Beleid inzake Informatie en Technologie (IT-beleid)

Versiedatum: 15 november 2022
Datum bestuursvergadering: 16 december 2022

Smurfit Kappa
Pensioenfonds

Inhoudsopgave

Managementsamenvatting

Voor u ligt het beleid ten aanzien van "Informatie en Technologie" ("IT") van Stichting Pensioenfonds Smurfit Kappa Nederland ("het pensioenfonds"). Dit beleid beschrijft de manier waarop het pensioenfonds wil omgaan met aan IT gerelateerde onderwerpen en processen en de beheersing van daaraan gerelateerde risico's.

Het pensioenfonds heeft als doelstelling het zo goed mogelijk beheren van de ingelegde pensioenpremies en het uitkeren van pensioenen aan deelnemers, oud-medewerkers en hun partner en/of kind(eren). Hierbij vertrouwen onze deelnemers, toezichthouders en andere belanghebbenden erop dat bij het pensioenfonds en haar medewerkers professionaliteit, vertrouwelijkheid en integriteit voorop staan. IT is daarbij een belangrijk bedrijfsmiddel, ook wanneer nagenoeg alle werkzaamheden zijn uitbesteed. Een visie op IT en IT-risicobeheersing is dan ook essentieel voor het goed kunnen functioneren van het pensioenfonds.

In dit IT-beleid staan principes en guidelines centraal. Deze principes en guidelines typeren het pensioenfonds op het gebied van IT. Per uitgangspunt zijn consequenties uitgewerkt en is beschreven op welke wijze het fondsbestuur hier invulling aan geeft.

Naast deze uitgangspunten en principes is uitgewerkt op welke wijze binnen het fondsbestuur invulling wordt gegeven aan IT-risicobeheer en IT-governance. Het IT-ricicobeheer en IT-governance is vormgegeven op basis van algemeen geaccepteerde standaarden, zoals de vier aandachtsgebieden (de 4 A's) uit het Basiskader Infrastructuur & IT van DNB: Availability, Access, Accuracy en Agility.

1 Inleiding

We leven in een tijd waarin technologische innovaties zich steeds sneller aandienen en elkaar opvolgen. Technologische innovatie leidt enerzijds tot betere en modernere financiële dienstverlening aan deelnemers, oud-medewerkers en hun partner en/of kind(eren) en biedt nieuwe mogelijkheden. Anderzijds kan technologische innovatie de bedrijfsmodellen van gevestigde partijen onder druk zetten en leiden tot verschuivingen in de markt. Ook kan technologische innovatie de operationele risico's beïnvloeden, bijvoorbeeld op het gebied van cybersecurity of bij uitbesteding van onderdelen van de waardeketen.

Pensioenfondsen en pensioenuitvoeringsorganisaties met complexe en soms ook verouderde systemen en administraties lopen verhoogde risico's wanneer de beveiliging, de functionaliteiten en aanpasbaarheid niet meer voldoen aan de eisen van deze tijd.

Daarnaast dwingen wet- en regelgeving en toezichthouders pensioenfondsen om meer aandacht te schenken aan risico's en beheersing van IT met als voorbeelden:

- De toenemende aandacht voor kosten per deelnemer en de hoge kosten van het beheren en onderhouden van de benodigde IT, voedt de trend van uitbesteding van bedrijfsprocessen en -functies. Ook de opkomst van nieuwe technologie speelt hierin een rol. Bij uitbesteding is het realiseren van een adequate risicobeheersing (deels) ook uitbesteed, omdat een aanzienlijk deel van de processen zich buiten de directe waarneming en invloedsfeer van de instellingen bevindt.
- Nieuwe regelgeving die pensioenfondsen dwingt hun deelnemers via internet informatie beschikbaar te stellen, wat IT-security risico's met zich meebrengt. Hierbij kan gedacht worden aan identiteitsfraude en cybercriminaliteit. Met de transitie naar een nieuw pensioenstelsel zullen instellingen nieuwe administratiefunctionaliteiten moeten ontwikkelen.
- DNB heeft cyberrisico's hoog op de agenda staan. DNB volgt al meerdere jaren het niveau van beheersing hiervan bij pensioenfondsen via informatiebeveiligingsonderzoeken (waaronder self assessments) en aanvullende thema-gerichte onderzoeken. Afgelopen jaren richtten deze thema-gerichte onderzoeken zich vooral op cybersecurity en op risicobeheersing op het gebied van uitbestede dienstverlening (cloud-computing). Daarnaast zijn bij uitvoerders onderzoeken op het gebied van informatiebeheer uitgevoerd.
- Autoriteit Persoonsgegevens die de naleving van de Algemene verordening gegevensbescherming (AVG) bewaakt. Ook pensioenfondsen en pensioenuitvoeringsorganisaties moeten aan deze verordening voldoen. De Autoriteit Persoonsgegevens kan hoge boetes opleggen als de organisatie niet 'compliant' is.

1.1 Doelstelling

Dit IT-beleid beschrijft de strategische en tactische wijze waarop het fondsbestuur van het pensioenfonds richting en invulling geeft aan de inbedding van IT binnen het pensioenfonds.

1.2 Scope

Op operationeel maar ook deels op tactisch niveau heeft het pensioenfonds haar IT-organisatie uitbesteed waarbij onderscheid wordt gemaakt tussen vier omgevingen die in de hiernavolgende tabel zijn weergegeven.

IT omgeving	Ter ondersteuning van	Uitbestedingspartij
Bestuursomgeving	Uitvoeren en ondersteunen van de bestuursactiviteiten van het pensioenfonds.	Smurfit Kappa
Pensioenbeheer - middelloonregeling	Pensioen- , uitkerings- en financiële administratie en pensioencommunicatie van het pensioenfonds inzake de middelloonregeling.	AZL
Pensioenbeheer – beschikbare premie regeling	Uitvoeren en ondersteunen van de beschikbare premie regeling van het pensioenfonds.	AAPS NN IP
Vermogensbeheer	Beleggingsactiviteiten van het pensioenfonds om te zorgen dat het pensioenfonds aan haar korte - en lange termijn verplichtingen kan blijven voldoen.	NN IP

Deze partijen hebben op hun beurt een eigen IT-strategie/-beleid en daarvan afgeleide IT-beheerorganisatie met IT-beheerprocessen.

