Stichting Pensioenfonds APF

Incidenten- en klokkenluidersregeling

Juli 2025

Stichting Pensioenfonds APF

Inhoud regeling

Incidenten- en klokkenluidersregeling

Aanleiding en doel

Stichting Pensioenfonds APF (het pensioenfonds) ziet de goede reputatie en integriteit van haar organisatie als een belangrijk vereiste om succesvol te opereren als pensioenfonds. Incidenten kunnen een risico vormen voor de integere en beheerste bedrijfsvoering van het pensioenfonds. Het doel van de incidentenregeling is om vast te leggen op welke wijze incidenten worden geconstateerd, gemeld, vastgelegd en aanleiding zijn voor het nemen van corrigerende maatregelen. Daarnaast wil het pensioenfonds leren van incidenten om herhaling te voorkomen. Het pensioenfonds streeft er naar een betrouwbare, transparante en lerende organisatie te zijn. Daarbij past een cultuur waarin medewerkers incidenten kunnen melden en waarin helder is hoe met deze meldingen zal worden omgegaan.

Deze incidentenregeling combineert de regelingen voor operationele- en integriteitsincidenten, de regeling misstanden en de klokkenluidersregeling. Deze regeling is niet van toepassing op incidenten die zich intern bij zakelijke relaties, zoals de uitvoerders, voordoen. Incidenten die zich daar voordoen kunnen echter wel gevolgen hebben voor het pensioenfonds en in sommige gevallen moeten deze door het pensioenfonds gemeld worden aan de toezichthouder.

Met deze regeling geeft het pensioenfonds uitvoering aan de onderstaande wetgeving. Deze wetgeving schrijft voor dat een pensioenfonds zijn organisatie zodanig inricht dat deze een beheerste en integere bedrijfsvoering waarborgt.

- ***De Pensioenwet[1] (Pw)***
  Deze schrijft voor dat een pensioenfonds zijn organisatie zodanig inricht dat deze een beheerste en integere bedrijfsvoering waarborgt.

- ***Besluit financieel toetsingskader[2] (Bftk)***
  Omdat sommige incidenten een gevaar (kunnen) vormen voor de beheersing en de integriteit van de bedrijfsvoering, is het van belang dat deze kunnen worden gemeld, zorgvuldig worden vastgelegd en afgehandeld. In het Bftk en de bijbehorende toelichting is dit nader uitgewerkt. Het Bftk voor pensioenfondsen stelt dat pensioenfondsen een systematische analyse moeten maken van integriteitrisico's en dat ten minste beleid, procedures en maatregelen aanwezig moeten zijn ten aanzien van integriteitgevoelige functies en Incidenten.

- ***Wet bescherming klokkenluiders***
  Deze wet schrijft voor dat het fonds beschikt over een procedure voor de Melding van en omgang met Meldingen van (vermoeden van) Misstanden.

- ***Digital Operational Resilience Act (DORA)***
  Met de komst van de Digital Operational Resilience Act (DORA) is wetgeving geïntroduceerd op basis waarvan ICT-gerelateerde incidenten en cyberdreigingen, die verband houden met de uitvoering van kritieke functies, moeten worden gemeld bij de toezichthouder (zie bijlage "ICT-incident onder DORA").

- ***Code Pensioenfondsen***
  In de Code Pensioenfondsen is bepaald dat een bestuur er zorg voor moet dragen dat alle personen die Betrokkene zijn bij of financieel afhankelijk zijn van het fonds, zonder gevaar voor hun positie, de mogelijkheid hebben te rapporteren over incidenten van algemene, operationele en financiële aard. Dit kan zowel gaan om incidenten binnen het fonds als bij partijen aan wie taken worden uitbesteed. Daarnaast moet duidelijk worden vastgelegd bij wie en op welke wijze hierover gerapporteerd kan worden. Met deze regeling wordt voorzien in deze eisen.

1 Definities

1.1 Toezichthouder:

[1] Artikel 143, Pw.
[2] Artikel 19a, Bftk.

