ICT bedrijfscontinuïteitsbeleid

Stichting Pensioenfonds Thales Nederland
(SPTN)

Stichting Pensioenfonds THALES NEDERLAND

Inhoudsopgave

1. ICT-Bedrijfscontinuïteitsbeleid

1.1 Doelstelling

Het bedrijfscontinuïteitsbeleid is erop gericht SPTN in staat te stellen om haar kritieke bedrijfsactiviteiten voort te zetten tijdens en na verstoringen, zoals rampen, technische storingen, cyberaanvallen of andere noodgevallen. Specifiek betreft dit:

(A) **Bescherming van Kritieke Functies**: Essentiële bedrijfsprocessen en diensten dienen operationeel te blijven of zo snel mogelijk te worden hersteld na een verstoring.

(B) **Risicobeheersing**: Risico's die de continuïteit van de bedrijfsvoering kunnen bedreigen worden geïdentificeerd, beoordeeld en gemitigeerd.

(C) **Naleving van toepasselijke Wet- en Regelgeving**: Ten behoeve van de veerkracht en regulatoire reputatie van SPTN moet SPTN voldoen aan eisen uit hoofde van wet- en regelgeving, zoals de Verordening betreffende digitale operationele weerbaarheid voor de financiële sector ('DORA').

(D) **Minimale Onderbreking**: De impact van verstoringen op SPTN en haar belanghebbenden wordt geminimaliseerd zodat de continuïteit van de dienstverlening zoveel mogelijk wordt gewaarborgd.

(E) **Vertrouwen Behouden**: Het handhaven van het vertrouwen van pensioendeelnemers, ketenpartners en andere belanghebbenden wordt geborgd door een adequate voorbereiding op verstoringen.

1.2 Reikwijdte

ICT-uitbestedingspartijen spelen een cruciale rol in het waarborgen van de continuïteit van de ICT-diensten binnen SPTN. Deze partijen ondersteunen SPTN door het leveren van essentiële diensten en infrastructuur, en dragen daarmee direct bij aan de operationele weerbaarheid. Het is essentieel dat deze partijen voldoen aan de gestelde continuïteitseisen en dat zij hun verantwoordelijkheden duidelijk begrijpen en nakomen. SPTN beoogt passende maatregelen ter beheersing van deze ICT-derdenrisico's te treffen, waarbij de ICT-uitbestedingspartijen de verantwoordelijkheid dragen voor maatregelen onder eindverantwoordelijkheid van SPTN. Het Dagelijks Bestuur ziet toe op de naleving hiervan als onderdeel van leveranciersmanagement.

Dit bedrijfscontinuïteitsbeleid omvat de volgende essentiële aspecten voor het waarborgen van de continuïteit van de bedrijfsvoering:

(A) **Organisatie van SPTN**

(i) **Alle Bedrijfsprocessen**: Het beleid is van toepassing op alle bedrijfsprocessen, vooral die processen die essentieel zijn voor de bedrijfsactiviteiten van SPTN, inclusief de dienstverlening van het fonds aan de pensioendeelnemers.

(ii) **Alle Medewerkers**: Het beleid geldt voor alle medewerkers, inclusief vast personeel, contractanten, en tijdelijk personeel, ongeacht hun functie of locatie.

(B) **Technologische Scope**:

(i) **ICT-Infrastructuur:** De reikwijdte omvat alle kritieke ICT-systemen en -infrastructuur die nodig zijn om bedrijfsactiviteiten te ondersteunen, inclusief servers, netwerken, databases, en communicatiekanalen.

(ii) **Data en Applicaties:** Het beleid dekt de continuïteit van gegevensbeheer en essentiële bedrijfsapplicaties die nodig zijn voor dagelijkse operationele activiteiten.

(C) **Externe Scope**:

(i) **Leveranciers en Partners**: Het beleid omvat ook externe partijen zoals leveranciers, (ICT-)dienstverleners, en de ketenpartners die bijdragen aan de bedrijfsvoering. Dit omvat afspraken over bedrijfscontinuïteit en het beheer van externe risico's.

(ii) **Uitbestede Activiteiten**: Activiteiten die zijn uitbesteed aan externe dienstverleners, zoals ICT-diensten, vallen eveneens onder dit beleid om te borgen dat deze diensten tijdens een verstoring blijven functioneren.

(D) **Verstoringen en andere noodscenario's**:

(i) **Verstoringen en Calamiteiten**: De reikwijdte omvat verschillende soorten verstoringen, variërend van technische storingen en cyberaanvallen tot natuurrampen en pandemieën.

(ii) **Herstel**: Het beleid voorziet in uitwijklocaties, back-up voorzieningen, en herstelstrategieën voor het geval dat normale bedrijfsvoering wordt onderbroken.

1.3 DORA

De DORA-verordening stelt de volgende eisen aan ICT-bedrijfscontinuïteit:

(A) **Risicobeoordeling:** Periodieke risicobeoordelingen van ICT-infrastructuur en -diensten, inclusief derde partijen.

(B) **Incidentbeheer:** Inrichting van een adequaat incidentbeheerproces dat snel kan reageren op ICT-verstoringen.

(C) **ICT Bedrijfscontinuïteitsplannen** ('ICT-BCP's')**:** Het hebben van gedocumenteerde en geteste ICT-BCP's.

(D) **Toezicht en rapportage:** Regelmatige rapportages aan toezichthouders over de staat van ICT-weerbaarheid en de uitkomsten van BCP-tests.

1.4 Prioriteiten en kernactiviteiten

(A) De prioriteiten van SPTN zijn:

(i) het tijdig en juist uitkeren van de pensioenbetalingen;

(ii) het op solide wijze beleggen en beheren van de pensioenpremies, de beleggingsopbrengsten en pensioenvermogen; en

(iii) helder en duidelijk communiceren met belanghebbenden.

(B) De kernactiviteiten van SPTN zijn:

(i) het administreren van pensioenaanspraken, rechten en kapitalen

(ii) het uitkeren van pensioenen

(iii) het beleggen van het vermogen

(iv) verantwoording afleggen aan stakeholders.

2. Betrokken Partijen, Rollen en Verantwoordelijkheden

2.1 Belangrijke stakeholders

De volgende partijen zijn nauw betrokken en spelen een belangrijke rol in het kader van dit beleid.

