Operationele en ICT-gerelateerde Incidentenregeling

SBZ Pensioen is een handelsnaam van Stichting Bedrijfstakpensioenfonds Zorgverzekeraars kvk 41178751

Inhoud

Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van SBZ Pensioen (hierna: het fonds). Deze Operationele en ICT-gerelateerde Incidentenregeling geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat er sprake is van een Operationeel Incident of een ICT-gerelateerd Incident binnen het fonds. Doel van deze regeling is aldus het beschrijven van de procedure omtrent het melden, vastleggen en afhandelen van deze Incidenten zodat eventuele schade kan worden voorkomen of beperkt en herhaling van het Incident wordt voorkomen. Deze regeling is van toepassing op de gehele bedrijfsvoering van SBZ Pensioen, inclusief de uitbestede werkzaamheden.

Artikel 1 Definities

Benadeling: omvat in ieder geval elke vorm van, dreiging of poging tot schorsing, een boete als bedoeld in artikel 650 van Boek 7 van het BW, een negatieve beoordeling, een schriftelijke berisping, discriminatie, intimidatie, smaad of laster, voortijdige beëindiging van een overeenkomst voor het leveren van goederen of diensten.

Betrokkene: iedere persoon die werkzaamheden gaat verrichten, verricht of heeft verricht voor, dan wel betrokken is of is geweest bij het fonds (dit met inbegrip van Verbonden personen).

Betrokken derde: een natuurlijk persoon verbonden met de Melder die kan worden benadeeld door de organisatie waar de Melder werkzaamheden voor verricht dan wel een persoon waarmee de Melder verbonden is binnen de context van diens werkzaamheden. Een rechtspersoon die eigendom is van de Melder, waarvoor de Melder werkt of deze binnen de context van diens werkzaamheden verbonden is.

Incident: Een gedraging of gebeurtenis die een ernstig gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening van het fonds. Deze regeling ziet toe op operationele incidenten en ICT-gerelateerde incidenten:

- **ICT-gerelateerd incident**: één gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door de financiële entiteit zijn gepland en die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of op de door de financiële entiteit verleende diensten;
- **Ernstig ICT-**gerelateerd Incident: een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen.
- **Operationeel incident**: een incident dat plaats heeft gevonden in de dagelijkse uitvoering van werkzaamheden door het fonds en waarbij een inbreuk is geweest op de beheerste bedrijfsvoering.

Het proces met betrekking tot ICT-gerelateerde incidenten dient te voldoen aan compliance en risicobeheersing. Indien relevant zijn in de beschrijving van het incidentenproces voor dit type Incidenten specifieke stappen opgenomen.

Incidentenregister: een register waarin de Uitvoerende Bestuursleden Incidenten vastleggen. Dat zijn Incidenten met betrekking tot het pensioen- en vermogensbeheer en de bestuursomgeving van het fonds.

Integriteitsincidenten: incidenten met een of meerdere kenmerken van een (ernstig) integriteitsincident zijn een gedraging of gebeurtenis als die in ieder geval:

a. Een strafbaar feit oplevert,
b. een schending inhoudt van interne of externe regelgeving of beleidsregels, waaronder de gedragscode,
c. autoriteiten of personen die belast zijn met de uitvoering van of het toezicht de naleving van wettelijke regelingen, of wettelijke opsporingsambtenaren beoogt te misleiden,
d. beoogt dat informatie over de hiervoor genoemde feiten wordt achtergehouden of,
e. op enigerlei wijze direct of indirect de goede naam van het fonds kan schaden.
f. leidt tot datalekken zoals beschreven in artikel 33 en 34 AVG (ook als zij een IT-component kennen).
g. leidt tot een Misstand, waarbij het maatschappelijk belang in het geding is bij de schending van een wettelijk voorschrift, een gevaar voor de volksgezondheid, een gevaar voor de veiligheid van personen, een gevaar

voor de aantasting van het milieu of een gevaar voor het goed functioneren van het fonds als gevolg van een onbehoorlijke wijze van handelen of nalaten. Ook ongewenst gedrag kan in bepaalde situaties een misstand zijn.

Melder: iedere persoon die in het kader van de Incidentenregeling een melding doet van een Incident.

Toezichthouder: De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de fiscus en overige publieke toezichtorganen met jurisdictie ten aanzien van (de werkzaamheden van) SBZ Pensioen.

Verbonden persoon (overeenkomst artikel 1.1 van de gedragscode van SBZ Pensioen):

a. De leden van het Bestuur van SBZ Pensioen (verder: het fonds);
b. De leden van het Verantwoordingsorgaan van het fonds;
c. Externe leden van commissies;
d. Sleutelfunctiehouders;
e. Het Bestuur kan andere (groepen van) personen als verbonden persoon aanwijzen.

