Stichting Pensioenfonds Thales Nederland

Beleidsnotitie ICT, informatievoorziening en cybersecurity

2025-2027

Inhoud

1 Management Summary

De doelstelling van de Beleidsnotitie ICT, informatievoorziening en cybersecurity (hierna: Beleidsnotitie ICT) is het handhaven van de beschikbaarheid, integriteit en vertrouwelijkheid (met inbegrip van authenticiteit, toerekenbaarheid en controleerbaarheid) en de veerkracht van de informatiesystemen en gegevens van het fonds.

Dit beleid van het fonds en de wijze waarop het zijn beleid auditeert, is gebaseerd op Verordening (EU) 2022/2554 inzake betreffende digitale operationele weerbaarheid voor de financiële sector (DORA) inclusief de gedelegeerde technische reguleringsnormen, en op de Algemene Verordening Gegevensbescherming (hierna: AVG). Daarnaast volgt dit beleid ook de meest recente richtlijnen van DNB en van de Pensioenfederatie.

In deze notitie wordt de huidige ICT-inrichting van het fonds beschreven. Ook wordt ingegaan op de gestelde eisen aan de ICT- en informatievoorziening en de wijze waarop deze eisen worden gerealiseerd. De structuur van deze beleidsnotitie is gebaseerd op vereisten die DORA stelt aan het ICT-risicobeheerkader van het fonds. Het fonds beheert haar eigen ICT-risico's door maatregelen op het gebied van i) governance en organisatie ii) het voeren van een kader voor ICT-risicobeheer iii) het opstellen en (laten) uitvoeren van een risicogebaseerd testprogramma en iv) de beheersing van ICT-risico's gerelateerd aan aanbieders van ICT-diensten.

Het beleid richt zich niet alleen richt op de ICT-omgeving van het fonds, maar richt zich nadrukkelijk ook op de ICT-omgeving van de primaire uitvoerders van het fonds.

Dit beleid wordt ten minste jaarlijks gereviewd om ervoor te zorgen dat het effectief, relevant en consistent blijft met de informatiebeveiligingsdoelstellingen en dreigingslandschap van het fonds. Dit beleid wordt indien nodig bijgewerkt om wijzigingen in regelgeving, technologische vooruitgang of de veranderende behoeften van het fonds weer te geven. Doorlopende verbetering van het ICT- en informatievoorzieningsbeleid heeft de aandacht van het bestuur.

2 Scope

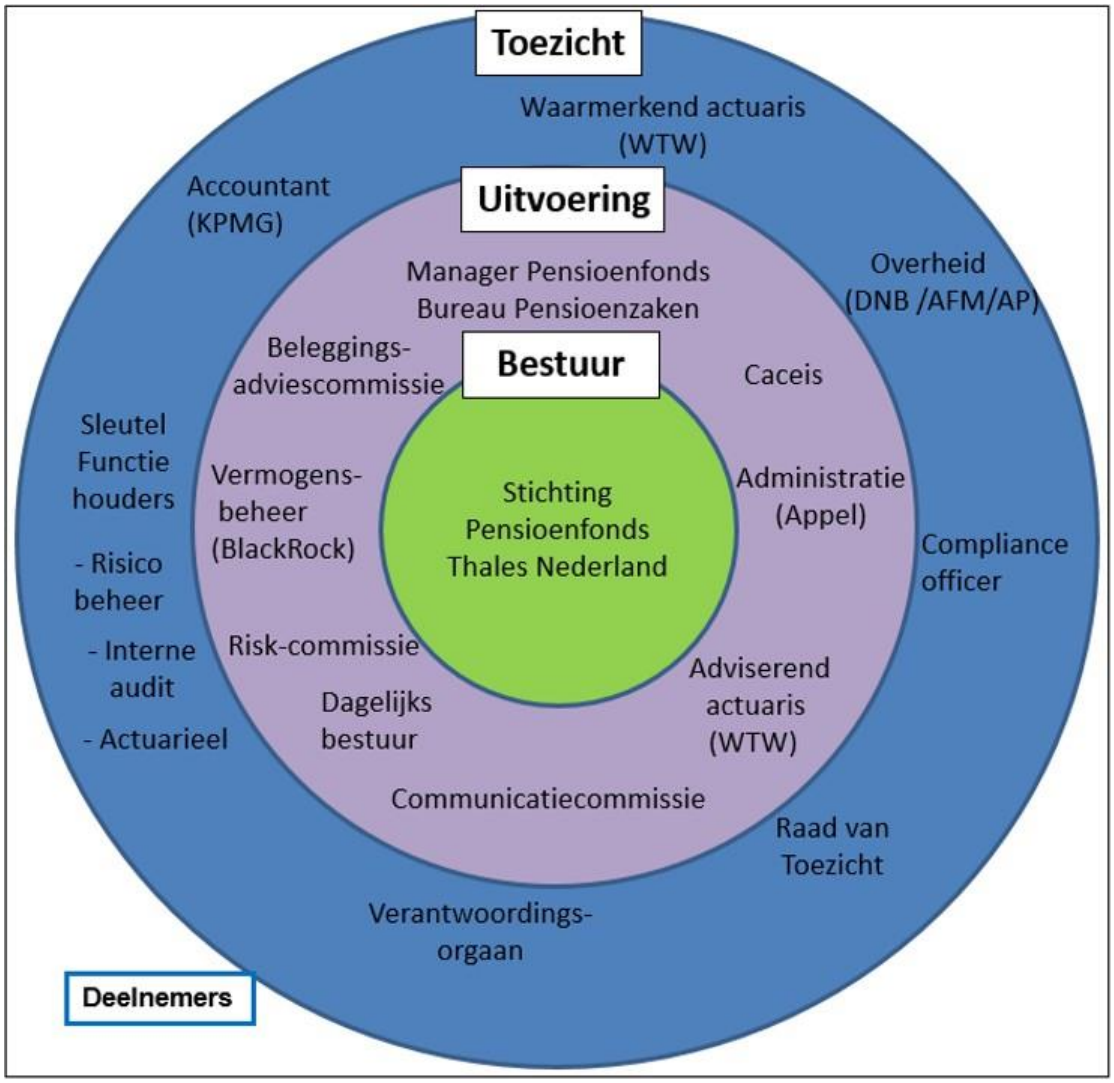
Het fonds beheerst haar eigen ICT-risico's door onder meer:

- Een gedegen, voor het fonds passende governance en organisatie;
- Het voeren van een kader voor ICT-risicobeheer;
- Het opstellen en (laten) uitvoeren van een risicogebaseerd testprogramma en
- De beheersing van ICT-risico's gerelateerd aan aanbieders van ICT-diensten.

Het fonds toont periodiek aan dat zij door middel van een geformaliseerd kader voor risicobeheer voldoet aan haar wettelijke verplichtingen ten aanzien van digitale weerbaarheid.

2.1 Overzicht van de betrokken partijen bij het fonds

Deze Beleidsnotitie ICT vormt een aanvullend kader om ICT-risico's van het fonds te beheersen. De hieronder weergegeven partijen hebben een actieve rol in dan wel belang bij een toereikende uitvoering van het ICT-risicobeheer.



2.2 Algemene beschrijving van het auditeringsproces van de uitbestede ICT

Bij het fonds zijn een aantal partijen betrokken zoals hierboven weergegeven. De uitvoeringspartijen in “de tweede schil om het fonds” hebben te maken met ICT- en informatievoorziening. Op deze partijen wordt toezicht gehouden door de toezichthouders in “de derde schil om het fonds”. Het voortdurend beheersproces van de ICT-toepassingen en informatievoorzieningen ”loopt door de schillen” van bestuur, naar uitvoering en vervolgens naar toezicht en weer terug.

