Modern pensioenfonds, moderne informatiebeveiliging

Drs. E.P. Rutkens RE en drs. P.C.J. van Toledo RE RA

Door het gebruik van internet en intranet voor de communicatie en verwerking van gegevens worden pensioenfondsen steeds afhankelijker van ICT. Daardoor ontstaan meer risico's op het gebied van informatiebeveiliging. Toezichthouder en pensioenfondsen zijn zich daarvan meer en meer bewust en onderzoeken de mogelijkheden om informatiebeveiliging op het gewenste niveau te krijgen en te houden.

Inleiding

Nederlandse bedrijven hebben hun informatiebeveiliging niet op orde, bleek in 2004 opnieuw door een onderzoek van het tv-programma Zembla. Bovendien heeft een groot deel van de computergebruikers last van internetmisbruik. Het thema informatiebeveiliging vraagt dan ook onverminderd om aandacht. Dat geldt ook in de pensioenwereld, waar informatieverstrekking en gegevensaanlevering via internet en/of intranet inmiddels gemeengoed is geworden. Toezichthouders zijn zich bewust van de risico's op dit gebied en hebben hun toezichtmodel hierop aangepast. Ook is een groot aantal pensioenfondsen en pensioenuitvoerders gestart met een informatiebeveiligingsproject.

Drs. E.P. Rutkens RE
is werkzaam als manager bij KPMG Information Risk Management. Hij houdt zich bezig met de dienstverlening van KPMG met betrekking tot Information Security. Verder is hij betrokken bij de ontwikkeling van producten op dit gebied, waaronder beveiligingsarchitecturen en risicoanalyse.

rutkens.erik@kpmg.nl

Drs. P.C.J. van Toledo RE RA
is werkzaam als senior manager bij KPMG Information Risk Management. Hij heeft zich gespecialiseerd in en is medeverantwoordelijk voor de dienstverlening aan pensioenfondsen en verzekeringsmaatschappijen.

vantoledo.peter@kpmg.nl

De groeiende noodzaak van informatiebeveiliging

Het wordt voor pensioenfondsen om meerdere redenen steeds belangrijker om te investeren in goede informatiebeveiliging.

Ten eerste vragen maatschappij, nieuwe wetten en toezichthouders nadrukkelijk om meer aandacht voor risicomanagement en informatiebeveiliging. De boekhoudaffaires laten hun sporen na in de financiële sector en hebben bijgedragen aan een aantal ontwikkelingen. Zo heeft De Nederlandsche Bank (DNB) de Methode voor de Analyse van Risico's (MARS) geïntroduceerd. Met deze methode inventariseert zij voor negen risicogebieden de inherente risico's van de instelling en de daarbijbehorende beheersingsmaatregelen. Eén van de risicogebieden is ICT. DNB heeft in september 2004 vragenlijsten gestuurd aan grotere pensioenfondsen en verzekeringsmaatschappijen, en heeft op beperkte schaal ook ICT-scans uitgevoerd, die zich onder meer richtten op informatiebeveiliging.

De verwachting is dat de fusie tussen De Nederlandsche Bank (DNB) en de PVK zal leiden tot adequater toezicht door het gebruik van uniforme onderzoekssystematiek en -rapportage. Momenteel wordt onderzocht in hoeverre dit toezichtmodel ook kan worden gehanteerd voor pensioenfondsen en verzekeringsmaatschappijen. De Regeling Organisatie en Beheersing (ROB) zal waarschijnlijk ook voor hen gaan gelden. Deze regeling spitst zich toe op de elementen risicobeheersing, organisatorische maatregelen, informatie en communicatie en toetsing, beoordeling en bijstelling.

Pensioenfondsen vragen in het kader van uitbesteding steeds vaker om SAS 70-verklaringen

DNB heeft de Beleidsregels uitbesteding[1] (outsourcing) opgesteld. Veel pensioenfondsen besteden (delen van) back-office- en ICT-activiteiten uit aan derden. De beleidsregel moet waarborgen dat er ook op deze uitbestede processen voldoende toezicht is. Pensioenfondsen moeten zorgen dat zij de risico's die samenhangen met uitbesteding grondig analyseren en adequaat beheersen. Pensioenfondsen vragen in dit kader steeds vaker om SAS 70-verklaringen. Met deze internationale auditstandaard van het American Institute of Certified Public Accountants (AICPA) voor serviceorganisaties verkrijgen zij zekerheid over de kwaliteit van de uitbestede werkzaamheden. SAS 70 omvat ook aspecten ten aanzien van informatiebeveiliging.

