GEVOLGEN VOOR INFORMATIETECHNOLOGIE BINNEN VERZEKERINGSMAATSCHAPPIJEN

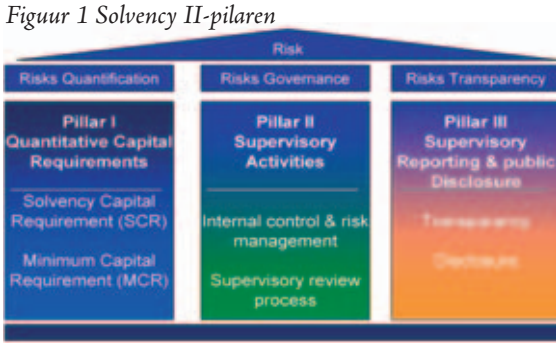
De IT-impact van Solvency II

In dit artikel komt de *impact* van Solvency II op de IT-functie van verzekeringsmaatschappijen aan bod. Recent onderzoek[1] onder de grote verzekeraars in Nederland heeft aangetoond, dat deze de betreffende impact over het algemeen onderschatten. De invoering van Solvency II in 2012 lijkt ver weg, maar dat is het gezien de benodigde inspanningen niet. Voor de verzekeringsbranche is het daarom van belang daar nu mee te starten.

AGE-JAN VAN DER MEER

Uit het genoemde onderzoek blijkt, dat de helft van het aantal respondenten slechts beperkte aanpassingen verwacht in de productadministraties en reken- en rapportagetools. Daarnaast verwacht 86 procent geen tot weinig problemen ten aanzien van het verkrijgen van adequate data (polisgegevens) uit bronsystemen en alle respondenten verwachten dat voldoende historische data (polisgegevens) voorhanden is in de eigen organisatie.

Figuur 1 Solvency II-pilaren



Ruim tachtig procent denkt dat kwaliteit van historische data voldoende is voor interne modellering.
De recente ervaring met de invoering van Basel II in de bancaire sector heeft aangetoond dat deze regelgeving grote gevolgen heeft gehad voor de IT-functie van banken. Vanwege de parallellen tussen Basel II en Solvency II is hieruit lering te trekken.

Allereerst wordt nu uiteengezet wat Solvency II omvat, met een toelichting bij de achtergrond van Solvency II, het binnen Solvency II gehanteerde conceptuele raamwerk en de fasering van Solvency II.

SOLVENCY II

Achtergrond

Solvency II is de opvolger van Solvency I. Solvency I is sinds 1973 door middel van tussentijdse akkoorden gevormd en is uiteindelijk door de Europese Commissie (EC) in 2002 aangenomen. Het doel van deze akkoorden is om de polishouders te beschermen tegen insolvabiliteit van de verzekeraars, door eisen te stellen aan de omvang van het kapitaal dat de verzekeraars moeten aanhouden. De akkoorden zijn van toepassing op *life* (bijvoorbeeld levensverzekeringen), *non-life* (bijvoorbeeld schadeverzekeringen) en herverzekeraars. De subdoelen van het Solvency II-akkoord zijn:

- zorgen dat de *supervisors* (onafhankelijke toezichthouders) over de juiste methoden en autoriteit beschikken;
- robuustheid, consistentie en harmonisatie van op verzekeraars van toepassing zijnde regelgeving;
- verbeteren van de onderlinge concurrentie;
- beter gebruik van de kapitaalmiddelen;
- invoering mag geen grote veranderingen veroorzaken in de markt.

Het huidige akkoord betreffende de solvabiliteitseisen voor verzekeraars, Solvency I, wordt door toezichthouders niet meer toereikend geacht. Het kapitaal dat volgens Solvency I door verzekeringsmaatschappijen dient te worden aangehouden, is geen goede maatstaf meer voor het kapitaal dat aangehouden zou moeten worden met het oog op de werkelijke risico's die een verzekeraar loopt. Het huidige akkoord houdt bijvoorbeeld onvoldoende rekening met het aantal polissen dat een onderneming uit heeft staan: hoe meer polissen een verzekeraar uit heeft staan, hoe groter het diversificatie-effect is en des te lager het verzekeringstechnische risico is dat de verzekeraar loopt.

Drie pijlers

Er zijn anno 2009 vele initiatieven en wijzigingen gaande in de regulatieve omgeving van de financiële sector, al dan niet versterkt door de kredietcrisis. Zo wordt het Basel II-akkoord momenteel ingevoerd binnen de bancaire sector. Het hoofddoel van Basel II is om het systeemrisico (risico dat voor de hele markt geldt) te reduceren door middel van het reguleren

Drie pillars

Bij Solvency II en Basel II worden in de eerste *pillar* de risico's in kaart gebracht en gekwantificeerd. In pillar 2 wordt intern risicomanagement beschreven en de controle door de supervisor die, indien nodig, een extra opslag op het kapitaal kan eisen. Daarnaast worden moeilijk te kwantificeren risico's geanalyseerd. In pillar 3 worden eisen vastgelegd ten aanzien van de wijze van rapporteren naar zowel de supervisor als naar het algemene publiek (de markt).

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).