1.3 Positionering ten opzichte van uitbesteding

Vanwege de hoge mate van uitbesteding is een uitbestedingsbeleid opgesteld. Dit uitbestedingsbeleid gaat niet expliciet in op IT, maar behandelt uitbesteding in z'n algemeenheid. Uitbesteding van IT-omgevingen en/of IT-dienstverlening is daar wel impliciet onderdeel van. Dit IT-beleid en het uitbestedingsbeleid hebben daarom een nauwe verwantschap aan elkaar, zeker wanneer het gaat om 'IT-uitbesteding'. Op dit gebied moet dit IT-beleid worden gezien als een explicitering van het algemene uitbestedingsbeleid van het pensioenfonds.

1.4 IT-governance

1.4.1 Rollen en verantwoordelijkheden

Het fondsbestuur is en blijft altijd eindverantwoordelijk voor alle werkzaamheden van het pensioenfonds, en dus ook voor de uitbestede activiteiten, inclusief de IT gerelateerde onderwerpen. In dit verband zijn taken, bevoegdheden en verantwoordelijkheden van het fondsbestuur en de uitbestedingspartner omschreven. Tussen partijen zijn daarover schriftelijk afspraken gemaakt. De taken, bevoegdheden en verantwoordelijkheden zijn duidelijk vastgelegd.

1.4.2 Deskundigheid en geschiktheid

Het fondsbestuur draagt zorg voor zijn eigen deskundigheid en geschiktheid zodat het voldoende 'countervailing power' heeft om IT en hieraan gerelateerde onderwerpen te kunnen beoordelen. Als het fondsbestuur van mening is dat deskundigheid en/of geschiktheid te kort schiet, zal het fondsbestuur altijd besluiten externe expertise in te winnen om te waarborgen dat de juiste keuzes worden gemaakt ten aanzien van de betrouwbaarheid, integriteit en vertrouwelijkheid van de (uitbestede) informatiesystemen.

1.5 Inwerkingtreding

Dit IT-beleid is voor het eerst in werking getreden na goedkeuring door het fondsbestuur van het pensioenfonds op 5 november 2021. IT is echter voortdurend in ontwikkeling, zodat dit IT-beleid ook regelmatig wordt bijgewerkt. Deze meest recente versie is vastgesteld tijdens de bestuursvergadering van 16 december 2022.

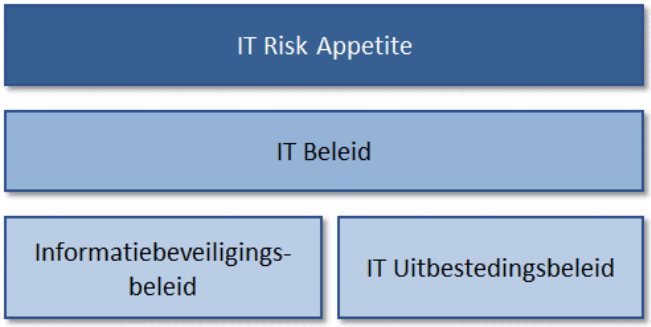
2 Positionering IT-beleid binnen IT-risicobeheer

In dit hoofdstuk behandelen wij op hoofdlijnen de positionering van het IT-beleid binnen het IT-risicobeheer.

2.1 Integraal risicomanagement beleid ("IRM-beleid")

Voor het beheersen van de risico's, passend bij de risk appetite heeft het pensioenfonds een IRM-beleid opgesteld. Het IT-risicobeheer geldt als een aanvulling op én een verdieping van het IRM-beleid van het pensioenfonds ten aanzien van IT-risico's en de beheersing daarvan.

De positionering van het IT-beleid binnen het IT-risicobeheer is weergegeven in de onderstaande afbeelding.



In de hiernavolgende paragrafen gaan wij kort in op de onderdelen van het IT-risicobeheer.

2.2 IT Risk Appetite

De uitvoering van het IT-risicobeheer begint bij het vaststellen van de IT Risk Appetite van het pensioenfonds. Hiertoe maakt het pensioenfonds gebruik van vier risicogebieden (de 4 A's) en het Basiskader Infrastructuur & IT van DNB, dat zich richt op:

1. **Beschikbaarheid (Availability):** Het draaiende houden van processen en het herstellen van verstoringen, met de ambitie de negatieve gevolgen zoveel mogelijk te beperken.
2. **Nauwkeurigheid (Accuracy):** Het opleveren van juiste, tijdige en volledige informatie aan alle relevante belanghebbenden.
3. **Toegankelijkheid (Access):** Het waarborgen dat de juiste mensen toegang hebben tot de juiste informatie en anderen niet.
4. **Aanpasbaarheid (Agility):** Verandering in bedrijfsvoering die benodigd kan zijn als gevolg van interne en externe oorzaken, zoals acquisities of nieuwe regelingen, tegen acceptabele kosten en acceptabele risico's.

Voor de processen die binnen de IT omgevingen van het pensioenfonds worden uitgevoerd, wordt door het bestuur bepaald welke impact maximaal is toegelaten.[1] Daarnaast wordt als onderdeel van dit proces de complexiteit van de IT-omgeving en wijze waarop deze wordt beheerd in kaart gebracht als randvoorwaarde voor het kunnen vaststellen van de risk appetite.

[1] Zie bijlage 1 voor de definities van de gehanteerde classificaties per risicogebied.