De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), De Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de Belastingdienst en overige publieke toezichtorganen met jurisdictie ten aanzien van (de werkzaamheden van) het pensioenfonds.

1.2 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 de verbonden personen).

1.3 Betrokken derde:
Een derde die is verbonden aan een (potentiële) Melder en die zou kunnen worden benadeeld door het fonds. Dit kan een persoon of een rechtspersoon zijn.

1.4 Melder:
iedere (rechts)persoon die werkzaamheden verricht voor, dan wel betrokken is bij het pensioenfonds (dit met inbegrip van de verbonden personen). Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

1.5 Meldpunt operationele incidenten:
het bestuur heeft de directeur bestuursbureau aangewezen als meldpunt voor operationele incidenten.

1.6 Meldpunt integriteit incidenten en misstanden:
het bestuur heeft de compliance officer aangewezen als meldpunt voor integriteitsincidenten en misstanden.

1.7 Incident:
Incidenten kunnen worden onderverdeeld in operationele incidenten, integriteitsincidenten en misstanden. In principe is een incident een eenmalige (of opvolgende reeks) gebeurtenis waarbij risico op schade is ontstaan. Het betreft:
a. een gebeurtenis die een gevaar vormt voor de integere bedrijfsuitoefening van het pensioenfonds (integriteitsincident of misstand), en/of
b. een gebeurtenis die een gevaar vormt voor de beheerste bedrijfsuitoefening van het pensioenfonds (operationeel incident).

1.8 Operationeel incident:
een gedraging of een gebeurtenis waarbij directe of indirecte financiële schade kan ontstaan door ontoereikende of falende interne processen of systemen, of door menselijk handelen. De oorzaak kan zowel intern als extern gelegen zijn:
a) ontoereikende of falende interne processen, verbonden personen, systemen of door externe gebeurtenissen en/of
b) fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in zijn/hun hoedanigheid van verbonden persoon en/of
c) een (in- of externe) gebeurtenis die wordt veroorzaakt door ontoereikende datakwaliteit of foutieve data. Welke voor het pensioenfonds heeft geresulteerd – of had kunnen resulteren – in financiële of reputatieschade, of ander nadelig effect (data-incident). Voor data-incidenten geldt een afzonderlijk ‘data-incidentenproces’ zoals omschreven in het datakwaliteitsbeleid van het pensioenfonds.
d) Voor de toepassing van deze regeling worden tevens ICT-gerelateerde incidenten die vallen onder de reikwijdte van de Digital Operational Resilience Act (DORA), waaronder ernstige ICT-storingen, inbreuken op de vertrouwelijkheid, integriteit of beschikbaarheid van IT-systemen en data, als operationele incidenten aangemerkt. De afhandeling en eventuele melding van dergelijke incidenten geschiedt conform de daartoe door DNB voorgeschreven vereisten.

1.9 Integriteitsincidenten en misstanden:
gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van het pensioenfonds met inbegrip van de bij het pensioenfonds betrokken (rechts)personen.
Men spreekt van een misstand in de volgende gevallen:

- een schending of een gevaar voor schending van het Unierecht, of
- een handeling of nalatigheid waarbij het maatschappelijk belang in het geding is bij:

- 1°. een schending of een gevaar voor schending van een wettelijk voorschrift of van interne regels die een concrete verplichting inhouden en die op grond van een wettelijk voorschrift door het fonds zijn vastgesteld, dan wel
- 2°. een gevaar voor de volksgezondheid, voor de veiligheid van personen, voor de aantasting van het milieu of voor het goed functioneren van de openbare dienst of een onderneming als gevolg van een onbehoorlijke wijze van handelen of nalaten.
  Het maatschappelijk belang is in ieder geval in het geding indien de handeling of nalatigheid niet enkel persoonlijke belangen raakt en er sprake is van oftewel een patroon of structureel karakter dan wel de handeling of nalatigheid ernstig of omvangrijk is;

1.10 Zwaar incident:
Een incident kwalificeert als Zwaar incident als er sprake is van

a. een ernstig gevaar voor de integere bedrijfsuitoefening van het pensioenfonds;
b. een groot afbreukrisico in de media;
c. een belangrijke invloed op de bedrijfsvoering;
d. de betrokkenheid van het Openbaar Ministerie;
e. fraude;
f. een aanwijzing van de toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen;
g. herhaalde overtredingen door dezelfde persoon of groep van personen.