(A) **Bestuur:** Eindverantwoordelijk voor de goedkeuring en periodieke evaluatie van het ICT BCP.

(B) **Dagelijks Bestuur:** Verantwoordelijk voor de ontwikkeling, coördinatie en evaluatie van de ICT BCP's.

(C) **Bureau Pensioenzaken:** Biedt ondersteuning aan het Dagelijks Bestuur bij de uitvoering van diens verantwoordelijkheden.

(D) **(externe) ICT-afdeling/-beheerder:** Implementatie van continuïteitsplannen, inclusief het uitvoeren van periodieke tests en rapportage van resultaten.

(E) **Crisismanagementteam ("CMT"):** Coördineert de reactie op verstoringen en rapporteert aan het Bestuur.

(F) **Externe (ICT-)Dienstverleners:** Verantwoordelijk voor de naleving van de continuïteitsafspraken zoals vastgelegd in SLA's.

(G) **Toezichthouder:** De Nederlandsche Bank, Autoriteit Financiële Markten, Autoriteit Persoonsgegevens

2.2 Stakeholder CMT nader uitgewerkt

Het Crisismanagementteam is verantwoordelijk voor het coördineren van de respons op ICT-incidenten en -crises. Het team bestaat uit:

(A) **Voorzitter Bestuur (Voorzitter CMT):** Verantwoordelijk voor het algemeen beheer en besluitvorming tijdens een crisis.

(B) **Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken):** Verantwoordelijk voor de beveiliging van ICT-systemen en het mitigeren van cyberrisico's. Verantwoordelijk voor het waarborgen dat alle herstelacties worden uitgevoerd en voldoen aan de eisen vanuit wet- en regelgeving.

2.3 Stakeholder Externe Dienstverleners nader uitgewerkt

(A) **Service Level Manager of vergelijkbare rol (bij ICT-dienstverlener)**: Verantwoordelijk voor het waarborgen van de naleving van SLA's en het activeren van back-up diensten.

(B) **Incident Response Team of vergelijkbare rol (bij ICT-dienstverlener)**: Verantwoordelijk voor het direct aanpakken van technische problemen en het herstellen van ICT-diensten.

(C) **Contractmanager of vergelijkbare rol (bij ICT-dienstverlener)**: Verantwoordelijk voor de communicatie met SPTN over de status van uitbestede diensten en het activeren van noodmaatregelen.

2.4 Toezichthouders nader uitgewerkt

De toezichthouders moeten worden geïnformeerd wanneer een ICT-incident een significante impact heeft op de operationele continuïteit of klantgegevens. De toezichthouders zullen toezicht houden op de reactie en herstelmaatregelen van de instelling.

3. Rol van ICT Uitbestedingspartijen in het ICT-Bedrijfscontinuïteitsbeleid

3.1 Algemeen

ICT-uitbestedingspartijen spelen een cruciale rol in het waarborgen van de continuïteit van de ICT-diensten binnen SPTN. Deze partijen ondersteunen SPTN door het leveren van essentiële diensten en infrastructuur, en dragen daarmee direct bij aan de operationele weerbaarheid. Het is essentieel dat deze partijen voldoen aan de gestelde continuïteitseisen en dat zij hun verantwoordelijkheden duidelijk begrijpen en nakomen.

3.2 Verantwoordelijkheden van ICT-uitbestedingspartijen

De verantwoordelijkheden van ICT-uitbestedingspartijen zijn onderstaand beschreven. In Hoofdstuk wordt rondom enkele van deze verantwoordelijkheden een nadere uitwerking geboden.

(A) **Naleving van Service Level Agreements (SLA's):**

(i) ICT-uitbestedingspartijen zijn verantwoordelijk voor het naleven van de afspraken zoals vastgelegd in de SLA's, waarin specifieke eisen voor beschikbaarheid, herstel, en beveiliging van diensten zijn opgenomen.

(ii) Zij dienen ervoor te zorgen dat hun diensten voldoen aan de overeengekomen prestatieniveaus, zelfs tijdens verstoringen of calamiteiten.

(B) **Ontwikkeling en Implementatie van Continuïteitsplannen:**

(i) Uitbestedingsrelaties en kritieke ICT-dienstverleners moeten hun eigen bedrijfscontinuïteitsplannen (BCP's) ontwikkelen en implementeren, die in lijn zijn met de continuïteitsdoelstellingen van SPTN.

(ii) Deze plannen moeten regelmatig getest en geactualiseerd worden om de effectiviteit ervan te waarborgen.

(C) **Herstel van Diensten:**

Bij een verstoring of calamiteit zijn uitbestedingsrelaties en kritieke ICT-dienstverleners verantwoordelijk voor het herstellen van hun diensten binnen de afgesproken tijdframes. Dit omvat het activeren van hun eigen disaster recovery-plannen (DRP) om de dienstverlening zo snel mogelijk te herstellen.

(D) **Risicomanagement en Rapportage:**

(i) Uitbestedingsrelaties en kritieke ICT-dienstverleners moeten een continu risicomanagementproces hebben dat identificeert, beoordeelt, en reageert op risico's die de continuïteit van hun diensten kunnen beïnvloeden.

(ii) Zij zijn verplicht om regelmatig rapportages over de status van hun BCP's en de resultaten van continuïteitstests te verstrekken aan SPTN.

(E) **Samenwerking tijdens Incidenten:**

(i) In geval van een ICT-incident moeten uitbestedingspartijen onmiddellijk SPTN informeren en nauw samenwerken met het crisismanagementteam (CMT) van SPTN om de impact te beperken.

(ii) Zij dienen tijdig updates te geven over de voortgang van herstelactiviteiten en eventuele benodigde aanvullende maatregelen.

(F) **Beveiliging en Bescherming van Gegevens:**

(i) Uitbestedingsrelaties en kritieke ICT-dienstverleners zijn verantwoordelijk voor het implementeren en onderhouden van adequate beveiligingsmaatregelen om de vertrouwelijkheid, integriteit, en beschikbaarheid van de gegevens die zij beheren, te beschermen.

(ii) Zij moeten ervoor zorgen dat er geen dataverlies optreedt tijdens een verstoring en dat gegevensherstel binnen de afgesproken tijd plaatsvindt.

(G) **Evaluatie en Actualisatie:**

(i) Uitbestedingsrelaties en kritieke ICT-dienstverleners moeten hun continuïteitsplannen minstens jaarlijks evalueren en actualiseren, of eerder indien significante wijzigingen in hun bedrijfsvoering of technologieën optreden.

