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 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 verzekeraars aanwezig.
2. Bij een groot aantal verzekeraars blijven regelmatig door de RMF en/of IAF geconstateerde 'hoog risico bevindingen' langer dan één jaar open staan.
3. De toetsing op de werking van beheersmaatregelen in de key bedrijfsprocessen vindt vooral handmatig plaats en slechts in beperkte mate door geautomatiseerde (systeem)controles.
4. Verzekeraars 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 verzekeraars 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 QRT's
6. Een groot aantal verzekeraars 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.

1. Beheersing van uitbestedingen

Uit de uitvraag blijkt dat verzekeraars een significant deel van hun activiteiten uitbesteden. Verzekeraars geven gemiddeld ongeveer een kwart van hun operationele kosten uit aan uitbestedingen. Veel verzekeraars laten hiaten zien in de beheersing van de uitbestedingen op de volgende punten:

1.1. Contractafspraken

- Bij ruim een derde van de verzekeraars 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 de verzekeraar, exitclausule en/of onderuitbestedingen.
- Bijna de helft van de verzekeraars sluit geen 'security agreement' af met 50% van hun kritieke of belangrijke dienstverleners, waardoor naleving van het informatiebeveiligingsbeleid van de verzekeraar niet geborgd is.

1.2 Monitoring en evaluatie van de uitbestedingen

- Ruim 40% van de verzekeraars heeft de beheersmaatregelen rondom de monitoring van de uitbesteding niet ingericht op basis van een vooraf uitgevoerde risicoanalyse.
- De helft van de verzekeraars verzuimt bij meer dan 50% van zijn kritieke of belangrijke uitbestedingen om de prestaties te monitoren door middel van SLA rapportages.
- Drie op de vier verzekeraars 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 40% van de verzekeraars voert bij meer dan 50% van zijn kritieke of belangrijke uitbestedingen geen periodieke (monitoring)gesprekken of geen periodieke leveranciersevaluaties uit.
- Meer dan 40% van de verzekeraars 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 verzekeraars:

(a) Bevat het datakwaliteitsbeleid geen richtlijnen voor 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 geen management- en rapporteringscyclus ten aanzien van datakwaliteit aanwezig binnen de organisatie.

Onvoldoende beheersing van datakwaliteit kan onjuistheden in de QRT's tot gevolg hebben. Ten aanzien van punt (a) verwacht DNB dat verzekeraars die EUC-toepassingen gebruiken, ook beschikken over beleid met het oog op de beheersing van risico's rond het gebruik daarvan.