RISK MANAGEMENT: HOE WEND- EN WEERBAAR IS UW PENSIOENFONDS?

Door Harry Geels

KAS BANK organiseerde dit jaar al twee Ronde Tafels over Risk Management. Het doel hiervan: pensioenfondsen laten nadenken over hun verandervermogen in een omgeving met een toenemende focus op risico. De drie invalshoeken van waaruit dit onderwerp belicht werd, waren uitbesteding, het pensioenfonds en de accountant. Financial Investigator was aanwezig bij de meest recente Ronde Tafel en doet verslag van de discussie.

'Het grootste risico is het niet-nemen van risico's', zo opende Mark Stoffels, Member Managing Board, CFRO bij KAS BANK, de Ronde Tafel over Risk Management. Daarmee zette hij meteen de toon voor een interessante discussie over het veelbesproken onderwerp risicomanagement, dat hoog op de agenda bij de toezichthouders staat. Bij uitbesteding is risicomanagement cruciaal. Hoe houdt een organisatie die uitbesteedt controle over de processen? Hoe worden de verschillende relevante risico's gemanaged? Het is dan ook niet voor niets dat KAS BANK, als een belangrijke Europese specialist voor de bewaarneming en administratie van effecten en risico- en rapportagediensten voor pensioenfondsen, het onderwerp risicomanagement in een discussie met verschillende partijen, zoals accountants en pensioenfondsen, ter sprake brengt. 'Bij uitbestedingsprocessen als bewaarneming en administratie draait het vooral om vertrouwen', zo stelde Stoffels. Frank Lürling, Managing Director Compliance & NFRM van KAS BANK, begon zijn presentatie met een analogie. 'Stel dat de klant in een taxi stapt: wat heeft hij nodig om veilig op de plek van bestemming te komen? Moet hij de motorkap openmaken en het dashboard inspecteren? Of moet hij checken of de taxichauffeur werkt voor een gerenommeerd taxibedrijf, waar de vergunning is afgegeven door de relevante toezichthouder en een assurance op de bedrijfsvoering is afgegeven door de accountant?' Lürling richtte zich bij deze vragen rechtstreeks tot de aanwezige pensioenfondsen. DNB verwacht namelijk van pensioenfondsen dat ze antwoorden op deze vragen klaar hebben. Hij sprak van drie niveaus waarop over de uitbesteding kan worden gerapporteerd: dagelijkse rapportages, SLA/SLR's en assurance van de accountant. Een van de pensioenfondsen noemde incidentenrapportage als een van de middelen om gevoel te krijgen bij de uitbesteding: 'Werkt het zoals het moet werken en als dat even niet zo was, wat is er dan gedaan om het op te lossen?' Een andere deelnemer aan de ronde tafel meende eveneens dat de discussie over de incidenten open en eerlijk moet zijn, maar dat niet iedere organisatie zo open en eerlijk over zijn incidenten rapporteert. De vraag is, zo stelde Stoffels, met welke informatie de klant uiteindelijk geholpen is. Overkill helpt de klant en de organisatie waaraan is uitbesteed niet. Een deelnemer merkte op dat 'als alles wat van de wagen valt moet worden gerapporteerd een onwerkbare situatie ontstaat. Het gaat om de juiste aard en hoeveelheid'. Er werd ook opgemerkt dat er een ontwikkeling is in SLA/SLR's (Service Level Agreements/ Service Level Requirements). Nog niet zo heel lang geleden werden SLA's gemaakt, opgeslagen en nooit ingezien, tenzij bij een juridisch conflict. 'Tegenwoordig vormen SLA's steeds meer een onderdeel van het in control raken van de uitbesteding.'

Lürling bracht de Systematische Integriteits Risico Analyse (SIRA) in als een aanpak die KAS BANK gebruikt om de risico's te beheersen. In de SIRA zitten vier fasen: risico-identificatie,

risicoanalyse, risicobeheersing en risicomonitoring en -herziening. Bij het identificeren van risico's gaat het erom risico's op geaggregeerd niveau te benoemen en vervolgens uit te splitsen, bijvoorbeeld naar regio's, typen klanten, producten, diensten en interne afdelingen. Zo kan een risico als cybercrime zich toespitsen op applicaties, regio's, klanten, IT-systemen, producten of specifieke projecten. Het advies: schrijf het scenario voor al deze combinaties uit. In de analysefase komen de kansberekening, impact, tegenmaatregelen en mogelijke effectiviteit daarvan aan bod. Als er zich dan daadwerkelijk een risico voordoet, moeten de voorgeschreven beheersingsmaatregelen toegepast worden en in de laatste fase moet de effectiviteit hiervan in de praktijk beoordeeld worden.