2. Algemeen

2.1 Het bestuur van het pensioenfonds draagt er zorg voor dat de incidenten- en klokkenluidersregeling bekend is bij alle betrokken personen.

2.2 De raad van toezicht is belast met het toezicht op de naleving van deze regeling vanuit haar algemene taak van toezichthouder op de integere en beheerste bedrijfsvoering.

2.3 Het meldpunt ontvangt de meldingen en beoordeelt of het een incident betreft in de zin van deze regeling.

2.4 Indien het meldpunt zich onbevoegd acht vanwege de aard van de melding, dan verwijst hij de melder door naar het bevoegde meldpunt.

2.5 Indien de melder vermoedt dat het aangewezen meldpunt betrokken is bij het incident, dan kan hij de melding verrichten bij het andere meldpunt dan wel bij de voorzitter van het bestuur of de voorzitter van de raad van toezicht.

3. Melding en meldpunt

3.1 Een vermoeden van een incident of misstand dient, bij voorkeur schriftelijk, te worden gemeld bij het meldpunt. De melder ontvangt hiervan een bevestiging. Het pensioenfonds heeft de compliance officer tevens aangewezen als vertrouwenspersoon voor meldingen van misstanden of integriteitsincidenten. De melder kan ervoor kiezen de melding vertrouwelijk via deze route te doen.

3.2 Indien de melder dit wenst, zal het meldpunt de naam van de melder geheimhouden. De melder kan er ook voor kiezen om de melding indirect te doen via een vertrouwenspersoon van het pensioenfonds. De melder accepteert dat dit de uitvoering van het onderzoek kan belemmeren. Het meldpunt bespreekt met de melder wanneer de anonimiteit een belemmering vormt.
Indien de melder niet zelf wil melden, kan hij of zij een vertrouwelijke melding doen via een vertrouwenspersoon van het pensioenfonds. De vertrouwenspersoon kan namens de melder contact opnemen met het meldpunt. De melder behoudt in dat geval zijn of haar rechten op bescherming zoals opgenomen in deze regeling.
Indien de melder volledig anoniem wil melden, kan een communicatiekanaal worden geopend dat anonimiteit waarborgt, bijvoorbeeld via een tijdelijk e-mailadres of een tussenpersoon.

3.3 Het meldpunt zal, eventueel na een verkort onderzoek, een zienswijze formuleren, zodra hij een melding van een melder heeft ontvangen. Deze zienswijze wordt binnen een redelijke termijn teruggekoppeld aan de melder.

3.4 Het meldpunt zal een binnengekomen melding met de voorzitter van het bestuur bespreken indien het een Zwaar incident betreft in de zin van deze regeling. Indien het geen Zwaar incident betreft, dan zal hij de melding in de reguliere rapportage benoemen.

3.5 Indien het een Zwaar incident betreft dat gelieerd is aan of betrokkenheid heeft met een lid van het bestuur of de raad van toezicht, dan zal het meldpunt het incident bespreken met:
- de voorzitter van het bestuur, als melding één van de overige bestuursleden betreft;
- de raad van toezicht als de melding de voorzitter van het bestuur betreft;
- de voorzitter van de raad van toezicht als de melding één van de overige leden van de raad van toezicht betreft;
- de andere leden van de raad van toezicht als de melding de voorzitter van de raad van toezicht betreft;
- de toezichthouder DNB als de melding de gehele raad van toezicht betreft.

