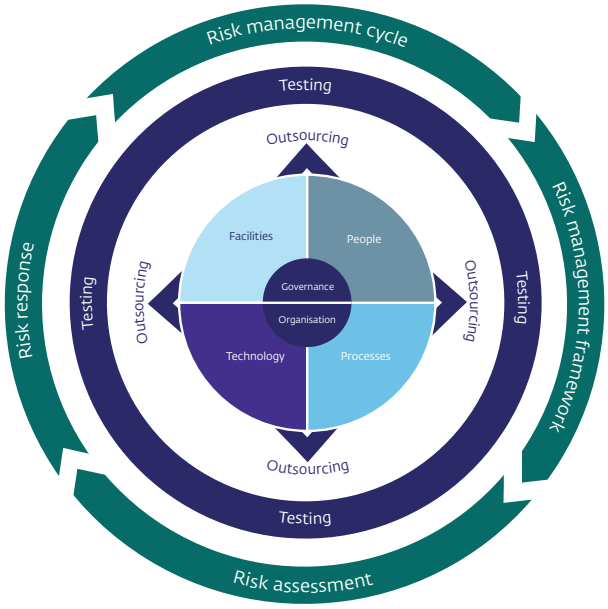
Het belang van een solide informatiebeveiligings-managementsysteem (ISMS)

In een tijdperk waarin verzekeraars en pensioenfondsen een overvloed aan gevoelige gegevens beheren, is informatiebeveiliging van cruciaal belang om het vertrouwen van klanten te behouden en de financiële stabiliteit te waarborgen. DNB is enkele jaren geleden gestart met het verzamelen van informatie over het volwassenheidsniveau van informatiebeveiligingsbeheersingsmaatregelen.

58 beheersingsmaatregelen

Na de Sector Brede Analyse Informatiebeveiliging (SBA-IB) van 2021 en 2022, heeft DNB een mitigatiebrief gestuurd naar een aantal van haar verzekeraars en pensioenfondsen, waarin wordt verzocht om binnen anderhalf jaar na de publicatiedatum te voldoen aan het gewenste volwassenheidsniveau van 58 beheersingsmaatregelen, zoals beschreven in de Good Practice Informatiebeveiliging [1].



DNB Toetsingskader Informatiebeveiliging 2019-2020

DNB vereist in haar mitigatiebrief dat er een onafhankelijke bevestiging wordt verkregen van de interne auditfunctie of een externe deskundige, waaruit blijkt dat de volwassenheidsniveaus in het ingevulde self-assessment van de organisatie voldoende is onderbouwd met documentatie. Deze validatie richt zich op het bevestigen van de betrouwbaarheid van het informatiebeveiligingsmanagementsysteem (ISMS), niet op de beoordeling van de effectiviteit en efficiëntie van specifieke beveiligingsmaatregelen.

1. https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf

Beheersing van informatiebeveiliging

De uitdaging waar veel organisaties voor staan is niet zozeer de validatie van het self-assessment maar de opzet van het ISMS. Het is van groot belang dat de plan-do-check-act cyclus wordt geïntegreerd in het ontwerp, de implementatie, monitoring en evaluatie van de beheersingsmaatregelen voor het verkrijgen van het gewenste volwassenheidsniveau zoals DNB deze voorschrijft.

We stellen vast dat verzekeraars en pensioenfondsen veelal beschikken over een dergelijk risicomanagementsysteem, waarbij informatiebeveiliging als onderdeel wordt toegevoegd. De omvang van de werkzaamheden voor een Information Security Officer (ISO) zijn vaak niet voldoende om een fulltime FTE mee te vullen, waardoor de rol doorgaans wordt vervuld door een risicomanager of ICT-manager. Voor deze functies is het vaak lastig qua kennis of tijd om de organisatie van informatiebeveiliging en het implementeren van het gehele ISMS te realiseren binnen de gewenste periode zoals DNB deze voorschrijft.

Informatiebeveiliging als expertise

Bij InAudit Information Security hebben we Information Security Officers die deskundig zijn in het implementeren van het volledige ISMS en beheersmaatregelen binnen uw organisatie. Daarnaast beschikt InAudit Audit Services over meerdere interne auditors met expertise op het gebied van informatiebeveiliging. Wij staan klaar om u te ondersteunen bij de uitdagingen van informatiebeveiliging en om ervoor te zorgen dat uw organisatie voldoet aan de vereisten vanuit DNB.