Incidentenregeling

Vastgesteld: 20.06.2025 [Algemeen bestuur]

Versie 3.0

1. Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van StiPP. Deze regeling geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat er sprake is van een incident binnen het fonds. Het doel van deze regeling is aldus het beschrijven van de procedure omtrent het melden, vastleggen en afhandelen van Incidenten, zodat eventuele schade kan worden voorkomen of worden beperkt en herhaling van het Incident wordt voorkomen.

Met deze regeling geeft StiPP uitvoering aan de vereisten van de Pensioenwet en de Digital Operational Resilience Act (DORA) over de omgang met en vastlegging van Incidenten.

Voor de volledigheid wordt hier vermeld dat StiPP het omgekeerd-gemengde bestuursmodel hanteert. Dit betekent dat het fonds bestuurd wordt door een algemeen bestuur. Dit algemeen bestuur bestaat uit:

- Een uitvoerend bestuur
- Een niet-uitvoerend bestuur
- Een onafhankelijk voorzitter

Meerdere van deze begrippen komen terug in onderhavige Incidentenregeling.

Artikel 1: Definities

Toezichthouder	De Nederlandsche Bank (DNB), de Autoriteit Financiële Markt (AFM), de Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de fiscus en andere publieke toezichtsorganen met jurisdictie ten aanzien van (de werkzaamheden van) StiPP.
Incident	Een gebeurtenis die een (ernstig) gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening of reputatie van StiPP en/of een gebeurtenis waarbij directe of indirecte (financiële) schade ontstaat door ontoereikende of falende interne processen, Verbonden personen of systemen of door externe gebeurtenissen dan wel een datalek zoals gedefinieerd in de Algemene Verordening Gegevensbescherming. Onder incidenten worden in ieder geval verstaan: o een (dreigende) bewuste schending van wet- en regelgeving; o een (dreiging van) bewust onjuist informeren van publieke organen; o een (dreigende) schending van binnen StiPP geldende gedragsregels; o (een dreiging van) het achterhouden, vernietigen of manipuleren van informatie over deze feiten; o een ernstig gevaar voor de integere bedrijfsuitoefening van StiPP; o gebeurtenissen die kunnen leiden tot een groot afbreukrisico in de media; o fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in de hoedanigheid van Verbonden persoon; o een (mogelijk) aanwijzing van een Toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen; o overige strafbare feiten. Er wordt een onderscheid gemaakt tussen Integriteitsincidenten, ICT-Beveiligingsincidenten, Operationele Incidenten en Overige Incidenten.
Integriteitsincident	Een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de desbetreffende organisatie.
Operationeel Incident	Een gebeurtenis die plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door StiPP en waarbij er een inbreuk is geweest op de (beheerste) bedrijfsvoering.
ICT-Beveiligingsincident	Een gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door StiPP gepland zijn en de netwerk- en informatiesystemen voor de dagelijkse uitvoering voor een integere en beheerste bedrijfsvoering in gevaar brengen,

	ofwel voor de beschikbaarheid, integriteit, authenticiteit en vertrouwelijkheid van de gegevens van StiPP. o Ernstig ICT-Beveiligingsincident: Een ICT-Beveiligingsincident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van StiPP ondersteunen. o Significante Cyberdreiging: Elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden, waarvan de technische kenmerken erop wijzen dat zij kan leiden tot een Ernstig ICT-Beveiligingsincident.
Overige Incidenten	Alle Incidenten die niet beschouwd kunnen worden als Integriteitsincidenten, ICT-Beveiligingsincidenten of Operationele Incidenten.
Compliance Officer	De functionaris die als Compliance Officer van StiPP is benoemd en verantwoordelijk is voor het uitvoeren van de compliance-werkzaamheden.
Verbonden Personen	o Leden van het algemeen bestuur; o Leden van het verantwoordingsorgaan; o Houders van sleutelfuncties; o Andere (groepen van) personen aangewezen door het algemeen bestuur van het fonds, conform de Gedragscode van StiPP.
Kritieke of belangrijke functie	Een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van StiPP, of aan de soliditeit of de continuïteit van StiPP haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door StiPP van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten.