(ii) Zij moeten SPTN onmiddellijk op de hoogte brengen van eventuele wijzigingen in hun continuïteitsplannen die het fonds kunnen beïnvloeden.

3.3 Toezicht en Audits

SPTN behoudt het recht om regelmatig audits uit te voeren op de continuïteitsplannen en -processen van de uitbestedingspartijen. Dit is om te verzekeren dat de plannen voldoen aan de gestelde eisen en dat de uitbestedingsrelaties en kritieke ICT-dienstverleners daadwerkelijk voorbereid zijn om tijdens een verstoring de afgesproken diensten te blijven leveren.

3.4 Communicatie en Coördinatie

(A) Uitbestedingsrelaties en kritieke ICT-dienstverleners moeten duidelijke communicatielijnen onderhouden met SPTN om ervoor te zorgen dat beide partijen goed geïnformeerd blijven over de status van ICT-diensten en de reactie op incidenten.

(B) Ze dienen deel te nemen aan gezamenlijke tests van continuïteitsplannen om de samenhang en effectiviteit van de reactiecapaciteit te waarborgen.

Door deze verantwoordelijkheden na te leven, dragen kritieke ICT-dienstverleners wezenlijk bij aan de algehele ICT-bedrijfscontinuïteit van het SPTN.

4. ICT-Bedrijfscontinuïteitsproces

4.1 Stappen ICT-bedrijfscontinuïteitsproces

Het ICT-bedrijfscontinuïteitsproces omvat de volgende stappen:

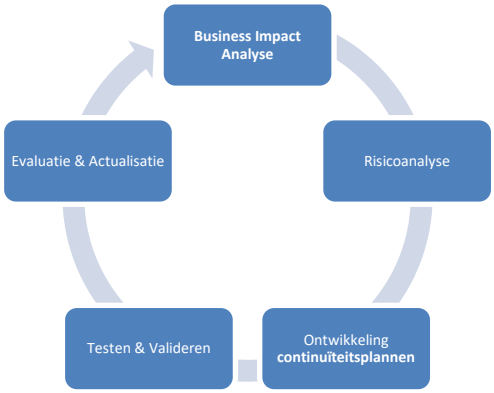
(A) **Business Impact Analyse (BIA):** Identificeer en evalueer de impact van potentiële verstoringen op kritieke ICT-diensten en -systemen.

(B) **ICT-risicoanalyse:** Beoordeel de risico's voor de continuïteit van ICT-diensten en ontwikkel strategieën om deze risico's te beperken.

(C) **Ontwikkeling van continuïteitsplannen:** Creëer en onderhoudt ICT-BCP’s die SPTN in staat stellen om snel te reageren op verstoringen en de dienstverlening te herstellen.

(D) **Testen en valideren:** Voer regelmatig tests uit om de effectiviteit van de ICT-continuïteitsplannen te waarborgen.

(E) **Evaluatie en actualisatie:** Evalueer de effectiviteit van het ICT-BCP na een incident en update de plannen waar nodig.



4.2 Business Impact Analyse (BIA)

De Business Impact Analyse (BIA) in het kader van DORA is een essentieel onderdeel om de impact van potentiële verstoringen op kritieke en belangrijke bedrijfsfuncties te evalueren. Het doel is om vast te stellen welke systemen, processen en diensten cruciaal zijn voor de continuïteit van een financiële instelling en welke gevolgen een onderbreking zou hebben op SPTN en de stakeholders van het fonds.

Een BIA moet als volgt worden uitgevoerd:

(A) **Frequentie:** Jaarlijks of na significante veranderingen in bedrijfsvoering of ICT-infrastructuur.

(B) **Uitvoerder:** Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken) in samenwerking met de (externe) ICT-afdeling/beheerder.

(C) **Criteria:** Evaluatie van de impact op kritieke processen, financiële verliezen, reputatieschade, en naleving van wet- en regelgeving.

De rollen en verantwoordelijkheden in deze stap zien er als volgt uit:

(A) **Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken)** voert de BIA uit. Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken) identificeert kritieke bedrijfsprocessen en evalueert de impact van mogelijke ICT-verstoringen op deze processen. Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken) brengt de bevindingen van de BIA in kaart en zorgt ervoor dat risicobeperkende maatregelen worden genomen.

(B) Het **Bestuur** is verantwoordelijk voor het goedkeuren van de criteria waarop de BIA wordt uitgevoerd en neemt beslissingen over de prioriteit van kritieke processen die uit de BIA naar voren komen. Daarnaast houdt het Bestuur toezicht op de risico's die de strategische doelen van SPTN kunnen beïnvloeden, gebaseerd op de resultaten van de BIA.

(C) De **ICT-dienstverlener** levert gedetailleerde informatie over de afhankelijkheden van de ICT-diensten en systemen die door SPTN worden gebruikt. ICT-dienstverleners ondersteunen bij de analyse van de impact van eventuele uitval van systemen of diensten en zorgen voor rapporten over de beschikbaarheid en prestaties van hun systemen, zodat deze kunnen worden meegenomen in de BIA.

4.3 Risicoanalyse

Bij de stap **risicoanalyse / risk self assessment (RSA)** binnen het ICT-bedrijfscontinuïteitsproces wordt een zorgvuldige evaluatie uitgevoerd van de potentiële risico's die de continuïteit van ICT-diensten en -systemen kunnen bedreigen. Dit is een cruciale stap om de veerkracht van SPTN in kaart te brengen. In de tabel hieronder staat een gedetailleerde beschrijving van de activiteiten die in dat kader uitgevoerd worden.