De commissie-Peters heeft in 1997 'Aanbevelingen inzake Corporate Governance in Nederland' gepubliceerd. De commissie heeft veertig aanbevelingen voor goed bestuur, adequaat toezicht en het afleggen van verantwoording opgesteld. Twee van deze veertig aanbevelingen hebben betrekking op risico's ofwel risicomanagement. De Code-Tabaksblat (2003) borduurt hierop voort en verplicht beursgenoteerde ondernemingen in Nederland te rapporteren over de werking van het risicobeheersings- en controlesysteem.

In wet- en regelgeving komt steeds meer aandacht voor informatiebeveiliging. Zo stelt de Wet bescherming persoonsgegevens (Wbp) normen voor een behoorlijke en

1) Onder uitbesteden wordt verstaan: het laten verrichten van instellingsactiviteiten door derden.

Pensioenfondsen krijgen straks te maken met een Pension Fund Governance-code. De hoofdlijnen daarvan zijn nu al duidelijk en pensioenfondsen moeten daarop inspelen door nu hun huis op orde te maken:

- *Zorg dragen voor onafhankelijk toezicht*. Het bestuur moet verantwoording kunnen afleggen aan een intern toezichtorgaan. Als het pensioenfonds bepaalde taken heeft uitbesteed, dient ook hierover verantwoording te worden afgelegd. Dit kan door middel van heldere SLA-rapportages van de uitvoerder aan het bestuur. Een SAS 70-verklaring van de uitvoerder kan daarnaast aantonen (ook aan de toezichthouder) dat de uitvoerder zijn processen beheerst.
- *Deskundigheid en integriteit van het bestuur*. Pensioenfondsen moeten een eigen interpretatie van de Pension Fund Governance-code (in de vorm van bijvoorbeeld een gedragscode) opstellen. Daarbij hoort een deskundigheidsplan, waarmee kan worden aangetoond dat wordt voldaan aan deskundigheidseisen. Ook kan het aanstellen van een compliance officer nodig zijn. Deze ziet onder meer toe op de naleving van de code en het voldoen aan de integriteitseisen.
- *Scheiding beleid en uitvoering*. Pensioenfondsen moeten een heldere scheiding aanbrengen tussen beleid en uitvoering van de pensioenregeling. In geval van uitbesteding moeten de taken, verantwoordelijkheden en bevoegdheden eenduidig worden verdeeld tussen het bestuur en de uitvoerder. Het bestuur is verantwoordelijk voor het beleid, de uitvoerder houdt zich bezig met de uitvoering en het afleggen van verantwoording daarover. Toezichthoudende taken horen niet tot de taken van beleidsmakers of uitvoerders, maar moeten door een onafhankelijk orgaan worden verricht.
- *Openheid en transparantie in verantwoording naar belanghebbenden*. Voor zowel het bestuur als de uitvoerder geldt dat zij op een open en transparante manier verantwoording moeten afleggen over het gevoerde beleid. Hulpmiddelen hierbij zijn een heldere SLA en een SAS 70-verklaring. Duidelijke communicatie naar alle belanghebbenden is belangrijk. Het bestuur kan daarvoor een communicatieplan maken, waarin helder wordt uiteengezet hoe invulling wordt gegeven aan de communicatie met alle belanghebbenden.
- *Medezeggenschap door belanghebbenden*. Pensioenfondsen moeten het bestuur op een juiste manier vormgeven. Afhankelijk van de specifieke situatie van het fonds kan het bestuur ervoor kiezen om alle belanghebbenden te laten vertegenwoordigen in het bestuur. Het bestuur kan daarnaast kiezen voor het inrichten van een deelnemersraad of college van belanghebbenden. Essentieel voor goede medezeggenschap is dat een dergelijk orgaan ook voldoende instemmings- en adviesrechten krijgt. Hierbij valt te denken aan het laten goedkeuren van de jaarrekening door de deelnemersraad of het college van belanghebbenden en hiermee decharge te verlenen aan het bestuur.