Artikel 2: Melden, beoordelen en vastleggen van Incidenten

1. Iedere Verbonden persoon die een (vermoeden van een) Incident constateert is gehouden dit onverwijld te melden aan de Compliance Officer. Heeft het incident betrekking op de Compliance Officer, dan wordt melding gemaakt bij de onafhankelijk voorzitter van StiPP. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen ook anoniem worden gedaan.

2. Als zich bij een partij waaraan StiPP werkzaamheden heeft uitbesteed een Incident voordoet, dan meldt deze uitbestedingsrelatie het Incident aan het uitvoerend bestuur. StiPP draagt er zorg voor dat de uitbestedingsrelatie bekend is met deze regeling en weet bij wie een Incident gemeld moet worden.

3. Indien in afwijking van de voorgaande bepalingen een Incident wordt gemeld aan een andere Verbonden Persoon, verwijst deze de melder naar de Incidentenregeling voor de te volgen procedure.

4. Het staat een Verbonden persoon vrij een (vermoeden van een) Incident ook aan het uitvoerend bestuur te melden. Het uitvoerend bestuur is eraan gehouden de Compliance Officer op de hoogte te brengen.

5. De Compliance Officer, of, in het geval het een Incident betreft dat zich heeft voorgedaan bij een uitbestedingsrelatie, het uitvoerend bestuur, beoordeelt de melding en bepaalt of er sprake is van een Incident en zo ja, of er dan sprake is van een Operationeel Incident, ICT-Beveiligingsincident, Integriteitsincident of een Overig Incident. Dit oordeel wordt vastgelegd. In geval het uitvoerend bestuur van oordeel is dat het Incident dat zich heeft voorgedaan bij een uitbestedingsrelatie, een Integriteitsincident betreft, meldt het dit ook bij de Compliance Officer.

6. In het geval van (het vermoeden van) een ICT-Beveiligingsincident dienen de volgende stappen doorlopen te worden ten behoeve van de beoordeling van het Incident:
   - Ten eerste dient bepaald te worden of (het vermoeden van) het ICT-Beveiligingsincident impact heeft op kritieke processen of diensten van StiPP;
   - Indien er impact is op kritieke processen of diensten van StiPP, moet (het vermoeden van) het ICT-Beveiligingsincident geclassificeerd worden op basis van de classificatiecriteria en materialiteitsdrempels opgenomen in Bijlage 1, om te bepalen of er sprake is van een Ernstig ICT-Beveiligingsincident of een Significante Cyberdreiging;
   - Indien er geen impact is op de kritieke processen of diensten van StiPP, dient gevalideerd te worden of één of meer van onderstaande criteria van toepassing zijn om te bepalen of de melding als ICT-Beveiligingsincident behandeld dient te worden als een Ernstig ICT-Beveiligingsincident:
     - Er is sprake van een succesvolle, kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen van StiPP;
     - Er zijn gevolgen voor de financiële diensten die worden verleend door StiPP, waarvoor een vergunning of registratie vereist is, of die onder toezicht staan van de Toezichthouder.
   - Indien geconcludeerd kan worden dat het Incident geen impact heeft op kritieke processen of diensten van StiPP en de twee bovenstaande criteria uit het vorige punt niet van toepassing zijn, dient het Incident beschouwd te worden als ICT-beveiligingsincident.

7. Wanneer het Incident geclassificeerd is als Ernstig ICT-Beveiligingsincident, dient het algemeen bestuur geïnformeerd te worden met een toelichting van de effecten, de respons en de in te stellen aanvullende controles ten gevolge van dergelijke Ernstige ICT-Beveiligingsincidenten.

