gedocumenteerd proces;
- toekomstgericht – Informatie bevat (ook) een toekomstgerichte visie.

Een risicorapportage kan bijvoorbeeld bestaan uit:

- een top 10 risico's;
- een heatmap waarin de top 10 risico's is opgenomen;
- belangrijkste interne/externe ontwikkelingen; en hiermee samenhangend

[12] Actuarial Aspects of ERM for Insurance Companies, paragraaf 3.8, International Actuarial Association, January 2016.

- de ontwikkeling van gedefinieerde KPI's, KRI's en KCI's, in relatie tot de risicobereidheid;
- verwachte interne/externe ontwikkelingen (nieuwe en/of opkomende risico's en scenario's);
- belangrijkste bevindingen en aanbevelingen; en eventueel
- relevante achtergrondinformatie.

In Bijlage II is een voorbeeld risicodashboard opgenomen. Een risicodashboard is een effectieve manier om beknopt over het algehele risicoprofiel te rapporteren.

3.5 Risicogovernance

Om ervoor te zorgen dat risico's worden meegenomen in besluitvormingsprocessen en verantwoording over risico's en risicobeheersing wordt afgelegd, dient de organisatie op een bepaalde manier te zijn ingericht. Relevante onderwerpen bij de inrichting van de organisatie zijn bijvoorbeeld:

- sleutelfuncties en het 3 Lines of Defence model (3LoD-model);
- uitbesteding;
- taken en verantwoordelijkheden (risico-eigenaarschap); en een
- risico-overlegstructuur.

Sleutelfuncties en het 3LoD-model

Met de invoering van de sleutelfuncties onder Solvency II (i.e. de risk management, compliance, actuariële en interne audit functie) is het 3LoD model verder geconcretiseerd. Met behulp van het model wordt het bestuur/senior management van de organisatie in staat gesteld risico's effectief te managen en de interne beheersing continu te verbeteren. Daarnaast draagt het model bij aan de versterking van de risicocultuur (zie paragraaf 3.6) en zorgt het voor 'countervailing power' bij besluit- en beleidsvorming, en de uitwerking ervan.

De eerste lijn

Tot de eerste lijn behoren de verschillende uitvoerende afdelingen en teams binnen de organisatie. Ook het management, en het bestuur/directie van de organisatie behoort tot de eerste lijn. De eerste lijn is verantwoordelijk voor de dagelijkse (operationele) bedrijfsvoering. Zij is verantwoordelijk voor het uitvoeren en monitoren van het risicobeleid (inclusief risicobereidheid) en het risicomanagementsysteem, en doen hierover verslag aan de Raad van Commissarissen, aandeelhouders, externe toezichthouders, en andere stakeholders. In hun werkzaamheden wordt de eerste lijn ondersteund door stafafdelingen, zoals HR en Finance. Ook de stafafdelingen zijn onderdeel van de eerste lijn. Alle processen die moeten worden uitgevoerd ter uitvoering van het verzekeringsbedrijf vallen in principe onder eerstelijnswerkzaamheden. De eerste lijn is hierbij zelf verantwoordelijk voor de kwaliteit en betrouwbaarheid van de uitvoering van deze processen en dient hierover verantwoording af te leggen (zie risico-overlegstructuur).

De tweede lijn

De tweede lijn wordt onder andere gevormd door de risicomanagement, compliance en actuariële functie. Iedere sleutelfunctie heeft haar eigen aandachtsgebieden en vormt zich een zelfstandig oordeel/advies over de risico's binnen haar aandachtsgebieden. De strategie, risicostrategie en risicobeleid, wordt hierbij als belangrijkste toetsingskader gehanteerd. Beleid wordt normaliter opgesteld door de tweede lijn, in nauwe samenwerking met de eerste lijn. Deze samenwerking draagt bij aan de praktische uitvoerbaarheid van het beleid.

Naast het vormen van een zelfstandig oordeel/advies over de risico's waaraan de organisatie is blootgesteld, of in de toekomst kan worden blootgesteld, voert de tweede lijn ook controlewerkzaamheden uit ten aanzien van bijvoorbeeld de toereikendheid van premies, voorzieningen, solvabiliteitskapitaalvereisten en de 'juistheid' van modellen (modelvalidatie). De tweede lijn heeft een onafhankelijke rol en rapporteert onafhankelijk naar het bestuur/directie en Raad van Commissarissen.

De derde lijn

De interne auditfunctie vormt de derde lijn. De interne audit functie geeft een onafhankelijke beoordeling van de doeltreffendheid van het algehele governance- en risicomanagementsysteem en daarmee over de samenwerking tussen de eerste en tweede lijn. Zij rapporteert direct aan het bestuur, door middel van een interne auditrapportage. In deze rapportage worden bevindingen en aanbevelingen geformuleerd, voortkomend uit de uitgevoerde onderzoeken conform het opgestelde auditplan. Het management wordt gevraagd te reageren op de bevindingen en aanbevelingen via een 'management response' en er worden afspraken gemaakt over de opvolging van de aanbevelingen en wie daarbij waarvoor verantwoordelijk is. De interne auditfunctie richt zich in haar auditplan veelal op de belangrijkste processen binnen het algehele governance- en risicomanagementsysteem. De risicomanagementprocessen kunnen onderdeel zijn van de scope van het auditplan, anderzijds kan ook gekozen worden voor het uitvoeren van proces audits op sub-processen zoals het PARP-proces[13] of het ORSA-proces.