Onderwerp	Doel en acties
Identificatie van Risico's	• **Doel**: Identificeren van alle mogelijke gebeurtenissen die een negatieve invloed kunnen hebben op de ICT-systemen en de continuïteit van de bedrijfsvoering. • **Acties**: ○ **Brainstormsessies**: Organiseer sessies met betrokken stakeholders (waaronder Thales Nederland als ICT-beheerder, het Dagelijks Bestuur en bureau Pensioenzaken) om potentiële risico's te identificeren. ○ **Review van bestaande documentatie**: Analyseer bestaande incidentrapportages, auditverslagen en eerdere risicoanalyses. ○ **Consultatie van ICT-dienstverleners**: Vraag externe ICT-dienstverleners om input over kwetsbaarheden en bedreigingen die specifiek zijn voor hun systemen en diensten.
Risico-evaluatie	• **Doel**: Beoordelen van de geïdentificeerde risico's op basis van hun waarschijnlijkheid en potentiële impact. • **Acties**: ○ **Beoordeling van de Waarschijnlijkheid**: Schat in hoe waarschijnlijk het is dat elk geïdentificeerd risico zich voordoet. Dit kan variëren van laag (onwaarschijnlijk) tot hoog (zeer waarschijnlijk). ○ **Impactanalyse**: Analyseer de potentiële impact van elk risico op SPTN. Dit omvat financiële verliezen, reputatieschade, operationele verstoringen, en juridische gevolgen. ○ **Risicoscore**: Combineer de waarschijnlijkheid en impact om een **risicoscore** te berekenen. Dit helpt bij het prioriteren van risico's.
Identificatie van Kritieke ICT-assets **Beoordeling van Bestaande Beheersmaatregelen**	• **Doel**: Bepalen welke ICT-assets (systemen, data, infrastructuur) essentieel zijn voor de bedrijfsvoering en de risicoanalyse daarop focussen. • **Acties**: ○ **Inventarisatie**: Maak een overzicht van alle kritieke ICT-assets, zoals servers, netwerken, applicaties, databases, en cloud-infrastructuren. ○ **Classificatie**: Rangschik deze assets op basis van hun kritikaliteit voor de bedrijfsvoering. • **Doel**: Evalueren van de huidige risicobeheersmaatregelen om te bepalen of ze voldoende zijn om geïdentificeerde risico's te mitigeren. • **Acties**:

Onderwerp	Doel en acties
	○ **Controleer Beveiligingsmaatregelen**: Analyseer bestaande beveiligingsmaatregelen, zoals firewalls, back-upsystemen, en failover-mogelijkheden. ○ **Evaluatie van Incidentrespons**: Beoordeel de huidige incidentresponsprocedures om te bepalen hoe snel en effectief risico's worden beheerd. ○ **Gap-analyse**: Identificeer eventuele lacunes in de huidige risicobeheersingsstrategieën en stel voor waar verbeteringen nodig zijn.
Ontwikkeling van Risicobeheerstrategieën	• **Doel**: Ontwikkelen van strategieën om geïdentificeerde risico's te beheersen of te mitigeren. • **Acties**: ○ **Preventieve Maatregelen**: Ontwikkel maatregelen om het optreden van risico's te voorkomen (bijv. regelmatige software-updates, verbeterde netwerkomgeving). ○ **Herstelmaatregelen**: Stel herstelstrategieën op voor het geval een risico zich voordoet (bijv. dataherstelprocedures, overschakeling naar back-upsystemen). ○ **Monitoring en Waarschuwing**: Implementeer monitoringtools om potentiële risico's vroegtijdig te detecteren en waarschuwingen te geven wanneer een risico zich voordoet.
Documentatie en Rapportage	• **Doel**: Zorg voor een gedocumenteerde analyse van alle geïdentificeerde risico's, de evaluatie ervan, en de geplande beheersmaatregelen. • **Acties**: ○ **Risicorapport**: Documenteer de resultaten van de risicoanalyse, inclusief de risicoscores, prioriteiten en voorgestelde maatregelen. ○ **Communicatie naar het Bestuur**: Rapporteer de bevindingen aan het Bestuur, inclusief aanbevelingen voor verdere actie en goedkeuring van risicobeheerstrategieën.
Review en Goedkeuring door het Bestuur	• **Doel**: Zorg ervoor dat het Bestuur op de hoogte is van de belangrijkste risico's en instemt met de voorgestelde beheersmaatregelen. • **Acties**: ○ **Presentatie aan het Bestuur**: Presenteer de risicobeoordelingen en risicobeheerstrategieën voor goedkeuring. ○ **Besluitvorming**: Het Bestuur neemt beslissingen over welke risico's moeten worden geaccepteerd, welke beheersmaatregelen moeten worden geïmplementeerd, en waar aanvullende middelen nodig zijn.
Betrokkenheid van ICT-dienstverleners	• **Doel**: Zorgen dat ICT-dienstverleners hun rol spelen in het beheren van de risico's die betrekking hebben op hun diensten. • **Acties**: ○ **Informatie-uitwisseling**: Deel de relevante bevindingen van de

Onderwerp	Doel en acties
	risicoanalyse met de ICT-dienstverleners. ○ **Contractuele Verplichtingen**: Bevestig dat de leveranciers verplicht zijn om bepaalde risicobeheersmaatregelen te implementeren. ○ **Evaluatie van Leveranciersrisico's**: Vraag leveranciers om hun eigen risicoanalyses te presenteren en zorg dat deze aansluiten bij de eisen van SPTN.

De rollen en verantwoordelijkheden in deze stap zien er als volgt uit:

(A) **Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken)** voert een grondige analyse uit van de potentiële risico's die de continuïteit van de ICT-diensten kunnen beïnvloeden en identificeert kwetsbaarheden in de ICT-infrastructuur en documenteert deze.

(B) **De ICT-dienstverlener** identificeert en levert gedetailleerde rapportages op aan het fonds over de potentiële risico's die verbonden zijn aan de diensten die geleverd worden aan SPTN, mogelijke (toekomstige) verstoringen en het effect ervan op de dienstverlening. Daarnaast worden preventieve maatregelen om risico's te verminderen geopperd.

(C) **Het Bestuur** van SPTN beoordeelt de belangrijkste ICT-risico's, bepaalt de risicotolerantie en keurt de maatregelen over geïdentificeerde risico's te mitigeren goed.

4.4 Continuïteitsplannen

Bij de stap **Ontwikkeling van Continuïteitsplannen** binnen het ICT-bedrijfscontinuïteitsproces worden gedetailleerde plannen opgesteld om SPTN in staat te stellen haar kritieke ICT-diensten en -systemen te blijven uitvoeren tijdens en na verstoringen. Deze plannen zorgen ervoor dat SPTN voorbereid is op verschillende noodscenario's en dat er duidelijke procedures zijn voor herstel. In de tabel hieronder wordt weer beschreven wat precies moet gebeuren in deze stap.