Kader 1. Hoofdlijnen van Pension Fund Governance.

zorgvuldige verwerking van persoonsgegevens (bijvoorbeeld gegevens van deelnemers). De wet vereist dat organisaties passende organisatorische en technische maatregelen treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

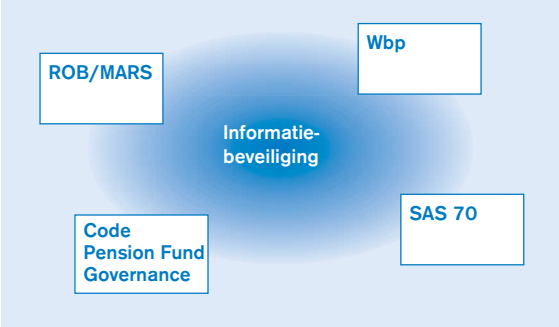
Ten tweede zijn pensioenfondsen steeds afhankelijker van ICT en integreren processen steeds verder. Pensioenfondsen automatiseren de gegevensuitwisseling in rap tempo. Daarmee bereiken ze een hogere efficiency en kunnen ze tevens een hoge servicegraad bieden aan deelnemers. Hierbij valt onder meer te denken aan pensioenplanners met mutatiefunctionaliteiten, de opkomst van zogenaamde HR-portals en de periodieke aanlevering van mutaties in werknemersgegevens door werkgevers. Sommige pensioenfondsen willen 7*24 uur in staat zijn informatie te verstrekken aan hun deelnemers. Verschillende applicaties moeten naadloos integreren en back-officesystemen moeten een flexibele architectuur hebben om aan de nieuwe eisen te voldoen.

Door deze ontwikkelingen worden pensioenfondsen afhankelijker van een betrouwbare werking van ICT. Die betrouwbaarheid is ook belangrijk vanuit imago- en privacyoverwegingen. Maatregelen op het gebied van betrouwbaarheid en beveiliging zijn veel omvangrijker geworden en vragen om een gestructureerde aanpak.

Ten derde vragen opkomende technologische ontwikkelingen aandacht voor informatiebeveiliging. Pensioenfondsen die internet als communicatiemedium gebruiken staan in toenemende mate bloot aan allerlei bedreigingen die samenhangen met gebreken in de beveiliging van informatiesystemen. De snel voortschrijdende technologische ontwikkelingen en de onbegrensde omgeving waarin de bedreigingen zich kunnen manifesteren spelen hierbij een belangrijke rol. Het gebruik van internet brengt bijvoorbeeld bedreigingen met zich mee ten aanzien van virusaanvallen[2] en zogenaamde Denial-of-Service aanvallen[3].

Beheersing van risico's ten aanzien van informatiebeveiliging

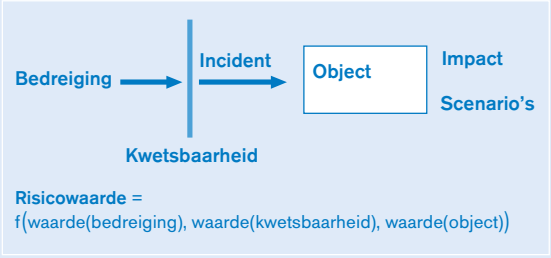
Veel pensioenfondsen worstelen met de vraag hoe zij een toetsbaar, efficiënt en effectief stelsel van maatregelen kunnen opzetten, dat is gebaseerd op risicoanalyse, en voldoet aan eisen van toezichthouders. Figuur 1 laat zien dat een adequaat niveau van informatiebeveiliging niet alleen essentieel is om bedrijfsrisico's te beheersen, maar ook kan bijdragen om te voldoen aan wettelijke en maatschappelijke eisen.
Veel organisaties gebruiken de Code voor Informatiebeveiliging (ISO 17799) als basis voor het opzetten van hun informatiebeveiliging. De Code is ontwikkeld door een groot aantal vooraanstaande ondernemingen en overheidsorganisaties en is in 1994 voor het eerst in Nederland uitgebracht door het Ministerie van Economische Zaken en het Nederlands Normalisatie-Instituut. ISO 17799 kan ook pensioenfondsen helpen om op efficiënte en effectieve wijze een beveiligingsniveau te bereiken dat aan de voor hen relevante eisen voldoet.



Figuur 1. Informatiebeveiliging kan een bijdrage leveren om te voldoen aan wet- en regelgeving.