In 2018 heeft het pensioenfonds een risico-analyse uitgevoerd van de financiële en niet-financiële risico's. Dit heeft onder andere betrekking gehad op het niet-financiële thema "ICT" dat onder andere bestaat uit de onderdelen "continuïteit van systemen", "beveiliging" en "autorisatie". Ten aanzien van "ICT" werd voorgesteld om een eigen beleid op te stellen om vast te stellen welke eisen aan de systemen van de werkgever worden gesteld, alsmede aan de systemen van de partijen waaraan de werkzaamheden zijn uitbesteed. Het voorliggende document is een uitwerking hiervan.

2.3 Informatiebeveiligingsbeleid

Informatiebeveiliging wordt beschouwd als een integraal onderdeel van IT-risicobeheer, zoals dit is opgezet door het pensioenfonds. Informatiebeveiliging loopt als het ware door het IT-beleidsproces heen en richt zich specifiek op de beschikbaarheid, integriteit en vertrouwelijkheid (toegang) van de (digitale) informatie en informatievoorziening van het pensioenfonds.

Dit geldt eveneens voor de processen en diensten bij uitbestedingsrelaties. Het niet of niet voldoende treffen van beheersingsmaatregelen kan ertoe leiden dat kwetsbaarheden ontstaan waardoor informatiebeveiligingsrisico’s kunnen optreden.

Ten aanzien van informatiebeveiliging maakt het pensioenfonds gebruik van de volgende publicatie van DNB: "Good Practice Informatiebeveiliging 2019/2020". Door middel van deze publicatie geeft DNB handvatten waarmee pensioenfondsen kunnen voldoen aan de wettelijke bepalingen om de integriteit, voortdurende beschikbaarheid en beveiliging van de geautomatiseerde gegevensverwerking te waarborgen.

Om het niveau van informatiebeveiliging te kunnen vaststellen, hanteert DNB een volwassenheidsmodel[2]. DNB verwacht dat pensioenfondsen op het gebied van informatiebeveiliging en cybersecurity aantoonbaar "in control" zijn. In het door DNB gehanteerde model met 58 beheersingsmaatregelen komt dat overeen met ten minste een volwassenheidsniveau van "3 – gedefinieerd" voor 55 beheersingsmaatregelen. Voor 3 beheersingsmaatregelen verwacht DNB een hoger volwassenheidsniveau van "4 – beheerst en meetbaar".

Periodiek verricht DNB een sectorbrede uitvraag informatiebeveiliging ("SBA IB"). Voor de SBA IB zijn 15 van de 58 beheersmaatregelen van belang, waarbij voor 12 van de 15 een volwassenheidsniveau van ten minste "3 – gedefinieerd" is vereist en voor de overige 3 een volwassenheidsniveau van "4 – beheerst en meetbaar".

2.4 Uitbestedingsbeleid

Vanwege de hoge mate van uitbesteding is een separaat uitbestedingsbeleid opgesteld. Dit uitbestedingsbeleid gaat niet expliciet in op IT, maar behandelt uitbesteding in z’n algemeenheid. Uitbesteding van IT-omgevingen en/of IT-dienstverlening is daar wel impliciet onderdeel van. Immers IT is een onderdeel van de uitbesteding. Dit IT-beleid en het uitbestedingsbeleid hebben daarom een nauwe verwantschap aan elkaar, zeker wanneer het gaat om uitbesteding met IT-aspecten. Op dit gebied moet dit IT-beleid worden gezien als een explicitering van het algemene uitbestedingsbeleid van het pensioenfonds.

[2] Zie bijlage 2 voor een toelichting op de definities van de volwassenheidsniveaus.

3 IT-principes en guidelines

Om te waarborgen dat IT-oplossingen in lijn zijn met de strategie van het pensioenfonds, heeft het pensioenfonds richting gegeven aan de IT-functie door het opstellen van de volgende IT-principes ten aanzien van gebruik, beheer en beveiliging van de IT.

1. IT-inrichting, ook bij uitbestedingspartners, moet bijdragen aan de pensioenfondsstrategie.
2. 'Smart adapter' van techniek.
3. Continu beoordelen IT-risico's op (IT)-uitbesteding.
4. Maatregelen voor informatiebeveiliging moeten passen binnen de IT Risk Appetite
5. Actualiseren risico controle raamwerk na uitbesteding of aanpassing IT.
6. Het pensioenfonds is compliant en 'in control'.

De IT-principes worden organisatie breed toegepast voor het managen van IT, inclusief IT-uitbesteding, en de besluitvorming.

In de hiernavolgende paragrafen zijn de IT-principes nader beschreven.

3.1 IT-inrichting, ook bij uitbestedingspartners, moet bijdragen aan de pensioenfondsstrategie

De fondsstrategie van het pensioenfonds is leidend. Dat betekent dat de IT, toekomstige IT-projecten en -activiteiten een bijdrage moeten leveren aan de realisatie van de strategie.

Dit principe is als volgt geborgd in de organisatie:

1. Het IT-beleid vormt de basis voor het plannen van aan IT gerelateerde onderwerpen binnen de verschillende (uitbestede) IT-omgevingen.
2. Het (verder) automatiseren van processen is nooit een doelstelling op zichzelf, het dient bij te dragen aan de efficiëntie en effectiviteit van processen.
3. Aanpassingen, zowel geïnitieerd door het pensioenfonds als door uitbestedingspartners, worden systematisch in kaart gebracht om de impact (in tijd, geld, kwaliteit, efficiency en effectiviteit) vast te stellen en te beoordelen of deze passen binnen de fondsstrategie en bijdragen aan de realisatie van de strategie.
4. IT-investeringen worden ook door de uitbestedingspartner voorzien van een 'business case' die de bijdrage aan de realisatie van de fondsstrategie expliciet maakt. De 'business case' wordt uiteindelijk goedgekeurd door het bestuur.
5. De impact van aanpassingen op de IT-risico's wordt zichtbaar gemaakt conform het geldend IRM-beleid en de gevolgen voor de realisatie van de strategie van het fonds worden vastgesteld.