Medewerkers van uitbestedingspartners zijn geen verbonden personen, tenzij deze op basis van lid e van dit artikel wel als zodanig door het Bestuur zijn aangewezen. Het fonds heeft afspraken met uitbestedingspartijen over het verplicht melden van incidenten aan het fonds.

Vertrouwelijk: niet openbaar of publiek maken van verkregen informatie of van omstandigheden waarin een Incident zich heeft voorgedaan dan wel de gevolgen van dat Incident.

Artikel 2 Melden, beoordelen en vastleggen van Incidenten

1. Het Bestuur van het fonds zal ervoor zorgdragen dat deze regeling bekend is bij Verbonden personen en uitbestedingspartijen.

2. Iedere Melder die een (dreigend) Incident constateert, is gehouden dit tijdig en duidelijk te melden aan de Uitvoerende Bestuursleden, direct of via bestuursondersteuning. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. De Uitvoerende Bestuursleden bevestigen de ontvangst van een mondelinge melding schriftelijk aan de melder en dragen zorg voor de registratie in het register.

3. De Uitvoerende Bestuursleden ontvangen zoals omschreven in artikel 2.2 de meldingen en beoordelen of het een Incident betreft in de zin van deze regeling. Bij de beoordeling kan advies van een derde worden ingewonnen, afhankelijk van waar het incident over gaat en wat voor type Incident het betreft. De Uitvoerende Bestuursleden beoordelen tevens of het Incident samenhangt met andere Incidenten en beoordeelt in dat geval de relevante Incidenten als één groot incident (zie hiertoe ook Bijlage 1, vereiste 15.1).

   Ook classificeren zij het Incident, waarbij de classificatiecriteria in lijn zijn gebracht met de risicokwantificatie van de niet-financiële risico's uit het Risicomanagementbeleid van het fonds:

Schaal	Impact Risicomanagementbeleid	Classificatie Incidenten
4	Hoog	Hoog
3	Aanzienlijk	Additioneel: ernstig (in geval van ICT-gerelateerde incidenten, zie hiertoe Bijlage 1)
2	Beperkt	Middel
1	Laag	Laag

Ook informeren zij in dit stadium de Sleutelfunctiehouder Risicobeheer over de melding wanneer dit, gelet op de aard van de melding, in het belang is van adequaat risicobeheer.

4. Het Bestuur beslist over communicatie, zowel intern als extern, met betrekking tot Incidenten.

5. Meldingen van Incidenten worden namens de Uitvoerende Bestuursleden geregistreerd in een Incidentenregister (door bestuursondersteuning). Gedurende het verdere proces worden in het dossier de naar het oordeel van de Uitvoerende Bestuursleden (ondersteund door bestuursondersteuning) relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages, de resultaten van eventueel onderzoek, wijze van opvolging, de genomen preventieve en repressieve maatregelen en de meldingen aan de relevante toezichthouder(s).

6. Eenieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een Incident behandelt dat als vertrouwelijk, 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 deze verplichting geheel of gedeeltelijk vervalt.

7. **Beveiliging van informatie:** De locatie waar het Incidentenregister en relevante documentatie met betrekking tot een incident is opgeslagen is enkel toegankelijk voor daartoe geautoriseerde personen:
    - Voor Operationele en ICT-gerelateerde incidenten betreft dit: Bestuur, Sleutelfunctiehouder Risicobeheer en Internal Audit, Bestuursondersteuning.
    - Voor Integriteitsincidenten betreft dit: de externe Compliance Officer.

    Bovenstaande toegangsrechten zijn gereflecteerd in de autorisatiematrix van het fonds, naleving hiervan wordt periodiek gecontroleerd. Indien relevante documentatie gedeeld dient te worden in het kader van deze regeling neemt de verzender adequate beveiligingsmaatregelen in acht, waaronder:
    - Informatie wordt enkel gedeeld op een need-to-know basis (beperk ontvangers).
    - Informatie wordt op een beveiligde manier gedeeld (bijvoorbeeld beveiligde transfer of encryptie van berichten in geval van gevoelige persoonsgegevens of cybersecurity gevoelige informatie zoals een forensisch rapport).

8. **Retentieduur:** Relevante documentatie wordt per incident opgeslagen, en bewaard in lijn met het archiefbeleid van het fonds.

Artikel 3 Behandeling van Incidenten met classificatie ‘laag’ of midden’

1. Indien de Uitvoerende Bestuursleden van mening zijn dat er sprake is van een Incident met classificatie ‘laag’ of ‘midden’ dan brengen zij de voorzitter van de Audit- Risk- en Compliance commissie daarvan achteraf per e-mail op de hoogte. Vanwege hun karakter en aard is bij deze categorie meldingen geen standaard betrokkenheid en taak voor de Compliance Officer weggelegd, tenzij een Incident aantoonbaar het gevolg is van moedwillig niet compliant handelen.