Het primaire proces van het fonds heeft betrekking op de uitvoering van de pensioenregeling en het vermogensbeheer. Het primaire proces wordt vormgegeven door onder andere de administratieve organisatie rondom dit primaire proces. Dit gaat kortgezegd over wie wat doet en hoe de functiescheiding geregeld is. ICT- en informatievoorziening dient de uitvoering van het primaire proces en de administratieve organisatie te ondersteunen. In deze beleidsnotitie wordt door het fonds weergegeven aan welke eisen de ICT-toepassingen en dataverwerking in het primaire proces moeten voldoen. Vervolgens geeft het fonds weer hoe zij monitort dat de uitvoeringspartijen die ICT- toepassingen gebruiken en data verwerken voor het fonds aan deze gestelde eisen voldoen.

Dat doet het fonds door de gestelde ICT-eisen specifiek en meetbaar te maken, deze contractueel overeen te komen en op te nemen in de uitbestedingsovereenkomst per uitbestedingspartij. Aanvullend kunnen in service level agreement ‘s (hierna: SLA ‘s) nadere afspraken gemaakt worden over de contractueel overeengekomen dienstverlening. Daarnaast zullen relevante processen en de daarbij gestelde eisen zoveel mogelijk binnen de scope van audits door onafhankelijke accountants gebracht worden (zoals bijvoorbeeld ISAE 3402 en/of ISAE 3000 audits). Op deze wijze kan een effectieve control bewerkstelligd worden. Als het bestuur dat wenselijk acht, kunnen steekproeven worden gedaan of de SLA’s goed genoeg werken. De input voor de SLA’s bestaat uit generiek gestelde eisen voor de gehanteerde tools en specifiek gestelde eisen voor de inhoud per uitvoeringspartij. In het navolgende gaat het fonds in op de gestelde eisen. De eisen rondom uitbesteding van ICT-diensten is onder meer verder uitgewerkt in het hoofdstuk over Eisen bij uitbesteding aan ICT-en informatievoorzieningen door het fonds.

2.3 ICT-diensten van de betrokken partijen bij het fonds

Het fonds zelf heeft geen specifieke ICT-diensten[1] in eigen beheer. Wel maakt het fonds gebruik van ICT-diensten van verscheidene derde aanbieders (‘ICT-dienstverleners’), conform DORA. De ICT-risico’s van het fonds worden daarom geacht zich met name te kunnen materialiseren bij deze ICT-dienstverleners. Het fonds beoogt passende maatregelen ter beheersing van deze ICT-derdenrisico’s te treffen. De betreffende maatregelen hangen samen met hoe de dienstverlening van de derde partijen gekwalificeerd wordt. Dit is hieronder beschreven.

Kwalificatie	Toelichting	Betrokken partij
Uitbestedingsrelatie (Pensioenwet)	Deze Beleidsnotitie heeft als voornaamste focus het pensioenbeheer en vermogensbeheer. De uitvoering van deze activiteiten is gedelegeerd aan externe dienstverleners. Op deze uitbestedingsrelaties zijn de uitgangspunten en criteria vanuit het uitbestedingsbeleid van toepassing. Deze uitbestedingsrelaties zijn daarnaast ook in scope van	

[1] “ICT-diensten”: Digitale en gegevensdiensten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten

	deze Beleidsnotitie, tenzij rondom specifieke ICT-maatregelen beschreven is dat deze maatregelen alleen van toepassing zijn (kritieke) ICT-dienstverleners	
ICT-dienstverleners (DORA)	Het fonds maakt ook gebruik van ICT-diensten van verscheidene derde aanbieders ('ICT-dienstverleners'). Daarbij maakt het fonds een onderscheid tussen ICT-dienstverleners die kwalificeren als: - ICT-dienstverleners van ICT-diensten die kritieke of belangrijke functies ondersteunen (zogeheten 'kritieke ICT-dienstverleners'); en - Overige ICT-dienstverleners. Alle ICT-dienstverleners zijn in scope van deze Beleidsnotitie ICT, waarbij geduid wordt welke ICT-maatregelen alleen van toepassing zijn op kritieke ICT-dienstverleners	Thales Nederland (niet kritiek)
Uitbestedingsrelaties die ook als ICT-dienstverlener kwalificeren	Uitbestedingsrelaties die in hun dienstverlening aan het fonds ook diensten verlenen die als (kritieke) ICT-diensten kwalificeren, kwalificeren zowel als uitbestedingsrelatie en als (kritieke) ICT-dienstverlener. Op deze partijen zijn de uitgangspunten en criteria uit het uitbestedingsbeleid van toepassing, inclusief de specifieke, aanvullende bepalingen ten aanzien risicobeheersing rondom de (kritieke) ICT-diensten die zij verlenen.	Appel (kritiek) BlackRock (kritiek) Caceis (kritiek)

Overzicht van ICT-dienstverleners
Voor het volledige overzicht van alle derde aanbieders van ICT-diensten die (uitbestede) functies van het fonds ondersteunen, wordt verwezen naar het Informatieregister. Zie ook sectie Informatieregister ICT-diensten.

3 De strategie van het fonds

De strategie van het fonds, voortkomend uit de missie en visie van het fonds luidt: SPTN zet in op continuïteit. Het bestuur heeft continue aandacht voor de communicatie en dialoog met alle deelnemers, evenals het beleggingsbeleid en de resultaten daarvan. Hiervoor heeft het een communicatie-, een integraal risicomanagement- en een beleggingsadviescommissie ingesteld, evenals een dagelijks bestuur. De effectiviteit van het beleid wordt voortdurend gemonitord en bekeken door het bestuur, in samenwerking met het verantwoordingsorgaan en de Raad van Toezicht.

4 Governance

Het fonds beschikt over een intern governance- en controlekader dat een doeltreffend en prudent beheer van het ICT-risico waarborgt om een hoog niveau van digitale operationele weerbaarheid te verkrijgen.

Het bestuur draagt de eindverantwoordelijkheid voor het ICT-risicobeheerkader. Dit betekent ook dat het bestuur de strategie voor digitale operationele weerbaarheid bepaalt, eindverantwoordelijk is voor de jaarlijkse ICT-risicoanalyse, alle beleidsuitingen vaststelt met betrekking tot het ICT-risicobeheer, het kader voor ICT-risicobeheer jaarlijks goedkeurt en toezicht houdt op de adequate uitvoering ervan.

De bestuursleden onderhouden actief voldoende kennis en vaardigheden om ICT-risico's en de gevolgen daarvan voor de verrichtingen van het fonds te begrijpen en te beoordelen. De leden volgen in dit kader specifieke opleidingen die in verhouding staan tot de te beheren ICT-risico's van het fonds en tot hun specifieke ICT-gerelateerde verantwoordelijkheden. Daarbij wordt ook geborgd dat er doorlopend toereikende kennis, ervaring en vaardigheden aanwezig is binnen het fonds om toezicht te houden op de overeenkomsten met ICT-dienstverleners.

De richtlijnen in het beleid worden door het bestuur gecommuniceerd naar alle relevante uitbestedingsrelaties en kritieke ICT-dienstverleners van het fonds. Eventuele wijzigingen in deze beleidsnotitie worden voorafgaand aan de definitieve goedkeuring beoordeeld op hun uitvoerbaarheid, indien nodig in overleg met de uitbestedingsrelaties en kritieke ICT-dienstverleners.

De rollen, taken en verantwoordelijkheden ten aanzien van het ICT-risicobeheerkader zijn in onderstaand RACI-schema weergegeven. RACI staat voor 'Responsible', 'Accountable', 'Consulted' en 'Informed'.