Door het Committee of European Insurance and Occupational Pension Supervisors (CEIOPS) wordt in overleg met de industrie momenteel een voorstel tot invulling gemaakt dat wordt gericht aan de EC. Door middel van de zogenaamde 'waves of calls for advise', die vanuit de EC zijn ontstaan, en de 'Quantitative Impact Studies' (QIS) zorgt het CEIOPS ervoor dat de markt, verzekeraars, actuarissen en accountants kunnen reageren op en meehelpen met de ontwikkeling van het akkoord. Het voordeel is dat de verzekeringsmaatschappijen zich hierdoor grotendeels achter het akkoord scharen en dat de vereisten van het akkoord technisch haalbaar zijn voor de verzekeraars.

Fasering

Het akkoord wordt ontwikkeld in drie fases. In fase 1 is de driepilarenstructuur gekozen en het besef gecreëerd dat een op risico gebaseerde solvabiliteit moest worden nagestreefd. Fase 1 is in 2003 afgerond. Nu is de tweede fase van toepassing, waarin het raamwerk van Solvency II wordt ontwikkeld en beschreven in een richtlijn van de Europese Commissie. Het eerste concept van de nieuwe richtlijn (*directive*) is op 10 juli 2007 verschenen. In de laatste fase, de implementatiefase, wordt het akkoord verder gekalibreerd en ingebed in de nationale wet- en regelgeving. In Nederland zal De Nederlandsche Bank (DNB) hierop toezicht houden. Daarnaast zal het nodige worden geëist van de verzekeraars, die het akkoord moeten implementeren binnen de eigen organisatie. De verwachting is dat Solvency II in 2012 binnen de Europese Unie van kracht wordt.

INFORMATIETECHNOLOGIE

Laten we beginnen met het zoeken van de woorden *technology* en *information system* in de Solvency II *draft directive*. Het resultaat van deze zoekactie is helder: geen treffers. Tenzij er verzekeringsmaatschappijen zijn die anno 2009 nog zonder IT werken, betekent het ontbreken van expliciete verwijzingen in de draft directive niet dat Solvency II geen gevolgen heeft voor IT.

De invloed van Solvency II op IT bestaat enerzijds uit de vereisten die Solvency II impliciet stelt aan de beheersing van IT: de zogenaamde *IT-governance*. Anderzijds is IT een belangrijke *enabler* voor het kunnen voldoen aan de Solvency II-vereisten, middels bijvoorbeeld het gebruik van gegevens uit (*legacy-*)systemen voor het berekenen van kapitaalvereisten, het interne *risk management*systeem en het vervaardigen van rapportages richting toezichthouders.

IT-GOVERNANCE

In deze paragraaf komt aan de orde wat IT-governance binnen Solvency II omvat.

Vier elementen

In artikel 41 van de draft directive wordt aangegeven dat verzekeringsmaatschappijen een effectief systeem van governance dienen te hebben, dat zorg draagt voor adequaat en zorgvuldig management van de dagelijkse gang van zaken. Het vervolg van artikel 41 leert dat dit governancesysteem uit ten minste vier elementen bestaat: risk management, *internal control*, *internal audit* en uitbesteding. Daarnaast wordt aangegeven dat het beleid inzake deze elementen dient te zijn geformaliseerd, gedocumenteerd en in de organisatie moet zijn geïmplementeerd. Dit geheel dient jaarlijks te worden geëvalueerd. Hierbij is de verwachting dat de toezichthouders, bij het gebruik van interne risicomodellen (waarover later meer), een hogere mate van detail in de beschrijvingen van de vier elementen vereisen, dan bij het hanteren van de standaardmodellen.

Risk management

Het risk managementsysteem (draft directive, artikel 43) bestaat uit het geheel van strategieën, processen en rapportages die nodig zijn om de risico's van verzekeringsmaatschappijen op een continue basis te monitoren, beheersen en rapporteren. Een bijzondere plaats in het risk managementsysteem neemt de beheersing van operationele risico's in. Pillar 1 van het Solvency II-akkoord kent twee kernbegrippen voor wat betreft de kapitaalvereisten: de Minimum Capital Requirement (MCR) en de Solvency Capital Requirement (SCR). De MCR kan worden beschouwd als de minimale kapitaalvereiste. De SCR vormt een reëlere inschatting op basis van het risicoprofiel van de verzekeraar. De berekening van de MCR en de SCR wordt binnen pillar 1 opgesplitst in een aantal blokken. Ieder blok vertegenwoordigt een bepaald risicotype. Dit betreft uiteraard het verzekeringsrisico en het marktrisico, maar daarnaast ook kredietrisico en operationeel risico. Operationeel risico valt op, omdat verzekeraars dit risicotype op dit moment nog niet (of slechts beperkt) modelleren voor het aanhouden van kapitaal. In het kader van de beheersing van de IT-aspecten van operationele risico's zal met name aandacht uitgaan naar de entity level controls (geformaliseerde en geïmplementeerde IT-strategie, beleid, planning, informatiebeveiliging et cetera) en IT general controls (waaronder logische toegangsbeveiliging, ▶

Operationeel risico

Operationeel risico is het risico op verliezen door tekortschietende of falende interne procedures, door personeel of systemen of door externe gebeurtenissen. Binnen de definitie van operationeel risico volgens Solvency II vallen de aspecten personeel, processen, systemen en externe gebeurtenissen. Het manifest worden van risico's ten aanzien van deze aspecten kan leiden tot verliezen, een element dat in de draft directive niet verder is uitgewerkt. De verwachting is dat op termijn de definities van Basel II inzake de gebeurtenissen *(events)* die tot verliezen kunnen leiden, worden overgenomen. Daarbij gaat het om de volgende aspecten.