Uitbesteding

Ook bij uitbesteding blijft de organisatie zelf eindverantwoordelijk voor de werkzaamheden en hieruit voortvloeiende consequenties. Solvency II stelt specifieke eisen voor wat betreft de uitbesteding van belangrijke 'kritieke' processen.[14] Zo dient de (her)verzekeraar DNB op de hoogte te stellen van de uitbesteding van kritieke of belangrijke functies of werkzaamheden en mag uitbesteding niet leiden tot afbreuk aan de kwaliteit van het governancesysteem van de organisatie.

[13] Sinds 1 januari 2013 voorziet het Besluit Gedragstoezicht financiële ondernemingen in eisen ten aanzien van de kwaliteit van productontwikkelingsprocessen van financiële ondernemingen en de daaruit voortvloeiende producten.
[14] Richtlijn Solvency II, artikel 49.

Taken en verantwoordelijkheden

In het governance- en risicomanagementsysteem spelen heldere taken en verantwoordelijkheden een cruciale rol. Zonder helder vastgelegde taken en verantwoordelijkheden kan geen verantwoording over risico's en risicobeheersing worden afgelegd. Een hulpmiddel om taken en verantwoordelijkheden binnen een proces in kaart te brengen is de zogenaamde RACI-matrix.

Door per processtap in te vullen wie 'Responsible', 'Accountable', 'Consulted', en 'Informed' is, worden de taken en verantwoordelijkheden concreet gemaakt.

Om verantwoording over risico's en risicobeheersing af te (kunnen) leggen dienen risico-eigenaren te worden aangewezen op bestuurs- en senior managementniveau. De risico-eigenaar is verantwoordelijk voor specifieke risico's en risicocategorieën en draagt zorg voor de opvolging van aanbevelingen vanuit de tweede en/of derde lijn.

Risico-overlegstructuur

Een risico-overlegstructuur is in het algemeen opgebouwd uit risico-overleggen op operationeel, tactisch en strategisch niveau. Op operationeel niveau vindt communicatie en overleg plaats met het management van de organisatie. Op tactisch niveau vindt communicatie en overleg plaats over die risico's die een afdelings-overstijgende aanpak vereisen. Dit is ook het niveau waarop wordt vastgesteld welke risico's op strategisch niveau behandeld dienen te worden; de risico's, of combinaties van risico's, die rechtstreeks en significant van invloed (kunnen) zijn op de gedefinieerde KPI's, KRI's en KCI's op strategisch niveau. De belangrijkste risico's waaraan de organisatie is blootgesteld worden behandeld in zogenaamde comités. Via deze comités vindt besluitvorming over de belangrijkste risico's en risicobeheersing plaats. Voorbeelden van comités zijn:

- Enterprise Risk Committee;
- Operational Risk Committee; en
- Financial Risk Committee.

In lijn met de doelstellingen van ERM kan in een Enterprise Risk Committee het risicoprofiel van de organisatie goed worden behandeld, omdat tijdens deze bijeenkomsten juist de correlaties en verbanden tussen de operationele en financiële risico's besproken kunnen worden (in de vorm van relevante oorzaak-gevolgrelaties). Aanvullend kunnen eventueel operationele (niet-financiële), en financiële committees worden ingericht. Relevante oorzaak-gevolg relaties spelen hierbij een belangrijke rol.

Via de risico-overlegstructuur wordt aantoonbaar verantwoording afgelegd over risico's en risicobeheersing. Eventuele ORSA-triggers[15] worden via de risico-overlegstructuur geïdentificeerd.

[15] Gebeurtenissen die aanleiding geven tot de uitvoering van een (ad hoc) ORSA.

3.6 Mensen en risicocultuur

De mensen die betrokken zijn bij de uitvoering van de risicomanagementprocessen dienen over de juiste kennis, kunde, vaardigheden en ervaring te beschikken. Dit geldt met name (ook) voor de beleidsbepalers van de organisatie (bijvoorbeeld bestuurs- en directieleden) en mensen die een sleutelfunctie vervullen.

Conform Solvency II moet elke verzekeraar beschikken over een beleidsdocument inzake deskundigheids- en betrouwbaarheidsvereisten waarin ten minste het volgende staat beschreven:

- de procedure voor het beoordelen van de deskundigheid en betrouwbaarheid van personen die de organisatie daadwerkelijk besturen of andere sleutelfuncties vervullen, zowel bij de selectie voor de specifieke positie als doorlopend tijdens het dienstverband;
- de situaties die aanleiding geven voor een herbeoordeling van de deskundigheids- en betrouwbaarheidsvereisten; en
- de deskundigheids- en betrouwbaarheidsprocedures voor het beoordelen van overig relevant personeel volgens interne normen, zowel bij de selectie voor de specifieke positie als doorlopend tijdens het dienstverband.[16]

Naast het borgen van voldoende kennis, kunde, vaardigheden en ervaring is het van belang dat een organisatie het mogelijk maakt om op objectieve en transparante wijze te rapporteren over risico's en dat problemen snel geëscaleerd kunnen worden, zodat deze vroegtijdig aangepakt kunnen worden tegen (uiteindelijk) lagere kosten. Ook het scheppen van een cultuur waarin fouten bespreekbaar kunnen worden gemaakt is van wezenlijk belang hierbij. Zelfs de meest geavanceerde ERM systemen en raamwerken zullen worden ondermijnd door het ontbreken van een 'juiste' risicocultuur.