Deze rollen zijn verdeeld tussen het Bestuur ('B'), het Dagelijks Bestuur ('DB'), het Bureau Pensioenzaken ('BPz'), de Risicomanager ('RM') en de Sleutelfunctiehouder Risicobeheer ('SHF RB').

Omschrijving	**B**	**DB**	**BPz**	**RM**	**SFH -RB**
Vaststelling Beleidsnotitie ICT (incl. strategie)	A	R	C	I	C
Uitvoering en monitoring Beleidsnotitie ICT (incl. taakstelling)	A	R	C	I	C
Vaststellen budget t.a.v. digitale operationele weerbaarheid	A	R	C		
Melden en rapporteren ICT-gerelateerde incidenten	A	R	C	I	I
Monitoren risicoblootstelling t.a.v. ICT-dienstverleners	A	R	C	I	I
Evaluatie tests Bedrijfscontinuïteitsplan	A	R	C	I	I
Evaluatie ICT-risicobeheerkader	A	R	C	I	C
Meldingskanalen	A	R	R	R	R

5 Uitgangspunten ICT-risicobeheer

Algemeen geformuleerd verlangt het fonds voor de uitvoering van het primaire proces een betrouwbare, efficiënte en flexibele informatievoorziening waarbij de operationele stabiliteit continu geborgd is, waarbij wordt voldaan aan wet- en regelgeving en waarbij aan de hand van de geïnventariseerde en geanalyseerde ICT-risico's deze risico's zoveel mogelijk prioriteitsafhankelijk gemitigeerd worden.

De uitgangspunten rondom ICT- en informatievoorziening zoals hieronder opgesomd, worden contractueel nader vastgelegd in SLA's per uitvoeringsorganisatie. Daarbij moet ook rekening worden gehouden met de uitkomsten van de ICT-risicoanalyse.

1. Kantoorautomatisering bij de uitvoeringspartijen
    - De ICT-toepassingen en dataverwerking bij de uitvoeringspartijen en de administratie en organisatie moet zodanig worden ingericht dat aan de verlangde eisen aan data hierna onder punt 2 tot en met 5 wordt voldaan.
2. Deelnemersdata
    - De deelnemersdata dient juist en volledig te zijn.
    - De beschikbaarheid en vertrouwelijkheid dienen te zijn gewaarborgd.

3. Pensioendata
    - Bij aanpassing van systemen of conversie van data dienen rechten/aanspraken/kapitaal van deelnemers op de juiste en volledige wijze in stand te blijven. De rechten/aanspraken/kapitaal dienen reproduceerbaar te zijn.
    - De beschikbaarheid en vertrouwelijkheid dienen te zijn gewaarborgd.
4. Data beleggingsportefeuille
    - De juistheid en volledigheid van transacties dient altijd reproduceerbaar te zijn.
    - Door het niet beschikbaar zijn van systemen of verlies van data mag geen waarde en bezit verloren gaan nog de gegevens omtrent waarde en bezit.
    - De vertrouwelijkheid dient te zijn gewaarborgd.
5. Data inzake middelen op de bankrekening
    - De bescherming van waarden omvattende onder andere betaling voor legitieme diensten en legitieme uitkering van pensioengelden.
6. Besluitvorming en monitoring door bestuur
    - Juiste en tijdige besluitvorming door tijdige, juiste en volledige informatie.

6 Eisen bij uitbesteding aan ICT- en informatievoorziening door het fonds

6.1 Uitgangspunten voor uitbesteding van ICT-diensten

De volgende uitgangspunten bij uitbesteding van ICT-diensten worden door het fonds gehanteerd.

- Het bestuur monitort de uitbestedingsrelaties en ICT-dienstverleners zoals gedefinieerd onder hoofdstuk 2.3 (hierna: uitvoeringspartijen). Belangrijk is dat dit toezicht en de monitoring zich ook uitstrekken tot sub-uitbestedingsrelaties. Hiervan is sprake wanneer een uitbestedingsrelatie of ICT-dienstverlener zelf gebruikmaakt van ICT-diensten van externe ICT-dienstverleners voor de dienstverlening aan het fonds.
- Het Dagelijks Bestuur heeft tot taak het monitoren van de risicoblootstelling ten aanzien van ICT-dienstverleners en de relevante documentatie. Hierbij wordt het Dagelijks Bestuur ondersteund door Bureau Pensioenzaken.
- De uitvoeringspartijen hebben een eigen ICT-beleid mede gebaseerd op de door het fonds aan ICT verlangde eisen, de benoemde ICT- risico's en gebaseerd op actuele marktconforme standaarden die voldoen aan wet- en regelgeving.
- Het fonds verlangt van de uitvoeringspartijen dat eventuele risico's door middel van een risicoanalyse worden vertaald naar operationele maatregelen. Vanuit integraal risico management gezien verlangt het fonds dat de risico's over de gehele uitbestede keten inzichtelijk zijn.
- Bij het voornemen tot uitbesteden van een ICT-dienst door het fonds wordt de algemene selectieprocedure conform het Uitbestedingsbeleid van het fonds uitgevoerd. Vervolgens worden de specifieke bepalingen rondom de selectieprocedure en risicoanalyse gevolgd zoals in dit ICT-beleid uiteengezet, gevolgd door het sluiten van de overeenkomst met de ICT-dienstverlener (inclusief Service Level Agreement).
- De inrichting en realisatie van de benodigde ICT-middelen zijn overgedragen aan de uitvoeringspartijen. De afspraken over deze dienstverlening worden overeengekomen in een contract per uitvoeringspartij zodanig dat de uitbestede- en bedrijfsprocessen van het fonds gewaarborgd zijn.
- Het fonds verlangt van haar uitvoeringspartijen met uitzondering van niet-kritieke ICT-dienstverleners een ISAE 3402 en/of ISAE 3000 rapportage welke aantoont dat de uitbestede processen beheerst zijn. Zowel de financial als de ICT controls moeten beschreven zijn.
- De uitvoeringspartijen beschikken over risicomanagement beleid, informatiebeveiligings-, cybersecuritybeleid en business continuïteitsbeleid. De uitvoeringspartijen zijn verantwoordelijk voor het inrichten van de specifieke controls op basis waarvan de beheersing kan worden getoetst.

Hierbij wordt rekening gehouden met de specifieke eisen vanuit wet- en regelgeving en toezichthouders. De wijze waarop het risicobeeld tot stand komt en de rapportage hierover aan het fonds wordt in onderling overleg bepaald waarbij het fonds zoveel mogelijk aansluit op de reguliere processen en rapportages vanuit de uitvoeringspartijen.
- Alle uitvoeringspartijen moeten voldoen aan de wet- en regelgeving die voortvloeit uit DORA en uit de Algemene Verordening Gegevensbescherming (AVG).

6.2 Due diligence op ICT-dienstverleners

Het bestuur van het fonds voert tijdens de selectieprocedure een risicogebaseerd due-diligence onderzoek uit op de ICT-dienstverlener. Dit onderzoek stelt vast of de beoogde partij voldoet aan de normen die het fonds stelt aan ICT-dienstverleners. De algemene beoordelingscriteria rondom alle ICT-dienstverleners alsook de aanvullende beoordelingscriteria ten aanzien van kritieke ICT-dienstverleners en kritieke ICT-onderaannemers, zijn opgenomen in Bijlage II. De uitvoering en uitkomst van de due diligence worden vastgelegd.