8. Elk kwartaal analyseert en rapporteert, indien zich ICT-beveiligingsincidenten bij het fonds hebben voorgedaan, de Compliance Officer en indien zich ICT-beveiligingsincidenten bij een uitbestedingsrelatie hebben voorgedaan, de betreffende uitbestedingsrelatie, aan het uitvoerend bestuur of terugkerende ICT-Beveiligingsincidenten samen beschouwd dienen te worden als Ernstig ICT-Beveiligingsincident. Dit is het geval indien deze incidenten aan de volgende voorwaarden voldoen:
   - De ICT-Beveiligingsincidenten hebben zich ten minste tweemaal binnen zes maanden voorgedaan;
   - De ICT-Beveiligingsincidenten hebben dezelfde onderliggende oorzaak;
   - De ICT-Beveiligingsincidenten voldoen gezamenlijk aan de classificatiecriteria uit Bijlage 1 om als een Ernstig ICT-Beveiligingsincident te worden beschouwd.

9. Meldingen van Incidenten en de oordelen van Incidenten worden geregistreerd in het Incidentenregister van StiPP, tenzij de gevoeligheid van de informatie een dergelijke registratie in de weg staat. Gedurende het verdere proces worden in het dossier van het Incident de naar het oordeel van de Compliance Officer en/of het uitvoerend bestuur relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel (extern uitgevoerd) onderzoek.

10. In het Incidentenregister dienen tevens Ernstige ICT-Beveiligingsincidenten gedocumenteerd te worden op basis van de volgende criteria:
    - Het aantal getroffen deelnemers, pensioengerechtigden, uitbestedingspartijen, financiële tegenpartijen en transacties;
    - Mate van reputatieschade;
    - Duur en uitvaltijd van de (ICT) dienst;
    - De geografische spreiding;
    - De gegevensverliezen;
    - De economische effecten.

11. Incidentendossiers worden zodanig in een beveiligde omgeving bewaard dat de vertrouwelijkheid is gewaarborgd. Indien er sprake is van de betrokkenheid van een Verbonden persoon, worden zijn identificatiegegevens op een zodanige wijze bewaard dat alleen de Compliance Officer toegang heeft tot deze gegevens.

12. De melding en de daarbij beschikbaar gestelde gegevens worden door alle betrokken partijen strikt vertrouwelijk behandeld. De identiteit van de melder wordt niet opgenomen in communicatie naar derden tenzij daartoe een wettelijke verplichting bestaat.

13. Een ieder die uit hoofde van deze regeling informatie krijgt over (de melding van) een Incident, betracht daarover uiterste geheimhouding, tenzij op basis van deze regeling of bij of krachtens de wet de bevoegdheid of de verplichting bestaat om die informatie aan een derde te verschaffen. Indien voor de afronding van het Incident openheid van zaken is vereist, kan het bestuur beslissen dat de verplichting tot geheimhouding geheel of gedeeltelijk vervalt.

Artikel 3: Behandeling van Incidenten

1. Indien de Compliance Officer of het uitvoerend bestuur van mening is dat er sprake is van een Operationeel Incident of een ICT-Beveiligingsincident, wordt dit Incident behandeld door het uitvoerend bestuur. Indien de Compliance Officer of het uitvoerend bestuur van mening is dat er sprake is of kan zijn van een Ernstig ICT-beveiligingsincident, Integriteitsincident of een Overig Incident, brengt hij/zij/hen (de voorzitter van) het algemeen bestuur op de hoogte. Door de voorzitter van het algemeen bestuur wordt, na advies van de Compliance Officer, besloten of en wanneer andere organen van StiPP, sleutelfunctiehouders en/of overige belanghebbenden op de hoogte worden gebracht van het Incident.

2. Vindt een Operationeel Incident of ICT-Beveiligingsincident plaats bij een partij aan wie StiPP werkzaamheden heeft uitbesteed, dan behandelt deze partij het Operationele Incident of ICT-Beveiligingsincident en rapporteert hierover aan het uitvoerend bestuur.