John de Waal, Senior Director Finance & Risk Management van Ahold Pensioenfonds, voegde aan de discussie toe dat risicomanagement niet alleen gemanaged moet worden door de risicomanager, maar door de verschillende lagen in de organisatie. Het moet ook gedragen worden door het bestuur. Hij sprak van de 'three lines of defense': eerstelijnsmanagement, de risicomanager en de onafhankelijke beoordeling door de accountant. Het verantwoordelijke management (eerste lijn) is primair verantwoordelijk voor de identificatie van de risico's en de beheersing ervan. Operationele risico's zijn in de loop der tijd bij Ahold volledig opnieuw benoemd met en onder verantwoordelijkheid van de eerste lijn. Het Ahold Pensioenfonds heeft daarbij de transformatie van een statistisch naar een dynamisch risicomanagement doorgemaakt, dat nu de noemer Integrated Risk Management (IRM) heeft gekregen. Hierin komen natuurlijk de benoeming van de risico's, mogelijke scenario's en beheersmaatregelen tot uiting, maar ook de veranderingen in operationele risico's, externe invloeden en eisen van de toezichthouder, beleidsbesluiten en incidenten. 'In de bestuursvergadering staat risicomanagement tegenwoordig vaker op de agenda.' Ahold heeft ter ondersteuning van risicomanagement gekozen voor Cerrix: 'Een mooie tool om risico's en beheersmaatregelen en dergelijke inzichtelijk te maken.' Een deelnemer vroeg of een dergelijke 'tool' echt nodig was. De Waal meent van wel: 'Als alle risico's en beheersmaatregelen volledig in het systeem worden vastgelegd, ontstaat een overzichtelijk dashboard. Voor het goed vastleggen van de uitvoering van beheersmaatregelen en het monitoren hiervan is een dergelijke tool onmisbaar. Het is dan wel zaak dat alle relevante personen ermee gaan werken. Het moet ook niet te ingewikkeld worden, want anders wordt het vastleggen in de tool een doel op zich en gaat er te veel tijd in zitten.'

Tot slot is er het belang van de 'third line of defense'. Jaap van Beek, partner bij KPMG, neemt de deelnemers mee in de reis die een aantal grote pensioenfondsen het afgelopen jaar heeft gemaakt. Traditioneel wordt gewerkt met een assurancerapport onder de ISAE3402 standaard. Als gevolg van wijzigingen in wet- en regelgeving is er behoefte bij pensioenfondsen aan assurance over een bredere set van onderwerpen. Bijvoorbeeld aan meer aandacht voor zaken als fraude, bescherming persoonsgegevens, cybercrime en IT-beveiliging. De ISAE3402 is daar niet voor bedoeld. 'Niet alles past in die standaard en de bevindingen worden in de context van de jaarrekening gewogen', zo stelde hij. De gevraagde assurance is veel meer gericht op operationele processen. Van Beek verwees daarbij onder andere naar de DNB Guidance uitbesteding pensioenfondsen. Gelukkig blijken deze onderwerpen prima te passen onder de ISAE3000 assurance standaard. Dit jaar zijn er voor het eerst door een aantal pensioenuitvoerders gecombineerde ISAE3402 en 3000 rapporten uitgebracht die een flinke stap in de goede richting zijn. De boodschap van Van Beek is dat, gezien die veranderingen, de assurance mee moet bewegen, maar het liefst zonder dat er alleen maar controls worden toegevoegd. 'Niet meer maar beter'. Het gaat uiteindelijk om een goede dialoog en vertrouwen tussen de accountant en het pensioenfonds, waarbij het hanteren van trust rules belangrijk is. Ter illustratie noemde hij het doorlopend melden van bijvoorbeeld incidenten. 'Het niet tijdig melden van incidenten geeft later veel schade, omdat het vertrouwen in de dialoog wegvalt en een tijdig herstel van problemen lastiger wordt.'«

Foto: Archief KAS BANK

Van links naar rechts: Frank Lürling, John de Waal, Mark Stoffels en Jaap van Beek.