Uitdagingen voor de Chief Risk Officer

De wereld verandert snel en daarmee ook de uitdagingen voor het risicomanagement systeem bij organisaties. Dit heeft ook gevolgen voor het takenpakket van de Chief Risk Officer (CRO). Dit artikel geeft een overzicht van enkele actuele uitdagingen voor de CRO en hoe te borgen dat het risicomanagementsysteem een goed-geoliede en effectieve machine blijft.

Dit artikel is geschreven door de Commissie ERM van het AG, bestaande uit Rik van Beers, Corné van Iersel, John Oost, Leendert de Rijke en Jan-Willem Zeijen.

DE ROL VAN DE CHIEF RISK OFFICER

De term CRO wordt vaak gebruikt voor de persoon die verantwoordelijk is voor het risicomanagementsysteem én lid is van het bestuur van een organisatie. Hoewel dit artikel zich op deze CRO richt, is veel ook van toepassing op de actuariële en risicomanagementfuncties. Deze zijn onderdeel zijn van dit systeem en ondersteunen de CRO bij de uitvoering van zijn/haar taken.

Deze taken zijn divers. De CRO houdt zich bezig met de inhoud, maar moet als bestuurslid ook meebeslissen over de strategische richting van de organisatie, dit alles terwijl een team van professionals met uiteenlopende achtergronden aangestuurd moet worden. Hierbij staan thema's als duurzaamheid en klimaatrisico hoog op de agenda. Daarnaast dienen tal van nieuwe onderwerpen zich aan, zoals cyberrisico en Artificial Intelligence (AI). Ook hier moet de CRO zich in verdiepen.

Dit brede takenpakket heeft geleid tot meer specialisten binnen het risicomanagement. De CRO zelf echter moet over al het bovenstaande een mening hebben. Recente ontwikkelingen zoals COVID-19, hoge inflatie en geopolitieke risico's laten zien dat de CRO voor veel uitdagingen staat. Tegelijkertijd biedt dit ook kansen, bijvoorbeeld een verdere integratie van het risicomanagement in de algehele bedrijfscultuur.

TEGENWOORDIG LIGT DE FOCUS OP EFFECTIVITEIT EN EFFICIËNTIE

UITDAGINGEN

De focus in het afgelopen decennium lag – onder andere door de invoering van Solvency II – op het opzetten van het risicomanagementsysteem. Tegenwoordig ligt de focus op effectiviteit en efficiëntie bij de uitvoering hiervan. Dit omvat meerdere aandachtsgebieden waarvan we de volgende willen aankaarten:

- Emerging risks
- Wet- en regelgeving
- Risicocultuur
- Standaardisatie en digitalisering
- Feedback loop

Emerging risks – Toegenomen complexiteit en veranderende risico's zorgen dat zowel het risicospectrum als de mogelijkheden voor de beheersing hiervan veranderen. Actuele thema's hierbij zijn duurzaamheid en AI. Maar ook geopolitieke, economische, financiële en technologische ontwikkelingen moeten onverminderd aandacht krijgen, waarbij de impact op de organisatie centraal staat. Dit vereist voor organisaties een open blik en voldoende tijd en aandacht om hier inzicht in te krijgen.

Wet- en regelgeving – Hetzelfde geldt voor nieuwe wet- en regelgeving. Naast voldoende tijd en aandacht moet hier ook worden aangetoond dat aan alle eisen wordt voldaan. Voorbeelden zijn de Solvency II 2020 review, invoering van IFRS9/17, nieuwe pensioenwet, duurzaamheidswet- en regelgeving, Digital Operational Resilience Act (DORA), AI Act en Customer Due Dilligence (CDD).

Risicocultuur – Het is cruciaal dat risicomanagement een integraal onderdeel is van de bedrijfscyclus. Risicomanagement moet niet alleen worden ingestoken als controlefunctie of compliancevereiste, maar daadwerkelijk door de business worden gezien als toegevoegde waarde. Een gezonde risicocultuur is hierin een essentiële succesfactor. Ook bij een goede inrichting van het risicomanagementsysteem, moet gewaarborgd worden dat voldoende aandacht wordt besteed aan training en bewustwording van alle risico's – zowel strategisch als operationeel – en op alle niveaus binnen de organisatie. Met risicocultuurbeoordelingen en het hebben van risico-indicatoren kunnen concrete doelen worden gesteld en kan de voortgang worden gemonitord.

Standaardisatie en digitalisering – Veel voorkomende handmatige stappen kunnen worden gestandaardiseerd. Daarnaast kunnen eerstelijnsprocessen worden gedigitaliseerd met het gebruik van data-gedreven controles en het gebruik van tools ter ondersteuning van de uitvoering van het risicomanagementsysteem. Deze tools worden vaak met de term *Governance, Risk en Compliance (GRC) tooling* aangeduid. Bij een geïntegreerd systeem kunnen geïntegreerde rapportages bottom-up worden gevoed met data. Dit alles leidt tot efficiëntere en effectievere risicomanagementprocessen.

