KoutersVanderMeer
bureau voor prestatieverbetering

SPRENKELS & VERSCHUREN
STRATEGY • GOVERNANCE • RISK • LEGAL

Wat is er aan de hand?

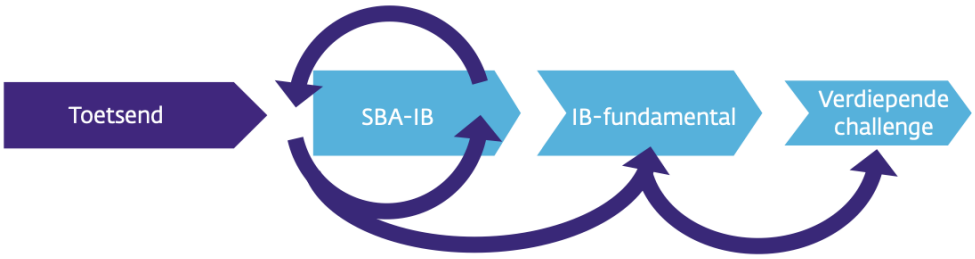
Op 16 december 2020 kondigde DNB via haar nieuwsbrief aan dat in 2021 een sectorbrede uitvraag onder pensioenfondsen wordt gedaan naar de volwassenheid van informatiebeveiliging (ook wel: IB) en de beheersing van uitbestedingsrelaties. Concreet betekent dit dat dit jaar van alle pensioenfondsen wordt verwacht dat zij een self-assessment IB uitvoeren, waarbij het volwassenheidsniveau van informatiebeveiliging wordt gerapporteerd aan DNB. Op basis van het te verkrijgen sectorbrede beeld voert DNB verdiepende onderzoeken uit, wellicht ook voor uw pensioenfonds.

Waarom aandacht voor informatiebeveiliging en cybersecurity?

De eisen van een integere en beheerste bedrijfsvoering waaraan het fonds moet voldoen, gelden ook voor de IT-functie die ten grondslag ligt aan de bedrijfsvoering van het fonds. Het beheersen van de uitbestedingsrelaties van het fonds en de bijbehorende risico's van informatiebeveiliging en cybersecurity maakt onverkort onderdeel uit van de integere en beheerste bedrijfsvoering. Met het oog op de verdere digitalisering van de bedrijfsvoering van het fonds is het noodzakelijk dat informatiebeveiliging en cybersecurity structureel is geborgd in de besturingscyclus van het fonds. Logische aanknopingspunten liggen in het risicomanagementproces alsook de uitbestedingscyclus van het fonds. Binnen het risicomanagementbeleid stelt het bestuur het (eigen) kader vast waaraan informatiebeveiliging en cybersecurity moet voldoen (door de risicohouding en risicobereidheidsprincipes te formuleren).

Waarom een sectorbrede uitvraag door DNB?

In haar jaarlijkse informatiebeveiligingsmonitor (april 2020) schetst DNB haar onderzoeksmethoden met betrekking tot informatiebeveiliging en cybersecurity binnen de sector. Deze onderzoeksmethoden vormen een samenhangend toetsingskader en hebben een onderling versterkend effect.



Onderzoeksmethoden informatiebeveiliging en cybersecurity DNB

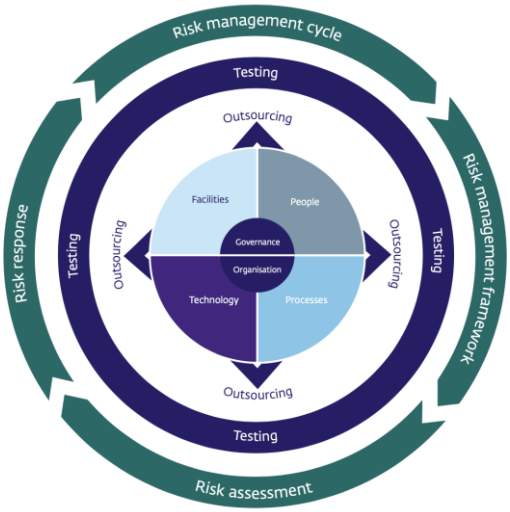
De Sectorbrede Analyse Informatiebeveiliging (SBA-IB) betreft een sectorbrede uitvraag op basis van de Good Practice Informatiebeveiliging, waarbij instellingen het volwassenheidsniveau van informatiebeveiliging 'scoren' en risico-indicatoren in kaart brengen aan de hand van een vragenlijst en een self-assessment.