- Interne fraude: verliezen die te wijten zijn aan handelingen om te bedriegen dan wel zaken te onthouden, het onrechtmatig toe-eigenen van goederen en/of zaken, het ontduiken van voorschriften, wetten en interne regelingen, met uitzondering van discriminatie en ongelijke behandeling van ten minste een interne partij.
- Externe fraude: verliezen die te wijten zijn aan handelingen om te bedriegen dan wel zaken te onthouden, het onrechtmatig toe-eigenen van goederen en/of zaken, het ontduiken van voorschriften, wetten en interne regelingen door een derde.
- Werkomstandigheden en veiligheid: verliezen die gebaseerd zijn op activiteiten die niet consistent zijn met de arbeidsvoorwaarden en -omstandigheden of betalingen voor persoonlijke schade, ongelijke of discriminerende gebeurtenissen.
- Claims van cliënten, fouten in producten en ondeugdelijke adviezen: verliezen die ontstaan zijn uit onopzettelijk gemaakte fouten die samenhangen met de nakoming van verplichtingen, zowel vertrouwelijke als logisch daarbij passende eisen, jegens een cliënt of fouten die voortvloeien uit het ontwerp van het product.
- Schade aan fysieke activa: verliezen die voortkomen uit het verloren gaan of de beschadiging van activa op basis van natuurrampen of andere gebeurtenissen.
- Verstoring van de bedrijfsuitvoering en systeemgebreken: verliezen die ontstaan zijn door storingen in businessapparatuur of IT-systemen.
- Uitvoering, levering en procesmanagement: verliezen die voortkomen uit de foutieve verwerking van transacties of foutief management en uit handelspartijen en leveranciers.

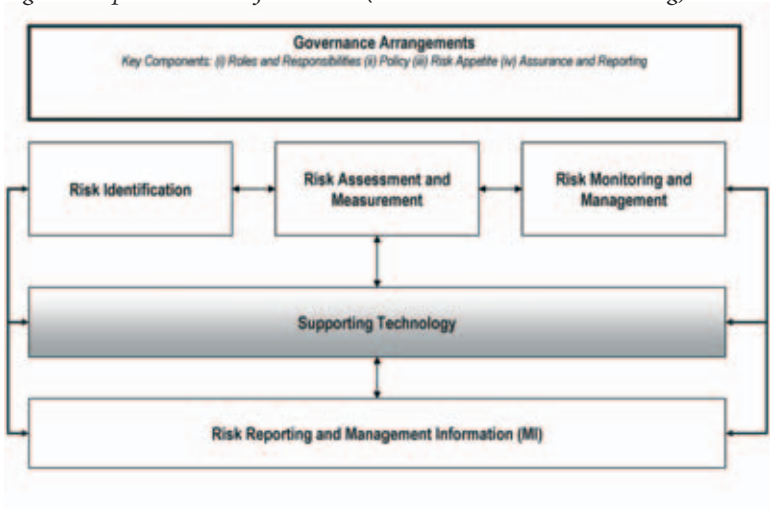
Uitgesloten van deze definitie van operationeel risico zijn de effecten die voortvloeien uit reputatierisico en strategische beslissingen.

change management en continuïteitsaspecten).

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* dat ontwikkeld is op basis van *best practices* (figuur 2) worden gehanteerd.

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

Figuur 2 Operational risk framework (ontwikkeld door Ernst & Young)



- *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 verzekeringsmaatschappij 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 continu 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 invloed 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 de genoemde activiteiten, aan zowel interne als externe belanghebbenden.

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 2 en 3, niet moeten worden onderschat. Daarnaast dienen vanzelfsprekend de (operationele) risico's ten aanzien van het gebruik van IT te worden beheerst, wat de opmaat is voor de behandeling van de andere drie governance-elementen: internal control, internal audit en uitbesteding.

Internal control en internal audit

Solvency II onderkent voor het internal controlsysteem ten minste de volgende onderdelen: administratieve en *accounting* procedures, een internal control framework, adequate rapportagelijnen en een permanente *compliance*functie. Een onafhankelijke internal auditfunctie dient periodiek te evalueren of het internal controlsysteem adequaat is ingericht en heeft gewerkt (draft directive, artikel 45 en 46). Gezien de hoge graad van automatisering bij verzekeraars zal een belangrijk deel van het internal control systeem steunen op IT. Zoals genoemd, zal met name aandacht uitgaan naar de entity level controls en IT general controls. Adequate beheersing van IT is derhalve essentieel.

