b

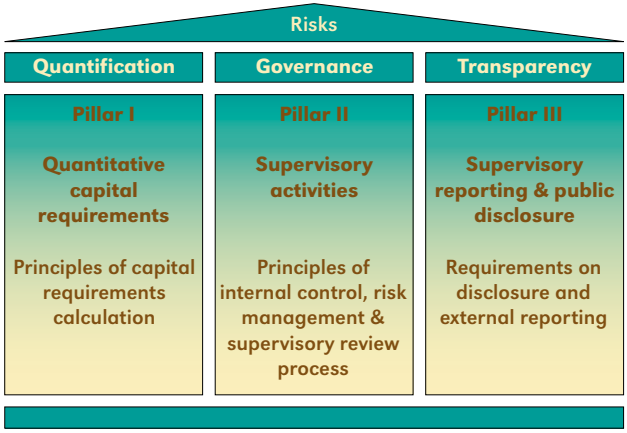
Risk management: over operationele risico's en IT

Age-Jan van der Meer

In de financiële sector is er steeds meer aandacht voor de beheersing van risico's. Gezien het feit dat recent de kredietcrisis in volle omvang is losgebroken, is risk management een actueel onderwerp. Of het nu gaat om Basel II in de bancaire wereld of Solvency II in verzekeringsland, het thema 'risk management' is hot.

Basel II en Solvency II

Er zijn anno 2008 vele initiatieven en wijzigingen gaande in de regulatieve omgeving van de financiële sector. Zo wordt het Basel II-akkoord momenteel ingevoerd binnen de bancaire sector. Hoofddoel van Basel II is om het systeemrisico (risico dat voor de hele markt geldt) te reduceren door middel van het reguleren van de kapitaaleisen op basis van de werkelijke risico's die banken lopen. De overeenkomst tussen Basel II en Solvency II is de conceptuele kapstok waar beide aan zijn opgehangen (zie figuur 1).



Figuur 1. Basel II en Solvency II.

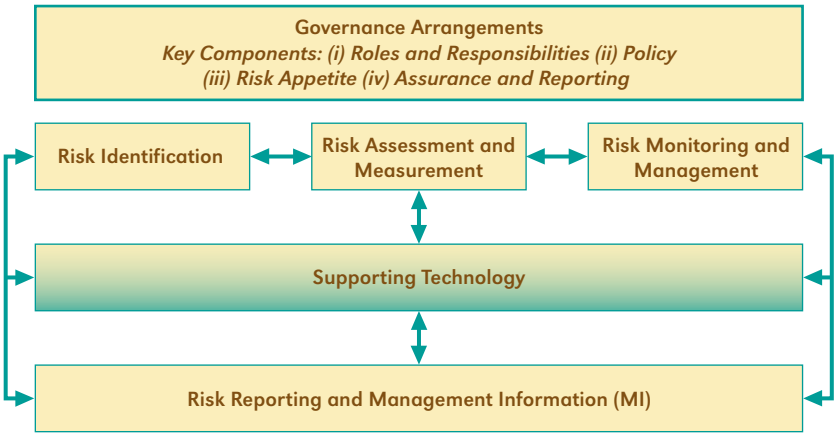
Drs. Age-Jan van der Meer RE RO is senior manager bij Ernst & Young Advisory en heeft meer dan tien jaar ervaring in de IT. Hij is gespecialiseerd in vraagstukken op het snijvlak van business en IT in het algemeen en risk management in het bijzonder. Hij geeft organisaties in met name de financiële sector advies over onder andere Basel II en Solvency II.

E-mail: age-jan.van.der.meer@nl.ey.com

Bij Solvency II en Basel II worden in de eerste pilaar (Pillar I) de risico's in kaart gebracht en gekwantificeerd. In Pillar II wordt intern risicomanagement beschreven, en de controle door de toezichthouder(s) die, indien nodig, een extra opslag op het kapitaal kan (kunnen) eisen. Daarnaast worden moeilijk te kwantificeren risico's geanalyseerd. In Pillar III worden eisen vastgelegd ten aanzien van de wijze van rapporteren naar zowel de toezichthouder(s) als naar het algemene publiek (de markt). Een bijzondere plaats in dit geheel wordt ingenomen door informatietechnologie. De invoering van Basel II heeft geleerd dat met name de inspanningen die nodig zijn op IT-gebied om te voldoen aan de regelgeving in Pillar II en III, niet moeten worden onderschat.