Het IB/Cyber fundament onderzoek betreft het 'reguliere' IB onderzoek dat DNB sinds 2010 uitvoert bij een selectie van instellingen. Dit onderzoek richt zich op het aanwezig zijn van een fundament voor informatiebeveiliging bij het pensioenfonds, waarin ook informatiebeveiliging als onderdeel van een beheerste uitbesteding wordt beschouwd. Input verkregen van de sector op basis van het SBA-IB onderzoek draagt bij aan de selectie voor het IB/Cyber fundament onderzoek.

Bij een beperkt aantal instellingen wordt een verdiepend IB/Cyber onderzoek uitgevoerd. Op basis van inzichten verkregen van het IB fundament wordt deze verdiepende challenge op maat ingestoken.

Wat is de Good Practice Informatiebeveiliging?

De self-assessment IB is gebaseerd op de Good Practice Informatiebeveiliging 2019/2020 van DNB. Dit raamwerk bestaat uit 9 domeinen met in totaal 58 controls. Per control zijn Good Practices uitgewerkt voor het pensioenfonds zelf en voor uitbestedingssituaties, inclusief concrete voorbeelden.



DNB toetsingskader informatiebeveiliging 2019/2020

Daarnaast heeft DNB een volwassenheidsmodel opgenomen, waarmee vastgesteld kan worden in hoeverre de beheersing van informatiebeveiliging en cybersecurity bij het pensioenfonds op het vereiste niveau is. Hierbij geldt dat vanwege de voortdurende ontwikkelingen op het gebied van informatiebeveiliging en cybersecurity pensioenfondsen permanent aandacht moeten besteden aan het op niveau brengen en houden van de inrichting van hun informatiebeveiliging.

Waarom kan ik voor informatiebeveiliging niet op mijn uitvoerder vertrouwen?

Bij uitbesteding van bedrijfsactiviteiten blijft het pensioenfonds eindverantwoordelijk voor de integere en beheerste bedrijfsvoering in lijn met de door het pensioenfonds gestelde kaders en de wet- en regelgeving.

Dit geldt ook voor informatiebeveiliging en cybersecurity in relatie tot de uitbestede bedrijfsactiviteiten en het daarvoor door de uitvoerder ingerichte IT-landschap. Om die reden zal IT-risicomanagement ook onderdeel zijn van het integraal risicomanagement raamwerk en de uitbestedingscyclus van het pensioenfonds.

Het fonds doet er daarom verstandig aan het volwassenheidsniveau vanuit twee invalshoeken inzichtelijk te maken[1]:

1. Volwassenheid van informatiebeveiliging vanuit fondsperspectief.
2. Volwassenheid van informatiebeveiliging vanuit het perspectief van uw uitvoerders.

Vanuit fondsperspectief ligt de focus op de wijze waarop informatiebeveiliging is opgenomen in de beleidskaders van het fonds en onderdeel is van de beheersing van de uitbestedingsrelaties. Daarnaast is informatiebeveiliging met betrekking tot de IT-omgevingen en IT-middelen in gebruik binnen de fondsorganisatie in scope. Veelal is vanuit fondsperspectief slechts een beperkt aantal van de 58 controls van toepassing. De eisen die u stelt zijn gebaseerd op de risicohouding en risicobereidheid en de IT-risicoanalyse van het pensioenfonds.

Vanuit het perspectief van uw uitvoerder wordt verwacht dat u als fonds een duidelijk beeld heeft van de volwassenheid van informatiebeveiliging door uw uitvoerder. Dat betekent dat uw uitvoerder de volwassenheid van informatiebeveiliging voor u inzichtelijk maakt.

Hierbij kunt u het proportionaliteitsbeginsel toepassen, waarbij de aard, omvang en complexiteit van de uitvoerder en haar informatiehuishouding bepalend is voor de wijze waarop de self-assessment wordt ingevuld.

Kijk bij de selectie van de uitvoerder verder dan alleen uw pensioenadministrateur. Neem ook uw kritieke en belangrijke uitbestedingen op het gebied van vermogensbeheer (fiduciair beheerder, property managers, custodian, etc.) en de bestuursomgeving (bestuursportaal, kantoorautomatisering, IT bij de sponsor, actuariële dienstverleners, etc.) in beschouwing.

