Onderdelen uitvraag operationele en IT risico's

De uitvraag in de vorm van een vragenlijst bevatte de volgende onderwerpen:

1. Vragenlijst ORM, met daarbinnen vragen over de opzet en werking van het risicomanagementsysteem, het interne controle raamwerk, de beheersmaatregelen ten aanzien van uitbestedingen, datakwaliteit en business continuity management (BCM).
2. Vragenlijst IB, met daarbinnen vragen die ingaan op verschillende aspecten van IT-systemen waaronder informatiebeveiliging/cyber-risico's, beheersing van (systeem)wijzigingen ('Change Management') en beschikbaarheid. Als basis hiervoor wordt de DNB Q&A en Good Practice informatiebeveiliging (LINK) gebruikt.

De belangrijkste waarnemingen uit de SBA ORM en SBA IB uitvraag

1. De basiselementen van een risicomanagementraamwerk zoals een beleid, risicobereidheid, periodieke risicoanalyses en een daarvan afgeleid beheersingsraamwerk zijn bij de meeste pensioenfondsen aanwezig, met de kanttekening dat veel pensioenfondsen voor hun belangrijke processen niet jaarlijks risicoanalyses uitvoeren.
2. Bij een groot aantal pensioenfondsen blijven door de Sleutelfunctiehouder Risicobeheer en/of Interne Audit geconstateerde 'hoog risico bevindingen' langer dan één jaar open staan.
3. De toetsing op de werking van beheersmaatregelen in de key bedrijfsprocessen vindt in de meeste gevallen handmatig plaats en slechts in beperkte mate door geautomatiseerde (systeem)controles.
4. Pensioenfondsen besteden een significant deel van hun operationele werkzaamheden uit aan dienstverleners, maar hebben tegelijkertijd belangrijke hiaten in de beheersing van deze uitbestedingen. Zo ontbreken vaak wettelijk verplichte bepalingen in de contracten en is de monitoring en evaluatie van de beheersing binnen de uitbestedingsketen veelal niet op orde.
5. Een groot aantal pensioenfondsen heeft hiaten in het beleid en de inrichting, uitvoering en monitoring van beheersmaatregelen ten aanzien van datakwaliteit, hetgeen tot uiting kan komen in de kwaliteit van de registratie van pensioenaanspraken.
6. Een groot aantal pensioenfondsen heeft de beheersmaatregelen ten aanzien van informatiebeveiliging onvoldoende op orde.

Hieronder vindt u onze belangrijkste observaties ten aanzien van uitbestedingen en datakwaliteit. Onze observaties ten aanzien van informatiebeveiliging kunt u lezen in de IB Monitor [Link naar artikel over IB-monitor]

1. Beheersing van uitbestedingen

Uit de uitvraag blijkt dat pensioenfondsen een significant deel van hun activiteiten uitbesteden. Pensioenfondsen die hun activiteiten aan een PUO hebben uitbesteed geven meer dan 80% van hun operationele kosten uit aan uitbestedingen. Voor de zelfadministrerende fondsen en PUO's is dit percentage lager. Veel pensioenfondsen laten hiaten zien in de beheersing van de uitbestedingen op de volgende punten:

1.1 Contractafspraken

- Bij een derde van de pensioenfondsen omvat een significant aantal (meer dan 15%) van hun contracten met kritieke of belangrijke dienstverleners niet alle wettelijk vereiste bepalingen inzake onderzoeksrecht van de toezichthouder, auditrecht van het pensioenfonds, exitclausule en/of onderuitbestedingen.
- Een derde van de pensioenfondsen sluit geen 'security agreement' af met 50% van hun kritieke of belangrijke dienstverleners, waardoor naleving van het informatiebeveiligingsbeleid van het pensioenfonds niet geborgd is.

1.2 Monitoring en evaluatie van de uitbestedingen

- Ca. 30% van de pensioenfondsen heeft de beheersmaatregelen rondom de monitoring van de uitbesteding niet ingericht op basis van een vooraf uitgevoerde risicoanalyse
- Bijna 40% van de pensioenfondsen verzuimt bij meer dan 50% van zijn kritieke of belangrijke uitbestedingen om de prestaties te monitoren d.m.v. SLA rapportages
- Bijna een derde[1] van de pensioenfondsen verzuimt bij meer dan 50% van zijn kritieke of belangrijke uitbestedingen om de werking van de beheersmaatregelen in de keten te monitoren, bijvoorbeeld door middel van assurancerapportages of audits bij leveranciers of onderaannemers.
- Ongeveer 30% van de pensioenfondsen voert bij meer dan 50% van zijn kritieke of belangrijke uitbestedingen geen periodieke (monitoring)gesprekken of geen periodieke leveranciersevaluaties uit
- Bijna 40% van de pensioenfondsen beschikt niet over periodieke risicorapportages aan het management over de effectiviteit van de beheersmaatregelen rondom uitbestedingen, zoals bijvoorbeeld de monitoring van prestaties en risicobeheersing bij kritieke dienstverleners.

2. Datakwaliteit (inclusief End Using Computing (EUC))

De beheersing van datakwaliteit is een aandachtspunt. Bij ruim één derde tot meer dan de helft van de pensioenfondsen[2]:

(a) Bevat het datakwaliteitsbeleid geen richtlijnen ten aanzien van het omgaan met dataincidenten en -herstel en/of de toepassing van End Using Computing (EUC).
(b) Is het gebruik van beheersinstrumenten (zoals het uitvoeren van een risico-analyse, het vaststellen van een risk appetite en het monitoren van adequate KPI's) niet op orde.
(c) Is er geen management- en rapporteringscyclus ten aanzien van datakwaliteit aanwezig binnen de organisatie.

Onvoldoende beheersing van datakwaliteit kan tot gevolg hebben dat pensioenaanspraken van deelnemers niet juist, volledig en reproduceerbaar zijn. Bovenstaande constateringen hebben vooral betrekking op de uitvoering van de pensioenadministratie, pensioenfondsbesturen blijven verantwoordelijk voor de beheersing van datakwaliteit ook als de uitvoering is uitbesteed. Ten aanzien van

[1] Uit de uitbestedingsonderzoeken die DNB heeft uitgevoerd bij instellingen blijkt dat een veel hoger percentage van de instellingen onvoldoende zicht heeft op de beheersing in de uitbestedingsketens.
[2] De antwoorden op de vragen over datakwaliteit zijn uitsluitend afkomstig van zelf administrerende pensioenfondsen en PUO's

punt (a) verwacht DNB dat pensioenfondsen die EUC-toepassingen gebruiken, ook beschikken over beleid met het oog op de beheersing van risico's rond het gebruik daarvan.