Risicocultuur kan gedefinieerd worden als de normen en het gedrag van individuen en groepen binnen een organisatie die bepalen hoe er wordt omgegaan met het identificeren, begrijpen, discussiëren en omgaan met de risico's die een organisatie loopt en aangaat.17 Het definiëren, inbedden en monitoren van de gewenste risicocultuur dient een integraal onderdeel te zijn van de governancestructuur en is daarmee een directe verantwoordelijkheid van het bestuur/directie. Het is essentieel dat het uitdragen van risicodenken en een risicocultuur start bij het bestuur/directie van een organisatie om het een slagingskans te geven ("tone at the top"). Het voorschrijven van gewenst gedrag is echter niet voldoende voor het creëren van een juiste risicocultuur. Dit zal altijd samen moeten gaan met een effectieve implementatie van een risicomanagementraamwerk en risicomanagementprocessen. De mensen in de organisatie moeten bereid zijn en in staat worden gesteld om het gewenste gedrag toe te

[16] Solvency II Richtsnoeren voor het governancesysteem, richtsnoer 13 - Beleidslijnen en procedures inzake de deskundigheid en betrouwbaarheid.
[17] IIF Report Reform in the Financial Services Industry: Strengthening Practices for a More Stable System, Institute of International Finance, 2009.

passen. Deze combinatie zal dan op langere termijn resulteren in de gewenste risicocultuur.

3.7 Datakwaliteit en IT infrastructuur

Datakwaliteit

Hieronder worden de vier criteria voor de beoordeling van de kwaliteit van data toegelicht: volledig, juist, tijdig, en adequaat.

Volledig

Een dataset is volledig wanneer aan een aantal kenmerken wordt voldaan:

- alle relevante bezittingen en verplichtingen zijn vertegenwoordigd;
- alle relevante datavelden, portefeuillekenmerken, en (homogene) risicogroepen worden onderkend.
- de data bevat voldoende detailinformatie en voldoende historische data voor de beoogde analyses.
- alle voor het doel materiële informatie is aanwezig.

Wanneer niet aan deze kenmerken wordt voldaan kan er niet op vertrouwd worden dat een analyse van de betreffende dataset de antwoorden oplevert waarnaar men op zoek is.

Juist

Een dataset is juist wanneer deze vrij is van materiële fouten, vergissingen en omissies. Deze fouten, vergissingen en omissies worden bijvoorbeeld veroorzaakt door menselijke fouten of IT-gerelateerde problemen en zijn daarmee sterk gerelateerd aan de inrichting van beheerste processen rondom data-entry, opslag en levering. Daarnaast is een correcte systeemtechnische inrichting (datamanagement) van belang om de juistheid van data te garanderen.

Tijdig

Een dataset is tijdig wanneer het rapportage- of verwerkingsproces op het moment dat de data geleverd moet worden ook beschikbaar is, en tegelijkertijd voldoet aan de eisen voor wat betreft volledigheid, juistheid en adequaatheid

Adequaat

Data zijn adequaat wanneer deze geschikt én relevant zijn voor het doel waarvoor de data wordt gebruikt. Daarnaast moet data representatief zijn voor de populatie waarvoor de analyse wordt uitgevoerd.

Volledigheid en juistheid dragen bij aan de adequaatheid van de data. Of een dataset adequaat is zal niet altijd kunnen worden aangetoond door de systeemeigenaar (dataleverancier). In veel gevallen moet aan de hand van het model dat door de data gevoed wordt, worden vastgesteld of de data adequaat is.

Het kan voorkomen dat een dataset niet 100% aan de volledigheids- en tijdigheidscriteria voldoet. In dat geval zal moeten worden bepaald of de afwijkingen materieel zijn of niet. In het geval dat een dataset niet adequaat (geschikt, relevant én representatief) is, zal een andere dataset samengesteld moeten worden.

IT infrastructuur

De IT infrastructuur voor datamanagement fungeert als dataleverancier naar diverse partijen binnen een organisatie en verzorgt deels ook de borging van juistheid, compleetheid en tijdigheid van data. Naast deze componenten is de beveiliging van data een belangrijk onderdeel dat vanuit de IT functie wordt gefaciliteerd.

3.8 Raamwerken en beleid

In raamwerken en beleid worden de criteria en randvoorwaarden vastgesteld waaraan de processen, output, mensen, en middelen waaruit het ERM-systeem is opgebouwd dienen te voldoen. Hierbij wordt de gekozen (risico)strategie als belangrijkste uitgangspunt gehanteerd.

Raamwerken zijn in het algemeen meer beschrijvend van aard; ze geven meer informatie over een specifiek overkoepelend onderwerp, zoals bijvoorbeeld een raamwerk voor:

- het ERM-systeem – hoe is het ERM-systeem binnen de organisatie opgezet en georganiseerd en wie is daarbij waarvoor verantwoordelijk;
- modelvalidatie – welke modellen worden door wie wanneer gevalideerd en hoe;
- risicobereidheid – hoe wordt de risicobereidheid van de organisatie gedefinieerd, vastgesteld en gemonitord;
- beleid – welke beleidsdocumenten worden onderscheiden en hoe verhouden zij zich tot de (proces)structuur van de organisatie; of
- performance management – op welke manier is risicomanagement geïntegreerd in de besturingsprocessen van de organisatie?