Wat is de toegevoegde waarde van de self-assessment IB?

De self-assessment IB geeft u inzicht in het volwassenheidsniveaus én het verbeterpotentieel met betrekking tot informatiebeveiliging en cybersecurity binnen uw pensioenfonds en bij uw uitvoerders. Het stelt u in staat om vast te stellen of het niveau van informatiebeveiliging van het pensioenfonds en de uitbestedingsrelaties in lijn zijn met uw risicohouding en risicobereidheid en voldoet aan de minimale eisen van DNB.

Ook is het een uitgelezen mogelijkheid om het net binnen uw eigen fondsorganisatie en bij uw uitvoerders op te halen. Dit kan een bijdrage leveren aan het verhogen van security awareness binnen het pensioenfonds of aan het voeren van het goede gesprek met uw uitvoerders over informatiebeveiliging en cybersecurity.

Tegelijkertijd bent u dan voorbereid op de verplichte sectorbrede uitvraag door DNB.

[1] In het artikel '[IT in control aan de bestuurstafel]' wordt het belang van deze perspectieven nader geduid.

Welke aanpak te volgen?

In onderstaande afbeelding is een stappenplan opgenomen dat gebruikt kan worden voor het uitvoeren van de self-assessment IB.

Stap 1 - Verkrijg inzicht in het toetsingskader
Neem kennis van de Good Practice Informatiebeveiliging 2019/2020 van DNB, de 58 controls en de minimaal vereiste volwassenheidsniveaus.
Stap 2 - Selecteer controls relevant vanuit fondsperspectief en uitvoerdersperspectief
Verkrijg inzicht in uw kritieke IT-ketens en de beheersing daarvan, waarbij proportionaliteit een belangrijke rol speelt. Maak hierbij het onderscheid tussen (eind)verantwoordelijkheid en uitvoering. Bepaal welke delen van de Good Practice direct op het fonds van toepassing zijn.
Stap 3 - Voer de self-assessment IB uit
• Voer de self-assessment IB uit, onderbouw uw scores met bewijslast (dossier) en laat dit challengen door uw sleutelfunctie Risicobeheer of een externe expert. • Bevraag uw uitvoerders expliciet op hun volwassenheid van informatiebeveiliging.
Stap 4 - Evalueer de uitkomsten van de self-assessment IB
• Bespreek de uitkomsten van de self-assessment binnen het bestuur en met uw uitvoerders. • Stel op basis van de uitkomsten eventueel een verbeterplan op om de vereiste volwassenheidsniveaus te behalen.
Stap 5 - Bestendig de self-assessment in uw risicomanagement cyclus
Maak het uitvoeren van het self-assessment IB tot een jaarlijkse exercitie en koppel deze evenals het verbeterplan aan de reguliere management cyclus (IT-)risicobeheersing.

Stappenplan uitvoering self-assessment IB

Wanneer te beginnen?

Wellicht is het periodiek vaststellen van de volwassenheid van informatiebeveiliging reeds een vast onderdeel van de IT-risicomanagement cyclus van het fonds. Mocht dat niet zo zijn dan is het raadzaam deze self-assessment op korte termijn uit te voeren. DNB heeft het sectorbrede onderzoek voor het tweede kwartaal van 2021 aangekondigd.

Heeft u behoefte aan hulp? Wij ondersteunen uw fonds bij het voorbereiden, invullen en/of challengen/valideren van de self-assessment IB. Dit leidt tot een ‘fool proof’ dossier en een pragmatisch uitvoerbaar verbeterplan met concrete acties.

Bij Sprenkels & Verschuren (S&V) helpen wij u bij complexe (maatschappelijke) vraagstukken op het gebied van pensioenen, beleggen, verzekeren en risicomanagement. Maar ook voor strategieontwikkeling, projectmanagement en het begeleiden van transities en fusies kunt u bij S&V terecht.

KoutersVanderMeer is een bureau voor prestatieverbetering op het gebied van IT-governance, IT-risicomanagement en compliance. KoutersVanderMeer helpt u ook bij de versimpeling van complexe vraagstukken rondom informatiebeveiliging en cybersecurity.