2. Na de behandeling van elk Incident wordt door de Uitvoerende Bestuursleden besloten of er (aanvullende) beheersmaatregelen genomen dienen te worden. De genomen beheersmaatregelen zullen 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. De eindverantwoordelijkheid voor de afronding van het Incident en de eventuele getroffen maatregelen ligt bij de Uitvoerende Bestuursleden.

Artikel 4 Behandeling van Incidenten met classificatie ‘hoog’ of ‘ernstig’

1. De Uitvoerende Bestuursleden melden Incidenten met classificatie ‘hoog’ of ‘ernstig’ eerst aan de voorzitter van het Bestuur en voorzitter van de Audit-, Risk- en Compliancecommissie en dan aan het voltallige Bestuur. De Uitvoerende Bestuursleden houden het Bestuur op de hoogte van de behandeling en afhandeling van het Incident, de impact op de dienstverlening van het fonds, en de genomen maatregelen om het Incident in de toekomst te voorkomen en/of de impact te verlagen.

2. Het Incident kan het Crisis Protocol van het fonds activeren. In dat geval worden de stappen en procedures van het Crisis Protocol gevolgd, waarbij de Uitvoerende Bestuursleden bewaken dat de behandeling en afhandeling van het ‘hoog’ of ‘ ernstig’ Incident tevens volgens de Incidentenregeling plaatsvindt.

Artikel 5 Melding van ICT-gerelateerde incidenten aan de toezichthouder

1. Het fonds legt afspraken vast met uitbestedingspartijen wie verantwoordelijk is voor het doen van een melding bij de toezichthouder indien een Incident classificeert als ‘ernstig’. Onverlet de afspraken blijven de Uitvoerende Bestuursleden nauw betrokken bij de behandeling en oplossing van het Incident. Voor het tijdig melden van Incidenten door de uitbestedingspartij aan het fonds heeft het fonds afspraken vastgelegd in de SLA en overeenkomst met uitbestedingspartijen.

2. ICT-gerelateerde Incidenten geclassificeerd als ‘ernstig’ meldt het Bestuur, of de uitbestedingspartij waar het incident zicht voordoet indien dit is afgesproken, aan de toezichthouder. Daarvoor wordt het format zoals opgenomen in tab ‘Template melding ICT-gerelateerd incident’ in het Incidentenregister gebruikt. Voor het melden van ICT-gerelateerde Incidenten geclassificeerd als ‘ernstig’ zijn onderstaande tijdslijnen toepassing:

- **Initiële melding:** In het geval van ‘ernstige’ ICT-gerelateerde Incidenten wordt de melding aan de toezichthouder binnen 24 uur na ontvangst van de melding en binnen 4 uur van classificatie als ‘ernstig’ ICT-gerelateerd incident gedaan of, wanneer deze deadline op een weekenddag of feestdag valt, voor het middaguur van de eerste daarop volgende werkdag (RTS voor art.20.a (Hoofdstuk III)). Wanneer een incident later dan 24 uur na ontvangst als ‘ernstig’ wordt geclassificeerd wordt deze binnen 4 uur van wijziging van de classificatie gemeld aan de toezichthouder.
- **Tussentijds rapport:** Er wordt in ieder geval binnen 72 uur na initiële melding en wanneer reguliere werkzaamheden zijn hersteld een tussentijd rapport met de toezichthouder gedeeld. Wanneer deze deadline op een weekenddag of feestdag valt, kan dit voor het middaguur van de eerste daarop volgende werkdag.
- **Eindrapport:** Het Bestuur stuurt de toezichthouder binnen een maand na het sturen van het laatste tussentijdse rapport of, wanneer deze deadline op een weekenddag of feestdag valt, voor het middaguur van de eerste daarop volgende werkdag, het eindrapport inzake het incident.

3. Wanneer tijdslijnen van incidentmelding niet worden gehaald informeert het Bestuur de toezichthouder zo snel mogelijk, en binnen de relevante tijdslijnen, met uitleg over de vertraging.

4. Wanneer het Bestuur een vrijwillige melding ten aanzien van significante cyberdreigingen doet bij de toezichthouder wordt hiervoor het template uit DORA gehanteerd. Deze is opgenomen in het Incidentenregister tabblad ‘Template melding cyberdreiging’.