3. De Compliance Officer behandelt de Integriteitsincidenten en Overige incidenten, en analyseert en rapporteert over ICT-Beveiligingsincidenten die zich bij het fonds hebben voorgedaan, tenzij het algemeen bestuur, door informatie en na advies van de Compliance Officer, besluit dat, gelet op de aard of achtergronden van het Incident, afwikkeling door een andere functionaris of een speciaal daarvoor te benoemen Onderzoekscommissie de voorkeur geniet. Een onderzoekscommissie kan bestaan uit medewerkers van het fonds en/of externe deskundigen.

4. In geval van een Integriteitsincident of Overig Incident wordt door de onafhankelijk voorzitter, na advies van de Compliance Officer, besloten of en wanneer andere organen van StiPP, sleutelfunctiehouders en/of andere belanghebbenden op de hoogte worden gebracht van het Incident.

5. Als, in geval van een Integriteitsincident of Overig Incident, een onderzoek wordt verricht door een andere persoon dan de Compliance Officer of door een Onderzoekscommissie, dan is/zijn de onderzoeker(s) gehouden de Compliance Officer op de hoogte te brengen en te houden van alle ontwikkelingen in het onderzoek vanwege zijn/haar/hen coördinerende en registrerende rol.

6. De Compliance Officer bewaakt, indien er sprake is van een Integriteitsincident of Overig Incident of een ICT-Beveiligingsincident dat zich bij fonds heeft voorgedaan, de voortgang van het meldproces, het onderzoek, alsmede de opvolging van acties en rapporteert hierover aan het algemeen bestuur.

7. Indien een Incident betrekking heeft op de Compliance Officer, behandelt de onafhankelijk voorzitter het Incident. De rollen en taken die bij dit reglement aan de Compliance Officer zijn toebedeeld, komen alsdan volledig te vervallen.

Artikel 4: Afronding Incidenten

1. Na de behandeling van elk Incident wordt, ter afronding, door StiPP besloten of er maatregelen genomen dienen te worden. De genomen maatregelen zijn gebaseerd op de aard van het Incident en de daaruit voortvloeiende gevolgen. De maatregelen kunnen onder meer zijn gericht op het beheersen en beperken van het optredende risico, het bevestigen van geldende normen en het voorkomen van negatieve effecten – zowel intern als extern – van het Incident om herhaling in de toekomst te voorkomen. Tevens kunnen afstemmingen met uitbestedingsrelaties ook plaatsvinden om het hoogste niveau van gegevensintegriteit te borgen. De eindverantwoordelijkheid voor de afronding van het Incident en de eventuele getroffen maatregelen ligt bij het algemeen bestuur.

Artikel 5: Post Ernstig ICT-Beveiligingsincident-evaluatie

1. Na de verstoringen van kernactiviteiten ten gevolge van een Ernstig ICT-Beveiligingsincident analyseert de Compliance Officer of de uitbestedingsrelatie de oorzaken van de verstoring en identificeert verbeteringen die aangebracht dienen te worden in de ICT-activiteiten of in het kader van het ICT-bedrijfscontinuïteitsbeleid door middel van de post Ernstig ICT-Beveiligingsincident-evaluatie.

2. In de post Ernstig ICT-Beveiligingsincident-evaluatie wordt bepaald of de vastgestelde procedures zijn gevolgd en of de genomen maatregelen doeltreffend zijn geweest, onder meer met betrekking tot:

- De snelheid waarmee is gereageerd op veiligheidswaarschuwingen, en de effecten en ernst van ICT-gerelateerde Incidenten zijn vastgesteld;
- De kwaliteit en de snelheid bij het verrichten van een forensische analyse, indien deze passend wordt geacht;
- De doeltreffendheid van Incidentescalatie binnen StiPP;
- De doeltreffendheid van interne en externe communicatie.