Feedback loop – Een eigen feedback loop voor het risicomanagement-systeem leidt tot een proces van continue verbetering, waarbij ook de verwachtingen van de business kunnen worden gemanaged. Deze feedback loop bestaat uit een periodieke evaluatie van het risicomanagementsysteem, waarbij de hiaten worden vastgesteld en nieuwe doelen worden gesteld. Een nauwe samenwerking met de business in alle stappen van het evaluatieproces, inclusief het stellen van nieuwe doelen, is hierin essentieel.

KANSEN OM HET GEHELE RISICOMANAGEMENTSYSTEEM VERDER TE VERBETEREN

HOE OM TE GAAN MET DEZE UITDAGINGEN?

De genoemde uitdagingen moeten vooral gezien worden als kansen om het gehele risicomanagementsysteem verder te verbeteren. De CRO is de uitgelezen persoon om hier verder richting aan te geven. Dit kan door:

- Invulling van de eigen rol als *teamleider* van de eerste en tweede lijn (inclusief de medebestuursleden en sleutelfunctionarissen). Een duidelijke rolverdeling tussen de sleutelfuncties (risicomanagement, actuarieel, compliance[1] en internal audit) en het delegeren van taken naar risico-eigenaren zijn hierin belangrijk. Dit draagt bij aan een cultuur van risicobewustzijn en zorgt dat de CRO de rol van teamleider op het gebied van risicomanagement kan invullen. Bij een duidelijke rolverdeling kan de actuariële functie bijvoorbeeld gebruikmaken van de uitkomsten van uitgevoerde controles door de risicomanagement-functie. Dit is belangrijk omdat falende controles kunnen leiden tot onzekerheden in de uitkomsten van de technische voorzieningen en kapitaalberekeningen.
- Te focussen op de *hoofdlijnen* van ontwikkelingen op het gebied van onder meer technologie en wetgeving, en de impact hiervan op de organisatie. De details hiervan kunnen dan door experts binnen de organisatie worden uitgewerkt. Een voorbeeld is informatiebeveiliging en IT-risicobeheer. Als er geen Chief Information Security Officer (CISO) is, valt dit in het takenpakket van de CRO. Gezien het toenemende belang van dit onderwerp – bijvoorbeeld door de invoering van DORA – moet dit met voldoende diepgang ingevuld worden.
- In het verlengde hiervan, te zorgen voor *voldoende kennis en kunde* bij de sleutelfunctionarissen en risico-eigenaren. Voldoende capaciteit om de genoemde ontwikkelingen te volgen en om te zetten in praktische adviezen is hierbij een randvoorwaarde.
- Het risicomanagementsysteem in te richten vanuit de *strategie en risicobereidheid* van de organisatie. Risico's en de activiteiten kunnen op basis hiervan worden geprioriteerd. Er moet een duidelijk normenkader zijn waaruit blijkt hoe strategische doelstellingen van de organisatie samenhangen met (strategische) risico's en welke principiële afweging tussen risico en rendement hierbij wordt genomen door het bestuur. De risicobeheersing dient vervolgens te passen bij deze afweging. Een instrument als de Own Risk & Solvency Assessment (ORSA) voor verzekeraars en de Eigen Risicobeoordeling (ERB) voor pensioenfondsen is hierbij een hulpmiddel.
- Te zorgen voor een *risico-oordeel* bij belangrijke bestuursbesluiten en beleidswijzigingen. Deze betrokkenheid bij het bestuur helpt de CRO om de rol van strategische partner en business partner in de bedrijfscyclus verder in te vullen.

WAT DOEN WE HIERMEE ALS KONINKLIJK ACTUARIEEL GENOOTSCHAP?

Het AG heeft risicomanagement opgenomen in de eigen producten en diensten waaronder de opleiding, permanente educatie, aanwijzingen, leidraden en publicaties. De commissie ERMO faciliteert hierbij en volgt de relevante ontwikkelingen op het gebied van risicomanagement. Voor de CRO specifiek, organiseert de commissie samen met het Verbond van Verzekeraars sinds vorig jaar de CRO Ronde Tafel waarmee een platform wordt geboden aan CRO's om over deze uitdagingen en mogelijkheden te sparren. ■

1 – Compliance is bij banken en verzekeraars een verplichte functie vanuit Solvency II, bij pensioenfondsen wijst IORP II enkel de functies risicobeheer, actuarieel en interne audit als verplicht aan.