3.6 Het meldpunt zal met de voorzitter van het bestuur (of degene als bedoeld in artikel 3.5) zijn zienswijze delen en adviseren over afhandeling van de melding dan wel het starten van nader onderzoek. Indien nader onderzoek gewenst is, dan zal de voorzitter hier namens het bestuur opdracht toe geven.

3.7 De melder ontvangt van het meldpunt algemene informatie over de afhandeling van de melding.

3.8 Meldingen van incidenten en de beoordeling worden geregistreerd in een incidentenregister. Gedurende het verdere proces worden in het dossier de naar het oordeel van het meldpunt relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek. Identificatiegegevens van de melder worden op zodanige wijze bewaard dat alleen het meldpunt en het bestuur toegang hebben tot deze gegevens, tenzij de anonimiteit verder dient te worden gewaarborgd.

4. Onderzoek

4.1 Indien van toepassing zal de raad van toezicht een onderzoek instellen. Het doel van het onderzoek is:
a. waarheidsvinding met betrekking tot het incident en de daarmee samenhangende bewijsvoering voor disciplinaire, civielrechtelijke en strafrechtelijke vervolgstappen;
b. het beperken van de (potentiële) schade naar een beheersbaar niveau; en
c. het herstel van de bedrijfsvoering, voor zover het incident daarop enige invloed had.

4.2 Het onderzoek naar het incident wordt uitgevoerd in opdracht van de raad van toezicht, door interne en/of externe deskundigen. Als de melding betrekking heeft op een incident bij een partij aan wie werkzaamheden zijn uitbesteed, wordt het onderzoek verricht in overleg met of door deze partij. Indien van toepassing wordt een onderzoeksprotocol opgesteld.

4.3 Het onderzoek wordt uitgevoerd onder de volgende voorwaarden:
- De beginselen van de AVG worden in acht genomen.
- Gegevens worden rechtmatig en proportioneel verzameld; van onrechtmatig verkregen gegevens wordt geen gebruik gemaakt.
- Degene naar wie onderzoek wordt gedaan, wordt direct geïnformeerd, tenzij dit in het belang van het onderzoek niet gewenst is.
- De gegevens worden zodanig vastgelegd dat hoor en wederhoor kan plaatsvinden, tenzij in redelijkheid kan worden aangenomen dat dit schadelijk kan zijn voor het onderzoek.
- De onderzoekers stellen de melder in de gelegenheid te worden gehoord. De onderzoekers dragen zorg voor een schriftelijke vastlegging hiervan.
- De onderzoekers kunnen ook anderen horen. De onderzoekers dragen zorg voor een schriftelijke vastlegging hiervan.
- Indien het een persoonsgericht onderzoek betreft, is de onderzoeker hiertoe bevoegd en worden de uitgangspunten van artikel 5 in acht genomen.

4.4 De onderzoekers rapporteren de onderzoeksresultaten aan het meldpunt en de raad van toezicht of degene als bedoeld in artikel 3.5. De rapportage bevat een kort relaas van feiten en omstandigheden en indien vastgesteld is dat sprake is van een incident, de bewijsvoering daarvoor in hoofdlijnen en een

advies met betrekking tot de te nemen maatregel(en). De melder en de personen op wie een melding betrekking heeft worden in de gelegenheid gesteld hier hun zienswijze op te geven. Deze zienswijzen worden toegevoegd aan het rapport.

4.5 Alle betrokkenen waarborgen een vertrouwelijke behandeling van de melding en het onderzoek. Informatie mag niet gedeeld worden, tenzij dit op grond van de wet of deze regeling noodzakelijk is.

4.6 Het traject tussen melding en afronding onderzoek duurt maximaal vier weken. Indien deze termijn wordt overschreden, worden betrokken partijen geïnformeerd en wordt de motivatie voor overschrijding van deze termijn vastgelegd.