5. Voor het invullen van het format voor de rapportages voor de melding aan de toezichthouder is het volgende van toepassing:

- Datavelden van latere rapporten kunnen in een eerder rapport ingevuld worden wanneer de relevante informatie beschikbaar is.
- De informatie in de initiële incidentenmelding, tussentijdse rapporten, en het eindrapport is compleet en nauwkeurig.
- Wanneer nauwkeurige data niet beschikbaar is bij het rapporteren van de initiële incidentmelding of een tussentijdsrapport gebruikt het fonds geschatte waardes op basis van beschikbare data.

- Bij het indienen van tussentijdse rapporten of het eindrapport werkt het fonds informatie uit eerdere rapporten bij waar van toepassing.
- De initiële melding, tussentijdse rapporten, en/of het eindrapport mogen gecombineerd ingediend worden wanneer reguliere activiteiten zijn hersteld en/of de Root Cause Analyse is uitgevoerd zolang de juiste tijdslijnen worden gevolgd.
- Wanneer herhaalde incidenten individueel niet als 'ernstig' ICT-gerelateerd incident classificeren maar gezamenlijk wel, dient het fonds hier geaggregeerde informatie over in bij de toezichthouder.
- De initiële melding, tussentijdse rapporten, en het eindrapport betreffende incidenten aan de toezichthouder worden gemeld via de door de toezichthouder bepaalde kanalen en afwijking hiervan gebeurt enkel na overleg met de toezichthouder;
- Wanneer over een eerder als 'ernstig' gerapporteerd ICT-gerelateerd incident blijkt dat deze nooit heeft voldaan aan de criteria voor een incident van deze soort dient het fonds een rapport in bij de toezichthouder waarin wordt beschreven waarom dit incident naar 'niet ernstig' is geherclassificeerd middels invulling van de velden 'Type of report' en 'Other information'.
- Wanneer het wegens technische omstandigheden niet mogelijk is om het incident aan de toezichthouder te melden via 'Template melding ICT-gerelateerd incident' zal het Uitvoerend Bestuur de toezichthouder op andere wijze voorzien van de nodige informatie waarmee de toezichthouder kan bepalen hoe kritiek het incident is.
- Tussentijdse rapporten worden onder andere opgesteld op aanvraag van de toezichthouder.
- Er wordt een eindrapport naar de toezichthouder gestuurd nadat er een Root Cause Analyse is uitgevoerd.

6. Templates voor het doen van een melding of het verstrekken van informatie aan de toezichthouder zijn in het Engels opgesteld. SBZ Pensioen doet dergelijke meldingen in het Engels en/of verwacht dit ook van haar uitbestedingspartijen.

7. Voor elk ICT-gerelateerd Incident met classificatie 'ernstig' berekent het Bestuur de gerelateerde kosten en verliezen en levert deze aan in de rapportages aan de toezichthouder.
De toezichthouder kan daarnaast op eigen initiatief een overzicht van de kosten en verliezen in een specifieke referentieperiode opvragen bij het fonds. Het berekenen van deze kosten en het template voor het aanleveren van dit overzicht is opgenomen in Bijlage 2.

Artikel 6 Evaluatie van ICT-gerelateerde incidenten

1. De Uitvoerende Bestuursleden evalueren het ICT-gerelateerd incident op onderstaande punten en leggen de beoordeling vast in het Incidentenregister:
- **Samenhang:** De samenhang met andere incidenten: zijn er terugkerende patronen of verbanden met eerdere incidenten? Is er sprake van structurele risico's?
- **Incidentescalatie:** was de incidentescalatie effectief in het versnellen van besluitvorming en interventie?
- **Preventie & detectie:**
    - Was het incident te voorkomen?
    - Hoe snel werd gereageerd op beveiligingsmeldingen en het bepalen van de impact van ICT-gerelateerde incidenten en diens ernst?
- **Oorzaakanalyse:** is de kernoorzaak vastgesteld en geadresseerd? Wat was de kwaliteit en snelheid van forensische analyse waar van toepassing?
- **Impactanalyse:** wat was de impact op processen, financiën en reputatie?
- **Communicatie:** was de interne en externe communicatie tijdig en effectief?
- **Lessons learned:** welke structurele verbeteringen zijn geïdentificeerd?

Artikel 7 Rapportage

1. De Uitvoerende Bestuursleden rapporteren over ICT-gerelateerde incidenten die als ‘laag’ of ‘midden’ zijn geclassificeerd aan het Bestuur. Voor overige classificaties is de rapportagelijn beschreven in de eerdere artikelen van deze regeling.

2. De Uitvoerende Bestuursleden beoordelen maandelijks het bestaan van terugkerende incidenten.

Artikel 8 Spoedeisend belang

Bij spoedeisend belang zijn de Uitvoerende Bestuursleden na afstemming met de voorzitter van de Audit-, Risk- en Compliance commissie gerechtigd om een voorlopig besluit te nemen over de afhandeling van een Incident. De Uitvoerende Bestuursleden stellen de leden van het Bestuur zo snel mogelijk op de hoogte van de verrichte acties en genomen (voorlopige) besluiten.