3.2 'Smart adapter' van techniek

Het pensioenfonds wil op het gebied van IT – ook niet via haar uitbestedingspartners – geen onverantwoorde risico's lopen. Daarom kiest het pensioenfonds bij voorkeur voor IT-toepassingen die zich hebben bewezen.

Dit principe is geborgd in de organisatie doordat het pensioenfonds al dan niet via haar uitbestedingspartners:

1. Aandacht heeft voor technologische innovaties en ernaar streeft constant op de hoogte te zijn van IT-toepassingen die de bedrijfsvoering (nog) effectiever en efficiënter kunnen maken.
2. Zoveel mogelijk 'proven technology' toepast binnen de beschikbare technische mogelijkheden.

3.3 Continu beoordelen IT-risico's op (IT)-uitbesteding

De uitbesteding van de IT-omgevingen is een strategische keuze van het pensioenfonds. Er is voor gekozen om gebruik te maken van betrouwbare (IT-)partners en de regie in handen te houden.

Dit principe is geborgd in de organisatie doordat het pensioenfonds:

1. Altijd een risicoanalyse uitvoert voordat uitbesteding van (IT-)diensten plaatsvindt, waarbij minimaal de volgende aspecten worden beoordeeld:
    a. Compliance met bestaande wet- en regelgeving.
    b. Gemaakte afspraken in de overeenkomst met betrekking tot de aangeboden diensten op de relevante IT aspecten.
    c. Stabiliteit en betrouwbaarheid van de serviceprovider.
    d. Locatie waar de diensten worden aangeboden.
    e. Belang, afhankelijkheid en aanpasbaarheid van de IT-diensten en/of IT-componenten.
2. Expliciet aandacht besteedt aan de kwaliteit, prijs en geschiktheid van IT-producten en IT-diensten bij het aangaan van nieuwe uitbestedingsrelaties.
3. Afspraken maakt met uitbestedingspartners over het:
    a. bijhouden van een up-to-date register van (onder)uitbestedingen, inclusief gemaakte afwegingen ten aanzien van materialiteit en bijbehorende risicoanalyses
    b. expliciet melden van elke (onder)uitbesteding bij het pensioenfonds.
4. Right to audit ook voor IT contractueel borgt om te waarborgen dat uitbesteding aan derden geen belemmering vormt voor het kunnen uitoefenen van toezicht.
5. Vooraf beoordeelt in hoeverre de beschikbare assurance verklaringen en overige informatie de DNB Good Practice - Informatiebeveiliging 2019/2020 afdekken (GAP-analyse), voor welke controls en risico's aanvullende afspraken moeten worden gemaakt en of het geheel past binnen de Risk Appetite van het pensioenfonds.
6. Periodiek de aanpasbaarheid, kwaliteit en geschiktheid van IT-producten en -diensten van uitbestedingsrelaties beoordeelt *in relatie* met de overige dienstverlening van de uitbestedingspartner.

Voorgenoemde punten zijn een nadere uitwerking van het uitbestedingsbeleid van het pensioenfonds.

3.4 Maatregelen voor informatiebeveiliging moeten passen binnen de Risk Appetite

Voor het pensioenfonds is het essentieel dat de beschikbaarheid, integriteit, vertrouwelijkheid en aanpasbaarheid van gegevens is gewaarborgd en dat kritieke bedrijfssystemen ongestoord kunnen worden gebruikt.

Dit principe is geborgd in de organisatie doordat het pensioenfonds:

1. De risk appetite op het gebied van informatiebeveiliging heeft gedefinieerd, periodiek toetst en zo nodig opnieuw vaststelt.
2. Vastgestelde richtlijnen en gedragscodes heeft met betrekking tot informatiebeveiliging en cybersecurity en de basiskennis bij medewerkers en bestuur op deze onderwerpen op peil houdt door opleidingsprogramma's.
3. Erop toeziet dat haar uitbestedingspartners in voldoende mate maatregelen hebben getroffen om de beschikbaarheid, integriteit, vertrouwelijkheid en aanpasbaarheid van haar informatie te waarborgen, in overeenstemming met DNB Good Practice - Informatiebeveiliging 2019/2020 en de risk appetite van het pensioenfonds.

4. Afspraken met haar uitbestedingspartners heeft gemaakt over de 'business continuity planning' zodat in geval van calamiteiten de dienstverlening kan worden gewaarborgd (Availability – Beschikbaarheid) op het afgesproken niveau. Hierbij wordt niet alleen aandacht besteed aan systemen, maar ook aan (IT-)ketens.
5. De ontwikkeling van het informatiebeveiligingsbewustzijn en de effectiviteit van beveiligings- en continuïteitsmaatregelen op bestuursniveau volgt en bewaakt waarbij periodiek wordt getoetst of de risico's in overeenstemming met de risk appetite van het pensioenfonds zijn. Indien nodig worden maatregelen getroffen

3.5 Actualiseren risico controle raamwerk na uitbesteding of aanpassing IT

Als wordt besloten tot de uitbesteding, inclusief IT of implementatie van nieuwe IT-producten en/of IT-diensten (bij de uibestedingspartner) wordt altijd onderzocht of dit geen nadelige invloed heeft op de mate waarin de uitbestedingspartner en als gevolg daarvan het pensioenfonds in staat is de risico's in voldoende mate en op adequate wijze te beheersen.

Dit principe is geborgd in de organisatie doordat het pensioenfonds:

1. Voorafgaand aan de uitbesteding, inclusief IT of implementatie van nieuwe IT-producten en/of IT-diensten (bij uitbestedingspartner) altijd een risicoanalyse uitvoert (of de door de uitbestedingspartner uitgevoerde analyse beoordeelt), inclusief een (Data) Privacy Impact Assessment (PIA). Bij de overgang naar een nieuwe uitbestedingspartner is IT ook onderdeel van de risicoanalyse.
2. Wijziging van risico's als gevolg van de aanschaf van nieuwe IT-producten en/of IT-diensten, waaronder de overgang naar een nieuwe uitbestedingspartner, verwerkt in het risico controle raamwerk zodat deze automatisch onderdeel worden van het integrale risicomanagement van het pensioenfonds.