Onderwerp	Doel en acties
Definiëren van Hersteldoelstellingen	• **Doel**: Bepalen van de tijdlijnen en niveaus waarop ICT-diensten moeten worden hersteld na een verstoring. • **Acties**: ○ **RTO (Recovery Time Objective)**: Stel vast hoe snel een kritieke dienst of systeem moet worden hersteld om ernstige schade te voorkomen. ○ **RPO (Recovery Point Objective)**: Bepaal de maximale hoeveelheid data die verloren mag gaan (bijv. hoeveel uur of dagen aan gegevensverlies aanvaardbaar is). ○ **SLA's met Leveranciers**: Definieer service level agreements (SLA's) met externe ICT-dienstverleners om ervoor te zorgen dat hun hersteldoelen overeenkomen met de verwachtingen van SPTN
Identificeren van Kritieke ICT-Assets en Processen	• **Doel**: Bepalen welke systemen, data en processen absoluut essentieel zijn voor de voortzetting van de bedrijfsvoering. • **Acties**:

Onderwerp	Doel en acties
	○ **Inventarisatie**: Maak een gedetailleerde lijst van alle ICT-assets die cruciaal zijn voor de continuïteit, zoals servers, netwerken, databases, en applicaties. ○ **Prioritering**: Rangschik deze assets op basis van hun kritikaliteit voor de bedrijfsvoering, rekening houdend met de bevindingen uit de Business Impact Analyse (BIA).
Ontwikkelen van Herstelstrategieën	• **Doel**: Ontwerpen van strategieën en procedures om de kritieke ICT-diensten te herstellen binnen de vastgestelde tijdslijnen. • **Acties**: ○ **Disaster Recovery Plan (DRP)**: Ontwikkel gedetailleerde DRP's voor elke kritieke ICT-component. Dit kan om technische oplossingen gaan zoals failover-oplossingen, back-up strategieën, en replicatie van data. Dit plan definieert duidelijk de rollen, verantwoordelijkheden en vereiste acties voor de personen die betrokken zijn bij de uitbestedingsrelatie, zodat ze in geval van een verstoring effectief kunnen handelen om de continuïteit van de dienstverlening voor het fonds te herstellen. Het BCP bevat ook procedures voor het informeren van het Bestuur en mogelijk de toezichthouder in geval van een calamiteit. De uitbestedingsrelatie of ICT-dienstverlener moet ervoor zorgen dat het disaster recovery plan is afgestemd op de kritieke of belangrijke processen, actueel is en jaarlijks wordt getest. Dit garandeert dat in geval van een noodsituatie, de in het plan opgenomen noodmaatregelen kunnen worden ingezet. Bovendien moet het plan specifieke procedures bevatten voor het ontsluiten van gegevens indien deze elders moeten worden hersteld. ○ **Dataherstel**: Specificeer procedures voor het herstellen van gegevens vanuit back-ups of andere herstelpunten. De uitbestedingsrelatie of ICT-dienstverlener moet zorgen voor de naleving van de BIV-classificatie voor kritieke of belangrijke gegevens door regelmatig back-ups te maken, deze op een veilige locatie op te slaan en de gegevens te bewaren volgens de geldende wettelijke richtlijnen. Periodieke verificatie is vereist om te waarborgen dat alle gegevens volledig, accuraat en tijdig worden geback-upt volgens de geldende bewaartermijnen. Daarom moet de uitbestedingsrelatie of ICT-dienstverlener passende procedures implementeren om ervoor te zorgen dat back-ups van alle kritieke of belangrijke systemen kunnen worden hersteld wanneer dit noodzakelijk is voor de dienstverlening aan het fonds. De resultaten van deze tests moeten worden gedocumenteerd en beoordeeld door een gemachtigde medewerker.

Onderwerp	Doel en acties
	○ **Systeemprestaties**: Bepaal noodprocedures voor het handhaven van systeemprestaties tijdens uitwijkoperaties, inclusief mogelijke gebruik van back-up servers of cloud-oplossingen. ○ **Menselijke Factor**: Ontwikkel instructies voor medewerkers over hun rollen tijdens een hersteloperatie, inclusief noodcontacten en communicatieprotocollen.
Ontwikkelen van Uitwijk- en Alternatieve Werkplekken	• **Doel**: Zorgen voor fysieke en digitale uitwijkmogelijkheden als de primaire werkomgeving niet toegankelijk is. • **Acties**: ○ **Uitwijklocaties**: Identificeer en contracteer secundaire locaties waar personeel kan werken als het hoofdkantoor niet beschikbaar is. ○ **Remote Work Protocols**: Ontwikkel en implementeer beleid voor werken op afstand, inclusief beveiligde toegang tot systemen en data. ○ **Cloud Services**: Overweeg het gebruik van cloudgebaseerde diensten om uitwijkopties te bieden voor dataopslag en applicaties.
Documenteren van de Continuïteitsplannen	• **Doel**: Zorg dat alle herstelstrategieën en procedures duidelijk gedocumenteerd zijn en gemakkelijk toegankelijk zijn voor alle betrokkenen. • **Acties**: ○ **Planstructuur**: Creëer een overzichtelijke structuur voor het continuïteitsplan, met secties voor specifieke dreigingen, systemen, en herstelprocedures. ○ **Beheer van Documenten**: Implementeren van een systeem voor versiebeheer zodat de meest recente versies van de plannen beschikbaar zijn. ○ **Toegankelijkheid**: Zorg dat de plannen fysiek en digitaal beschikbaar zijn voor alle relevante stakeholders, inclusief het Crisismanagementteam (CMT) en ICT-dienstverleners.
Communicatie en Training	• **Doel**: Voorbereiden van personeel en betrokken partijen om effectief te reageren op noodsituaties volgens het continuïteitsplan. • **Acties**: ○ **Trainingen**: Organiseer trainingen voor personeel over hun specifieke rollen binnen het continuïteitsplan. ○ **Communicatieprotocollen**: Ontwikkel communicatieprotocollen voor zowel interne als externe communicatie tijdens een verstoring. ○ **Awareness Campagnes**: Voer bewustwordingscampagnes om ervoor te zorgen dat alle medewerkers bekend zijn met de noodprocedures.
Afstemming met Externe Partijen	• **Doel**: Zorgen dat externe partijen, zoals ICT-dienstverleners en uitbestedingsrelaties, afgestemd zijn op de continuïteitsplannen van SPTN. • **Acties**:

Onderwerp	Doel en acties
	○ **SLA's en Contracten**: Werk nauw samen met ICT-dienstverleners om ervoor te zorgen dat hun herstelplannen aansluiten op die van SPTN. ○ **Periodieke Overleggen**: Organiseer periodieke meetings met externe partijen om plannen te bespreken en te actualiseren. ○ **Testen en Validatie**: Zorg dat externe leveranciers betrokken zijn bij testscenario's om de effectiviteit van de gezamenlijke herstelstrategieën te valideren.
Goedkeuring en Toezicht	• **Doel**: Zorgen voor de formele goedkeuring en toezicht op de continuïteitsplannen. • **Acties**: ○ **Goedkeuring door het Bestuur**: Het continuïteitsplan moet ter goedkeuring worden voorgelegd aan het Bestuur van SPTN. ○ **Implementatie Toezicht**: Het Bestuur moet toezien op de effectieve implementatie van het plan en de naleving ervan door alle betrokkenen. ○ **Continu Monitoring**: Zorg voor voortdurende monitoring en periodieke herziening van het plan om de relevantie en effectiviteit te waarborgen.

In deze stap zijn de volgende rollen belangrijk.

(A) **Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken)** ontwikkelt en documenteert de ICT-bedrijfscontinuïteitsplannen (BCP's) die herstelstrategieën bevatten voor de geïdentificeerde kritieke systemen en processen en draagt er zorg voor dat het BCP is afgestemd op andere continuïteitsplannen binnen SPTN, zoals het Disaster Recovery Plan.

(B) De **ICT-dienstverlener** moet eraan bijdragen dat diens eigen BCP aansluit bij het BCP van SPTN en zorgen voor de noodzakelijke infrastructuur en middelen om de continuïteit te waarborgen. De ICT-dienstverlener levert hierover gedetailleerde input op ten behoeve van het BCP van het fonds.

(C) Het **Bestuur** keurt het BCP en de bijbehorende herstelstrategieën goed en zorgt ervoor dat er voldoende middelen beschikbaar zijn voor de implementatie van het BCP. Ook wordt toezicht gehouden op de naleving van het BCP en de voorbereidingen op noodsituaties.

4.5 Testen en valideren

De frequentie van tests voor het ICT-bedrijfscontinuïteitsbeleid hangt af van verschillende factoren, waaronder de aard van SPTN, het kritieke belang van de processen, en de vereisten vanuit de regelgeving zoals DORA. Algemeen wordt het volgende aangeboden:

(A) **Reguliere Tests**: Ten minste jaarlijks moeten volledige tests worden uitgevoerd van het ICT-bedrijfscontinuïteitsplan (BCP) met betrekking tot ICT-systemen die kritieke of belangrijke functies ondersteunen. Dit kan bijvoorbeeld een simulatie van een storing of een daadwerkelijke uitwijkoefening omvatten en SPTN kan een derde aanwijzen om die tests uit te voeren.

(B) **Bij Significante Veranderingen**: Elke keer dat er significante wijzigingen zijn in de ICT-infrastructuur, bedrijfsprocessen, of bij de implementatie van nieuwe technologieën, moet een test worden uitgevoerd om te bevestigen dat de BCP's nog steeds effectief zijn.

(C) **Na een Incident**: Na een verstorend incident moet het plan worden geëvalueerd en getest om te verzekeren dat eventuele aanpassingen goed functioneren.

(D) **Ad-hoc Tests**: Afhankelijk van de risicobeoordeling kunnen ad-hoc tests noodzakelijk zijn, bijvoorbeeld als er nieuwe dreigingen of kwetsbaarheden worden geïdentificeerd.

Door regelmatig te testen, kan SPTN ervoor zorgen dat het ICT-bedrijfscontinuïteitsplan robuust en effectief blijft, en dat alle betrokkenen goed voorbereid zijn om te reageren op verstoringen.

Er zijn specifieke BCP-tests die gericht zijn op ICT-omgevingen. Deze tests zijn ontworpen om de robuustheid en het herstelvermogen van ICT-systemen te waarborgen in het geval van verstoringen. In de tabel hieronder staan enkele van de belangrijkste ICT-specifieke BCP-tests.

Onderwerp	Doel en acties

Disaster Recovery (DR) Tests	• **Doel:** Testen van het vermogen van SPTN om ICT-systemen te herstellen na een ramp.
	• **Voorbeelden**:
	  ○ **Failover Tests**: Test het automatisch overschakelen van systemen naar een secundaire locatie.
	  ○ **Data Recovery Tests**: Verifieer of back-ups correct kunnen worden hersteld en binnen de vereiste tijdframes.
	  ○ **Cold, Warm, Hot Site Testing**: Test de overnamecapaciteit van de back-up locaties (afhankelijk van het type site).

Backup and Restore Tests	• **Doel**: Controleren of data back-ups correct worden uitgevoerd en of de data binnen een redelijke tijd kan worden hersteld.
	• **Voorbeelden**:
	  ○ Test de hersteltijd van kritieke gegevens van back-ups.
	  ○ Valideer de integriteit van back-upbestanden.

Incident Response Tests	• **Doel**: Simuleren van cyberaanvallen of ICT-incidenten om de respons van het ICT-team en de effectiviteit van incidentresponsprocedures te testen.
	• **Voorbeelden**:
	  ○ **Phishing** Simulation: Test de reacties van medewerkers op phishing e-mails.
	  ○ **DDoS Attack Simulation**: Simuleer een Distributed Denial of Service-aanval en test de verdediging en herstelprocessen.

Failover and Redundancy Tests	• **Doel**: Testen of de ICT-infrastructuur daadwerkelijk kan overschakelen naar redundante systemen zonder verlies van gegevens of functionaliteit. • **Voorbeelden**: ○ **Network Redundancy Tests**: Controleer of het netwerkverkeer naadloos overschakelt naar een alternatieve route.