Om dat te realiseren zijn de volgende processtappen nodig:
- *Bepalen van de gewenste situatie:* met behulp van een systematische en eenvoudige risicoanalyse de minimaal noodzakelijke maatregelen uit de Code voor Informatiebeveiliging bepalen om tot een acceptabel risiconiveau te komen (zie kader 2).
- *Beleid opstellen:* op basis van het globale risicoprofiel en de bedrijfsdoelstelling een beveiligingsbeleid opstellen. Het beleid geeft een kader aan waarbinnen maatregelen kunnen worden ingevoerd en/of verbeterd. Dit kader wordt gevormd door de uitgangspunten van beleid en de inrichting van de beveiligingsorganisatie.
- *In kaart brengen huidige situatie:* onderzoeken in hoeverre het huidige stelsel beveiligingsmaatregelen voldoet aan de gewenste situatie. Dit resulteert in een overzicht van mogelijk te treffen of te verbeteren maatregelen. Per maatregel dient te worden aangegeven welke maatregel een hoge prioriteit heeft (op basis van het gepercipieerde risico en de kosten om de maatregel te realiseren) en welke maatregel minder urgent is.
- *Opstellen van een beveiligingsplan:* vaststellen hoe beveiligingsmaatregelen kunnen worden ontwikkeld en geïmplementeerd. Het beveiligingsplan omvat ten minste een beschrijving van de te verrichten werkzaamheden, doorlooptijden, benodigde capaciteit en de projectorganisatie. Het plan kan onderscheid maken tussen maatregelen die met weinig inspanning snel te realiseren zijn (de 'quick wins') en de maatregelen die meer tijd zullen vergen ('slow gains').
- *Ontwikkeling en implementatie van beveiligingsmaatregelen:* de te treffen of te verbeteren organisatorische en technische maatregelen op basis van het beveiligingsplan ontwikkelen en implementeren.
- *Monitoren en testen:* het inrichten van een proces waarmee continu de effectiviteit van de geïmplementeerde beveiligingsmaatregelen wordt gecontroleerd en waarmee mogelijke kwetsbaarheden worden ontdekt.
- *Bijsturen:* het nemen van correctieve en preventieve maatregelen, gebaseerd op de resultaten uit de vorige fase, om het niveau van informatiebeveiliging continu te verbeteren.

2) Virussen zijn programma's die zich onopgemerkt verspreiden en schadelijke handelingen kunnen verrichten.
3) Bij een Denial-of-Service-aanval wordt een computersysteem overladen met verzoeken tot informatie waardoor het buiten werking wordt gesteld, aangezien het systeem deze grote hoeveelheid verzoeken niet kan verwerken.



Figuur 2.CRAMM.

Voor de inventarisatie van risico's en de afweging van de invoering van beveiligingsmaatregelen met betrekking tot kosten en baten van deze maatregelen, zijn verschillende risicoanalysemethoden beschikbaar. Figuur 2 geeft het risicomodel weer zoals dat in de aanpak van CRAMM wordt gehanteerd. CRAMM staat voor CCTA Risk Analysis Management Method en is door CCTA (Central Computer and Telecommunications Agency) in Engeland ontwikkeld. CRAMM wordt ondersteund door een softwarepakket dat ook in het Nederlands verkrijgbaar is.

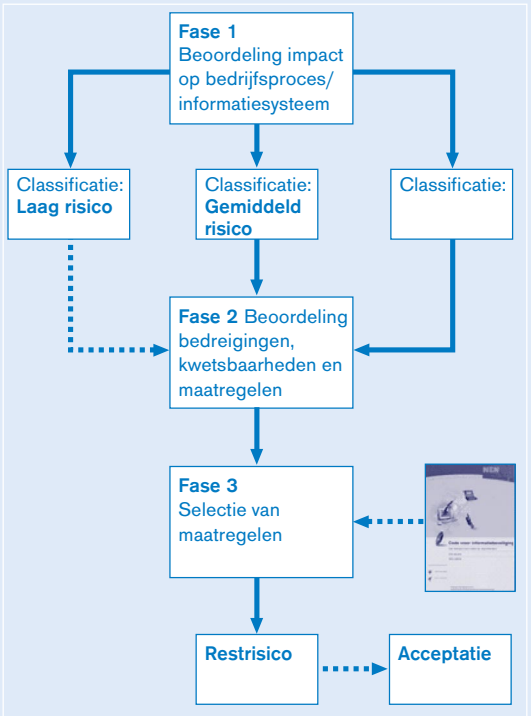
Een ander voorbeeld is de Afhankelijkheids- en Kwetsbaarheidsanalyse, zoals deze door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is uitgewerkt op basis van het Voorschrift Informatiebeveiliging Rijksdienst (VIR). In de afhankelijkheidsanalyse worden betrouwbaarheidseisen aan een te onderzoeken informatiesysteem of -systemen vastgesteld. In de kwetsbaarheidsanalyse wordt de impact van de relevante bedreigingen (voor het betreffende informatiesysteem of -systemen) vastgesteld. Op basis van de kwetsbaarheidsanalyse wordt een pakket maatregelen geselecteerd dat voldoet aan de gestelde betrouwbaarheidseisen.