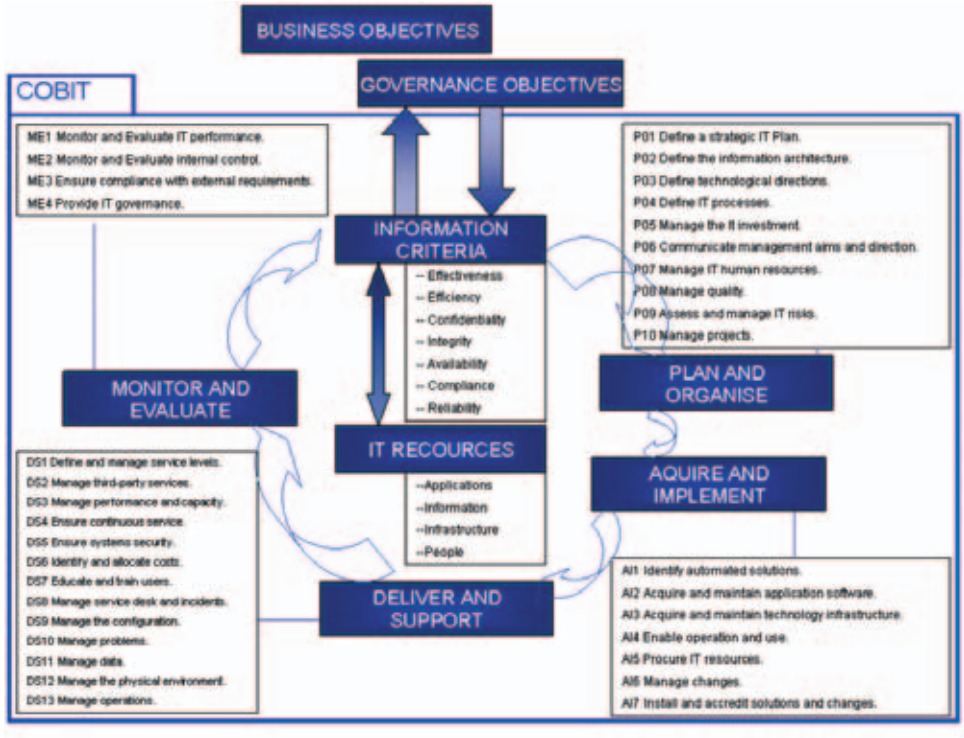
Het hanteren van een op best practices gebaseerde methodiek zoals het CobIT-raamwerk (**C**ontrol **ob**jectives for **I**nformation and related **T**echnology), is daarbij aan te bevelen. CobIT is een internationale *de facto* standaard voor het beheersen van IT. In de huidige, vierde versie van het CobIT-raamwerk worden 318 beheersdoelstellingen onderscheiden, die zijn gerangschikt naar vier beheersdomeinen:

- Plan and Organise;
- Acquire and Implement;
- Deliver and Support;
- Monitor and evaluate.

Figuur 3 geeft het CobIT-raamwerk weer.

Het CobIT-raamwerk kan zowel worden gebruikt voor de inrichting van het IT-gerelateerde deel van het internal controlsysteem, alsook door internal auditfuncties voor het beoordelen van dit systeem.

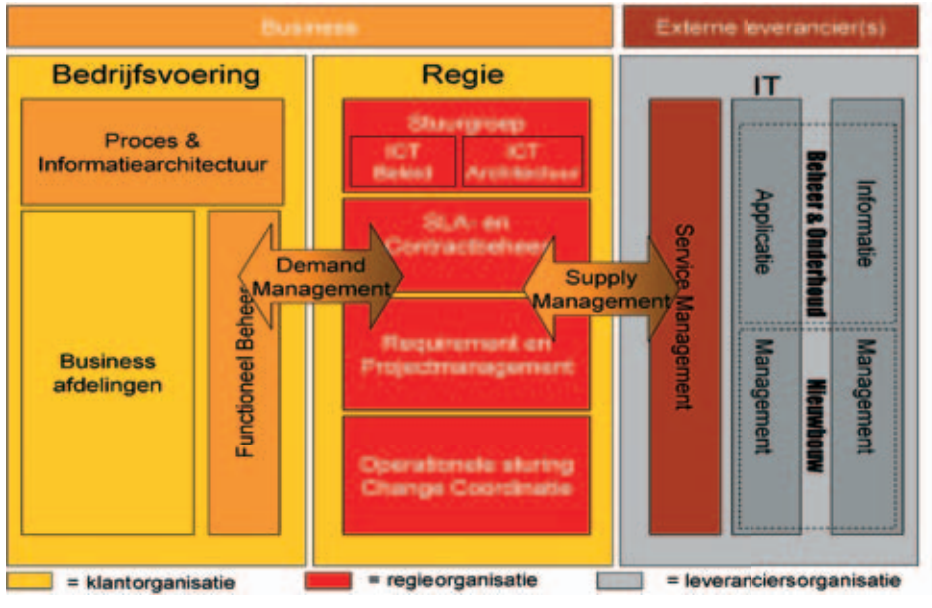
Figuur 3 Het CobIT-raamwerk



Uitbesteding

Het uitbesteden van operationele processen mag niet leiden tot verminderde kwaliteit van het governancesysteem, het substantieel vergroten van de operationele risico's en/of ondermijnen van een continue en adequate service aan polishouders (draft directive, artikel 48). De verzekeringsmaatschappij blijft daarbij altijd verantwoordelijk voor die activiteiten die zij heeft uitbesteed. Uitbesteding van (delen van) de IT-functie en ook operationele processen is tegenwoordig gemeengoed: het zogenaamde *business process outsourcing*. Dit vraagt een sterk sturende rol van de verzekeringsmaatschappij, bijvoorbeeld door middel van een zogenaamde regieorganisatie. Een regieorganisatie is een organisatieonderdeel dat een regiefunctie vervult tussen de vraag vanuit de business en het aanbod vanuit de externe leverancier (figuur 4). Het CobIT-raamwerk schenkt specifiek aandacht aan de beheersing van enerzijds de selectie van uitbestedingpartners (beheersdomein 'AI5 Procure IT recources') en anderzijds het beheersen van de

Figuur 4 Regieorganisatie



dienstverlening door deze externe partij (beheersdomein 'DS2 Manage third party services').