3.6 Het pensioenfonds is compliant en 'in control'

Randvoorwaarde voor de bescherming van de privacy van de deelnemers en een betrouwbare gegevensverwerking zijn een veilige inrichting, gebruik en beheer van de IT-omgeving. Om dit te realiseren volgt het pensioenfonds de geldende richtlijnen voor informatiebeveiliging en relevante wet- en regelgeving. Het is belangrijk voor het pensioenfonds om compliant en 'in control' te zijn.

Dit geldt in dezelfde mate voor het op orde houden van de reputatie van het pensioenfonds. Door voortdurend compliant en 'in control' te zijn laat het pensioenfonds zien dat ze de IT risico's kent en beheerst en de kwaliteit van de IT-functie op het gewenste niveau is en blijft.

Dit principe is geborgd in de organisatie doordat het pensioenfonds:

1. Voor het vormgeven van haar IT control framework en monitoring van IT-risicobeheersing van uitbestedingspartners de DNB Good Practice – Informatiebeveiliging gebruikt.
2. Bij haar uitbestedingspartners controleert dat deze aantoonbaar in control zijn en compliant zijn op het gebied van informatiebeveiliging, cyber security en privacy (norm AVG).
3. Bij haar uitbestedingspartners erop toeziet dat bij het doorvoeren van wijzigingen in de IT-omgeving en informatievoorziening een proces voor wijzigingenbeheer wordt gebruikt, waarbij ook de impact van veranderingen op de IT-risico's en op het IT-beveiligingsniveau wordt getoetst.

4 IT-omgevingen en -organisaties

In dit hoofdstuk behandelen wij op hoofdlijnen de IT-omgevingen waar het pensioenfonds afhankelijk van is voor haar bedrijfsvoering, alsook de wijze waarop assurance wordt afgegeven door de uitbestedingspartijen.

4.1 Bestuursomgeving

Het pensioenfonds maakt voor de bestuursomgeving gebruik van de ICT omgeving van de werkgever Smurfit Kappa. De werkgever maakt hiervoor gebruik van de eigen ICT omgeving om de diensten en services uit te voeren.

Er wordt geen ISAE rapportage opgesteld ten aanzien van deze ICT omgeving, maar er wordt wel jaarlijks een intern statement opgesteld in samenwerking met de accountant van de werkgever. Dit interne statement wordt ter beschikking gesteld aan het pensioenfonds.

4.2 Pensioenbeheer – middelloonregeling

Het pensioenfonds heeft haar pensioenbeheer uitbesteed aan AZL. Diverse applicaties, systemen en componenten[3] ondersteunen de primaire processen van AZL voor de klanten onder de reikwijdte van de Standaard ISAE rapportages. Deze rapportages worden ter beschikking gesteld aan het pensioenfonds.

AZL is – mede met het oog op het nieuwe pensioen stelsel – de inrichting van de IT aan het herzien. Het pensioenfonds volgt deze ontwikkelingen nauwgezet door bijvoorbeeld periodieke overleggen, themabijeenkomsten, assurance diensten et cetera.

4.3 Pensioenbeheer – beschikbare premie regeling

Het pensioenfonds heeft de uitvoering van de beschikbare premie regeling uitbesteed aan ABN AMRO Pension Services (AAPS) en Nationale Nederlanden Investment Partners (NN IP). AAPS en NN IP maken hiervoor gebruik van eigen ICT omgevingen om de diensten en services uit te voeren. Door deze partijen worden ook ISAE rapportages ter beschikking gesteld aan het pensioenfonds.

4.4 Vermogensbeheer

Het pensioenfonds heeft haar vermogensbeheer sinds december 2022 uitbesteed aan NN IP. Daarvoor werd het fiduciaire vermogensbeheer uitgevoerd door PGGM. De IT-omgeving is onderdeel geweest in het selectieproces om te komen tot een nieuwe fiduciaire vermogensbeheerder.

Ook NN IP stelt jaarlijks een ISAE rapportage ter beschikking aan het pensioenfonds.

4.5 Actiepunten ten aanzien van de IT-omgevingen in -organisaties

Voor 2023 zijn de volgende actiepunten gedefinieerd om het IT-beleid verder te verbeteren:

- Inventariseer de datastromen tussen de diverse partijen en personen, en leg vast aan welke eisen deze uitwisseling van informatie dient te voldoen. Maak hierbij onderscheid in vertrouwelijkheid en de wijze waarop de informatie wordt uitgewisseld.
- Beoordeel de ISAE-verklaringen en besteedt daarbij aandacht aan de scope van de verklaring.

[3] De gebruikte applicaties, systemen en componenten worden bijgehouden in een apart applicatieoverzicht door AZL waarin de IT-specificaties, gegevensverwerking, uitvoerder beheersingstaken (logische toegangsbeveiliging, incident- en change management, operationeel beheer) zijn beschreven.

5 Informatiebeveiliging

In deze paragraaf worden de volwassenheidsniveaus getoond van de 15 beheersingsmaatregelen zoals genoemd in de paragraaf 2.3 "Informatiebeveiligingsbeleid". Per beheersingsmaatregel worden de volgende kenmerken vermeld:

- Volwassenheidsniveau 2021
- Volwassenheidsniveau 2022
- Toelichting

Voor een uitgebreide beschrijving van de 15 beheersingsmaatregelen wordt verwezen naar de betreffende DNB-publicatie.