Artikel 9 Rechtsbescherming

1. Het Bestuur zal de Melder niet benadelen in verband met het te goeder trouw en naar behoren melden van een vermoeden van een Incident.

2. Van Benadeling als bedoeld in artikel 9.1 is ook sprake als een redelijke grond aanwezig is om de Melder aan te spreken op zijn functioneren of een benadelende maatregel als bedoeld in lid 3 jegens hem te nemen, maar de maatregel die het fonds neemt niet in redelijke verhouding staat tot die grond.

3. Indien het Bestuur jegens de Melder binnen afzienbare tijd na het doen van een melding overgaat tot het nemen van een benadelende maatregel motiveert het waarom het deze maatregel nodig acht en dat deze maatregel geen verband houdt met het te goeder trouw en naar behoren melden van een vermoeden van Incident.

4. Het Bestuur draagt er zorg voor dat leidinggevenden en collega’s van de Melder zich onthouden van iedere vorm van Benadeling in verband met het te goeder trouw en naar behoren melden van een vermoeden van een Incident, die het professioneel of persoonlijk functioneren van de Melder belemmert.

5. Het Bestuur spreekt Verbonden personen die zich schuldig maken aan Benadeling van de Melder daarop aan en kan hen een waarschuwing of een disciplinaire maatregel opleggen.

6. In geval de Melder de melding intrekt, vergewist het Bestuur zich ervan dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

Artikel 10 Integriteitsincidentenregeling

Het fonds beschikt tevens over een Integriteitsincidentenregeling. Deze regeling is van toepassing bij Integriteitsincidenten. Indien een gebeurtenis kwalificeert als een Integriteitsincident, dan kan de Melder de procedure zoals beschreven in de Integriteitsincidentenregeling volgen.

Artikel 11 Klokkenluidersregeling

Het fonds beschikt tevens over een Klokkenluidersregeling. Deze regeling is van toepassing op integriteitsmeldingen die voldoen aan de criteria van een Misstand of een inbreuk op Unierecht. Er is sprake van een Klokkenluidersincident als de Melder besluit om een melding te doen buiten het fonds en/of direct de publiciteit zoekt. Onder de Wet bescherming klokkenluiders is het volgen van een intern meldproces niet langer verplicht. Extern melden kan ook het gevolg zijn van onvrede bij de Melder over de manier waarop, dan wel de uitkomst van een intern onderzoek naar aanleiding van een melding door de Melder.

Artikel 12 Regeling datalekken

Het fonds beschikt tevens over een Regeling datalekken. Deze regeling is van toepassing bij (een vermoeden van) een datalek. Indien een gebeurtenis kwalificeert als een datalek, dan kan de Melder de procedure zoals beschreven in de Regeling datalekken volgen.

Artikel 13 Overig

Deze regeling is vastgesteld door het Bestuur op 16 december 2024 en treedt in werking op 16 december 2024.

Deze regeling wordt ten minste een keer in de drie jaar geëvalueerd en geactualiseerd via de Audit-, Risk- en Compliance commissie, tenzij tussentijds sprake is van belangrijke wijzigingen. Dan wordt deze Regeling onverwijld aangepast.

Zeist, 16 december 2024.

Ties Tiessen
Onafhankelijk voorzitter

Edwin Schokker
Uitvoerend bestuurslid

Bijlage 1: Classificatieschema en materialiteitsdrempels 'ernstige' ICT-gerelateerde incidenten

Een ernstig ICT-gerelateerd Incident betreft een incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van het fonds ondersteunen.

Deze bijlage bevat de uitwerking van RTS 83 van de DORA wetgeving. Een incident zal overeenkomstig artikel 8 geclassificeerd worden als 'ernstig' indien:

1. Het impact heeft op kritieke dienstverlening van het fonds;
2. De materialiteitsdrempel uit RTS 83, artikel 13.b (opgenomen in onderstaande tabel) is behaald;
3. Twee of meer materialiteitsdrempels in deze bijlage zijn behaald.