6.3 Contractuele overeenkomst met ICT-dienstverleners

Het fonds legt de afspraken met de ICT-dienstverleners schriftelijk vast in een overeenkomst. Als uit de due diligence is gebleken dat de ICT-dienstverlener een kritieke ICT-dienstverlener betreft en eventueel ook gebruik maakt van ICT-onderaannemers, zorgt het fonds ervoor dat de betreffende aanvullende bepalingen in de contractuele overeenkomst worden opgenomen. In Bijlage III zijn de vereiste contractuele bepalingen nader uitgewerkt.

6.4 Exitstrategieën en bedrijfscontinuïteit voor kritieke ICT-dienstverlener

Het fonds heeft voor elke uitvoeringspartij met uitzondering van niet-kritieke ICT-dienstverleners een risicogebaseerde exitstrategie c.q. exitplan opgesteld. Daarin heeft het fonds tenminste passende noodmaatregelen (incl. geplande uitvoeringstiming) ter borging van de bedrijfscontinuïteit beschreven.

Onderdeel van de exitstrategieën zijn ook overgangsplannen die het fonds in staat stellen om een adequate overdracht van kritieke ICT-diensten en gegevens naar het fonds of een alternatieve ICT-dienstverlener te borgen.

De exitplannen worden op een risicogebaseerde wijze getest en geëvalueerd.

6.5 Informatieregister ICT-diensten

Het fonds houdt een doorlopend actueel informatieregister bij van alle ICT-diensten en daaraan gerelateerde overeenkomsten, waarin een onderscheid wordt gemaakt tussen diensten ter ondersteuning van kritieke en niet-kritieke diensten.

6.6 Rapportage en meldplicht richting DNB

Het fonds rapporteert jaarlijks aan DNB over het aantal nieuwe overeenkomsten inzake het gebruik van ICT-diensten, de categorieën van ICT-dienstverleners, het soort contractuele overeenkomsten en de ICT-diensten en -functies die worden geleverd.

Op verzoek van DNB wordt door het fonds het informatieregister ter beschikking gesteld, incl. alle overige relevante informatie. Bij voorziene veranderingen binnen de uitbestedingsketen inzake ICT-diensten die kritieke of belangrijke functies ondersteunen, wordt DNB tijdig geïnformeerd in de volgende gevallen:

- Geplande nieuwe overeenkomsten;

- Materiële wijzigingen binnen overeenkomsten;
- Het feit dat een bestaande uitbestede ICT-dienst belangrijk of kritiek is geworden.

6.7 Monitoring uitgangspunten ICT-risicobeheer bij uitvoeringspartijen

Het Dagelijks Bestuur, met ondersteuning van Bureau Pensioenzaken, monitort met behulp van het informatieregister voor ICT-dienstverleners de overeenkomsten met ICT-dienstverleners en houdt toezicht op risicoblootstelling en de relevante documentatie.

De contractuele afspraken die gemaakt zijn met de uitvoeringspartijen dienen beoordeeld te worden met betrekking tot het onderdeel ICT- en informatievoorziening. Vastgelegd dient te worden hoe de uitvoeringspartijen (laten) inventariseren, analyseren en rapporteren dat hun ICT en informatievoorziening voldoet aan door het fonds verlangde en de wettelijke gestelde eisen.

Met SLA ‘s en andere rapportages wordt aangetoond dat wordt voldaan aan de verlangde eisen uit deze beleidsnotitie. Periodiek stelt het bestuur van het fonds vast of de uitvoeringspartijen voldoen aan de verlangde beleidseisen rondom ICT-risicobeheer. Het Dagelijks Bestuur met ondersteuning van Bureau Pensioenzaken en relevante commissie(s) bereiden deze vaststelling voor ten behoeve van het bestuur van het fonds.

In opdracht van het bestuur wordt per uitvoeringsorganisatie gecontroleerd of de gestelde uitgangspunten rondom ICT-risicobeheer worden nageleefd, hetgeen tenminste moet blijken uit SLA rapportages en ISAE- en/of Cobit-rapportages. Hierbij wordt opgemerkt dat de Cobit-rapportages naar verwachting op termijn vervangen zullen worden door rapportages die assurance over DORA-compliance afgeven.

7 Gestelde beleidseisen per aandachtsgebied

Hierna volgen de door het fonds verlangde eisen per aandachtsgebied om de ICT- en informatievoorzieningsbeleidseisen te realiseren. De aandachtsgebieden zijn Risicomanagement cyclus, Cloudcomputing, Informatiebeveiliging, , Cybersecurity, Testen, Aanpasbaarheid en Beschikbaarheid.

7.1 Risicomanagementcyclus

De ICT-risico’s worden opgenomen als onderdeel van de reguliere risicomanagementcyclus welke onderdeel is van het integraal risicomanagement. De cyclus kent de volgende fasen, identificeren, evalueren, beheersen en bewaken. Bij het fonds houdt de Risk- commissie zich bezig met het begeleiden en challengen van de 1e lijn, bestuur, beleggingsadviescommissie, communicatie commissie en dagelijks bestuur commissie die hiervoor primair verantwoordelijk is. De Risk-commissie rapporteert aan het bestuur.

7.1.1 Risicobereidheid

Het bestuur stelt de risicobereidheid voor het ICT-domein van het fonds vast. De uitvoeringspartijen zijn verantwoordelijk voor het vaststellen van hun risicobereidheid van de operationele risico ’s en sluiten aan bij de risicobereidheid van het fonds.

7.1.2 ICT-risicoanalyse

Het fonds voert tenminste jaarlijks of wanneer daar eerder aan aanleiding toe is, een ICT-risicoanalyse uit. Tijdens deze ICT-risicoanalyse worden de ICT-risico’s en bijhorende beheersmaatregelen geïdentificeerd in relatie tot de processen en functies van het fonds. Dit betreffen zowel processen binnen het fonds als bij de uitbestedingsrelaties en ICT-dienstverleners.

Op basis van deze ICT-risicoanalyse bepaalt het fonds welke ICT-activa processen en functies van het fonds ondersteunen die als kritiek of belangrijk kwalificeren. Bij het uitvoeren van de ICT-risicoanalyse wordt de guidance vanuit de actuele DNB Good Practices Informatiebeveiliging meegenomen.

7.1.3 Business Impact Analyse (BIA)

Onderdeel van het ICT-beleid is het uitvoeren van een periodieke Business Impact Analyse (BIA) op de processen van het fonds waarbij substantieel wordt gesteund op ICT. Daarbij worden de voorgenoemde visie en strategie van het fonds als uitgangspunt gehanteerd.

De analyse wordt uitgevoerd op basis van de belangrijkste functies van het fonds, de zogenaamde “kritieke of belangrijke functies”. Op basis van deze kritieke of belangrijke functies worden de risico’s gedefinieerd die een duidelijke relatie hebben met ICT, waaronder ook informatiebeveiligingsrisico’s. De risico’s zijn nader ingedeeld in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV-score). De BIV-score vormt de input bij de jaarlijkse ICT-risicoanalyse. Het resultaat van deze analyse is een overzicht van de belangrijkste risico ’s per proces bij de uitvoeringspartijen.

7.1.4 Beheersen

De uitvoeringsinstanties zijn verantwoordelijk dat de geïdentificeerde beheersmaatregelen zichtbaar worden geïmplementeerd in de bedrijfsprocessen. Van belang hierbij zijn de verlangde eisen van het fonds zoals beschreven, de toezichthouders, wet- en regelgeving en intern gehanteerde standaarden. Wanneer deze maatregelen niet of onvoldoende voorhanden zijn maken de uitvoeringspartijen een verbeterplan dat jaarlijks door de directie wordt vastgesteld. Voor het bestuur van het fonds werkt dit plan als stuur- en verantwoordingsdocument voor de inrichting van de risico mitigerende maatregelen.