5.1 Volwassenheidsniveaus beheersingsmaatregelen informatiebeveiliging

Beheersingsmaatregel 1 – Governance – 1.1 Information Security Plan

- Volwassenheidsniveau 2021 2
- Volwassenheidsniveau 2022 3
- Toelichting
    - "Het pensioenfonds heeft in 2021 een "Beleid inzake Informatie en Technologie" (IT-beleid) ontwikkeld. Dit beleid is momenteel nog in ontwikkeling en wordt door het bestuur ook beschouwd als "work in progress". Het volwassenheidsniveau is van 2 naar 3 gegaan."

Beheersingsmaatregel 2 – Risk management cycle – 4.1 Risk Management framework

- Volwassenheidsniveau 2021 2
- Volwassenheidsniveau 2022 3
- Toelichting
    - "Het volwassenheidsniveau is van 2 naar 3 gegaan; in 2023 zal dit niveau worden verhoogd naar een 4 voor dit onderdeel."

Beheersingsmaatregel 3 – Risk management cycle – 4.2 Risk assessment

- Volwassenheidsniveau 2021 2
- Volwassenheidsniveau 2022 3
- Toelichting
    - "Het volwassenheidsniveau is van 2 naar 3 gegaan; in 2023 zal dit niveau worden verhoogd naar een 4 voor dit onderdeel."

Beheersingsmaatregel 4 – Risk management cycle – 4.3 Maintenance and monitoring of a risk action plan

- Volwassenheidsniveau 2021 2
- Volwassenheidsniveau 2022 3
- Toelichting
    - "Het volwassenheidsniveau is van 2 naar 3 gegaan; in 2023 zal dit niveau worden verhoogd naar een 4 voor dit onderdeel."

Beheersingsmaatregel 5 – Organisation – 7.1 Segregation of duties

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 6 – People – 9.3 Employee awareness

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 7 – Processes – 11.1 IT Continuity plans

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 8 – Processes – 11.2 Testing of the IT Continuity plan

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 9 – Outsourcing – 14.1 Monitoring and reporting of Service Level Achievements

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 10 – Outsourcing – 14.2 Supplier risk management

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 11 – Processes – 15.1 Security incident definition

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 12 – Processes – 15.2 Incident escalation

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 13 – Outsourcing – 16.3 Internal control at third parties

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 14 – Processes – 17.1 Identity & Access Management

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

Beheersingsmaatregel 15 – Processes – 17.2 User account management

- Volwassenheidsniveau 2021 3
- Volwassenheidsniveau 2022 3

5.2 Actiepunten ten aanzien van informatiebeveiliging

In 2022 is er begonnen met het verbeteren van het volwassenheidsniveau van de hiervoor genoemde beheersingsmaatregelen 2, 3 en 4. In hoofdstuk 7 "Bijlage beheersingsmaatregelen" is een integrale weergave van de betreffende beheersingsmaatregelen opgenomen vanuit de "Good Practice Informatiebeveiliging 2019/2020" van DNB. Het pensioenfonds streeft er naar om het volwassenheidsniveau 4 te bereiken in de eerste helft van 2023 en zal daarvoor de komende tijd de benodigde acties ondernemen.