5. Persoonsgericht onderzoek

5.1 Indien een redelijk vermoeden bestaat dat een betrokkene verantwoordelijk is voor, of zich schuldig heeft gemaakt aan, een incident, of als daar, naar het oordeel van de voorzitter van de raad van toezicht of degene als bedoeld in artikel 3.5 aanleiding toe bestaat, kan de raad van toezicht of degene als bedoeld in artikel 3.5 een persoonsgericht onderzoek instellen. De persoon naar wie het persoonsgericht onderzoek zich richt, wordt onverwijld op de hoogte gebracht van het persoonsgericht onderzoek.

5.2 Een persoonsgericht onderzoek wordt ingesteld binnen een redelijke termijn nadat voldoende aanwijzingen bekend geworden zijn dat de desbetreffende betrokkene zich schuldig heeft gemaakt aan het incident en een persoonsgericht onderzoek noodzakelijk is gebleken voor een correcte procesgang en afhandeling van de melding.

5.3 De betrokkene naar wie het persoonsgericht onderzoek verricht wordt, wordt in de gelegenheid gesteld zijn zienswijze kenbaar te maken. Zijn zienswijze wordt schriftelijk vastgelegd.

5.4 Indien het onderzoek en/of het belang van het pensioenfonds dit vereist, kan, in overleg met de voorzitter van de raad van toezicht, door de onderzoekers opdracht gegeven worden om bepaalde gegevens of zaken veilig te stellen. Daartoe wordt een belangenafweging gemaakt.

5.5 Na de uitvoering van een persoonsgericht onderzoek wordt een schriftelijk advies uitgebracht aan het bestuur (of de raad van toezicht). Het op schrift gestelde advies wordt door de compliance officer bewaard.

5.6 Alle relevante documenten, daaronder begrepen de zienswijze van de verschillende betrokkenen, rapportages en het op schrift gestelde advies worden opgenomen in een dossier.

6. Standpunt bestuur en maatregelen

6.1 Het bestuur (of raad van toezicht) neemt op basis van het onderzoeksrapport een standpunt in. Indien het standpunt afwijkt van de conclusies en aanbevelingen van de onderzoekers, dan onderbouwt zij haar standpunt.

6.2 In het geval van onderzoek oordeelt het bestuur op basis van de onderzoeksresultaten, over de te nemen maatregel(en), zoals:

a. disciplinaire maatregelen;
b. civielrechtelijke maatregelen, zoals regres;
d. melden van het voorval bij de toezichthouder(s) indien sprake is van een antecedent;
e. interne en externe openbaarmaking;
f. aanpassing van procedures; en/of
g. overige maatregelen voor het herstel van de bedrijfsvoering.

Indien het incident betrekking heeft op één van de bestuursleden, beoordeelt de raad van toezicht over de te nemen maatregel(en) zoals hiervoor aangegeven.
Zowel het Meldpunt als de Melder worden binnen redelijke termijn maar maximaal vijf werkdagen na oplevering van het incidentrapport geïnformeerd over het standpunt van het bestuur en de eventueel genomen of te nemen maatregelen.

6.3 Indien een integriteitsincident veroorzaakt is door een verbonden persoon, wordt bij het bepalen van de maatregel(en) en sancties in overweging genomen dat een integriteitsincident als een ernstige schending wordt beschouwd van de vertrouwensrelatie tussen het pensioenfonds enerzijds en de verbonden persoon anderzijds.

6.5 Het veroorzaken van een integriteitsincident of anderszins daarbij betrokken zijn, kan leiden tot ontheffing uit de functie die de verbonden persoon bij het pensioenfonds vervult. Indien sprake is van opzettelijk en ernstige strafbare feiten, zoals misdrijven genoemd in het Wetboek van Strafrecht en de Wet op de economische delicten, wordt in beginsel aangifte gedaan bij justitie of de politie.

7. Escalatie

7.1 Indien de melder het niet eens is met het standpunt van het bestuur, dan kan hij het vermoeden van de misstand melden bij de voorzitter van de raad van toezicht.