7.1.5 Bewaken

De uitvoeringspartijen moeten periodiek een Risk Self Assessment op informatiebeveiliging uitvoeren. Daarbij kan gebruik worden gemaakt van de door DNB beschreven Good Practice Informatiebeveiliging[5]. Om de kwaliteit van deze controls te toetsen stellen de uitvoeringspartijen jaarlijks een testplan op.
Hieruit komt een risicobeeld naar voren dat wordt aangevuld met incidenten en tussentijds uitgevoerde risico assessments. Afhankelijk van de risicobereidheid wordt bepaald of de risico ’s aanleiding geven tot mitigerende acties.

7.1.6 Integraal risicomanagement

Het bestuur van het fonds eist een integraal risicomanagement over de gehele uitbestede ICT- en informatiebeveiligingsketen in te richten. De risicobeheersingsmaatregelen passend bij de BIV-scores zoals toegekend aan de kritieke of belangrijke processen en daaraan gerelateerde informatiesystemen zoals applicaties, databases, infrastructuurcomponenten dienen hierbij aantoonbaar te zijn geïmplementeerd. Dit waarborgt dat de fondsdata adequaat zijn beveiligd tegen ongeautoriseerde wijzigingen, dat de dataprivacy voldoende gewaarborgd is en dat de data tijdig beschikbaar is voor de betrokken partijen bij het fonds.

7.1.7 Periodieke audit van ICT-risicobeheerkader

Het fonds zorgt ervoor dat het interne auditplan een periodieke audit van het kader voor ICT-risicobeheer bevat, waarvan de frequentie en focus in verhouding staat tot de vastgestelde ICT-risico’s. De audits worden uitgevoerd door auditors die over voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT-risico en over de nodige onafhankelijkheid beschikken. Bevindingen vanuit de audits worden gedocumenteerd en aanbevelingen worden gemonitord om een tijdige opvolging te borgen.

In de overeenkomst die het fonds heeft afgesloten met de ICT-dienstverleners is daartoe ook een “right

to audit" opgenomen.

7.1.8 Evaluatie van het ICT-risicobeheerkader

Ten minste jaarlijks voert het fonds een evaluatie uit van het ICT-risicobeheerkader (en ICT-beleid als wezenlijk onderdeel daarvan), waarbij de naleving van wet- en regelgeving, uitvoerbaarheid, toekomstgerichtheid, kosten en passend budget, ICT-gerelateerde risico's (middels een evaluatie van de ICT-risicoanalyse), het ICT-risicoraamwerk en 'best practices' in de sector worden beoordeeld. Het is ook mogelijk dat er een ad hoc-herziening nodig is als gevolg van veranderende wetgeving of andere omstandigheden.

Deze evaluatie zal worden voorbereid door het Dagelijks Bestuur met ondersteuning van Bureau Pensioenzaken en zal worden besproken en vastgesteld door het bestuur van het fonds. De verschillende vormen van input voor de beleidsevaluatie worden hieronder verder toegelicht.

- **Jaarlijkse ICT-risicoanalyse:** Dit begint met de jaarlijkse ICT-risicoanalyse die gericht is op de vastgestelde normen van deze Beleidsnotitie. Informatiebeveiliging en continuïteit staan daarbij centraal als de belangrijkste risicothema's. Deze jaarlijkse ICT-risicoanalyse wordt uitgevoerd door het fonds en vormt de basis voor verbeterplannen per uitbestedingsrelatie en (kritieke) ICT-dienstverlener.

- **Uitkomsten monitoring uitbestedingsrelaties en ICT-dienstverleners:** Het fonds neemt de relevante uitkomsten mee vanuit de monitoring op ICT-beheersing door de uitbestedingsrelaties en (kritieke) ICT-dienstverleners van het fonds. Daarnaast ontvangt en bespreekt het bestuur jaarlijks een rapportage over de lessen opgedaan uit: 1) tests op de digitale operationele weerbaarheid, 2) ICT-gerelateerde incidenten, 3) opstartproblemen van het ICT-bedrijfscontinuïteitsplan en ICT-herstelplannen en 4) uit toetsingen in het toezicht in het ICT-risicobeoordelingsproces.

7.2 Cloudcomputing

Cloudcomputing zorgt ervoor dat het lastiger wordt om aan te tonen dat aan de gevraagde beveiligingseisen is voldaan. Indien bij een uitvoeringspartij sprake is van Cloudcomputing past dit binnen de risicobereidheid van het bestuur. Een eis die wordt gesteld aan de uitvoeringspartijen is dat wanneer deze overgaan tot Cloudcomputing altijd eerst een risicoanalyse moet worden uitgevoerd. De uitvoeringspartijen dienen overgang naar of veranderingen omtrent Cloudcomputing vooraf te melden aan het fonds. Om de specifieke risico 's te beheersen rondom Cloudcomputing dienen de uitvoeringspartijen te beschikken over een actueel en geïmplementeerd Cloudbeleid en dit te communiceren met het fonds.

7.3 Informatiebeveiliging

Omdat het fonds en de uitvoeringspartijen een belangrijke maatschappelijke functie vervullen is het evident dat bij de verwerking van informatie rekening wordt gehouden met informatiebeveiliging. Het fonds stelt als eis dat zowel het fonds zelf als alle uitvoeringspartijen qua inrichting en kaders rondom de beveiliging van informatie, minimaal moeten voldoen aan de betreffende vereisten uit DORA en de AVG, en de specifieke eisen van de toezichthouders DNB en Autoriteit Persoonsgegevens.

Belangrijke ICT-beveiligingsbeheermaatregelen om bovenstaande beheersingsdoelen te bewerkstelligen zijn:

- Toegangsbeveiliging (zowel fysiek als logisch)
- Backup en Recovery
- Contingency Planning

- Change- en Incident Management procedures
- Logging
- Scheiding tussen Ontwikkel-, Test- en Productieomgeving

Bovenstaande beheersmaatregelen zijn nader uitgewerkt in het Informatiebeveiligingsbeleid en het ICT-bedrijfscontinuïteitsbeleid (zie ook de eisen onder het hoofdstuk over Beschikbaarheid). Om de specifieke risico 's rondom informatiebeveiliging te beheersen, verwacht het fonds dat de uitvoeringspartijen en kritieke ICT-dienstverleners ook beschikken over een actueel, geïmplementeerd en tenminste gelijkwaardig informatiebeveiligingsbeleid en bedrijfscontinuïteitsbeleid en dit communiceren met het fonds.

In verband met het toezicht op naleving van DORA en de AVG wil het bestuur van het fonds aanvullend dat de uitvoeringspartijen en ICT-dienstverleners aansluiten bij goedgekeurde certificeringsmechanismes, bij voorkeur Cobit en/of ISAE 3402 en/of ISAE 3000 (assurance over niet financiële informatie) en/of bijvoorbeeld ISO 27000 (informatiebeveiligingsnormen).

Daarmee tonen deze partijen aan dat wordt voldaan aan de AVG en de principes privacy by design en privacy by default. Privacy by design houdt in dat bij de verwerking gehanteerde mechanismen en systemen zo zijn ontworpen dat zoveel als mogelijk rekening wordt gehouden met de privacy van de deelnemers en de AVG. Privacy by default is het zodanig instellen van de standaardinstellingen dat de privacy zoveel als mogelijk wordt gewaarborgd.