Smurfit Kappa
Pensioenfonds

6 Bijlage BIVA-classificatie

BIVA	Classificatie	Criteria
Beschikbaarheid Availability *Het binnen een redelijke tijdstermijn kunnen raadplegen of wijzigen van gegevens wanneer dit bij het uitvoeren van werkzaamheden nodig is, ofwel het draaiend houden van bestaande processen en het herstellen van verstoringen, waarbij de negatieve gevolgen van incidenten (uitval, beveiligingslekken) worden beperkt.*	**0 - Niet nodig**	Het verlies van beschikbaarheid leidt niet tot interne negatieve / kritische berichtgeving (inclusief uitvoerders). Het niveau van dienstverlening van het fonds wordt beïnvloed, echter geen gevolgen voor de tevredenheid van deelnemers. Eventuele herstelkosten zijn laag en de dekkingsgraad van het fonds wordt niet negatief beïnvloed.
	1 - Belangrijk	Het verlies van beschikbaarheid leidt tot negatieve / kritische berichtgeving (inclusief uitvoerders). Het niveau van dienstverlening van het fonds wordt beïnvloed met als gevolg een beperkte daling van de tevredenheid van deelnemers. Eventuele herstelkosten en/of daling van de dekkingsgraad is beperkt.
	2 - Noodzakelijk	Het verlies van beschikbaarheid leidt tot negatieve publiciteit richting de pensioensector en/of negatieve reacties vanuit DNB/AFM. Het niveau van dienstverlening van het fonds wordt beïnvloed met als gevolg een behoorlijke daling van de tevredenheid van deelnemers. Eventuele herstelkosten en/of daling van de dekkingsgraad is aanzienlijk.
	3 - Essentieel	Het verlies van beschikbaarheid leidt tot negatieve publiciteit richting pensioensector en/of structureel negatieve reacties vanuit DNB/AFM. Het niveau van dienstverlening van het fonds wordt beïnvloed met als gevolg een grote daling van de tevredenheid van deelnemers. Eventuele herstelkosten en/of daling van de dekkingsgraad is zeer groot.
Integriteit Accuracy *Het in overeenstemming zijn van gegevens met het afgebeelde deel van de realiteit en dat niets ten onrechte is achtergehouden of verdwenen, i.c. de aspecten juistheid, volledigheid en tijdigheid, ofwel het opleveren van juiste, tijdige en volledige informatie aan alle relevante belanghebbenden.*	**0 - Niet Zeker**	Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
	1 - Beschermd	De informatie of het bedrijfsproces heeft geen directe hinder van (integriteits)fouten. Een basisniveau van bescherming is noodzakelijk. Schending van deze classificatie kan enige financiële schade en/of reputatieschade (werkgevers, deelnemers, toezichthouder) tot gevolg hebben.
	2 - Hoog	De informatie of het bedrijfsproces staat zeer weinig (integriteits)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze financiële schade en/of reputatieschade (werkgevers, deelnemers, toezichthouder) tot gevolg hebben.
	3 - Absoluut	De informatie of het bedrijfsproces staat geen (integriteits)fouten toe. Schending van integriteit kan (zeer) grote financiële schade en/of reputatieschade (werkgevers, deelnemers, toezichthouder) tot gevolg hebben.
Vertrouwelijkheid Access *De beperking van de bevoegdheid en mogelijkheid tot uitlezen, kopiëren of kennisnemen van informatie en van andere systeemcomponenten tot een gedefinieerde groep van gerechtigden, ofwel het waarborgen dat de juiste mensen toegang hebben tot de juiste informatie en anderen niet.*	**0 - Openbaar**	Het openbaar maken van de informatie kan het fonds en/of haar deelnemers en overige betrokkenen op geen enkele wijze schaden.
	1 - Bedrijfsvertrouwelijk	Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Ongeautoriseerde toegang tot informatie kan het fonds en/of haar deelnemers en overige betrokkenen enige schade toebrengen en/of het imago (reputatie) schaden.
	2 - Vertrouwelijk	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers, waaronder persoonsgegevens. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Ongeautoriseerde toegang tot informatie kan serieuze schade toebrengen aan de bedrijfsvoering en/of het imago (reputatie) van het fonds en/of haar deelnemers en overige betrokkenen.
	3 - Geheim	Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde, waaronder bijzondere persoonsgegevens. Ongeautoriseerde toegang tot informatie kan zeer grote (vrijwel niet te repareren) schade toebrengen aan de bedrijfsvoering en/of het imago (reputatie) van het fonds en/of haar deelnemers en overige betrokkenen.
Aanpasbaarheid Agility *Verandering in bedrijfsvoering die benodigd kan zijn als gevolg van interne en externe oorzaken, zoals acquisities of nieuwe regelingen, tegen acceptabele kosten en acceptabele risico's.*	**0 - Standaard**	Dit proces en/of applicatie die dit proces ondersteunt worden als standaard binnen de markt beschouwd. Dit proces is evengoed onder te brengen bij een andere dienstverlener en/of andere applicatie. De behoefte aan aanpasbaarheid of maatregelen daarvoor is laag.
	1 - Onderscheidend	Dit proces en/of applicatie die dit proces ondersteunt is onderscheidend voor het fonds en/of de uitvoerder ten opzichte van andere fondsen en/of uitvoerders. Dit is ook het geval indien sprake is van maatwerk door de uitvoerder voor het fonds. De behoefte aan aanpasbaarheid of maatregelen daarvoor is hoog.
	2 - Innovatief	Voor dit proces en/of applicatie die dit proces ondersteunt wordt verwacht dat op korte of middellange termijn sprake is van veranderingen als gevolg van ontwikkelingen in de markt (veranderingen wet- en regelgeving, veranderende marktomstandigheden) en/of als gevolg van veranderingen in behoefte van het fonds t.a.v. de dienstverlening. De behoefte aan aanpasbaarheid of maatregelen daarvoor is hoog.
	3 - Compliance	Dit proces en/of applicatie die dit proces ondersteunt is onderhevig aan het voldoen aan verplichtingen vanuit wet- en regelgeving waar het pensioenfonds aan moet voldoen. De behoefte aan aanpasbaarheid of maatregelen daarvoor is cruciaal.

7 Bijlage Volwassenheidsniveaus

Niveau:	Definitie van het volwassenheidsniveau	Criteria ter verduidelijking
0	**Niet bestaand** – Aan deze beheersingsmaatregel is geen aandacht besteed.	
1	**Initieel** – De beheersingsmaatregel is (gedeeltelijk) gedefinieerd maar wordt op inconsistente wijze uitgevoerd. Er is een grote afhankelijkheid van individuen bij de uitvoering van de beheersingsmaatregel.	■ Geen of beperkte beheersingsmaatregel geïmplementeerd. ■ Niet of ad-hoc uitgevoerd. ■ Niet /deels gedocumenteerd. ■ Wijze van uitvoering afhankelijk van individu (niet gestandaardiseerd)
2	**Herhaalbaar maar informeel** – De beheersingsmaatregel is aanwezig en wordt op consistente en gestructureerde, maar op informele wijze uitgevoerd.	■ De uitvoering van de beheersingsmaatregel is gebaseerd op een informele maar wel gestandaardiseerde werkwijze. Deze werkwijze is niet volledig gedocumenteerd.
3	**Gedefinieerd** – De opzet van de beheersingsmaatregel is gedocumenteerd en wordt op gestructureerde en geformaliseerde wijze uitgevoerd. De vereiste effectiviteit van de beheersingsmaatregel is aantoonbaar en wordt getoetst.	■ Beheersingsmaatregel is gedefinieerd o.b.v. risico assessment. ■ Gedocumenteerd en geformaliseerd. ■ Verantwoordelijkheden en taken zijn eenduidig toegewezen. ■ Opzet, bestaan en effectieve werking zijn aantoonbaar. ■ Effectieve werking van controls wordt periodiek getoetst. ■ De toetsing vindt risicogebaseerd plaats en toont aan dat de control effectief is over een langere periode (>6 maanden). ■ De uitvoering van de beheersingsmaatregel wordt aan het management gerapporteerd.
4	**Beheerst en meetbaar** – De effectiviteit van de beheersingsmaatregel wordt periodiek geëvalueerd. Daar waar nodig wordt de beheersingsmaatregel verbeterd of vervangen door andere beheersingsmaatregel(en). De evaluatie wordt vastgelegd.	Criteria voor niveau 3 plus de volgende onderscheidende criteria: ■ Periodieke (control) evaluatie en opvolging vindt plaats. ■ Evaluatie is gedocumenteerd. ■ Taken en verantwoordelijkheden voor het evalueren zijn geformaliseerd. ■ Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de instelling en is minimaal jaarlijks. ■ In de evaluatie worden (operationele) incidenten meegenomen. ■ De uitkomsten van de evaluatie wordt aan het management gerapporteerd.
5	**Continu verbeteren** – De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering van de effectiviteit van de maatregelen. Hierbij wordt gebruik gemaakt van externe data en benchmarking. Medewerkers zijn pro-actief betrokken bij de verbetering van de beheersingsmaatregelen	Criteria voor niveau 4 plus de volgende onderscheidende criteria: ■ Continu evalueren van de beheersingsmaatregelen om de effectiviteit van beheersmaatregelen voortdurend te verbeteren. ■ Gebruik makend van resultaten uit self-assessments, gap en root cause analyses. ■ De getroffen beheersingsmaatregelen worden gebenchmarkt op basis van externe data en zijn 'Best Practice' in vergelijking met andere organisaties.