7.2 Na het doen van een interne melding van een vermoeden van een misstand, kan de melder ook direct een externe melding doen indien:

- de melding niet-ontvankelijk is verklaard en de melder zich niet in de motivatie hiervan kan vinden;
- de melder zich benadeelt voelt naar aanleiding van de melding;
- de voorgeschreven termijnen worden overschreden zonder bericht waarom deze in redelijkheid worden overschreden;
- een eerdere melding de misstand niet heeft weggenomen;
- indien het eerst doen van een interne melding in redelijkheid niet van hem kan worden gevraagd.

7.3 De melder kan de externe melding doen bij een instantie die daarvoor naar het redelijk oordeel van de melder het meest in aanmerking komt en naar het oordeel van de melder mogelijk actie tegen de misstand kan ondernemen. Dit betreft bijvoorbeeld politie, justitie, toezichthouder of het Huis voor Klokkenluiders.

8. Bescherming van de melder tegen benadeling

8.1 Het pensioenfonds zal de melder niet benadelen in verband met het te goeder trouw en naar behoren melden van een vermoeden van een misstand, Incident indien aan de voorwaarden van art. 17e en f Wbk wordt voldaan.

8.2 Onder benadeling als bedoeld in lid 1 wordt in ieder geval verstaan het nemen van een benadelende maatregel, zoals:

a. het tussentijds beëindigen of het niet verlengen van een tijdelijk dienstverband of opdracht;
b. het treffen van een disciplinaire maatregel;
c. het opleggen van een onderzoek-, spreek-, werkplek- en/of contactverbod aan de melder of collega's van de melder;
d. het uitbreiden of beperken van de taken van de melder, anders dan op eigen verzoek;
e. het onthouden van salarisverhoging, incidentele beloning, bonus, of toekenning van vergoedingen;
f. het onthouden van promotiekansen;
g. het niet accepteren van een ziekmelding, of het als ziek geregistreerd laten;
h. het afwijzen van een verlofaanvraag;
i. het verlenen van verlof, anders dan op eigen verzoek.

8.3 Artikel 8.1 en 8.2 zijn ook van toepassing op benadeling van betrokken derden, het meldpunt en/of de onderzoekers.

9. Melden aan toezichthouder(s)

9.1 Zware incidenten worden onverwijld en tijdig door de voorzitter van het bestuur of degene als bedoeld in artikel 3.5 aan de relevante Toezichthouder(s) gemeld onder opgaaf van de feiten en omstandigheden van het incident, alsmede de informatie over de functie, de hoedanigheid en de positie van de betrokken (rechts)perso(o)n(en) die verantwoordelijk is/zijn voor het ontstane incident. Voor de toepassing van

deze regeling worden ICT-gerelateerde incidenten in de zin van DORA als operationele incidenten aangemerkt (zie bijlage 1 voor toelichting).

9.2 De voorzitter informeert de relevante toezichthouder(s) tevens over de maatregelen die naar aanleiding van het incident zijn genomen of nog zullen worden genomen.

9.3 Indien de raad van toezicht dit noodzakelijk acht dan kan zij, zonder instemming van bestuur, zelfstandig een melding verrichten bij de Toezichthouders. De Sleutelfunctiehouders hebben van rechtswege een vergelijkbare verplichting ten aanzien van meldingen inzake incidenten en misstanden.

10. Rol voorzitter bestuur

10.1 Indien door de aard van het incident snel handelen vereist is, is de voorzitter van het bestuur, of diens plaatsvervanger, bevoegd een (voorlopig) besluit te nemen.

10.2 De voorzitter van het bestuur is gehouden de overige leden van het bestuur zo spoedig mogelijk op de hoogte te brengen van de door hem/haar verrichte acties en genomen (voorlopige) besluiten en deze, indien nodig, alsnog ter definitieve besluitvorming aan het bestuur aan te bieden.