Het recent verschenen *issues paper* over governance[2] geeft een aantal specifieke handvatten ten aanzien van het uitbesteden van activiteiten. Essentieel is daarbij dat een verzekeringsmaatschappij altijd verantwoordelijk blijft voor die activiteiten die zij heeft uitbesteed. Zo is expliciet aangegeven dat een effectief beheersingsraamwerk voor de uitbestede activiteiten bij de externe dienstverlener moet zijn geïmplementeerd, welke ▶

onderdeel uitmaakt van het risk managementsysteem van de verzekeraar. Het is daarbij niet voldoende dat de externe dienstverlener zelf een beheersingsraamwerk en risk managementsysteem heeft geïmplementeerd. Dit betekent dat met inachtneming van figuur 4 een deel van de regieorganisatie van de verzekeraar zich bij de externe dienstverlener zal bevinden.

IT ALS ENABLER

Solvency II heeft grote gevolgen voor het gebruik van gegevens binnen verzekeringsmaatschappijen. Solvency II vereist bijvoorbeeld het gebruik van gegevens uit (legacy-)systemen voor het berekenen van kapitaalvereisten, het interne risk managementsysteem en het vervaardigen van rapportages richting toezichthouders. Daarbij is IT een belangrijke enabler voor het kunnen opleveren en gebruiken van de benodigde gegevens.
Hierna wordt allereerst uiteengezet wat onder Solvency II gaat veranderen aan het berekenen van kapitaalvereisten, het interne risk managementsysteem en het vervaardigen van rapportages richting toezichthouders. Vervolgens wordt behandeld wat de invloed hiervan is op het gebruik van gegevens.

Berekenen kapitaalvereisten

Onder Solvency II is het mogelijk dat een verzekeringsmaatschappij voor het berekenen van haar kapitaalvereisten gebruik maakt van interne risicomodellen. Bij het opstellen en toepassen van interne risicomodellen wordt gebruikgemaakt van gegevens uit diverse onderliggende (legacy-) systemen. Met behulp van de risicomodellen kunnen diverse scenario's worden doorgerekend, risico's van portefeuilles en producten worden bepaald en kan het benodigde kapitaal worden berekend om deze risico's te kunnen absorberen.

Onder Basel II wordt ook een dergelijke werkwijze gevolgd. De inzichten die voortkomen uit historische gegevens en risicomodellen kunnen worden vertaald naar bijvoorbeeld *risk based pricing*: het doorberekenen van risico-opslagen aan klanten. Vanwege de kredietcrisis met de sub prime hypotheken is op deze aanpak forse kritiek geuit. De kern van de zaak is het gebruik van historische interne gegevens voor het voorspellen van toekomstige scenario's en daarbij behorende risico's. Een Europese bank die bijvoorbeeld niet rechtstreeks is getroffen door de gebeurtenissen op 11 september 2001 of de orkaan Katrina, heeft deze schok niet in haar interne historische gegevens en modellen verwerkt. Echter door de mondiale

'Verzekeraars onderschatten de impact van Solvency II'

impact van deze gebeurtenis, heeft dit wel effect gehad op het risicoprofiel van de betreffende bank en haar portefeuille. De verwachting is dat onder Solvency II naast het gebruik van interne gegevens voor het hanteren van interne modellen, tevens gegevens dienen te worden gebruikt uit externe bronnen, wat over het algemeen complex is vanwege bijvoorbeeld andere gegevensformats en -definities die worden gehanteerd.

Verder moet niet uit het oog worden verloren dat het ontwikkelen en gebruiken van een model slechts één element van risicokwantificatie is. In aanvulling hierop dienen scenario's en stress tests te worden uitgevoerd. Hiermee kan worden voorkomen, dat er blind op een model wordt gestuurd, zonder na te denken over bijzondere omstandigheden of mogelijke risico's die niet zijn gemodelleerd. De verwachting is dat hiervoor in de nabije toekomst veel meer aandacht komt.

Risk managementsysteem

Zoals eerder beschreven, vereist Solvency II een adequaat risk managementsysteem. Een onderdeel van dit systeem zijn risk managementrapportages, naast de dagelijkse operationele rapportages. Risk managementrapportages moeten alle belangrijke risicocategorieën omvatten, afgezet tegen de vooraf door de verzekeringsmaatschappij bepaalde risicotoleranties. In aansluiting op de eerder beschreven risicomodellen vereist dit het verzamelen, analyseren en rapporteren van gegevens uit zowel interne als externe bronnen. Dit vindt plaats op zowel kwantitatieve als kwalitatieve wijze. Het verzamelen van gegevens vanuit de diverse organisatieonderdelen en een grote variëteit aan interne en externe systemen brengt datakwaliteitsproblemen met zich mee op bijvoorbeeld het gebied van integriteit en continuïteit van gegevens.