3. Op verzoek van de bevoegde autoriteit deelt StiPP de wijzigingen die na de post Ernstig ICT-Beveiligingsincident-evaluatie zijn doorgevoerd.

Artikel 6: Rapportage

1. De voortgang van de behandeling en afronding van Incidenten wordt in de vergadering van het algemeen bestuur geagendeerd. Het algemeen bestuur is eindverantwoordelijk voor het toezien op de opvolging van de genomen acties. Namens het algemeen bestuur kunnen de Compliance Officer en/of het uitvoerend bestuur toezien op de daadwerkelijke opvolging.

2. In de rapportage(s) zoals die periodiek aan het Bestuur worden aangeboden, wordt inzicht gegeven in het aantal Incidenten en de classificatie van Incidenten dat zich in de betreffende periode heeft voorgedaan en de aard daarvan. Tevens bevat de rapportage informatie over de voortgang van de behandeling van Incidenten en naar aanleiding van deze Incidenten genomen maatregelen.

Artikel 7: Spoedeisend belang

1. Als de aard van het Incident snel handelen vereist, dan zijn de onafhankelijk voorzitter of het uitvoerend bestuur bevoegd om het Incident te behandelen en namens het algemeen bestuur een (voorlopig) besluit te nemen over de afronding van het Incident.

2. De onafhankelijk voorzitter en/of het uitvoerend bestuur is gehouden om de overige leden van het algemeen bestuur en de Compliance Officer zo snel mogelijk op de hoogte te brengen van de door hem verrichte acties en genomen (voorlopige) besluiten en deze, indien nodig, alsnog ter definitieve besluitvorming aan het algemeen bestuur voor te leggen.

Artikel 8: Melden Toezichthouder en overige communicatie

1. Door of namens het algemeen bestuur wordt onverwijld de relevante Toezichthouder over een Incident geïnformeerd als er sprake is van een Incident dat een ernstig gevaar vormt voor de beheerste en integere bedrijfsvoering. Hiervan is in ieder geval sprake als:
   - aangifte is of wordt gedaan bij justitiële autoriteiten;
   - het voortbestaan van StiPP wordt bedreigd of zou kunnen worden bedreigd;
   - er sprake is van een ernstige tekortkoming in de opzet en werking van de maatregelen ter bevordering of handhaving van een integere bedrijfsvoering door StiPP;

- mede gelet op verwachte publiciteit, rekening behoort te worden gehouden met (een ernstige mate van) reputatieschade voor StiPP;
- of de ernst, de omvang of de overige omstandigheden van het Incident in aanmerking genomen, de Toezichthouder in verband met zijn toezichtstaak redelijkerwijs, of op basis van een wettelijke verplichting, behoort te worden geïnformeerd.

2. Wanneer Ernstige ICT-Beveiligingsincidenten geconstateerd zijn, dient dit door het fonds of namens het fonds door de uitbestedingsrelatie waar het Ernstige ICT-Beveiligingsincident zich heeft voorgedaan, aan de Toezichthouder(s) gemeld te worden middels een door de Toezichthouder opgestelde template. Voor de melding van Ernstige ICT-Beveiligingsincidenten zijn de volgende rapportages en tijdslijnen van toepassing:
   - Initiële melding:
     - De initiële melding dient, ten minste binnen vier uur en niet later dan 24 uur, nadat StiPP op de hoogte is over het Ernstig ICT-Beveiligingsincident, plaats te vinden.
     - Bij de melding dient minimaal de volgende informatie opgenomen te worden; primaire informatie over het Ernstig ICT-Beveiligingsincident zoals mogelijke oorzaken, de vastgestelde impact en de betrokken systemen.
   - Tussentijds rapport:
     - Het tussentijdse rapport dient binnen 72 uur na de initiële melding en bij significante veranderingen in de situatie ingediend te worden;
     - Bij het tussentijdse rapport dient minimaal de volgende informatie opgenomen te worden; uitgebreide informatie over het Ernstig ICT-Beveiligingsincident met inbegrip van de voortgang van herstelmaatregelen en een verdere impactanalyse.
   - Eindrapport:
     - Het eindrapport dient uiterlijk één maand na de indiening van het meest recente bijgewerkte tussentijdse rapport ingediend te worden;
     - Bij het eindrapport dient minimaal de volgende informatie opgenomen te worden; volledig overzicht over het Ernstig ICT-Beveiligingsincident inclusief lessons learned en aanbevelingen voor toekomstige preventie.