	○ **Server Failover Tests**: Test de failover-functionaliteit van serverclusters.
Tabletop Exercises	• **Doel**: Simuleren van verstorende gebeurtenissen door middel van theoretische oefeningen en scenario's, waarbij ICT- en crisisteams gezamenlijk een incident doorlopen. • **Voorbeelden**: ○ **Scenario Planning**: Doorloop een hypothetisch scenario van een ICT-crisis, zoals een ransomware-aanval, en bespreek de stappen die moeten worden ondernomen.
Application and Data Recovery Tests	• **Doel**: Verifieer het vermogen om kritieke applicaties en data na een storing opnieuw te starten en operationeel te krijgen. • **Voorbeelden**: ○ Test het herstel van een bedrijfsapplicatie in een uitwijkcentrum. ○ Valideer de integriteit en beschikbaarheid van gegevens na herstel.
Network Recovery Tests	• **Doel**: Beoordeel de hersteltijd van netwerksystemen en de beschikbaarheid van communicatiekanalen na een netwerkuitval. • **Voorbeelden**: ○ **VPN Failover Test**: Test de functionaliteit van VPN-verbindingen bij een failover. ○ **Firewall Recovery Test**: Herstel en test firewallconfiguraties na een storing.
Operational Readiness Tests	• **Doel**: Controleren of de volledige ICT-infrastructuur in staat is om operationeel te blijven tijdens een geplande of ongeplande onderbreking. • **Voorbeelden**: ○ Complete System Restart Test: Test het vermogen om alle systemen opnieuw op te starten na een volledige stroomuitval. ○ Power Failure Simulation: Simuleer een stroomuitval om te testen of noodbatterijen en generatoren correct functioneren.

Deze tests moeten periodiek worden uitgevoerd om te zorgen dat de ICT-systemen van SPTN veerkrachtig blijven en dat eventuele tekortkomingen in het continuïteitsplan tijdig worden aangepakt. Taken en verantwoordelijkheden binnen deze stap zijn de volgende.

(A) **Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken)** is verantwoordelijk voor het plannen en uitvoeren van regelmatige tests van het ICT-Business Continuity Plan (ICT-BCP). Dit omvat onder andere failover-tests, herstel van gegevens, en simulaties van cyberaanvallen. Na de tests evalueert Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken) de resultaten en identificeert eventuele zwakke punten in de continuïteitsplannen die moeten worden verbeterd.

(B) De **ICT-dienstverlener** neemt deel aan de gezamenlijke tests om ervoor te zorgen dat hun diensten effectief hersteld kunnen worden en operationeel blijven tijdens een verstoring. Zij rapporteren de testresultaten aan de klantorganisatie en doen aanbevelingen voor verbeteringen. Op basis van de testresultaten passen zij hun eigen Business Continuity Plans (BCP's) en Disaster Recovery Plans (DRP's) aan om eventuele tekortkomingen te verhelpen.

(C) Het **Bestuur** beoordeelt de resultaten van de tests en grijpt waar nodig in om verbeteringen te eisen. Ze zien erop toe dat SPTN voldoet aan alle regelgeving met betrekking tot de frequentie en het type tests die uitgevoerd moeten worden. Bovendien is het Bestuur verantwoordelijk voor het goedkeuren van eventuele wijzigingen in het BCP die voortvloeien uit de testresultaten.

4.6 Evaluatie en Actualisatie

De stap **Evaluatie en Actualisatie** binnen het ICT-bedrijfscontinuïteitsproces is essentieel om ervoor te zorgen dat de continuïteitsplannen up-to-date blijven en effectief zijn in het geval van een verstoring. Deze stap omvat een grondige beoordeling van het bestaande continuïteitsplan, het identificeren van verbeterpunten, en het doorvoeren van noodzakelijke wijzigingen. In de tabel hieronder wordt beschreven wat er precies moet gebeuren in deze stap.

Onderwerp	Doel en acties
Evaluatie van de Effectiviteit van het Plan	• **Doel**: Bepalen of het huidige ICT-bedrijfscontinuïteitsplan (BCP) effectief is in het waarborgen van de continuïteit van kritieke ICT-diensten en -systemen. • **Acties**: ○ **Analyse van Incidenten en Oefeningen**: Evalueer de resultaten van recente tests, incidenten, of echte verstoringen om te bepalen hoe goed het plan heeft gewerkt. ○ **Feedback Verzamelen**: Verzamel feedback van medewerkers, het Crisismanagementteam (CMT), en externe partijen (zoals ICT-dienstverleners) die betrokken waren bij tests of daadwerkelijke incidenten. ○ **Prestatie-indicatoren**: Analyseer relevante KPI's (Key Performance Indicators) zoals herstelduur, data-integriteit, en communicatie-efficiëntie tijdens verstoringen.
Identificatie van verbeterpunten	• **Doel**: Vaststellen van de gebieden waar het plan tekortschiet of waar verbeteringen mogelijk zijn. • **Acties**: ○ **Gap-analyse**: Voer een gap-analyse uit om de verschillen tussen de geplande en werkelijke prestaties van het BCP te identificeren. ○ **Risicoanalyse Herzien**: Herzie de risicoanalyse om nieuwe of veranderde risico's te identificeren die mogelijk niet adequaat zijn afgedekt door het huidige plan. ○ **Lessons Learned**: Documenteer en bespreek lessen die zijn geleerd uit recente incidenten of tests, en identificeer potentiële verbeteringen.
Actualisatie van het Continuïteitsplan	• **Doel**: Bijwerken van het BCP om ervoor te zorgen dat het actueel blijft en effectief inspeelt op de huidige en toekomstige risico's. • **Acties**: ○ **Herziening van Hersteldoelstellingen (RTO/RPO)**: Controleer of de Recovery Time Objectives (RTO) en Recovery Point Objectives (RPO) nog steeds realistisch en haalbaar zijn, en pas deze zo nodig aan. ○ **Bijwerken van Procedures en Contactinformatie**: Zorg ervoor