Beleidsdocumenten dienen, conform Solvency II, afgestemd te worden op elkaar en de (risico)strategie van de organisatie. Hierbij geldt dat elk beleidsdocument ten minste een duidelijke beschrijving bevat van:

- de met het beleidsdocument nagestreefde doelstellingen;
- de taken die moeten worden uitgevoerd en de persoon of functie die daarvoor verantwoordelijk is;
- de processen en rapportageprocedures die moeten worden toegepast; en
- de verplichting van de desbetreffende organisatorische eenheden om de personen die verantwoordelijk zijn voor de risicomanagement, interne audit, compliance, en actuariële functie, in kennis te stellen van alle relevante feiten die nodig zijn voor de uitvoering van hun taken.[18]

[18] Solvency II Richtsnoeren voor het governancesysteem, richtsnoer 7 - Beleidslijnen.

Er kan onderscheid worden gemaakt in risico- en proces-gerelateerd beleid. In risico-gerelateerde beleidsdocumenten staan de toe te passen risicomanagementprocessen centraal. In proces-gerelateerd beleid staan de toe te passen operationele processen centraal, en de manier waarop de risicomanagementprocessen hierop inhaken (zoals beschreven in risico-gerelateerd beleid).

Voorbeelden van beleidsdocumenten zijn:

Risico-gerelateerd

- verzekeringstechnisch risicobeleid;
- marktrisicobeleid;
- liquiditeitsrisicobeleid;
- tegenpartijrisicobeleid;
- operationeel risicobeleid;
- compliance risicobeleid.

Proces-gerelateerd

- beleggingsbeleid;
- prijsbeleid;
- herverzekeringsbeleid;
- voorzieningenbeleid;
- product- en acceptatiebeleid.

3.9 Risicomodellen en tools

Risicomodellen worden meestal gebruikt om risico's te analyseren in termen van kans en impact. Tools kunnen helpen bij het verzamelen, analyseren en interpreteren van risicomanagement-informatie.

Risicomodellen

Het adequaat modelleren van risico's kent diverse voordelen:

- er kunnen gemakkelijker prioriteiten worden gesteld;
- kosten van risicobeheersing kunnen worden afgewogen tegen de baten;
- er bestaat voldoende inzicht in het benodigd kapitaal om risico's te kunnen dragen; en
- er wordt voldaan aan relevante wet- en regelgeving.

Bij het ontwikkelen van risicomodellen spelen aspecten als impact en complexiteit (i.e. materialiteit) een belangrijke rol; voor kleine organisaties en/of minder materiële risico's volstaat wellicht een minder verfijnd model. De mate van verfijning kan uitgedrukt worden in termen van nauwkeurigheid waarmee een risico wordt gemodelleerd, met behulp van:

- *Een (enkelvoudig) factor model*: dit is de meest eenvoudige vorm van risicomodellering. Een voorgeschreven factor wordt vermenigvuldigd met een bekende basishoeveelheid om de hoogte van het risico in te schatten.
- *Standaardschokken of stress testen*: de hoogte van een risico wordt ingeschat door de (financiële) impact vast te stellen van een voorgeschreven stress test of combinatie van stress testen. De Solvency II-standaardformule is bijvoorbeeld opgebouwd uit standaardschokken.
- *Intern model*: in plaats van standaardschokken door te rekenen, kunnen ook eigen schokken worden doorgerekend. De eigen schokken worden hierbij gekalibreerd op het specifieke risicoprofiel van de organisatie.
- *Een partieel intern model*: een partieel intern model bestaat voor een deel van de risico's uit een eigen inschatting van kansverdelingen (deterministisch of stochastisch vastgesteld) en voor de overige risico's uit de Solcency II standaardschokken of stress testen. Overigens is het bij gebruik van de Solvency II-standaardformule ook mogelijk om organisatie-specifieke parameters vast te stellen en toe te passen.
- *Een volledig intern model*: een volledig intern model betreft een inschatting van de kansverdeling van het totale risicoprofiel van de organisatie (deterministisch of stochastisch vastgesteld). De kansverdeling kan bijvoorbeeld worden vastgesteld met behulp van een multivariate kansverdelingsfunctie. Een andere mogelijkheid is om alle risico's (of risicocategorieën) separaat te modelleren en de resultaten vervolgens op te tellen met behulp van copula's.

Tools

Diverse software leveranciers hebben oplossingen ontwikkeld voor de governance, risk en compliance (GRC) uitdagingen waar verzekeraars mee te maken hebben. Zij bieden zogenaamde "GRC-tools" die ingezet kunnen worden voor verbetering van de effectiviteit van het risicomanagement- en interne controlesysteem. GRC-tools kunnen worden gebruikt om preventieve geautomatiseerde controles in te richten, te faciliteren en daarover te rapporteren.

Aandachtspunten voor een (effectieve) implementatie van een GRC-tool kunnen zijn:

- de volwassenheid van de (IT-)organisatie en interne controlesysteem in termen van gestandaardiseerde processen en controles; en
- de mate waarin de organisatie transparant wil zijn.