In het informatievoorzieningsbeleid van het fonds zal rekening gehouden worden met de AVG. Het fonds beschikt over de bewijslast dat aan de AVG regelgeving wordt voldaan. Om aan te tonen dat aan de wetgeving wordt voldaan dienen alle risicovolle verwerkingen van persoonsgegevens onderworpen te worden aan een risicoanalyse. Een zogeheten Data Privacy Impact Assessment, afgekort DPIA. Ook zal het fonds een "verwerkingsregister" opstellen dat inzicht geeft in alle persoonsgegevens die door de organisatie en haar partners wordt beheerd. In het register moet onder andere inzicht worden gecreëerd welke persoonsgegevens het fonds verwerkt, welke verwerkingsdoeleinden er zijn, hoe lang de gegevens worden bewaard en welke maatregelen zijn getroffen om de privacyrisico's te beperken. Verder heeft het fonds haar activiteiten en processen conform de AVG ingericht. Het fonds draagt zorgt voor documenteren, evalueren, wijzigen en verbeteren indien nodig.

7.4 Cybersecurity

Het fonds ziet cybersecurity als integraal onderdeel van informatiebeveiliging. Cybersecurity en de daarmee gepaard gaande risico 's hebben een hoge prioriteit, een lage risicobereidheid (risico willen lopen) en een lage risicotolerantie (risico kunnen lopen). Een eis is dat de uitvoeringspartijen zorgdragen voor een organisatie van de beveiliging die erop ingericht is de met cybersecurity gepaard gaande risico's te beheersen, tijdig te detecteren en de eventuele gevolgen van een incident te minimaliseren. De communicatiecommissie van het fonds draagt ook zorg voor het beperken van de impact van een incident door tijdige en duidelijke informatie. Periodiek wordt het fonds door de uitvoeringspartijen geïnformeerd over het gevoerde cybersecurity beleid en de beheersing van de cyberrisico's. Het fonds stelt verder als eis dat de uitvoeringspartijen voldoen aan de wet- en regelgeving op dit gebied (waaronder DORA en AVG) alsmede de actuele versie van de Good Practice Informatiebeveiliging van DNB.

Daarnaast wil het fonds geïnformeerd worden over welke persoon bij een uitvoeringorganisatie de Functionaris Gegevensbescherming (FG), de ketenregisseur en de incidentenmanager voor het fonds is.

7.5 Testen

Het fonds beschikt over en geeft uitvoering aan een risicogebaseerd testprogramma dat gericht is op het testen van digitale operationele weerbaarheid.

Het fonds beschikt over een risicogebaseerd testprogramma dat gericht is op het testen van digitale operationele weerbaarheid. Dit programma omvat het plannen, ontwerpen en laten uitvoeren van beoordelingen en tests (waaronder eventuele (gebundelde) dreigingsgestuurde penetratietesten, of 'TLPT') om de weerbaarheid van de ICT-systemen en -processen te waarborgen.

Het programma volgt een risicogebaseerde benadering, waarbij het fonds rekening houdt met veranderende ICT-risico's, specifieke risico's, kritieke ICT-activa en verleende ICT-diensten. Dit betekent dat de tests worden afgestemd op de risico's en prioriteiten van het fonds. Het programma wordt periodiek geëvalueerd.

Het programma heeft met name betrekking op tests die bij en door de kritieke ICT-dienstverleners uitgevoerd moeten worden namens het fonds. Het Dagelijks Bestuur monitort met ondersteuning van het Bureau Pensioenzaken de uitvoering en uitkomsten van deze tests, op basis van informatievoorziening vanuit de ICT-dienstverleners.

Het is uitvoeringspartijen toegestaan om onder eigen regie testen uit te laten voeren door een gerenommeerde partij. Bij de selectie van geschikte uitvoerders van de testen, borgt het fonds dat de testers over de benodigde kwalificaties en expertise beschikken en dat eventuele belangenconflicten worden voorkomen die zich kunnen voordoen tijdens de hele ontwerp- en uitvoeringsfase (borging objectiviteit en onafhankelijkheid).

7.6 Aanpasbaarheid

Het fonds stelt als eis dat de uitvoeringspartijen hun producten en diensten beschikbaar stellen afgestemd op de specifieke behoefte van het fonds tegen een zo laag mogelijke investering en jaarlijkse kosten. De uitvoeringspartijen realiseren deze eis met inzet van geautomatiseerde systemen, waarin standaardisatie en klantdifferentiatie in onderling evenwicht zijn geoptimaliseerd. Dit houdt in harmonisatie van processen en standaardisatie van systemen. Een harde eis voor alle uitvoeringspartijen is dat ICT is aangelijnd aan de "business". Dit houdt in dat ICT-specialisten samenwerken met pensioendeskundigen en beleggingsdeskundigen. Verder eist het fonds dat projectdoelen tijdig gehaald worden en dat de bestaande ICT toekomstbestendig is. De ICT dient de overgang naar WTP aan te kunnen. De uitvoeringspartijen dienen te onderbouwen waarom hun systemen toekomst bestendig zijn. Deze onderbouwing dienen zij te rapporteren aan het fonds.

7.7 Beschikbaarheid

De uitvoeringspartijen bieden producten en diensten met een overeengekomen stabiliteit van de bedrijfsvoering op het gebied van vermogensbeheer, pensioenbeheer en ICT voor het bestuur en bureau pensioenzaken. De uitvoeringspartijen zijn voorbereid op eventuele calamiteiten die de dienstverlening kunnen raken in de vorm van een Business Continuity Management Beleid en aantoonbare werking daarvan. Een onderdeel hiervan is minimaal een jaarlijkse crisismanagement oefening en ICT-uitwijktest. De uitvoeringspartijen hanteren een locatieonafhankelijke werkwijze met bijbehorende methoden en technieken. De bedrijfsinrichting en het ontwerp van de informatievoorziening wordt gekenmerkt door een aanpak, waarbij waar nodig, schaalbare oplossingen worden ingezet, gebaseerd op marktstandaarden. Als randvoorwaarde voor operationele stabiliteit geldt dat hard- en software verregaand is gestandaardiseerd en risicogedreven wordt beheerd.

BIJLAGES

Bijlage I - Versiebeheer

Versie	Wijzigingen Bijzonderheden	Auteur	Datum vaststellen
Versie 1 Beleidsnotitie ICT en informatievoorziening 2018-2020	Initiële vastlegging ICT en informatievoorziening beleid	Werkgroep ICT De heer Mulders De heer Tijhuis De heer Heemskerk De heer Harperink	Bestuur 19-1-2018
Versie 2 Beleidsnotitie ICT en informatievoorziening 2021-2023	Algehele update beleid. De 54-Cobit controls van DNB zijn uitgebreid naar 58-Cobit controls. Deze uitbreiding van de controls ziet op cybercrime.	De heer Harperink Review de heer Heemskerk	Bestuur 6-11-2020
Versie 3 Beleidsnotitie ICT, informatievoorziening en cybersecurity 2023-2025	Algehele update beleid. Beleid in lijn brengen met de Good Practice IB 2019-2020 van DNB. Naam uitbreiden met cybersecurity.	De heer Harperink Review de heer Heemskerk	Bestuur 22-9-2023
Versie 4 Beleidsnotitie ICT, informatievoorziening en cybersecurity 2025-2027	Beleid actualiseren met de verplichtingen vanuit DORA	AF Advisors	Bestuur 06-12-2024

Bijlage II – Due diligence op ICT-dienstverleners

Due diligence op ICT-dienstverleners
Het bestuur van het fonds voert tijdens de selectieprocedure een due-diligence onderzoek uit op de ICT-dienstverlener. Dit onderzoek stelt vast of de beoogde partij voldoet aan de normen die het fonds stelt aan ICT-dienstverleners. Deze toetsing wordt ingevuld en vastgelegd.