De nummering in onderstaande tabel refereert aan DORA RTS 83 sectie I en sectie II volgens formaat: [artikel.lid.sub]

Classificatie categorieën	**Classificatie criteria**	**Materialiteitsdrempels ernstige incidenten**	**Materialiteitsdrempels significante cyberdreiging**
Deelnemers, financiele tegenpartijen en transacties (artikel 1)	1.1 Aantal deelnemers dat door het incident geen gebruik heeft kunnen maken van de dienstverlening van het fonds of negatieve effecten heeft ervaren.	9.1.a) Aantal deelnemers > 10 %	16.1 Een cyberdreiging wordt als significant beschouwd wanneer aan **alle** voorwaarden is voldaan: a) de cyberdreiging kan gevolgen hebben of zou gevolgen kunnen hebben voor kritieke of belangrijke functies van het fonds, of voor andere financiële entiteiten, derde aanbieders, cliënten of financiële tegenpartijen, op basis van informatie waarover Het fonds beschikt; b) de cyberdreiging heeft een grote kans om werkelijkheid te worden bij het fonds of bij andere financiële entiteiten, zoals uiteengezet in 16.2. c) De cyberdreiging kan de criteria in artikel 6 of de materialiteitsdrempels in artikel 6 en 12 overschrijden deze zich voordoet. Indien, afhankelijk van de type dreiging en beschikbare informatie, het fonds concludeert dat de materialiteitsdrempel in artikelen 10, 11, 13 en 14 overschreden zouden kunnen worden wanneer de cyberdreiging zich voordoet kunnen deze ook overwogen worden. 16.2 Bij het beoordelen van de kans dat een cyberdreiging materialiseert t.b.v. artikel 16.1 neemt het fonds tenminste het volgende in acht:
		9.1.b) Aantal deelnemers > 100 000	
	1.2 Aantal financiële tegenpartijen dat een overeenkomst heeft met het fonds en diensten uitvoeren gerelateerd aan de dienstverlening geraakt door het incident.	9.1.c) Aantal financiële tegenpartijen > 30 %	
	1.3 Met betrekking tot de relevantie van deelnemers en financiële tegenpartijen houdt het fonds rekening met de mate waarin de impact op een cliënt of een financiële tegenpartij de implementatie van de bedrijfsdoelstellingen van de financiële entiteit zal beïnvloeden, evenals met de potentiële impact van het incident met betrekking tot de marktefficiëntie.	9.1.f) Elke geïdentificeerde impact voor deelnemers of financiële tegenpartijen die als relevant zijn aangemerkt onder 1.3.	
	1.4 Hoeveelheid of aantal transacties waarbij een geldbedrag betrokken is waarbij ten minste één deel van de transactie in de EU wordt uitgevoerd	9.1.d) Aantal transacties > 10 % het gemiddelde dagelijkse aantal uitgevoerde transacties	
		9.1.e) Waarde transacties > 10 % de dagelijkse gemiddelde waarde van de uitgevoerde transacties	
	1.5 Indien het fonds het daadwerkelijk aantal deelnemers, financiële tegenpartijen of aantal/ waarde van de transacties beïnvloed door het incident niet kan bepalen, maakt het fonds een inschatting hiervan op basis van beschikbare gegevens van vergelijkbare referentieperiodes.	9.2 Indien het fonds het daadwerkelijk aantal deelnemers, financiële tegenpartijen of aantal/ waarde van de transacties beïnvloed door het incident niet kan bepalen, maakt het fonds een inschatting hiervan op basis van beschikbare gegevens van vergelijkbare referentieperiodes.	

Reputatieschade (artikel 2)	2.1. De mate van zichtbaarheid die het incident heeft of wellicht zal hebben met betrekking tot tenminste één van de volgende criteria: a) Er is over het incident bericht in de media; b) Het incident heeft geleid tot herhaalde klachten van verschillende cliënten of financiële tegenpartijen over diensten of kritieke zakelijke relaties c) […] zal als gevolg van het incident niet in staat zijn om aan de wettelijke vereisten te voldoen; d) Verlies van cliënten of financiële tegenpartijen met als gevolg een materiële impact op de bedrijfsvoering van het fonds.	10. Elke impact voortkomend uit 2.1.a)-d) zal resulteren in het overschrijden van de materialiteitsdrempel.	a) toepasselijke risico's in verband met de cyberdreiging op kritieke of belangrijke functies zoals benoemt in artikel 16.1.a., met inbegrip van potentiële kwetsbaarheden van de systemen van de financiële entiteit die kunnen worden uitgebuit. b) de capaciteiten en intentie van dreigingsactoren voor zover bekend bij het fonds. c) de aanhoudende dreiging en alle verworven kennis over incidenten die gevolgen hebben gehad voor de financiële entiteit of haar derde aanbieder, cliënten of financiële tegenpartijen.
Duur en uitvaltijd van de dienst (artikel 3)	3.1. Meten duur van incident vanaf: - Het moment waarop het incident zich voordoet tot het moment het is opgelost; of - Het moment het incident is ontdekt; of - Het moment waarop het incident is geregistreerd in netwerk- of systeemlogbestanden of andere gegevensbronnen.	11.a) Incident duurt > 24 uur	
	3.2 Meten uitvaltijd van de dienst vanaf: - Het moment dat de dienst geheel of gedeeltelijk niet beschikbaar is voor cliënten, financiële tegenpartijen of andere interne of externe gebruikers tot het moment waarop de reguliere activiteiten of verrichtingen zijn hersteld tot het niveau van dienstverlening dat vóór het incident werd verleend - Indien de uitvaltijd van de dienst vertraging veroorzaakt nadat de geregelde activiteiten of activiteiten zijn hersteld, wordt de uitvaltijd gemeten vanaf het begin van het incident tot het moment waarop die vertraagde dienst volledig wordt verleend. - Indien het tijdstip dat de dienst uitviel niet te bepalen is, wordt de uitvaltijd gemeten vanaf het moment dat deze werd ontdekt.	11.b) Uitvaltijd van de dienst > 2 uur voor ICT-diensten die kritieke of belangrijke functies ondersteunen	
Geografische spreiding (artikel 4)	4. Incident heeft significante gevolgen voor: a) Cliënten en financiële tegenpartijen in andere lidstaten; b) Zuster/dochterondernemingen of andere financiële entiteiten binnen de groep die activiteiten verrichten in andere lidstaten; c) Financiële marktinfrastructuren of derde aanbieders, die potentieel gevolgen kunnen hebben voor andere financiële entiteiten in andere lidstaten waaraan zij diensten verlenen, voor zover dergelijke informatie beschikbaar is bij het fonds.	12. incident heeft gevolgen in 2 of meer lidstaten.	
Gegevensverliezen (artikel 5)	5.Voor het bepalen van gegevensverliezen houdt het fonds de volgende criteria aan: - **5.1 Beschikbaarheid van de gegevens:** Gegevens zijn tijdelijk of permanent ontoegankelijk of onbruikbaar.	13. Indien aan één van de volgende criteria wordt voldaan:	