In de aanloop naar Solvency II zijn naast GRC-tools ook diverse tools ontwikkeld ter ondersteuning van het voldoen aan de Solvency II-vereisten op het gebied van de solvabiliteitskapitaalvereisten (Pillar I), het governancesysteem en ORSA (Pillar 2) en interne en externe verslaglegging (Pillar 3).

4 Monitoring en beoordeling ERM-systeem

Bij de monitoring en beoordeling van een ERM-systeem speelt zowel de risicomanagement functie als de interne audit functie een belangrijke rol. Door het ERM-systeem te monitoren en beoordelen, wordt gestreefd naar continue verbetering van het volwassenheidsniveau van het ERM-systeem.

De risicomanagement functie is verantwoordelijk voor het monitoren en beoordelen van het ERM-systeem. Een volwassenheidsmodel is hierbij een handig hulpmiddel.

Een volwassenheidsmodel bestaat in het algemeen uit drie componenten:

- criteria;
- niveaus;
- competenties.

Voorbeelden van bestaande ERM volwassenheidsmodellen zijn het ERM Maturity Model van Standard & Poor's en het volwassenheidsmodel risicomanagement van Management of Risk (M_o_R).

Aan de hand van de criteria wordt de volwassenheid van het ERM-systeem beoordeeld, dit kunnen bijvoorbeeld de in dit document gedefinieerde bouwstenen zijn.

De (volwassenheids-)niveaus geven aan op welk niveau de bouwsteen zich 'bevindt'.

Voorbeelden van niveaus zijn:

- *Initieel*. Risico's worden ad hoc geïdentificeerd en beoordeeld. De risicobereidheid is niet gedefinieerd. De risicomanagementprocessen zijn niet ingericht en/of aangesloten op het strategievormingsproces van de organisatie. Managementacties zijn met name reactief in plaats van proactief;
- *Herhaalbaar*. Er is een risicomanagementraamwerk ontwikkeld en er is capaciteit ter beschikking gesteld ter uitvoering van de risicomanagementprocessen. Er bestaat inzicht in het risicoprofiel van de organisatie;
- *Gedefinieerd*. Het ERM proces en risicomanagementprocessen zijn verder ontwikkeld en aangescherpt. Er wordt voldoende en geschikte capaciteit ter beschikking gesteld ter uitvoering van de processen. Het risicoprofiel wordt regelmatig in kaart gebracht. Risicomanagement wordt gebruikt om de prestaties van de organisatie te verbeteren;
- *Gemanaged*. Taken en verantwoordelijkheden zijn volledig helder en vastgelegd. Het ERM proces en risicomanagementprocessen worden structureel uitgevoerd en verbeterd. Risicomanagement staat gelijk aan 'kansenmanagement' en draagt aantoonbaar bij aan de prestaties van de organisatie;
- *Optimalisering*. Er is sprake van continue verbetering van de uitvoering van het ERM proces en de risicomanagementprocessen.

De competenties geven antwoord op de vraag: wat is er voor criterium X precies nodig om op niveau Y te komen?

Met behulp van een volwassenheidsmodel kan de risicomanagement functie een zo objectief mogelijk oordeel vellen over de status van het ERM-systeem binnen de organisatie. Daarnaast kunnen op basis van het volwassenheidsmodel relevante bevindingen en aanbevelingen worden geformuleerd. De huidige status van het risicomanagementsysteem binnen de organisatie kan uitgevraagd worden met behulp van bijvoorbeeld interviews, vragenlijsten en/of enquêtes.

De interne auditfunctie is verantwoordelijk voor de beoordeling van de effectiviteit van het algehele governancesysteem binnen de organisatie, waar het risicomanagement- en interne controlesysteem onderdeel van uitmaken. Ook de rol van de risicomanagementfunctie in het governancesysteem valt binnen de scope van de werkzaamheden van de interne auditfunctie.

5 Rollen binnen het ERM-systeem

De actuariële professional kan op verschillende gebieden werkzaam zijn binnen het ERM-systeem, bijvoorbeeld op het gebied van:

- risicomanagement;
- actuariële functie;
- modelontwikkeling;
- modelvalidatie;
- kapitaal- en risicobeheersing; en
- directie en CRO.

Risicomanagement

Risicomanagers waarborgen dat risico's die een bedreiging vormen voor de realisatie van doelstellingen worden geïdentificeerd, geanalyseerd, geëvalueerd en behandeld. Daarnaast draagt de risicomanager zorg voor communicatie en overleg met betrekking tot risico's en zorgt zij ervoor dat monitoring en beoordeling van het risicoprofiel plaatsvindt, in relatie tot de door de organisatie vastgestelde risicobereidheid. De risicomanager fungeert als sparring partner voor het bestuur/directie van de organisatie.

De rol van risicomanager is veelomvattend is en direct gekoppeld aan de strategie van de organisatie. Daarom zijn diverse vaardigheden van belang. Deze vaardigheden variëren van technische vaardigheden met betrekking tot het meten van risico's tot communicatieve vaardigheden met betrekking tot de toelichting op risicoposities en het creëren van draagvlak voor eventuele benodigde acties. Door de International Actuarial Association is eerder een uitvraag gedaan onder actuarissen over de vaardigheden die zij in de praktijk het meest van belang achten bij het uitoefenen van de rol van risicomanager. De resultaten hiervan zijn onderstaand weergegeven.