Algemene beoordelingscriteria due diligence
Het fonds beoordeelt risicogebaseerd als onderdeel van de due diligence op een voorgenomen ICT-dienstverlener tenminste:

- of de beoogde ICT-dienst een kritieke of belangrijke functie ondersteunt;
- of de ICT-dienstverlener gebruik maakt van ICT-onderaannemers;
- welke risico's kunnen voortkomen uit de contractuele overeenkomst en in hoeverre deze risico's worden beheerst. Hierbij wordt tenminste beoordeeld of sprake is van (een toename van) een concentratierisico en van het risico op belangenverstrengeling;
- of de ICT-dienstverlener deel uitmaakt van dezelfde groep als het fonds;
- of de ICT-dienstverlener ten goede naam en faam bekend staat op het gebied van ethiek en maatschappelijke verantwoordelijkheid.
- of de ICT-dienstverlener beschikt over voldoende capaciteiten, deskundigheid en adequate financiële, personele en technische middelen, passende organisatiestructuur, risicobeheer en interne controles;
- of de ICT-dienstverlener voldoet aan passende normen afgeleid van de voor het fonds geldende kernindicatoren en maatregelen op het gebied van informatiebeveiliging; en
- of de ICT-dienstverlener bereid is te voldoen aan de toezichtvoorwaarden voor het sluiten van het contract.

Aanvullende beoordelingscriteria rondom kritieke ICT-dienstverleners
Als de beoogde ICT-dienst een kritieke of belangrijke functie ondersteunt, beoordeelt het fonds t.a.v. het concentratierisico aanvullend:

- of de beoogde kritieke ICT-dienstverlener moeilijk substitueerbaar zou zijn; en
- of het fonds bij dezelfde of een nauw verbonden kritieke ICT-dienstverlener al meerdere ICT-diensten heeft afgenomen die kritieke of belangrijke functies ondersteunen (het fonds raadpleegt hiertoe het informatieregister).

Hierbij weegt het fonds de baten en kosten af van alternatieve oplossingen die op gelijke wijze zouden aansluiten bij de behoefte en doelstellingen van het fonds.

Aanvullende beoordelingscriteria rondom kritieke ICT-onderaannemers
Als het fonds heeft vastgesteld dat de beoogde kritieke ICT-dienstverlener gebruik maakt van ICT-onderaannemers, toetst het fonds aanvullende de onderstaande beoordelingscriteria.

Onderwerp	**Beoordelingscriteria**
Baten en risico's	De baten en risico's die uit een (onder)uitbesteding voortkomen, waaronder tenminste: - de aard van de ICT-diensten die door de onderaannemers worden verleend;

	- de lengte van de keten van onderaannemers; - de geografische risico's verbonden aan de onderaannemer, waarbij tenminste wordt gekeken naar de vestigingslocatie van de onderaannemers, de aard van de gedeelde (persoons)gegevens en de verwerkingslocatie van (persoons)gegevens (ook met het oog op de AVG); - het behoren van de onderaannemers tot de groep van de ICT-dienstverlener; - het (gebrek aan) het onder toezicht staan van de onderaannemers; - de overdraagbaarheid van de ICT-dienst gegeven de gehanteerde technologie; - de impact van verstoringen op de continuïteit en beschikbaarheid van de ICT-diensten; en - de moeilijkheidsgraad rondom re-integratie van de diensten.
Insolventie	Toepasselijke bepalingen inzake insolventierecht in geval van faillissement of surseance van betaling
Due diligence	De kritieke ICT-dienstverlener beschikt over due diligence-processen om de (operationele en financiële) bekwaamheden van potentiële ICT-onderaannemers te selecteren en te beoordelen om de ICT-diensten die kritieke of belangrijke functies ondersteunen te leveren, incl. via door het fonds vereiste operationele rapportage en tests.
Notificatieplicht	De kritieke ICT-dienstverlener is bereid om het fonds te informeren en betrekken bij besluitvorming tot onderuitbesteding wanneer relevant en passend geacht door de kritieke ICT-dienstverlener.
Contracteren	De kritieke ICT-dienstverlener neemt in de contractuele overeenkomst met onderaannemers dezelfde contractbepalingen op als in de overeenkomst tussen het fonds en de kritieke ICT-dienstverlener, waardoor het fonds compliant blijft aan relevante wet- en regelgeving ten aanzien van (onder)uitbesteding van ICT-diensten.
Monitoring door ICT-dienstverlener	De kritieke ICT-dienstverlener beschikt over adequate bekwaamheden, expertise, financiële, menselijke en technische middelen, passende informatiebeveiligingsnormen toepast, en een passende organisatiestructuur heeft, incl. risicobeheer en interne controles, incidentenrapportage en -reacties, om de onderaannemers te monitoren.
Monitoring en bijsturing door het fonds	Het fonds beschikt over adequate bekwaamheden, expertise, financiële, menselijke en technische middelen, passende informatiebeveiligingsnormen toepast, en een passende organisatiestructuur heeft, incl. risicobeheer, incidentenrespons en bedrijfscontinuïteitsbeheer en interne controles, om de onderuitbestede ICT-dienst te monitoren en te controleren en, desnoods, de ICT-onderaannemers rechtstreeks bij te sturen.
Toezichtsrisico's	De aanwezigheid van eventuele obstakels voor de samenwerking met autoriteiten (incl. DNB), alsmede uitoefening van audit-, informatie- en toegangsrechten door de bevoegde autoriteiten, afwikkelingsautoriteiten en het fonds, incl. aangestelde personen.

Bijlage III – Contractuele overeenkomst met ICT-dienstverleners

Algemene contractuele bepalingen
Het fonds legt de afspraken met de ICT-dienstverleners schriftelijk vast in een overeenkomst. Hierbij borgt het fonds dat in ieder geval de onderstaande informatie in de overeenkomst wordt gevangen**.**

Onderwerp	**Beschrijving**
Dienstenbeschrijving	Een gedetailleerde beschrijving van de geleverde functies en diensten, incl. de toestemming en voorwaarden voor uitbesteding van kritieke functies
Locatie en gegevensverwerking	Een specificatie van de locaties waar de ICT-diensten worden geleverd en gegevens worden verwerkt, inclusief de notificatieplicht aan het fonds bij wijzigingen
Gegevensbescherming	De bepalingen over gegevensbescherming, incl. beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid.
Toegang, herstel en teruggave	De bepalingen voor toegang, herstel en teruggave van gegevens bij insolventie, stopzetting van de bedrijfsactiviteiten of beëindiging van de overeenkomst.
Service Level Agreement (SLA)	Een beschrijving van het dienstenniveau, incl. actualisering en herziening daarvan.
Incidenten	De verplichting van de ICT-dienstverlener tot het verlenen van bijstand aan het fonds bij incidenten zonder extra kosten of tegen kostprijs.
Medewerking aan autoriteiten	De verplichting van de ICT-dienstverlener tot volledige medewerking aan bevoegde autoriteiten en afwikkelingsautoriteiten, incl. aangestelde personen.
Beëindiging	Een beschrijving van de beëindigingsrechten en opzegtermijnen, conform de verwachtingen van de toezichthouder.
Training	De voorwaarden voor deelname van ICT-dienstverleners aan bewustmakingsprogramma's en opleidingen over ICT-beveiliging.

Aanvullende contractuele bepalingen rondom kritieke ICT-dienstverleners
Als een ICT-dienstverlener een kritieke ICT-dienstverlener betreft, zorgt het fonds ervoor dat de onderstaande aanvullende bepalingen in de contractuele overeenkomst worden.