3. StiPP kan Significante Cyberdreigingen op vrijwillige basis melden aan de Toezichthouder(s) wanneer zij van oordeel is dat de dreiging relevant is voor het financiële stelsel, de gebruikers van diensten of deelnemers van StiPP.

4. De Toezichthouder zal door of namens het algemeen bestuur op de hoogte worden gebracht van alle feiten, omstandigheden en achtergronden van het Incident, alsmede de maatregelen die naar aanleiding van het Incident zijn genomen.

5. Het algemeen bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot Incidenten en significante Cyberdreigingen.

6. In het geval een Ernstig ICT-Beveiligingsincident zich voordoet, wordt het crisiscommunicatieplan in gang gezet en besluit het uitvoerend bestuur welke rol fungeert als woordvoerder naar het publiek en de media. Het crisiscommunicatieplan maakt het mogelijk om ten minste Ernstig ICT-Beveiligingsincidenten of kwetsbaarheden op verantwoordelijke wijze bekend te maken aan deelnemers en tegenpartijen en, in voorkomend geval, aan het publiek.

7. In het geval van een Significante Cyberdreiging stelt StiPP in voorkomend geval, haar deelnemers die mogelijk getroffen zijn, in kennis van passende beschermingsmaatregelen die zij kunnen nemen.

8. Wanneer een Ernstig ICT-Beveiligingsincident optreedt en gevolgen heeft voor de financiële belangen van deelnemers, stelt StiPP zodra het Ernstig ICT-Beveiligingsincident te hebben opgemerkt, haar deelnemers onverwijld in kennis van het Ernstig ICT-Beveiligingsincident en van de maatregelen die zijn genomen om de negatieve gevolgen van een dergelijk Incident te beperken.

9. Op verzoek van de bevoegde autoriteit deelt StiPP een raming van de geaggregeerde jaarlijkse kosten en verliezen als gevolg van Ernstige ICT-Beveiligingsincidenten.

Artikel 9: Omgang met meldingen

1. StiPP gaat er altijd vanuit dat een melding van een Incident te goeder trouw is gedaan, tot het moment dat zij overtuigd is geraakt van het tegendeel.

2. StiPP draagt er zorg voor dat een melder, ongeacht de wijze waarop hij melding heeft gemaakt van een Incident, op geen enkele wijze in zijn positie bij StiPP benadeeld wordt, voor zover te goeder trouw gehandeld is.

3. StiPP draagt er zorg voor dat niemand wordt benadeeld in zijn of haar positie bij StiPP vanwege het uitoefenen van de taken en/of verplichtingen uit deze regeling.

4. In geval van intrekking van een melding zal StiPP, ongeacht de wijze waarop melding is gemaakt van een Incident, zich ervan vergewissen dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

5. Een Verbonden Persoon die willens en wetens heeft deelgenomen aan of veroorzaker is van een Incident, zal bij melding van dit Incident geen recht kunnen ontlenen aan de beschermingsregels, zoals die gelden voor een te goeder trouw handelende Verbonden Persoon.

Artikel 10: Overig

1. Deze regeling is vastgesteld door het algemeen bestuur en in werking getreden op 16 april 2021 en laatstelijk gewijzigd op 7 februari 2025.