Figuur 2. Risicomanagementvaardigheden

In bovenstaand overzicht is te zien dat management vaardigheden het meest van belang worden geacht om de rol van risicomanager goed in te kunnen vullen. Kennis van de business van de organisatie, technische vaardigheden en communicatieve vaardigheden worden hierna van vrijwel gelijk belang geacht. Tot slot volgt relatiemanagement en kennis op het gebied van wet- en regelgeving en accounting.

Actuariële functie

Binnen verzekeraars is een actuariële functie ingericht conform de vereisten zoals gedefinieerd in Solvency II. Deze actuariële functie is een zogenaamde 2e lijns rol (zie ook paragraaf 3.5 over risicogovernance). De actuariële functie houdt zich voornamelijk bezig met onafhankelijke waarborging van de toereikendheid van de technische voorzieningen, acceptatie, herverzekering en premiestelling. Bovendien wordt van de actuariële functie een bijdrage aan de risicomanagement functie verwacht. De actuariële functie vervult op deze manier een belangrijke rol op het gebied van de verzekeringstechnische risico's binnen een ERM-systeem.

De actuaris werkzaam binnen deze rol richt zich inhoudelijk op de relevante onderwerpen en geeft daarmee mede invulling aan het monitoren van de verzekeringstechnische risico's en de wijze waarop deze passen binnen de strategie en binnen de risicobereidheid van de organisatie. Ook het adviseren aan bestuurlijke organen omtrent deze risico's en de manier waarop deze kunnen worden beheerst is een belangrijke taak van de actuariële functie.

Modelontwikkeling

Modellen vervullen een belangrijke rol binnen een ERM-systeem van verzekeraars. Veel risico's worden door middel van modellen gekwantificeerd, waarna besluitvorming plaats kan vinden over de beheersing ervan, kapitalisatie en mitigatie van risico's. Het is daarom voor een ERM-systeem van belang dat deze modellen effectief en betrouwbaar zijn. Actuariële professionals vervullen vaak een rol binnen de ontwikkeling van deze modellen.

Een model is een vereenvoudigde weergave van de werkelijkheid en beschrijft de samenhang tussen de belangrijkste (economische) grootheden. Een model reduceert de complexiteit en helpt om beter begrip van de werkelijkheid te krijgen, nu en in de toekomst. Op basis van een beter begrip kunnen meer onderbouwde besluiten worden genomen.

Voor financiële instellingen zijn onder andere economic capital modellen van belang. Dergelijke modellen ondersteunen bij het inzichtelijk maken van het algehele (integrale) risicoprofiel en het vaststellen van het vereist kapitaal hiervoor. Daarbij wordt veelal uitgegaan van een 'Value at Risk'-benadering, waarbij de omvang van risico's bij een bepaald betrouwbaarheidsniveau wordt aangegeven. Voorbeelden hiervan zijn de Solvency Capital Requirement (SCR) onder Solvency II voor (her)verzekeraars, waarbij een betrouwbaarheidsniveau van 99,5% geldt, en het Vereist Eigen Vermogen (VEV)

onder het FTK voor pensioenfondsen, waarbij een betrouwbaarheidsniveau van 97,5% geldt.

Begrip van en communicatie over dergelijke modellen en de wijze waarop de uitkomsten geïnterpreteerd kunnen/moeten worden is essentieel voor een goed werkend ERM-systeem.

Modelvalidatie

Het doel van modelvalidatie is om te beoordelen of een model functioneert zoals het is bedoeld. Modelvalidatie is een continu cyclisch proces. Validatie wordt veelal uitgevoerd of ondersteund door actuariële professionals of professionals met vergelijkbare kennis en ervaring. De scope loopt van initiële implementatie tot dagelijks gebruik. De frequentie en diepgang wordt mede bepaald door de materialiteit van het onderhavige risico. Er zijn meerdere manieren om een validatie uit te voeren.

Validatie in bredere zin is het controleren van een waarde of methode op geldigheid. Aan de hand van een aantal vooraf gestelde eisen wordt door middel van verificatie of kwalificatie aangetoond dat een waarde of methode met grote mate van zekerheid de resultaten oplevert zoals deze zijn bedoeld. Aangezien besluitvorming binnen een ERM-systeem mede wordt gebaseerd op de resultaten van modellen is gedegen validatie een belangrijk onderdeel.

Solvency II stelt eisen aan zowel modelbouw- als validatie en beschrijven de eisen die aan een intern model worden gesteld.[19] Voor modelbouw betreffen dit bijvoorbeeld eisen aan de modelwijzigingen, gebruikerstest, aannames en deskundig advies, methodologische consistenties, kansverdelingsprognose, kalibratiebenaderingen en documentatie.

Daarnaast worden vanuit Solvency II en de International Actuarial Note ook eisen gesteld aan de data voor wat betreft geschiktheid, volledigheid en nauwkeurigheid (adequaat, compleet, juist, tijdig).

Kapitaal- en risicobeheersing

Het doel van kapitaal- en risicobeheersing is om door middel van de vaststelling/toepassing van beheersmaatregelen de risico's en het daaruit volgende kapitaalsbeslag voor de verzekeraar tot een acceptabel niveau te beperken (i.e. binnen de grenzen van de risicobereidheid). Hiervoor is kennis van zowel de risico's als het vereist kapitaal – en de modellen waarmee deze wordt afgeleid – cruciaal. Daarnaast heeft de bewaking tot doel om vroegtijdig potentiële negatieve ontwikkelingen op te sporen en hier beheersmaatregelen voor te treffen.