Onderwerp	**Beschrijving**
Dienstenbeschrijving	Een beschrijving van de gedetailleerde dienstverleningsniveaus met prestatiedoelstellingen (kwantitatief en kwalitatief).
Kennisgeving en rapportageverplichtingen	De kennisgevingstermijnen en rapportageverplichtingen van de ICT-dienstverlener rondom ontwikkelingen die materiële gevolgen kunnen hebben voor de dienstverlening aan het fonds.

Incidenten	De termijnen en verplichtingen van de ICT-dienstverlener richting het fonds rondom het informeren over ICT-gerelateerde incidenten en betalingsgerelateerde operationele of beveiligingsincidenten. Dit betreft zowel de initiële melding als tussentijdse en definitieve rapportages.
Bedrijfsnoodplannen en ICT-beveiliging	De verplichting van de ICT-dienstverlener tot implementatie en testen van bedrijfsnoodplannen en adequate ICT-beveiligingsmaatregelen.
Testen	De verplichting van de ICT-dienstverlener om deel te nemen aan en volledig mee te werken bij de TLPT van het fonds.

Rechten ter borging van adequate monitoring door het fonds	• Het recht van het fonds om de prestaties van de ICT-dienstverlener doorlopend te monitoren, incl.:
	  ○ Het recht tot onbeperkte toegang, inspectie en audit door het pensioenfonds of aangestelde derde partij en toezichthouder (DNB), incl. maken van kopieën; en
	  ○ Het recht tot aanpassing van overeenkomen garantieniveaus, indien de rechten van andere cliënten worden aangetast.
	  ○ De effectieve uitoefening van dit recht wordt niet belemmerd door andere contractuele overeenkomsten of uitvoeringsbeleid.
	  ○ De mogelijkheid om de ICT-dienstverlener te verzoeken de certificeringen of auditverslagen uit te breiden naar andere relevante systemen en controles;
	  ○ De mogelijkheid voor het fonds om naar eigen goeddunken individuele en gebundelde audits met betrekking tot de contractuele overeenkomsten uit te voeren en die rechten uit te voeren in overeenstemming met de afgesproken frequentie.
	• De verplichting voor de ICT-dienstverlener om specifieke details te verstrekken over het toepassingsgebied van inspecties en audits, de procedures die worden gevolgd, en hoe vaak dergelijke inspecties en audits plaatsvinden.

Exitstrategieën	• De implementatie van een verplichte passende overgangsperiode om verstoring voor het fonds te beperken of voor een doeltreffende afwikkeling en herstructurering te zorgen. • De mogelijkheid om over te stappen naar een andere derde aanbieder van ICT-diensten of interne oplossingen, afhankelijk van de complexiteit van de diensten.
Onderuitbesteding	De verplichting van de ICT-dienstverlener richting het fonds om: • Materiële wijzigingen rondom ICT-onderaannemers tijdig, binnen een kennisgevingsperiode, te melden zodat het fonds in staat is om de impact op de risico's te beoordelen waar zij (mogelijk) aan wordt blootgesteld; • Het pensioenfonds in staat te stellen dat de ICT-dienstverlener de materiële wijzigingen alleen implementeert na goedkeuring van de wijzigingen door het pensioenfonds of er geen bezwaar maakt tegen het einde van de kennisgevingsperiode.

	• Wijzigingen in de voorgestelde uitbestedingsregelingen te verzoeken vóór hun implementatie als de resultaten van de risicobeoordeling daartoe aanleiding geeft, mede in het licht van de risico's van de due diligence voor de gehele uitbesteding.

Aanvullende contractuele bepalingen in geval van kritieke of belangrijke ICT-onderaannemers
Als uit de due diligence is gebleken dat een kritieke ICT-dienstverlener gebruik maakt van ICT-onderaannemers, dan zorgt het fonds ervoor dat de onderstaande aanvullende informatie in de overeenkomst wordt opgenomen.

Onderwerp	Beschrijving
Beschrijving onderaannemers	Een beschrijving van de ICT-diensten die kritieke of belangrijke processen ondersteunen, die door een ICT-onderaannemer uitgevoerd mogen worden.
Verantwoordelijkheid voor ICT-onderaannemers	De ICT-dienstverlener is te allen tijde verantwoordelijk voor de dienstverlening vanuit de ICT-onderaannemers en voor het bijhouden van een actueel overzicht van ICT-onderaannemers.
Monitoring op ICT-onderaannemer	De verplichting van de ICT-dienstverlener om alle ICT-onderaannemers te monitoren die ICT-diensten verlenen die een kritieke of belangrijke functie ondersteunen, op doorlopende nakoming van de contractuele verplichtingen die de ICT-dienstverlener heeft met het fonds.
Rapportage aan het fonds	De monitoring- en rapportageverplichtingen rondom ICT-onderaannemers van de ICT-dienstverlener jegens het fonds.
Beoordeling locatierisico's	De verplichting van de ICT-dienstverlener om alle risico's te monitoren, incl. ICT-risico's, i.v.m. de locatie van de potentiële onderaannemer en diens moederbedrijf en de locatie waar de ICT-dienst wordt geleverd.
Locatierisico's	De locatie en eigendom van gegevens die worden verwerkt of opgeslagen door de ICT-onderaannemer.
Specificatie rapportagevereisten	De verplichting van de ICT-dienstverlener om in de overeenkomst met de ICT-onderaannemer de monitoring- en rapportageverplichtingen van de onderaannemer jegens de ICT- dienstverlener te specificeren en, waar relevant, de directe rapportage aan het fonds.
Waarborging continuïteit	De verplichting van de ICT-dienstverlener om de doorlopende levering van de ICT-diensten die kritieke of belangrijke functies ondersteunen te monitoren, zelfs in geval van tekortkoming door een onderaannemer in serviceniveaus of andere contractuele verplichtingen.
Incidentenrespons	De verplichting van de ICT-dienstverlener om in de overeenkomst met de ICT-onderaannemer de vereisten rondom incidentenrespons- en bedrijfscontinuïteitsplannen en de serviceniveaus te specificeren.
Beveiligingsnormen	De verplichting van de ICT-dienstverlener om in de overeenkomst met ICT-onderaannemers om de ICT-beveiligingsnormen en eventuele aanvullende beveiligingsfuncties die moeten worden nageleefd, te specificeren.

Toegang-, inspectie-, en auditrechten	De verplichting van de ICT-onderaannemer om dezelfde audit-, informatie- en toegangsrechten te verlenen aan het fonds en toezichthouders als de ICT-dienstverlener die verleent.
Dienstenniveaus	Het fonds heeft beëindigingsrechten in het geval dat de dienstverlening niet voldoet aan de dienstenniveaus die zijn overeengekomen door het fonds.
Beëindigingsrechten	Het fonds is bevoegd de overeenkomst (gedeeltelijk) te beëindigen als: a) Als de ICT-dienstverlener materiële wijzigingen aanbrengt aan onderuitbesteding waar het fonds geen goedkeuring of verklaring van geen bezwaar op heeft gegeven. b) Indien het onderuitbesteding betreft die niet is vastgelegd in de overeenkomst met de ICT-dienstverlener: c) De overeenkomst kan altijd beëindigd worden in geval van: • Ernstige overtreding van toepasselijke wetten, voorschriften of contractuele voorwaarden; • Omstandigheden die (nadelige) wijzigingen kunnen meebrengen in de uitvoering van de functies; • Zwakheden i.v.m. algemeen beheer van het ICT-risico's door ICT-dienstverlener, incl. omgang gegevens inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van (niet-)persoonlijke of anderszins gevoelige; • Indien de bevoegde autoriteit (DNB) niet langer doeltreffend toezicht kan uitoefenen op het fonds vanwege de overeenkomst.