8 Bijlage Beheersingsmaatregelen

4.1 IT Risk Management framework

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling ontwikkelt en onderhoudt een IT risk management framework.
- Het IT-risk management framework sluit aan op het risk management raamwerk van de instelling.
- De instelling adresseert risico's op het gebied van informatiebeveiliging en cybersecurity in het IT-risk management raamwerk.
- De risicotoleranties ten aanzien van informatiebeveiliging en cybersecurity zijn bepaald en vastgelegd.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling ervoor verantwoordelijk dat (IT) risico's met betrekking tot de uitbestede activiteiten/systemen zijn beheerst. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de beheersing van (IT) risico's conform het beleid en risicotoleranties van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden.

Voorbeelden hierbij zijn:

- De instelling hanteert in haar IT-risk management framework eenduidige definities voor informatiebeveiliging en cybersecurity; deze zijn ontleend aan markt standaarden zoals NIST CF, ISO 27000 en CobiT en worden consistent binnen alle documenten en rapportages in het IT risk management framework gehanteerd.
- Actuele cyberdreigingen zoals malware, cryptoware, DDoS aanvallen en phishing maken deel uit van het risk management raamwerk.
- In de keten van uitbestede diensten werken partijen in overeenstemming met het IT risk management framework van de instelling.
- De instelling beoordeelt periodiek in hoeverre partijen aan wie activiteiten/systemen zijn uitbesteed, werken in overeenstemming met het IT-risk management framework van de instelling.
- De instelling verkrijgt op grond van interne rapportages en rapportages van dienstverleners een integraal beeld van de beheersing van de risico's op het gebied van informatiebeveiliging en cybersecurity.

4.2 Risk assessment

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling voert periodiek IT-risicoanalyses uit op basis van kwalitatieve en kwantitatieve methoden.
- De kans en impact van inherente risico's op het gebied van informatiebeveiliging en van restrisico's worden hierbij in kaart te gebracht.
- Actuele cyberdreigingen worden meegenomen in de IT-risicoanalyses.
- Restrisico's worden ter (tijdelijke) acceptatie voorgelegd op het management niveau dat past bij de aard en omvang van het restrisico.
- Geaccepteerde restrisico's worden periodiek opnieuw geëvalueerd en opnieuw ter acceptatie aangeboden wanneer zij buiten de risicotolerantie van de instelling vallen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de analyse van risico's op het gebied van informatiebeveiliging en cybersecurity met betrekking tot de uitbestede activiteiten/systemen. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het uitvoeren van risicoanalyses conform het risicoraamwerk van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling voert jaarlijks een IT-risicoanalyse uit met alle voor de analyse relevante stakeholders binnen de instelling. Op basis hiervan worden actuele cyberdreigingen gewogen en geprioriteerd.
- De instelling brengt haar 'kroonjuwelen' in kaart, evalueert deze periodiek en relateert deze aan actuele cyberdreigingen en getroffen beheersingsmaatregelen. Daar waar nodig treft de instelling aanvullende beheersingsmaatregelen. Maatregelen die niet (meer) effectief werken worden aangepast, vervangen door andere maatregelen of uitgefaseerd.
- De instelling beoordeelt periodiek de risicoanalyses van partijen in de keten op relevantie en stelt vast in hoeverre deze voldoen aan de eisen van de instelling.
- De gewogen en geprioriteerde risico's op het gebied van informatiebeveiliging en cyberdreigingen worden door de instelling geadresseerd en beperkt naar een acceptabel niveau dat past bij de risicotolerantie van de instelling.

4.3 Maintenance and monitoring of a risk action plan

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling stelt voor niet geaccepteerde risico's een 'risk action plan' op dat verdere uitwerking geeft aan de risk response.
- In dit risk action plan zijn onder meer rest risico's en compenserende maatregelen opgenomen.
- Restrisico's op het gebied van cybersecurity zijn onderdeel van het 'risk action plan' van de instelling.
- Het risk action plan wordt geaccordeerd door het management niveau dat past bij de aard en omvang van het restrisico's.
- Het risk action plan is actueel; opvolging van de acties wordt bewaakt.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat niet geaccepteerde restrisico's op het gebied van informatiebeveiliging en cybersecurity met betrekking tot de uitbestede activiteiten/systemen, worden gemitigeerd. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het uitvoeren van risicoanalyses conform het risicoraamwerk van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft voor actuele cyberdreigingen expliciet gemaakt welke risico's formeel worden geaccepteerd en voor welke restrisico's aanvullende maatregelen noodzakelijk zijn.
- Beoogde acties op het gebied van cybersecurity en de status van uitvoering zijn beschreven in het risk action plan. Afwijkingen ten opzichte van de oorspronkelijke planning worden periodiek gerapporteerd aan het senior management.

De instelling laat het lijnmanagement jaarlijks een 'in control' statement (ICS) opstellen.

- De instelling beoordeelt op periodieke basis de risk action plannen van dienstverleners in de keten op relevantie en stelt vast dat deze voldoen aan de eisen van de instelling. Bij afwijkingen maakt de instelling afspraken met die partijen om het risico te beperken naar een acceptabel niveau dat past binnen de risicotolerantie van de instelling.