[19] Solvency II Richtsnoeren inzake het gebruik van interne modellen.

Bestuur en CRO

Het bestuur/directie van de organisatie is eindverantwoordelijk voor een goed werkend ERM-systeem. In toenemende mate is hierin bij financiële instellingen een Chief Risk Officer (CRO) opgenomen. Teneinde die verantwoordelijkheid goed op zich te kunnen nemen dient een bestuurder en functiehouders derhalve te allen tijde voldoende deskundig en betrouwbaar te zijn. Bij de aanstelling zal hier door DNB dan ook expliciet op getoetst worden.

Om aan te kunnen tonen dat de instelling doorlopend aan geldende wet- en regelgeving voldoet zal het bestuur zorg moeten dragen voor een goede risicogovernance, voldoende en kwalitatief goed beleid alsmede processen om zodoende ook de effectiviteit van de governancestructuur en het beleid periodiek te kunnen toetsen. Daarnaast heeft het bestuur ook een voorbeeldfunctie en leidende rol om te borgen dat ERM niet alleen een management tool is, maar iets is wat door de gehele organisatie gedragen en doorleefd wordt.

Bijlage I: Definities risicocategorieën

Verzekeringstechnisch risico

Het risico op verliezen of op een ongunstige verandering in de waarde van verzekeringsverplichtingen door een ondeugdelijke prijsstelling en/of inadequate aannames met betrekking tot de voorzieningen.

Marktrisico

Het risico op verliezen of op een ongunstige verandering in de financiële situatie als direct of indirect gevolg van schommelingen in het niveau en/of in de volatiliteit van de marktprijzen van activa, verplichtingen en financiële instrumenten.

Liquiditeitsrisico

Liquiditeitsrisico is het risico dat men over onvoldoende middelen beschikt om aan de directe verplichtingen te voldoen.

Tegenpartijrisico

Het risico op verliezen als gevolg van onverwachte wanbetaling of een verslechtering van de kredietwaardigheid van de tegenpartijen en debiteuren van verzekerings- en herverzekeringsondernemingen.

Operationeel risico

Het risico op verliezen door inadequate of falende interne procedures, personeel of systemen of door externe gebeurtenissen.

Compliance risico

Het risico op verliezen of op een ongunstige verandering in de financiële situatie als gevolg van het niet voldoen aan interne dan wel externe wet- en regelgeving.

Strategisch risico

Risico's die het behalen van de strategische doelstellingen van de organisatie in de weg kunnen staan en tot verliezen kunnen leiden of juist toegevoegde waarde kunnen genereren.

Groepsrisico

Risico's vanuit het gezichtspunt van de groep, in plaats van de individuele juridische entiteit.