Bijlage: ICT-incident onder DORA

Inleiding

Met de komst van de Digital Operational Resilience Act (DORA) is wetgeving geïntroduceerd op basis waarvan ICT-gerelateerde incidenten en cyberdreigingen, die verband houden met de uitvoering van kritieke functies, moeten worden gemeld bij de toezichthouder.

Incident

Er is hierbij sprake van een ICT gerelateerd incident of significant beveiligings- of operationeel incident als kritieke diensten worden getroffen en ongeautoriseerde toegang tot netwerk- en informatiesystemen wordt geïdentificeerd, wat kan leiden tot gegevensverlies of als de drempelwaarde van twee aanvullende criteria is voldaan die worden gerelateerd aan:

- Cliënten of financiële tegenpartijen en transacties i.c.m. reputatierisico
- Uitvaltijd van (IT-) diensten
- Geografische spreiding
- Informatiebeveiliging
- Getroffen cruciale diensten
- Economische impact

Ongeacht de classificatie van het incident zal het incidenten worden gemeld bij Risicomanagement en wordt er een vastlegging van het incident gemaakt in het incidentenregister.

Ernstige ICT-gerelateerde incidenten worden gerapporteerd aan de toezichthouder.

Indien een ernstig incident wordt geconstateerd wordt hierover relevante informatie verzameld en geanalyseerd en worden betreffende verslagen ingediend bij DNB.

De rapportage van ICT-incidenten aan de toezichthouder kent drie stappen:

1. Een eerste kennisgeving (binnen 4 uur);
2. Een tussentijds verslag zodra de status van het incident ingrijpend is veranderd of de behandeling daarvan is gewijzigd. Dit moet steeds gebeuren zodra de status ingrijpend wijzigt (binnen 72 uur);
3. Een eindverslag zodra de analyse van de onderliggende oorzaken klaar is.

Deze rapportages gebruiken de toezichthouders om te bepalen hoe ingrijpend het incident is en of er grensoverschrijdende gevolgen zijn.

Uitwerking drempelwaarden meldingscriteria:

Deelnemers of financiële tegenpartijen en transacties i.c.m. reputatierisico
Bij een incident zal worden beoordeeld of, en hoeveel, getroffen deelnemers en/of financiële tegenpartijen (mogelijk) betrokken zijn geraakt bij het incident en daardoor geen gebruik kunnen maken van de dienstverlening of nadelige gevolgen hebben ondervonden. Verder wordt een inschatting gemaakt in hoeverre de bedrijfsdoelstellingen van het fonds worden beïnvloed als gevolg van het incident en voor welk deel (aantal en omvang) dit betrekking heeft op transacties buiten de EU.

De materialiteitsdrempel voor deelnemers of financiële tegenpartijen en transacties wordt bepaald door te beoordelen of een gebeurtenis één van de volgende kenmerken heeft:

- >10% van alle deelnemers die de betreffende service gebruiken;
- >30% van alle financiële tegenpartijen (aantal) die door het fonds worden gebruikt;
- >10% van het dagelijkse gemiddelde aantal transacties;
- >10% van het dagelijkse gemiddelde bedrag aan transacties;
- eventuele geïdentificeerde gevolgen voor financiële tegenpartijen die door het fonds als relevant zijn aangemerkt.

Er is sprake van reputatieschade als aan één van de volgende voorwaarden is voldaan:

- Het incident is in de media verschenen
- Er zijn herhaaldelijk klachten ontvangen van deelnemers, tegenpartijen en/of cruciale relaties
- Wettelijke vereisten kunnen niet (meer) worden nagekomen

Uitvaltijd van (ICT-) diensten
De duur van incidenten wordt gemeten vanaf het moment dat het incident zich voordoet tot en met het moment dat het incident is opgelost. Als het moment van ontstaan niet kan worden vastgesteld dan wordt het moment dat het incident wordt geconstateerd gehanteerd.