	- **5.2 Authenticiteit van gegevens**: De betrouwbaarheid van de gegevensbron is in het gedrang gebracht. • **5.3 Integriteit van de gegevens:** Incident heeft geleid tot niet-toegestane wijzigingen van gegevens waardoor die onjuist of onvolledig zijn geworden. • **5.4 Vertrouwelijkheid van gegevens:** Gegevens zijn geraadpleegd door of vrijgegeven aan een niet-gemachtigde partij of systeem.	a) Een effect op de criteria heeft een negatief effect of zal een negatief effect hebben op de verwezenlijking van de bedrijfsdoelstellingen of op het vermogen om aan de regelgevingsvereisten te voldoen; b) een succesvolle, kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen niet ondervangen in a) waarbij die toegang tot gegevensverliezen kan leiden.	
Mate waarin getroffen diensten als cruciaal kunnen worden aangemerkt (artikel 6)	6. Incident beïnvloedt kritieke diensten, waaronder transacties en bedrijfsvoering: a) Het incident heeft gevolgen (gehad) voor ICT-diensten of netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen; b) Incident heeft gevolgen (gehad) voor financiële diensten waarvoor een vergunning of registratie vereist is of die onder toezicht staan van bevoegde autoriteiten; c) Incident uit zich in een succesvolle, kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen.	Het ICT-gerelateerd incident classificeert, in lijn met artikel 8, 'ernstig' indien aan één van de drie voorwaarden is voldaan.	
Economische effecten (artikel 7)	7.1. Voor het bepalen van de economische effecten houdt het fonds rekening met de volgende directe en indirecte kosten en verliezen: a) onteigende gelden of financiële activa waarvoor zij aansprakelijk zijn, met inbegrip van door diefstal verloren gegane activa; b) kosten voor de vervanging of verplaatsing van software, hardware of infrastructuur; c) personeelskosten, incl. kosten in verband met de vervanging of verhuizing van personeel, de aanwerving van extra personeel, de bezoldiging voor overuren en het terugverdienen van verloren of verminderde vaardigheden; d) vergoedingen wegens niet-naleving van contractuele verplichtingen; e) kosten voor verhaal en compensatie voor klanten; f) verliezen als gevolg van gederfde inkomsten; g) kosten voor interne en externe communicatie; h) advieskosten, met inbegrip van kosten in verband met juridisch advies, forensische diensten en saneringsdiensten. 7.2 Kosten en verliezen voor de reguliere bedrijfsvoering worden niet in rekening gebracht, specifiek:	14.1 Kosten en verliezen overstijgen (naar alle waarschijnlijkheid) > 100 000 euro 14.2 Het fonds sommeert de kosten en verliezen van onderdelen 7.1a)-h). 14.3 Indien kosten en verliezen niet bepaald kunnen worden, maakt het fonds een inschatting op basis van beschikbare data.	