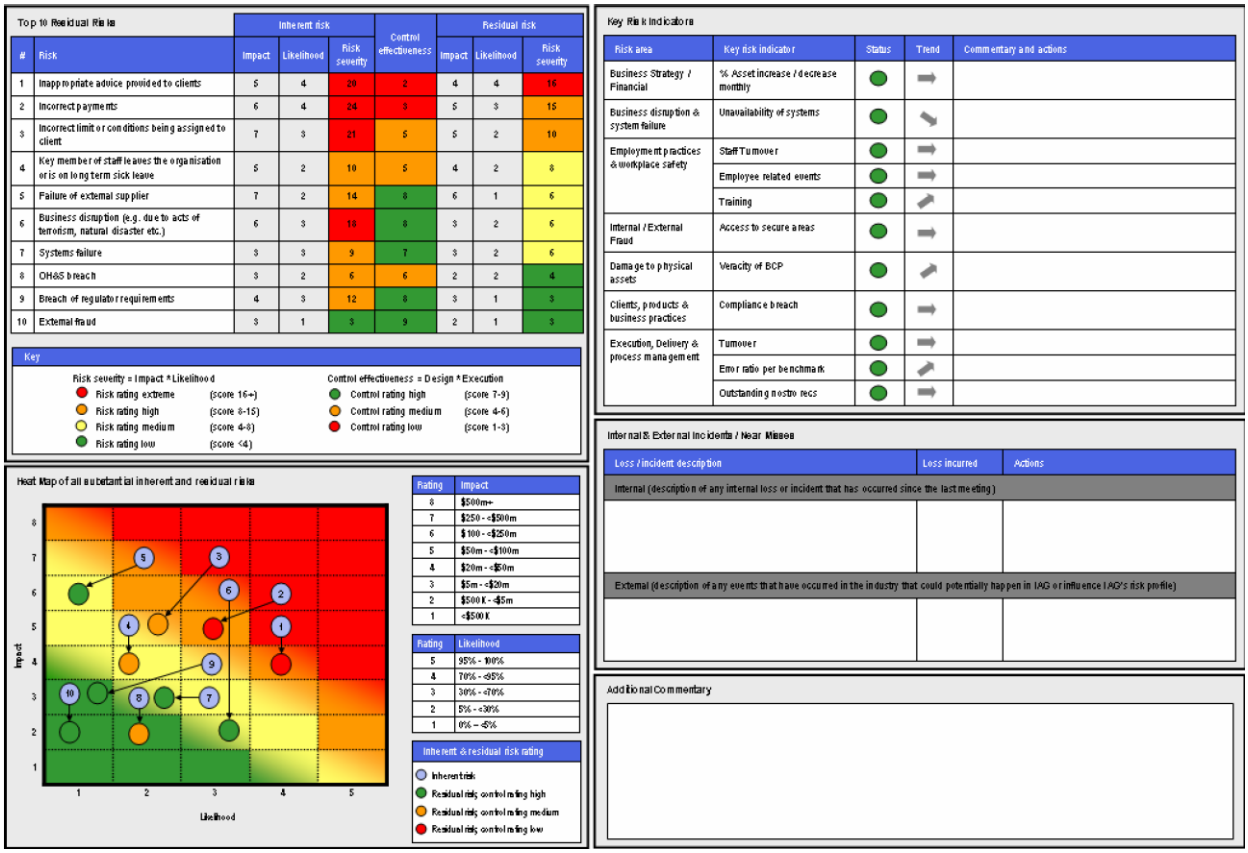
Nieuw of opkomend risico

Risico's die nog niet zijn geïdentificeerd of risico's waarmee (nog) geen rekening wordt gehouden met bestaande beheersmaatregelen.

Reputatierisico

Het risico dat door het handelen van de organisatie reputatieschade wordt geleden bij stakeholders.

Bijlage II: Voorbeeld risicodashboard[20]



Top 10 Residual Risks

		Inherent risk			Control effectiveness	Residual risk		
#	Risk	Impact	Likelihood	Risk severity		Impact	Likelihood	Risk severity
1	Inappropriate advice provided to clients	5	4	20	2	4	4	16
2	Incorrect payments	6	4	24	3	5	3	15
3	Incorrect limit or conditions being assigned to client	7	3	21	5	5	2	10
4	Key member of staff leaves the organisation or is on long term sick leave	5	2	10	5	4	2	8
5	Failure of external supplier	7	2	14	8	6	1	6
6	Business disruption (e.g. due to acts of terrorism, natural disaster etc.)	6	3	18	8	3	2	6
7	Systems failure	3	3	9	7	3	2	6
8	OH&S breach	3	2	6	6	2	2	4
9	Breach of regulator requirements	4	3	12	8	3	1	3
10	External fraud	3	1	3	9	2	1	3

Key

Risk severity = Impact * Likelihood

- Risk rating extreme (score 16+)
- Risk rating high (score 8-15)
- Risk rating medium (score 4-8)
- Risk rating low (score <4)

Control effectiveness = Design * Execution

- Control rating high (score 7-9)
- Control rating medium (score 4-6)
- Control rating low (score 1-3)

Heat Map of all substantial inherent and residual risks

Rating	Impact
8	$500m+
7	$250 - <$500m
6	$100 - <$250m
5	$50m - <$100m
4	$20m - <$50m
3	$5m - <$20m
2	$500 K - <$5m
1	<$500 K

Rating	Likelihood
5	95% - 100%
4	70% - <95%
3	30% - <70%
2	5% - <30%
1	0% - <5%

Inherent & residual risk rating

- Inherent risk
- Residual risk; control rating high
- Residual risk; control rating medium
- Residual risk; control rating low

Key Risk Indicators

Risk area	Key risk indicator	Status	Trend	Commentary and actions
Business Strategy / Financial	% Asset increase / decrease monthly			
Business disruption & system failure	Unavailability of systems			
Employment practices & workplace safety	Staff Turnover			
	Employee related events			
	Training			
Internal / External Fraud	Access to secure areas			
Damage to physical assets	Veracity of BCP			
Clients, products & business practices	Compliance breach			
Execution, Delivery & process management	Turnover			
	Error ratio per benchmark			
	Outstanding nostro recs			

Internal & External Incidents / Near Misses

Loss / incident description	Loss incurred	Actions
Internal (description of any internal loss or incident that has occurred since the last meeting)		
External (description of any events that have occurred in the industry that could potentially happen in IAG or influence IAG's risk profile)		

Additional Commentary

[20] Actuarial Aspects of ERM for Insurance Companies, paragraaf 3.8, International Actuarial Association, January 2016.

Bijlage III: Relevante verwijzingen

NEN-ISO 31000. Risicomanagement – Principes en richtlijnen, 2009.

Robert J. Chapman. Simple tools and techniques for enterprise risk management.

Society of Actuaries in Ireland. Creating Effective Actuarial and Risk Management Functions under Solvency II, March 2013.

Office of Government Commerce. M_o_R (Management of Risk): Richtlijn voor Practitioners, 2009.

Standard & Poor's. RatingsDirect – Enterprise Risk Management, May 7, 2013.

International Actuarial Association, Actuarial Aspects of ERM for Insurance Companies, January 2016.

International Actuarial Association, IAA Risk Book - Governance, Management and Regulation of Insurance Operations.

Solvency II, Richtlijn 2009/138 EG.

Solvency II, Gedelegeerde Verordering (EU) 2015/35.

COSO, Embracing Enterprise Risk Management: Practical Approaches for Getting Started (2011).

International Association of Insurance Supervisors (IAIS), International regulatory standard on ERM (Insurance Core Principle 16 ERM for solvency purposes, 2010).

Society of Actuaries, Enterprise risk management specialty guide (2006).