Contactpersonen zoals bedoeld in dit reglement

Compliance Officer BDO / mevrouw Maters-de Groen	lilian.maters.de.groen@bdo.nl +31 6 41 57 78 67
Onafhankelijk voorzitter / mevrouw Edelenbos	edelenbos@mac.com +31 6 53 50 13 46
Uitvoerend bestuur / de heer Ganzeboom	r.ganzeboom@stippbestuur.nl +31 6 51 99 25 89

Bijlage 1: Classificatiecriteria en materialiteitsdrempels voor Ernstige ICT-beveiligingsincidenten en Significante Cyberdreigingen

Ernstige ICT-Beveiligingsincidenten

	Deelnemers, Pensioengerechtigden, Uitbestedingspartijen, financiële tegenpartijen en transacties	Mate van reputatieschade	Duur en uitvaltijd van de (ICT) dienst	Geografische spreiding	Gegevensverliezen	Economische effecten
Detail informatie	- Alle getroffen klanten, deelnemers, pensioengerechtigden of uitbestedingspartijen die niet in staat zijn om gebruik te maken van de diensten van STIPP, of zijn benadeeld door het Incident; - Alle getroffen deelnemers, pensioengerechtigden of uitbestedingspartijen met een overeenkomst met het fonds; - Relevante deelnemers, pensioengerechtigden of uitbestedingspartijen die invloed uitoefenen op de bedrijfsvoering van STIPP; - Alle getroffen monetaire transacties waarbij ten minste één van de betrokken	- Het Incident behaalt de media; - Herhaaldelijke klachten van deelnemers, pensioengerechtigden of uitbestedingspartijen - Mogelijk niet kunnen voldoen aan wet- en regelgeving; - Mogelijk verlies van uitbestedingspartijen als gevolg van het Incident. In de beoordeling wordt rekening gehouden met de mate van zichtbaarheid van het Incident op bovenstaande criteria.	- (Geschatte) duur wordt gemeten vanaf het moment dat het Incident is opgemerkt tot het moment dat het is opgelost; - Downtime van de dienst wordt gemeten vanaf het moment dat deze geheel of gedeeltelijk niet beschikbaar is voor deelnemers, pensioengerechtigden, uitbestedingspartijen of externe gebruikers, tot het moment dat de dienstverlening hersteld is tot het niveau van voor het Incident.	Bepaal de significante impact van het Incident in andere EU-lidstaten op: - Deelnemers, pensioengerechtigden, of uitbestedingspartijen - Financiële marktstructuur of third party providers die andere financiële entiteiten kunnen beïnvloeden.	- Beschikbaarheid van data: gegevens zijn tijdelijk of permanent ontoegankelijk of onbruikbaar; - Authenticiteit van data: de betrouwbaarheid van de gegevensbron is in het gedrang gebracht door het Incident; - Integriteit van data: data is onjuist of onvolledig door niet-geautoriseerde modificatie; - Vertrouwelijkheid van data: toegang tot gegevens door een niet geautoriseerde partij of systeem.	Soorten directe -en indirecte kosten en verliezen: - Vervreemde fondsen of financiële assets; - Vervangings- of relocatiekosten van software, hardware of infrastructuur; - Personeelskosten; - Fees als gevolg van non-compliance met contracten; - Compensatiekosten en schadevergoedingen; - Gederfde inkomsten; - Kosten voor adviseurs; - Kosten voor interne en externe communicatie.