Operational Risk Framework

Vanzelfsprekend dienen de (operationele) risico's ten aanzien van het gebruik van IT te worden beheerst. Operationeel risico is het risico op verliezen door tekortschietende of falende interne procedures, door personeel of systemen of door externe gebeurtenissen. Om de operationele risico's te managen kan een aantal activiteiten worden uitgevoerd met als doel het op adequate wijze inventariseren en beheersen van deze risico's. Hiertoe kan het Operational Risk Framework worden gehanteerd dat door Ernst & Young is ontwikkeld op basis van best practices (zie figuur 2).



Figuur 2. Operational Risk Framework (Ernst & Young).

De activiteiten uit het framework zijn als volgt onder te verdelen:

- *Governance Arrangements:* het bepalen van de beheersingsstructuren met betrekking tot operational risk management. Hierbij kan worden gedacht aan het bepalen van taken en verantwoordelijkheden, beleid en rapportagelijnen alsmede het risicoprofiel dat de organisatie voor zichzelf onderkent (risk appetite).
- *Risk Identification:* het identificeren en vaststellen van de operationele risico's aan de hand van bijvoorbeeld risk self-assessments door het (lijn)management. Audits zoals uitgevoerd door internal audit en/of externe partijen kunnen hieraan bijdragen.
- *Risk Assessment and Measurement:* het meten en beoordelen van operationele risico's aan de hand van verliezen die zich hebben voorgedaan (loss database) en interne en externe ervaringscijfers (bijvoorbeeld benchmarking).
- *Risk Monitoring and Management:* het op periodieke wijze dan wel continue basis monitoren van de beheersing van de operationele risico's en het aan de hand van de voorgaande twee activiteiten ontwerpen en implementeren van adequate beheersingsmaatregelen om de kans en impact op het zich manifesteren van operationele risico's te beperken.
- *Supporting Technology:* IT-applicaties die de uitgevoerde activiteiten ondersteunen, bijvoorbeeld tools voor het modelleren en berekenen van risico's.

- *Risk Reporting and Management Information:* het rapporteren over bovenstaande activiteiten aan zowel interne als externe belanghebbenden.

In het kader van de beheersing van de IT-aspecten van operationele risico's zal met name aandacht uitgaan naar de entity level controls (IT-strategie, beleid, planning, informatiebeveiliging, et cetera) en IT general controls (waaronder logische toegangsbeveiliging, change management en continuïteitsaspecten). Daarnaast is IT een belangrijke enabler voor het kunnen opleveren en gebruiken van de benodigde gegevens. Het gebruik van een grote verscheidenheid aan gegevens wordt onder Basel II en Solvency II vergroot door het wijzigen van de manier van het berekenen van kapitaalvereisten, het vergroten van de nadruk op een adequaat risk-managementsysteem en de aanpassing van de rapportages richting toezichthouders. Het thema 'datakwaliteit' wordt onder Basel II en Solvency II dan ook urgenter: er is meer inzicht vereist in de dagelijkse operatie van de organisatie. Financiële instellingen zijn over het algemeen van oudsher met name productgericht georganiseerd en ook de IT-systemen zijn daardoor gericht op het administreren van producten. Vanwege de jarenlange groei van financiële instellingen door middel van consolidaties, productinnovaties en diversificatie naar nieuwe distributiekanalen, is de kwaliteit van gegevens of ook wel datakwaliteit op dit moment nog steeds een zeer belangrijk thema. Basel II en Solvency II vereisen inzicht en rapportages op holdingniveau (geconsolideerd). Dit inzicht wordt verkregen uit het combineren en vervolgens analyseren van de diverse gegevens die beschikbaar zijn in de IT-systemen, zoals geïncasseerde premies, uitgekeerde bedragen, ingenomen (beleggings)posities, storingen en fouten. Omdat de gemiddelde financiële instelling een veelvoud aan administratieve (product)systemen gebruikt per business line, is het relatief complex om een centraal geconsolideerd inzicht te verkrijgen in de dagelijkse operatie van de organisatie. Immers, dit inzicht op holdingniveau van de financiële instelling is tot op heden met name gericht op de processen die financiële cijfers opleveren en in veel mindere mate op de processen van de operatie.