Onderwerp	Doel en acties
	dat alle procedures, contactinformatie en verantwoordelijkheden binnen het BCP up-to-date zijn. Dit omvat wijzigingen in personeelsrollen, nieuwe technologieën, of veranderingen in de infrastructuur. ○ **Integratie van Nieuwe Technologieën**: Actualiseer het plan om rekening te houden met nieuwe technologieën of veranderingen in de ICT-omgeving, zoals cloudmigraties of nieuwe beveiligingsoplossingen.
Communicatie van Wijzigingen	• **Doel**: Zorgen dat alle relevante stakeholders op de hoogte zijn van de wijzigingen in het continuïteitsplan en hun rol daarin begrijpen. • **Acties**: ○ **Distributie van de Geactualiseerde Plannen**: Zorg ervoor dat de geactualiseerde versie van het BCP wordt verspreid naar alle betrokkenen, inclusief interne teams en externe leveranciers. ○ **Informatieoverdracht naar Externe Partijen**: Informeer ICT-dienstverleners en andere externe partijen over de wijzigingen, en zorg ervoor dat zij hun eigen plannen hierop afstemmen. ○ **Training en Oefeningen**: Organiseer aanvullende training of oefenprogramma's om personeel bekend te maken met de geactualiseerde procedures en nieuwe rollen of verantwoordelijkheden.
Goedkeuring door het Bestuur	• **Doel**: Formele goedkeuring verkrijgen voor de geactualiseerde versie van het BCP, zodat deze als officieel beleid kan worden geïmplementeerd. • **Acties**: ○ **Presentatie aan het Bestuur**: Presenteer de bevindingen van de evaluatie en de voorgestelde actualisaties aan het Bestuur. ○ **Besluitvorming**: Het Bestuur neemt een formeel besluit over de goedkeuring van de geactualiseerde plannen en wijst eventueel aanvullende middelen toe indien nodig. ○ **Toezicht op Implementatie**: Het Bestuur houdt toezicht op de implementatie van het geactualiseerde plan en zorgt dat de wijzigingen effectief worden doorgevoerd
Periodieke Herziening en Planning van de Volgende Evaluatie	• **Doel**: Bepalen van de frequentie voor toekomstige evaluaties om ervoor te zorgen dat het BCP voortdurend wordt bijgewerkt. • **Acties**: ○ **Frequentie Vaststellen**: Stel een schema op voor reguliere evaluaties, bijvoorbeeld jaarlijks of na significante organisatorische veranderingen. ○ **Plan van Aanpak**: Ontwikkel een plan voor de volgende evaluatiecyclus, inclusief wie verantwoordelijk is voor het toezicht op de evaluaties en hoe deze zullen worden uitgevoerd. ○ **Opvolging van Acties**: Zorg ervoor dat alle geïdentificeerde

Onderwerp	Doel en acties
	verbeteracties worden opgevolgd en dat er een duidelijke verantwoordingsstructuur is voor de implementatie ervan.

In deze stap zijn de volgende rollen en taken van belang

(A) **Het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken)** draagt zorg voor het periodiek beoordelen van de effectiviteit van het ICT-bedrijfscontinuïteitsplan ("ICT-BCP"), met name na incidenten, organisatorische veranderingen, of technologische upgrades. Verder draagt het Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken) zorg voor het actualiseren van de plannen op basis van nieuwe risico's, veranderde bedrijfsdoelstellingen, of na evaluatie van testresultaten.

(B) De **ICT-dienstverlener** zorgt voor regelmatige updates van hun eigen continuïteits- en herstelplannen, zodat deze blijven aansluiten bij de behoeften van de klantorganisatie. Ze zijn verplicht om melding te maken van eventuele wijzigingen in hun infrastructuur die de continuïteit kunnen beïnvloeden. Daarnaast nemen ze actief deel aan de evaluatie en aanpassing van de integrale ICT-BCP's van de klant.

(C) Het **Bestuur** beoordeelt de resultaten van de tests en is verantwoordelijk voor de goedkeuring van de geactualiseerde versies van het ICT-BCP. Het Bestuur zorgt voor een cultuur van voortdurende verbetering binnen SPTN en houdt toezicht op de implementatie van de veranderingen in de plannen.

5. ICT-Bedrijfscontinuïteitsbeleid in relatie tot andere Beleidsterreinen van DORA

Binnen DORA is een bedrijfscontinuïteitsbeleid slechts één van de vele beleidsterreinen die financiële instellingen moeten implementeren en onderhouden.

(A) **ICT-Risicomanagement:** ICT-risicomanagement vormt de basis voor het bedrijfscontinuïteitsbeleid omdat het de risico's identificeert die de continuïteit van de bedrijfsvoering kunnen bedreigen. Beide beleidsterreinen moeten nauw worden afgestemd om effectief te zijn.

(B) **Incidentmanagement:** Incidentmanagement ondersteunt het bedrijfscontinuïteitsbeleid door ervoor te zorgen dat incidenten snel en effectief worden aangepakt, waardoor de impact op de bedrijfscontinuïteit wordt geminimaliseerd.

(C) **ICT-uitbesteding:** Omdat veel kritieke bedrijfsprocessen afhankelijk kunnen zijn van externe leveranciers, moet het bedrijfscontinuïteitsbeleid ook strategieën bevatten voor het omgaan met uitbestedingsrisico's.

(D) **Incidentrapportage en Informatiedeling:** Onder DORA moeten financiële instellingen ICT-incidenten melden aan de bevoegde autoriteiten. Dit beleidsterrein beschrijft de procedures en verantwoordelijkheden voor het tijdig rapporteren van incidenten.

Effectieve incidentrapportage en informatiestroom zijn cruciaal voor het handhaven van bedrijfscontinuïteit, vooral in complexe en gecoördineerde incidenten of crises.

Het bedrijfscontinuïteitsbeleid onder DORA is een kerncomponent dat sterk afhankelijk is van en geïntegreerd moet zijn met andere beleidsterreinen zoals ICT-risicomanagement, incidentmanagement, en ICT-security. DORA vereist dat al deze terreinen naadloos samenwerken om de algehele operationele weerbaarheid van financiële instellingen te waarborgen.

6. Toetsing en Herziening van het ICT-Bedrijfscontinuïteitsbeleid

Het ICT-bedrijfscontinuïteitsbeleid moet aan de volgende eisen voldoen.

(A) **Frequentie:** Minimaal elke twee jaar worden herzien.

(B) **Bij een incident:** Direct na een groot verstorend incident worden geëvalueerd en geactualiseerd.

(C) **Wie:** Dagelijks Bestuur (ondersteund door Bureau Pensioenzaken) en goedkeuring door het Bestuur.

Bij de herziening wordt rekening gehouden en afstemming gezocht met gerelateerde beleids- en procesdocumenten, waaronder het testprogramma en het communicatiebeleid.

*****

Bijlage– Versiebeheer

Overzicht aanpassingen ICT-Bedrijfscontinuïteitsbeleid

Datum vaststelling	Versie	Auteur	Omschrijving
29-11-2024	1.0	AF Advisors	Nieuw opgesteld als gevolg van implementatie DORA verplichtingen