De materialiteitsdrempel wordt overschreden als:
- de incidentduur langer is dan 24 uur; of
- de uitvaltijd van de service langer is dan 2 uur voor ICT-diensten die kritieke of belangrijke functies ondersteunen

Geografische spreiding
Een incident heeft impact op geografische spreiding als gevolg van een incident zijn vastgesteld op het grondgebied van ten minste twee Europese lidstaten en een relatie hebben tot:

- Deelnemers
- Financiële tegenpartijen;
- Financiële marktinfrastructuren of externe aanbieders die andere financiële instellingen kunnen beïnvloeden.

Informatiebeveiliging
Om te bepalen of de drempelwaarde voor criteria van informatiebeveiliging wordt overschreden wordt beoordeeld of een incident gegevensverliezen heeft veroorzaakt ten aanzien van:
- Beschikbaarheid; gegevens waar het fonds, deelnemers of tegenpartijen om verzoeken zijn, tijdelijk of permanent, ontoegankelijk
- Authenticiteit; is de betrouwbaarheid van de gegevensbron in gevaar gebracht
- Integriteit; zijn er ongeautoriseerde wijzigingen van gegevens waardoor deze onnauwkeurig of onvolledig zijn geworden
- Vertrouwelijkheid; zijn gegevens ingezien door, of openbaar gemaakt aan een onbevoegde partij of systeem. De behandeling van persoonsgegevens is nader uitgewerkt in het “Privacy beleid” van het fonds

Getroffen cruciale diensten (5)
Om te bepalen of een incident kritieke diensten treft, met inbegrip van de transacties en activiteiten van het fonds, beoordeelt het fonds of het incident:
- gevolgen heeft of heeft gehad voor ICT-diensten of netwerk- en informatiesystemen die kritieke of belangrijke functies van het fonds ondersteunen;
- gevolgen heeft of heeft gehad voor financiële diensten waarvoor een vergunning of registratie vereist is of die onder toezicht staan van bevoegde autoriteiten; of
- een succesvolle, kwaadwillige en ongeautoriseerde toegang tot het netwerk en de informatiesystemen van het fonds vertegenwoordigt.

Economische Impact
Bij het bepalen van de economische impact van een incident, houdt het fonds rekening met de volgende soorten directe en indirecte kosten en verliezen die als gevolg van het incident worden geleden, zonder rekening te houden met financiële terugvorderingen:
- onteigende gelden of financiële activa waarvoor het fonds aansprakelijk is, met inbegrip van activa die verloren zijn gegaan door diefstal;
- vervangings- of verplaatsingskosten van software, hardware of infrastructuur;
- personeelskosten, met inbegrip van kosten in verband met het vervangen of verhuizen van personeel, het inhuren van extra personeel, de vergoeding van overuren en het herstellen van verloren of verminderde vaardigheden van het personeel;
- vergoedingen wegens niet-naleving van contractuele verplichtingen;
- verhaals- en compensatiekosten voor deelnemers;
- verliezen als gevolg van gederfde inkomsten;
- kosten verbonden aan interne en externe communicatie;
- advieskosten, inclusief kosten in verband met juridisch advies, forensische diensten en hersteldiensten.

Bij het bepalen van deze directe en indirect kosten wordt geen rekening gehouden met:
- kosten van algemeen onderhoud van infrastructuur, uitrusting, hardware, software, infrastructuur en vaardigheden van het personeel;
- interne of externe uitgaven om het bedrijf te verbeteren; En
- verzekeringspremies.

Terugkerende incidenten die afzonderlijk niet voldoen aan de criteria van een incident met economische impact, worden als één incident beschouwd als de incidenten aan alle volgende voorwaarden voldoen:

- de incidenten hebben zich binnen zes maanden minimaal twee keer voorgedaan;
- de incidenten hebben dezelfde schijnbare hoofdoorzaak hebben;
- de incidenten worden gezamenlijk geclassificeerd als een groot incident

Als de werkelijke kosten en verliezen niet kunnen worden vastgesteld, maakt het fonds een schatting van de kosten op basis van de beschikbare gegevens.

De drempelwaarde voor een incident met economische impact bedraagt € 100.000.