Een belangrijke valkuil van de genoemde methoden[4] is de mate van detaillering. De complexiteit en de hoeveelheid werk neemt explosief toe naarmate een hogere detaillering wordt gehanteerd bij de keuze van het object en de opsplitsing van het object in deelobjecten. Daarom behandelen we in dit artikel de methode SPARK.

SPRINT (Simplified Process for Risk Identification) is een kwalitatieve risicoanalysemethode ontwikkeld door het Information Security Forum (ISF)[5], voorheen het European Security Forum (ESF). SPRINT is door KPMG Information Risk Management verder ontwikkeld en geïntegreerd met de Code voor Informatiebeveiliging tot de methode SPARK (Simplified Process for Analyzing Risks by KPMG).
SPARK is een gestructureerde en relatief eenvoudige methode om de risico's met betrekking tot informatie en de ondersteunende processen, systemen en netwerken te onderzoeken. De methode is eveneens een hulpmiddel bij het selecteren van passende beveiligingsmaatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en bedrijfsvoering te garanderen. De methode bestaat uit drie fasen.

In fase 1 wordt de impact op bedrijfsprocessen en hieraan gerelateerde informatiesystemen van het verliezen van informatie (in termen van beschikbaarheid, integriteit en vertrouwelijkheid) bepaald. Op basis van deze inventarisatie wordt het informatiesysteem geclassificeerd. Voor systemen met een middelhoog en hoog gepercipieerd risico wordt verder gegaan met fase 2 van SPARK. In deze fase worden de bedreigingen, kwetsbaarheden en reeds getroffen beveiligingsmaatregelen in detail geïnventariseerd en onderzocht. Op basis van de relevante bedreigingen worden in fase 3 van SPARK, in overleg met het management, beveiligingsmaatregelen geselecteerd. Bij deze selectie kan gebruik worden gemaakt van standaard-vragenlijsten en referentiemaatregelen uit de Code voor Informatiebeveiliging. Hierdoor zijn concrete aanknopingspunten voorhanden voor het treffen van maatregelen.

De methode wordt schematisch weergegeven in figuur 3.



Figuur 3. Schematische weergave van SPARK.

4) Naast de in dit artikel genoemde voorbeelden zijn er tal van andere risicoanalysemethoden zoals OCTAVE (CERT), SARA (ISF), RiskMetriX (Le Platane Management) en de Risk Control Method (KPMG).

5) ISF is een internationale vereniging van meer dan 250 vooraanstaande organisaties die praktisch onderzoek verricht naar informatiebeveiliging.

Kader 2. Risicoanalyse.

Faal- en succesfactoren

De praktijk leert dat het implementeren en onderhouden van een informatiebeveiligingsbeleid en een hiermee samenhangend stelsel beveiligingsmaatregelen geen sinecure is. De praktijk laat zien waarom het vaak fout gaat:

- *Beveiliging scoort niet*. Veel beveiligingsmaatregelen zijn niet zichtbaar voor het management. Het gaat in veel gevallen om nogal specialistische maatregelen in en rondom de informatiesystemen die voor een buitenstaander niet zichtbaar zijn en waar dus weinig goede sier mee te maken valt.
- *Beveiliging is lastig*. Als beveiligingsmaatregelen wel zichtbaar zijn leveren zij voor de gebruiker doorgaans ongemak op. Dit ongemak kan een einde maken aan bepaalde privileges en soms leiden tot omslachtige handelingen voor ogenschijnlijk eenvoudige functies.
- *Beveiliging is duur*. Sommige beveiligingsmaatregelen hebben meer voeten in de aarde dan oorspronkelijk was gedacht, waardoor de kosten tegenvallen. Daarbij komt dat de kosten voor het implementatietraject meestal verborgen zijn gebleven. Als de totale kosten tijdens het traject inzichtelijk worden gemaakt, zal vaak weerstand ontstaan bij het management.
- *Beveiliging is geen eenmalige aangelegenheid*. Veel bedrijven ontwikkelen een beleid voor informatiebeveiliging, voeren dit in en laten vervolgens de aandacht verslappen. Om aantoonbaar 'in control' te zijn is echter een continu proces van risicoanalyse en toetsing noodzakelijk. Ook de toezichthouders vereisen dit.

