Publicatieblad
van de Europese Unie

NL
L-serie

2025/302

20.2.2025

UITVOERINGSVERORDENING (EU) 2025/302 VAN DE COMMISSIE

van 23 oktober 2024

tot vaststelling van technische uitvoeringsnormen voor de toepassing van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot de door financiële entiteiten te gebruiken standaardformulieren en modellen en te volgen procedures voor de rapportage van een ernstig ICT-gerelateerd incident en voor de kennisgeving van een significante cyberdreiging

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 ([1]), en met name artikel 20, vierde alinea,

Overwegende hetgeen volgt:

(1) Om ervoor te zorgen dat financiële entiteiten ernstige incidenten op consistente wijze aan hun bevoegde autoriteiten rapporteren, en om ervoor te zorgen dat zij aan deze autoriteiten gegevens van goede kwaliteit verstrekken, moet worden aangegeven welke gegevensvelden financiële entiteiten in de verschillende fasen van de in artikel 19, lid 4, van Verordening (EU) 2022/2554 bedoelde rapportage moeten verstrekken. Het is belangrijk dat die informatie zodanig wordt gepresenteerd dat één overzicht van het incident mogelijk is. Daarom moet voor deze doeleinden één rapportagemodel worden vastgesteld.

(2) Financiële entiteiten moeten de gegevensvelden van het rapportagemodel invullen die horen bij de informatievereisten van de kennisgeving of het verslag in kwestie. Financiële entiteiten die al over informatie beschikken die zij moeten verstrekken in een latere rapportagefase, d.w.z. in het tussentijdse verslag of het eindverslag, moeten de gegevens echter vroeger kunnen indienen.

(3) Aangezien meerdere of terugkerende incidenten een ernstig incident kunnen vormen als bedoeld in artikel 8 van Gedelegeerde Verordening (EU) 2024/1772 van de Commissie ([2]), moet het ontwerp van het rapportagemodel en van de gegevensvelden financiële entiteiten in staat stellen dergelijke terugkerende incidenten te rapporteren.

(4) Om ervoor te zorgen dat informatie nauwkeurig en actueel blijft, moet het rapportagemodel financiële entiteiten de gelegenheid bieden om bij de indiening van het tussentijdse en het eindverslag alle eerder ingediende informatie bij te werken en, indien nodig, ernstige incidenten als niet-ernstig te classificeren.

(5) De juridische identificatie van entiteiten moet worden afgestemd op de identificatiecodes van de technische uitvoeringsnormen die zijn vastgesteld op grond van artikel 28, lid 9, van Verordening (EU) 2022/2554.

(6) Wanneer financiële entiteiten de verplichtingen om ernstige ICT-gerelateerde incidenten te rapporteren, uitbesteden aan een derde, moeten de bevoegde autoriteiten vóór de indiening van de eerste kennisgeving of het eerste verslag op de hoogte zijn van de identiteit van de derde die namens de financiële entiteit rapporteert, zodat de legitimiteit van de rapporterende derde kan worden geverifieerd.

([1]) PB L 333 van 27.12.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Gedelegeerde Verordening (EU) 2024/1772 van de Commissie van 13 maart 2024 tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen tot nadere bepaling van de criteria voor de classificatie van ICT-gerelateerde incidenten en cyberdreigingen, tot vaststelling van materialiteitsdrempels en tot bepaling van de nadere informatie van verslagen over ernstige incidenten (PB L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(7) Om de gevolgen van een incident dat zich heeft voorgedaan bij of werd veroorzaakt door een derde aanbieder en dat meerdere financiële entiteiten binnen één lidstaat treft, gemakkelijk te kunnen bepalen en om de rapportage-inspanning voor financiële entiteiten te beperken, moet het rapportagemodel de indiening mogelijk maken van een geaggregeerd verslag met geaggregeerde informatie over de gevolgen van het incident voor alle geraakte financiële entiteiten die het incident als ernstig hebben geclassificeerd.

(8) Het rapportagemodel moet op een technologieneutrale manier worden ontworpen zodat het kan worden toegepast in verschillende oplossingen voor het rapporteren van incidenten die al bestaan of kunnen worden ontwikkeld voor de uitvoering van de vereisten van Verordening (EU) 2022/2554.

(9) Het ontwerp van het rapportagemodel en de gegevensvelden moet de rapportage vergemakkelijken van ernstige ICT-gerelateerde incidenten door derden waaraan financiële entiteiten hun rapportageverplichting overeenkomstig artikel 19, lid 5, van Verordening (EU) 2022/2554 hebben uitbesteed.

(10) Deze verordening is gebaseerd op de ontwerpen van technische uitvoeringsnormen die de Europese toezichthoudende autoriteiten (ETA's) bij de Commissie hebben ingediend.

(11) De Europese toezichthoudende autoriteiten hebben open publieksraadplegingen gehouden over de ontwerpen van technische uitvoeringsnormen waarop deze verordening is gebaseerd, de mogelijke daaraan verbonden kosten en baten geanalyseerd en het advies van de overeenkomstig artikel 37 van de Verordeningen (EU) nr. 1093/2010 ([3]), (EU) nr. 1094/2010 ([4]) en (EU) nr. 1095/2010 ([5]) van het Europees Parlement en de Raad opgerichte Stakeholdergroep bankwezen ingewonnen.