Rapportages toezichthouders

Door de nieuwe Solvency II-regelgeving is de verwachting dat de huidige door DNB gehanteerde verslagstaten komen te vervallen. De verwachting is dat met name de huidige staten Solvabiliteit en Organisatie & Risico's zullen worden vervangen door nieuwe staten. Het merendeel van de informatie uit Solvency II zal echter moeten worden gerapporteerd in het (nieuwe) Financial Conditions Report (FCR). Omdat de Solvency II-regels nog niet definitief zijn, is op dit moment nog onvoldoende duidelijk wat op dit gebied gaat veranderen. De ervaring leert dat toezichthouders op basis van voortschrijdend inzicht (bijvoorbeeld de huidige kredietcrisis!) hun vereisten aan verslagstaten bijstellen, waardoor de rapportagedruk zal toenemen. Ook de doorlooptijd voor het vervaardigen en opleveren van rapportages wordt steeds korter. Dit vereist enerzijds gebruik van andere gegevens dan tot op heden, anderzijds vereist dit een zekere mate van flexibiliteit van de aanleverende (legacy-)systemen alsmede de rapportagesystemen. Vanwege de beperkte flexibiliteit van

(verouderde) legacy-systemen is een in de praktijk veelvuldig gekozen oplossing hiervoor de implementatie van een *datawarehouse*, die wordt gevoed door data uit de onderliggende bronsystemen.

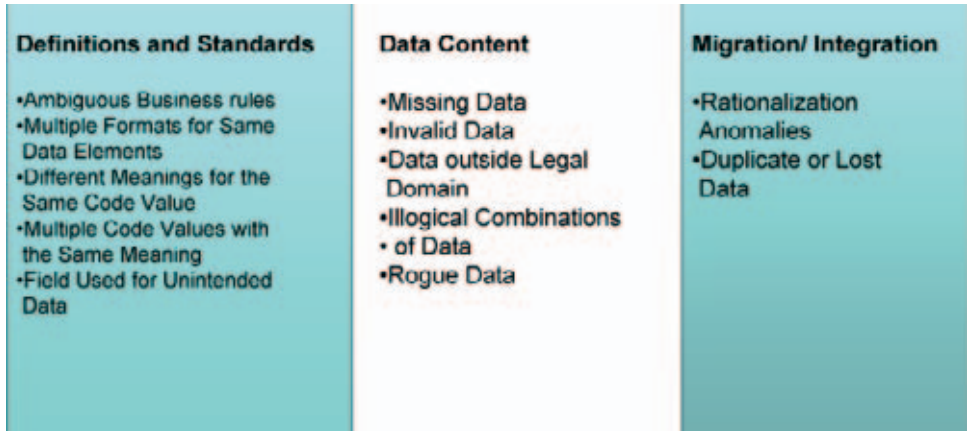
Gebruik gegevens

Vanwege de jarenlange groei van verzekeringsmaatschappijen 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:

- verzekeringsmaatschappijen hebben grote hoeveelheden en soorten gegevens;
- dezelfde gegevens worden in meerdere systemen opgeslagen;
- elk systeem dat gegevens oplevert, kan eigen dataregels en -definities hebben;
- onduidelijk is welke organisatieonderdelen eigenaar zijn van de data en de systemen die deze data bevatten;
- organisatiebreed beleid ten aanzien van data ontbreekt (regels ten aanzien van bewaartermijnen en eigenaarschap).

Het gebruik van een grote verscheidenheid aan gegevens wordt onder Solvency II vergroot door het wijzigen van de wijze 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 Solvency II dan ook meer urgent: er wordt meer inzicht vereist in de dagelijkse operatie van de verzekeringsmaatschappij. Verzekeraars zijn over het algemeen van oudsher met name productgericht georganiseerd, ook de IT-systemen zijn daardoor gericht op het administreren van producten. Solvency II vereist inzicht en rapportages op *holding*niveau (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 (belegging)posities, storingen, fouten et cetera. Vanwege het feit dat de gemiddelde verzekeringsmaatschappij een veelvoud aan administratieve (product)systemen gebruikt per *businessline*, is het relatief complex om een centraal geconsolideerd inzicht te verkrijgen in de dagelijkse operatie van de verzekeraar. Immers, dit inzicht op holdingniveau van de verzekeringsmaatschappij is tot op heden met name gericht op de processen die financiële cijfers opleveren en in veel mindere mate gericht op de processen van de operatie.

Figuur 5 Veelvoorkomende problemen ten aanzien van datakwaliteit



Het voorgaande wordt versterkt door het feit dat binnen verzekeringsmaatschappijen onderscheid wordt gemaakt tussen *exposure data* (gegevens betreffende polishouder en het onderliggende contract), *risico data* (financiële gegevens betreffende markt- en kredietrisico's en verzekeringstechnische gegevens zoals sterfteresultaten en -claims) en *reporting data* (gegevens benodigd voor rapportages richting interne en externe toezichthouders). Voor het vastleggen, bewerken en bewaren van deze data worden vaak separate IT-systemen gebruikt. Solvency II verenigt echter het gebruik van alle soorten data, wat relatief complex is door deze beperkte mate van integratie van IT-systemen, maar ook vanwege het risico van beperkte kwaliteit van data: door bijvoorbeeld datavervuiling kunnen rapportages onbetrouwbare resultaten opleveren. De volgende aspecten bepalen de kwaliteit van data:

- Integriteit: de mate waarin de weergegeven data in overeenstemming is met de werkelijkheid. Dit omvat elementen als juistheid, volledigheid en tijdigheid. Dit vereist eenduidige datadefinities en technische informatie over dataformats en waar deze data is opgeslagen (de zogenaamde data over data: metadata).
- Exclusiviteit: de mate waarin uitsluitend geautoriseerde personen en systemen toegang hebben tot en gebruikmaken van bepaalde dataelementen. Dit vereist strikte logische en fysieke toegangsbeveiligingsprocessen en procedures. Tevens dient daarbij het eigenaarschap van gegevens in de organisatie te zijn belegd.
- Controleerbaarheid: de mate waarin het (achteraf) is vast te stellen dat de integriteit en exclusiviteit van gegevens gewaarborgd is en blijft. Ervaringen uit de praktijk leren dat dit onderwerp als lastig wordt ervaren. Met name de administratieve lasten in de vorm van het vastleggen en accorderen van toegang tot gegevens zullen hierdoor toenemen.
- Continuïteit: de mate waarin de data beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben. Hierbij moet worden gedacht aan zaken als *back-up* en *recovery* en uitwijkmogelijkheden.

Internal auditfunctie

De draft directive geeft de functie en activiteiten van de internal auditfunctie aan. In artikel 46 staat daaromtrent het volgende aangegeven:

Internal Audit

1. Insurance and reinsurance undertakings shall provide for an effective and permanent internal audit function.
2. The internal audit function shall include the examination of the compliance of the activities of an insurance and reinsurance undertaking with all its internal strategies, processes and reporting procedures.
3. The internal audit function shall also include an evaluation of whether the internal control system of the undertaking remains sufficient and appropriate for its business.
4. The internal audit function shall be objective and independent from the operational functions.
5. Any findings and recommendations of the internal audit shall be reported to the administrative or management body which shall ensure compliance with the internal audit findings and recommendations.

Het internal controlsysteem kent ten minste administratieve en accounting procedures, een internal control framework, adequate rapportagelijnen en een permanente compliancefunctie. Een onafhankelijke internal auditfunctie dient periodiek te evalueren of het internal controlsysteem adequaat is ingericht en heeft gewerkt. Gezien de hoge graad van automatisering zal een belangrijk deel van het internal controlsysteem steunen op IT. Adequate beheersing van IT is derhalve essentieel.

Niet alleen technische uitwijk verdient daarbij de aandacht, maar met name ook businessuitwijk: waar gaan de mensen naar toe die verantwoordelijk zijn voor bijvoorbeeld het samenstellen van rapportages?

Uit internationaal onderzoek (uitgevoerd door Ernst & Young) blijkt er een aantal veelvoorkomende issues te zijn ten aanzien van datakwaliteit. Deze zijn in figuur 5 weergegeven.

In het algemeen genomen, kunnen vier categorieën worden onderkend ten aanzien van het gebruik van gegevens. Deze categorieën zijn weergegeven in figuur 6.

1. Data: het gebruik van gegevens als basis om in een informatiebehoefte te voorzien. Centraal hierbij staat het op adequate wijze beheren van gegevens, zodat de integriteit en betrouwbaarheid van gegevens aantoonbaar is gewaarborgd.
2. Informatie: gegevens met elkaar in verband brengen teneinde verklaringen te vinden voor gebeurtenissen die reeds hebben plaatsgevonden (beschrijvende data-analyse)
3. Kennis: het gebruik van gegevens voor modellen en validatie van modellen, zodat een verklaring kan worden gevonden waarom gebeurtenissen zich hebben voorgedaan.
4. *Business intelligence:* gegevens gebruiken voor voorspellende modellen om een antwoord te geven op de vraag wat er in de (nabije) toekomst zal gebeuren.

In de praktijk blijkt dat op dit moment met name aandacht uitgaat naar categorie 1 (data) en categorie 2 (informatie). Voor menig verzekeraar zit daar al voldoende uitdaging om zaken goed te laten verlopen. Solvency II vereist echter voornamelijk het gebruik van gegevens in categorie 4 (business intelligence). Hierbij moet worden vooropgesteld dat om business intelligence te kunnen uitvoeren, alle onderliggende categorieën ook op adequate wijze moeten worden uitgevoerd. Voorwaar een uitdaging voor veel verzekeringsmaatschappijen! De verwachting is dat datakwaliteit de komende jaren een belangrijk onderwerp is voor verzekeringsmaatschappijen, overigens niet alleen gedreven door Solvency II, maar ook vanwege de operationele sturing van de organisatie.

Om kwaliteit van data te adresseren is een gestructureerde organisatiebrede aanpak noodzakelijk. De eerste stap van deze aanpak bestaat uit het met een datakwaliteitsprogramma. Dit programma kan bestaan uit de volgende drie onderdelen.

1. *Assess:* analyseren van de huidige in- en externe (legacy-)systemen en de data die daarin beschikbaar is. Daarnaast moet de verzekeraar bepalen wat de businessvereisten zijn ten aanzien van data (informatiebehoefte). Daarbij dient zoveel mogelijk rekening gehouden te worden met Solvency II.
2. *Improve:* op basis van de analyse uit de vorige fase bepalen welke dataelementen kunnen worden gegroepeerd en welke data dient te worden opgeschoond. Belangrijk onderdeel hierbij is het hanteren van eenduidige datadefinities en formats in een bedrijfsbreed datamodel (metadata). Hierbij worden datawarehouse oplossingen gehanteerd, welke een sterke organisatorische aansturing vereisen in verband met bijvoorbeeld eigenaarschap van data (data governance organisation).
3. *Monitor:* het op continue basis monitoren van de datastromen, om de integriteit, exclusiviteit, controleerbaarheid en continuïteit van de gegevens en datastromen te waarborgen.