Elk beveiligingstraject is dan ook een uitdagende onderneming, waarbij een zeer zorgvuldige aanpak en voorbereiding noodzakelijk zijn. Daarbij zijn ten minste de volgende succesfactoren aan te wijzen:

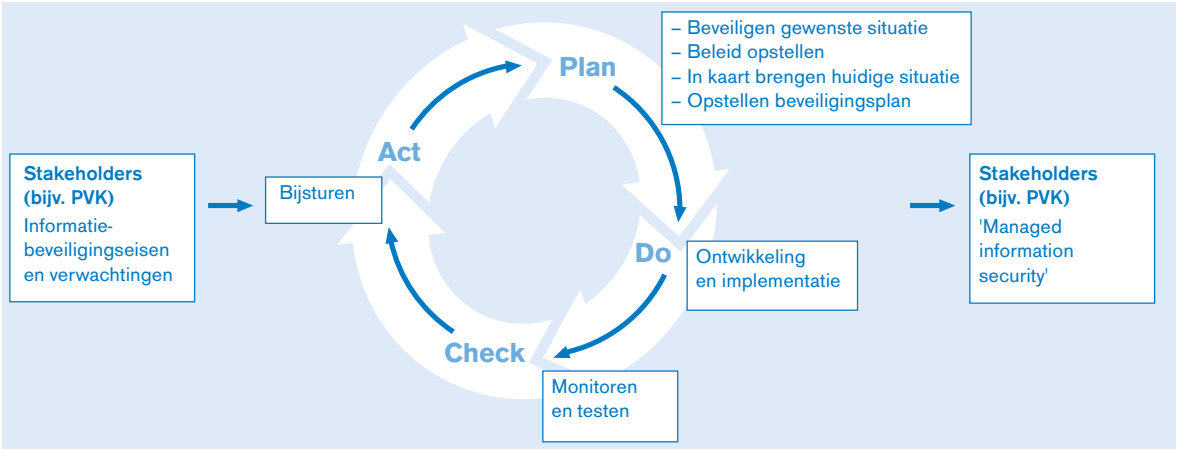
- *Draagvlak van het management*. Om een beveiligingstraject tot een succes te maken dient het hoogste management zich volledig en actief achter het beleid op te stellen. Dit betekent onder meer dat het voldoende middelen (tijd en geld) voor informatiebeveiliging ter beschikking moet stellen.
- *Communicatie en bewustzijn*. Voor, tijdens en na het beveiligingstraject is optimale communicatie met en de bewustwording van alle betrokkenen van het grootste belang.
- *Gestructureerde aanpak*. Het implementatietraject dient volgens een gestructureerde en projectmatige aanpak te worden uitgevoerd.

Streepje voor

Informatiebeveiliging is een essentieel thema voor moderne pensioenfondsen en uitvoerders. Ten opzichte van belanghebbenden – toezichthouders, aangesloten organisaties/werkgevers, werknemers en de deelnemers – moeten zij aantonen dat ze een 'goed huisvader' zijn. Ze moeten laten zien dat ze beschikken over een toetsbaar stelsel van maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen te waarborgen. Om zover te komen is een gestructureerde en procesmatige aanpak nodig. Pensioenfondsen en uitvoerders die dat goed op orde hebben, hebben een streepje voor. Voor een pensioenuitvoerder kan een goede beheersing van risico's zelfs een unique selling point zijn.

Literatuur

[KPMG05] KPMG Business Advisory Services, *De pensioenwereld in 2005*, KPMG, 2005.
[NNI00] Nederlands Normalisatie Instituut (NNI), *Code voor Informatiebeveiliging*, 2000.
[Over00] P.L. Overbeek, M. Spruit en E.E.O. Roos Lindgreen, *Informatiebeveiliging onder controle*, Prentice Hall, 2000.
[Roos98] E.E.O. Roos Lindgreen, *Corporate Information Security – geen halve maatregelen*, Compact 1998/5.
[Rutk04] E.P. Rutkens, H. Bouthoorn en L.P.F. Tushuizen, *Risicoanalyse gemakkelijk gemaakt*, Compact 2004/1.



Figuur 4. De Code voor Informatiebeveiliging kan pensioenfondsen helpen om op efficiënte en effectieve wijze een voldoende beveiligingsniveau te bereiken.