	Deelnemers, Pensioengerechtigden, Uitbestedingspartijen, financiële tegenpartijen en transacties	Mate van reputatieschade	Duur en uitvaltijd van de (ICT) dienst	Geografische spreiding	Gegevensverliezen	Economische effecten
	partijen in de EU gevestigd is.					
Materialiteitdrempels Ernstig ICT-Beveiligings incident	Eén of meerdere van onderstaande criteria is van toepassing: - >10% van alle deelnemers, pensioengerechtigden, of uitbestedingspartijen maakt gebruik van de getroffen dienst; - >100.000 deelnemers, pensioengerechtigden, of uitbestedingspartijen maken gebruik van de getroffen dienst; - >30% van alle deelnemers, pensioengerechtigden, of uitbestedingspartijen van STIPP worden geraakt; - >10% van het dagelijks aantal uitkeringen wordt geraakt; - Impact op deelnemers pensioengerechtigden of uitbestedingspartijen wordt door STIPP als relevant beoordeeld.	Iedere schade aan de reputatie van STIPP, of waarbij één of meerdere van bovenstaande criteria van toepassing is.	Eén of meerdere van onderstaande criteria is van toepassing: - Het Incident duurt langer dan 24 uur; - Downtime is langer dan twee uur voor kritieke of belangrijke functies.	Het Incident heeft impact in twee of meer lidstaten in de EU.	Iedere impact op beschikbaarheid, integriteit, authenticiteit en vertrouwelijkheid van data, die een negatieve invloed heeft of zal hebben op de bedrijfsvoering van STIPP of het voldoen aan wet- en regelgeving.	(Geschatte) kosten en verliezen voor STIPP bedragen meer dan € 100.000,-

Significante Cyberdreigingen

Een Cyberdreiging wordt als significant beschouwd wanneer aan alle onderstaande voorwaarden is voldaan:	
1	De cyberdreiging, indien zij werkelijkheid wordt, kan gevolgen hebben of zou gevolgen kunnen hebben voor kritieke of belangrijke functies van STIPP, uitbestedingspartijen, deelnemers, of financiële tegenpartijen op basis van informatie waarover STIPP beschikt.
2	De cyberdreiging heeft een grote kans om werkelijkheid te worden bij STIPP of bij uitbestedingspartijen, rekening houdend met ten minste de volgende elementen: - Toepasselijke risico's in verband met de in punt 1 genoemde cyberdreiging, met inbegrip van potentiële kwetsbaarheden van de systemen van STIPP die kunnen worden uitgebuit; - De capaciteiten en intentie van dreigingsactoren voor zover bekend bij STIPP; - De aanhoudende dreiging en alle verworven kennis over ICT-Beveiligingsincidenten die gevolgen hebben gehad voor STIPP of haar uitbestedingspartijen, deelnemers of financiële tegenpartijen.
3	De cyberdreiging kan, indien zij werkelijkheid wordt aan een van de volgende situaties voldoen: - Het vastgestelde classificatiecriterium voor Ernstige ICT-Beveiligingsincidenten wordt bereikt; - De vastgestelde materialiteitsdrempel voor Ernstige ICT-Beveiligingsincidenten voor Deelnemers, Pensioengerechtigden, Uitbestedingspartijen, financiële tegenpartijen en transacties wordt bereikt; - De vastgestelde materialiteitsdrempel voor Ernstige ICT-Beveiligingsincidenten voor het classificatiecriterium Geografische spreiding wordt bereikt.
4	Wanneer STIPP, afhankelijk van het soort cyberdreiging en de beschikbare informatie, concludeert dat de volgende vastgestelde materialiteitsdrempels voor Ernstige ICT-Beveiligingsincidenten kunnen worden bereikt, kunnen deze drempels ook in aanmerking worden genomen: - De vastgestelde materialiteitsdrempel voor Ernstige ICT-Beveiligingsincidenten voor het classificatiecriterium voor Reputatieschade; - De vastgestelde materialiteitsdrempel voor Ernstige ICT-Beveiligingsincidenten voor het classificatiecriterium voor Duur en uitvaltijd van de dienst; - De vastgestelde materialiteitsdrempel voor Ernstige ICT-Beveiligingsincidenten voor het classificatiecriterium voor Gegevensverliezen; - De vastgestelde materialiteitsdrempel voor Ernstige ICT-Beveiligingsincidenten voor het classificatiecriterium voor de Economische effecten.