ROL IT-AUDITOR

Een gekwalificeerde IT-auditor geeft onpartijdige oordelen en adviezen over de kwaliteitsaspecten van IT. Een bredere definitie is dat de IT-auditor betrokken is bij het beoordelen van en adviseren over de inzet van IT binnen organisaties. Over het algemeen genomen kan de (interne en externe) IT-auditor ten aanzien van Solvency II optreden vanuit een attestfunctie of vanuit een adviserende functie.

De *attest*functie van de IT-auditor houdt in het geven van een onafhankelijk en onpartijdig oordeel over de mate waarin één of meer (bestaande dan wel toekomstige) objecten uit de IT voldoen aan de in de opdracht overeengekomen kwaliteitsaspecten. Daarnaast wordt van de IT-auditor verwacht dat hij niet alleen een oordeel weet te geven omtrent IT-objecten, maar ook in staat is om, mede op basis van zijn werkzaamheden, adviezen te geven ter opheffing van geconstateerde gebreken, zowel gevraagd als ongevraagd (natuurlijke adviesfunctie).

De adviesfunctie van de IT-auditor behelst het doen van aanbevelingen respectievelijk het geven van advies op het deskundigheidsgebied van de IT-auditor (dat is ontleend aan zijn

kennis en ervaring op het gebied van IT). Het essentiële verschil ten opzichte van de attestfunctie zit in het doel van de adviesfunctie, te weten het doen van voorstellen voor het creëren van nieuwe (toekomstige) situaties. Daarnaast verwacht het management dat de IT-auditor zich in deze functie vereenzelvigt met zijn advies en het welslagen van zijn advies in de praktijk.

Figuur 6 Data: de vier kernvragen

Gezien de complexiteit en de organisatorische impact van Solvency II voor verzekeringsmaatschappijen, met name ook op het gebied van IT, heeft het naar mijn mening sterk de voorkeur dat de IT-auditor vanaf de start van een Solvency II-implementatie is betrokken. Niet alleen een beoordeling achteraf (attestfunctie), maar ook een actieve betrokkenheid van de IT-auditor tijdens het project als adviseur of bewaker van de kwaliteit van opgeleverde producten (adviesfunctie).

Figuur 7 Datakwaliteitsprogramma: Assess, Improve en Monitor

De IT-auditor is bij uitstek de onafhankelijke deskundige op het gebied van IT. Met name voor het onderdeel waarbij IT als enabler fungeert: de voor interne modellering benodigde infrastructuren, het ontsluiten van gegevens uit bronsystemen en datawarehousing behoren tot het deskundigheidsgebied van de IT-auditor. Noodzakelijke Solvency II-kennis is daarbij niet a priori aanwezig. Dit betekent dat de IT-auditor zich zal moeten verdiepen in de Solvency II-regelgeving om een goede sparringpartner te kunnen zijn van projectbetrokkenen, zoals actuarissen. Daarnaast is mijn ervaring dat advisering en beoordeling op het kennisgebied IT-governance niet voor iedere IT-auditor is weggelegd. Om op directieniveau over deze materie te kunnen meepraten en adviseren zijn naast inhoudelijke kennis met name meer adviesgerichte vaardigheden noodzakelijk. Daar waar mogelijk zal de (interne) IT-auditor zich dan ook moeten laten opleiden dan wel laten ondersteunen of vervangen door (externe) IT-auditors met de juiste kennis en vaardigheden.

TOT SLOT

Door verzekeringsmaatschappijen in Nederland wordt op dit moment onderkend dat Solvency II gevolgen heeft voor de berekeningswijze van kapitaalvereisten, echter de impact van de aanvullende eisen die Solvency II met zich meebrengt voor met name IT worden over het algemeen onderschat. De invoering van Basel II heeft geleerd dat de inspanningen die nodig zijn om te voldoen aan de regelgeving in de praktijk groter zijn dan aanvankelijk werd verwacht. In de bancaire sector is hiervoor inmiddels leergeld betaald. De invoering van Solvency II in 2012 lijkt ver weg, maar dat is het gezien de benodigde inspanningen niet. Voor de verzekeringsbranche is het zaak nu te starten om hier in een later stadium de vruchten van te plukken. ■

Drs. A.J. (Age-Jan) van der Meer RE RO is senior manager bij Ernst & Young Advisory en heeft meer dan tien jaar ervaring in de IT. Vanwege zijn achtergrond als bedrijfskundige is hij gespecialiseerd in vraagstukken op het snijvlak business en IT in het algemeen en *risk management* in het bijzonder. Hij adviseert organisaties in met name de financiële sector onder andere op het gebied van Bazel II en Solvency II, alsmede risicomanagement in het algemeen. Dit artikel is op persoonlijke titel geschreven en bevat niet noodzakelijkerwijs het standpunt van Ernst & Young.

Noten

1 Ernst & Young Technology & Security Risk Services, 2008.

2 CEIOPS Issues paper, implementing measures on system of governance, 3 november 2008.