	a) kosten voor algemeen onderhoud van infrastructuur, materiaal, hardware, software, infrastructuur, en kosten voor het up-to-date houden van de vaardigheden van het personeel; b) interne of externe kosten om het bedrijf na het incident te verbeteren, met inbegrip van upgrades, verbeteringen en risicobeoordelingsinitiatieven; c) verzekeringspremies. 7.3 Het Uitvoerend Bestuur berekent de kosten en verliezen op basis van gegevens beschikbaar gedurende het classificeren van het incident. Indien kosten en verliezen niet bepaald kunnen worden, maakt het fonds een inschatting.		
Terugkerende incidenten	n.v.t.	15.1 Terugkerende incidenten die afzonderlijk geen groot incident vormen, worden als één groot incident beschouwd indien de incidenten aan alle volgende voorwaarden voldoen: a) de incidenten hebben zich binnen zes maanden minimaal twee keer voorgedaan; b) de incidenten hebben dezelfde schijnbare hoofdoorzaak. c) de incidenten worden gezamenlijk geclassificeerd als een groot incident overeenkomstig artikel 8. 2. Het fonds beoordeelt maandelijks het bestaan van terugkerende incidenten.	

Bijlage 2: Kosten en verliezen ICT-gerelateerde incidenten

De toezichthouder kan op eigen initiatief een overzicht van de kosten en verliezen gerelateerd aan ICT-gerelateerde incidenten in een specifieke referentieperiode opvragen bij het fonds. DORA stelt vereisten aan het berekenen van kosten en verliezen als gevolg van ICT-gerelateerde incidenten, welk nader is toegelicht in 'GL 34 on costs & losses', in 'Title III'. De vereisten hieromtrent zijn in deze bijlage uitgewerkt.

Berekenen van kosten en verliezen

Voor het berekenen van kosten en verliezen gerelateerd aan een ICT-gerelateerd incident stelt DORA de volgende vereisten (de nummering verwijst naar het relevante artikel):

- 5. Kosten en verliezen dienen per de gevraagde referentieperiode te worden berekend. Het fonds kan kiezen om de referentieperiode van een boekjaar of kalenderjaar aan te houden.
- 6. Tenminste de volgende incidenten dienen te worden opgenomen:
    - (a) ICT-gerelateerde incidenten met classificatie 'ernstig;
    - (b) ICT-gerelateerde incidenten waarvoor een finale rapportage is ingediend bij de toezichthouder;
    - (c) Elk incident waarvoor het fonds in de referentie periode een kwantificeerbare financiële impact ondervonden heeft.
- 7. Bij het inschatten van de kosten doorloopt het fonds de volgende stappen:
    - (a) Schat te kosten in van de incidenten die onder '6' vallen.
    - (b) Neem de financiële terugvorderingen gerelateerd aan de ICT-gerelateerde incidenten mee.
    - (c) Aggregeer de bruto kosten, verliezen en terugvorderingen voor de 'ernstige' ICT-gerelateerde incidenten
- 8. Als basis voor de inschattingen gebruikt het fonds de kosten, verliezen en terugvorderingen zoals opgenomen in de financiële verslaglegging, waaronder de winst & verlies rekening en boekhoudkundige voorzieningen.
- 9. Het fonds neemt aanpassingen van de kosten en verliezen van een schatting die zij voor een vorig jaar heeft ingediend op in de schatting van het relevante referentiejaar waarin de aanpassingen worden doorgevoerd.
- 10. Het fonds neemt in het rapport van de raming van de geaggregeerde jaarlijkse kosten en verliezen ook de uitsplitsing van de brutokosten en verliezen en van de financiële terugvorderingen op voor elk 'ernstig' CT-incident dat in de aggregatie is opgenomen.
- 11. Het fonds gebruikt het onderstaande sjabloon om de raming van de geaggregeerde jaarlijkse kosten en verliezen voor het referentiejaar bij de bevoegde autoriteit in te dienen. Voor elk ICT-gerelateerd incident dat in de schatting van het referentiejaar is opgenomen, gebruikt het fonds dezelfde door de financiële entiteit verstrekte incidentreferentiecodes als degene die in het eindrapport worden gebruikt indien over een individueel ICT-gerelateerd incident gerapporteerd is aan de toezichthouder.

Rapportage template voor bruto kosten, verliezen en financiële terugvorderingen voor de referentieperiode

Name of the financial entity			Stichting SBZ Pensioen	
Legal entity identifier			<LEI>	
Start and end date of the reference year of the financial entity			01-01-2024 – 31-12-2024	
Currency			EUR	
Number of incident	Date of the submission of the final incident report	Incident reference number	Gross costs and losses of the incident in the reference year (1000s of units)	Recoveries of the incident in the reference year (1000s of units)
1.				
2.				
3.				
…				
Total for reference Year	n.v.t.	n.v.t.	€ …	€ …