(12) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]) en heeft op 22 juli 2024 een positief advies uitgebracht. Elke verwerking van persoonsgegevens die binnen het toepassingsgebied van deze verordening valt, moet plaatsvinden in overeenstemming met de toepasselijke beginselen inzake gegevensbescherming en de bepalingen van Verordening (EU) 2018/1725,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Model voor het rapporteren van ernstige ICT-gerelateerde incidenten

1. Financiële entiteiten gebruiken het model in bijlage I voor de indiening van de eerste kennisgeving, het tussentijdse verslag en het eindverslag als bedoeld in artikel 19, lid 4, van Verordening (EU) 2022/2554, en wel als volgt:

a) financiële entiteiten die een eerste kennisgeving doen, vullen de gegevensvelden van het model in die horen bij de informatie die overeenkomstig artikel 2 van Gedelegeerde Verordening (EU) 2025/301 van de Commissie ([7]) moet worden verstrekt, en mogen indien zij al over die informatie beschikken, gegevensvelden invullen waarvoor invulling niet vereist is bij een eerste kennisgeving, maar wel bij een tussentijds of een eindverslag;

([3]) Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48, http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie (PB L 331 van 15.12.2010, blz. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Gedelegeerde Verordening (EU) 2025/301 van de Commissie van 23 oktober 2024 tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen voor de inhoud en termijnen van de eerste kennisgeving van en het tussentijdse en het eindverslag over ernstige ICT-gerelateerde incidenten en voor de inhoud van de vrijwillige kennisgeving van significante cyberdreigingen. (PB L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) financiële entiteiten die een tussentijd verslag indienen, vullen de gegevensvelden van het model in die horen bij de informatie die overeenkomstig artikel 3 van Gedelegeerde Verordening (EU) 2025/301 moet worden verstrekt, en mogen indien zij al over de desbetreffende informatie beschikken, gegevensvelden invullen waarvoor invulling niet vereist is bij het tussentijdse verslag, maar wel bij het eindverslag.

c) financiële entiteiten die een eindverslag indienen, vullen de gegevensvelden van het model in die horen bij de informatie die overeenkomstig artikel 4 van Gedelegeerde Verordening (EU) 2025/301 moet worden verstrekt.

2. Financiële entiteiten zorgen ervoor dat de informatie in de eerste kennisgeving en in het tussentijdse en het eindverslag volledig en nauwkeurig is.

3. Financiële entiteiten verstrekken, voor zover mogelijk, geraamde waarden op basis van andere beschikbare gegevens en informatie wanneer er op het moment van de rapportage geen nauwkeurige gegevens beschikbaar zijn voor de eerste kennisgeving of het tussentijdse verslag.

4. Bij de indiening van een tussentijds verslag of een eindverslag gebruiken financiële entiteiten het model van bijlage I om alle vereiste informatie in te dienen en, in voorkomend geval, de informatie van de eerste kennisgeving of van het tussentijdse verslag bij te werken.

5. Financiële entiteiten volgen bij het invullen van het model in bijlage I het glossarium van de gegevens en de instructies in bijlage II.

Artikel 2

Gezamenlijke indiening van de eerste kennisgeving, het tussentijdse en het eindverslag

Financiële entiteiten kunnen de indiening van de eerste kennisgeving, het tussentijdse en het eindverslag combineren en twee van de drie of alle drie tegelijk verstrekken wanneer de regelmatige activiteiten zijn hersteld of de analyse van de onderliggende oorzaken is voltooid en mits de termijnen van artikel 5 van Gedelegeerde Verordening (EU) 2025/301 in acht zijn genomen.

Artikel 3

Terugkerende ICT-gerelateerde incidenten

Financiële entiteiten die informatie verstrekken over niet-ernstige terugkerende ICT-gerelateerde incidenten die cumulatief beantwoorden aan de voorwaarden voor één ernstig ICT-gerelateerd incident als bedoeld in artikel 8, lid 2, van Gedelegeerde Verordening (EU) 2024/1772, verstrekken die informatie in geaggregeerde vorm.

Artikel 4

Gebruik van beveiligde elektronische kanalen

1. Financiële entiteiten gebruiken beveiligde elektronische kanalen zoals beschikbaar gesteld door hun bevoegde autoriteit om de eerste kennisgeving en het tussentijdse en het eindverslag in te dienen.

2. Financiële entiteiten die de door hun bevoegde autoriteit beschikbaar gestelde beveiligde elektronische kanalen niet kunnen gebruiken, stellen hun bevoegde autoriteit via andere beveiligde middelen in kennis van een ernstig ICT-gerelateerd incident, in overleg met de bevoegde autoriteit. Indien de bevoegde autoriteit zulks verlangt, dienen financiële entiteiten de eerste kennisgeving, het tussentijdse verslag of het eindverslag via het door hun bevoegde autoriteit beschikbaar gestelde beveiligde elektronische kanaal opnieuw in zodra dit voor hen mogelijk is.

Artikel 5

Herclassificatie van ernstige ICT-gerelateerde incidenten

Indien de financiële entiteit na een verdere beoordeling concludeert dat het eerder als ernstig gerapporteerde ICT-gerelateerde incident op geen enkel moment beantwoordde aan de classificatiecriteria en drempels van artikel 8 van Gedelegeerde Verordening (EU) 2024/1772, stelt de financiële entiteit de bevoegde autoriteit ervan in kennis dat zij het ICT-gerelateerde incident heeft geherclassificeerd van ernstig in niet-ernstig, en verstrekt zij de informatie over die herclassificatie in het model in bijlage II bij deze verordening onder de velden "soort verslag" en "overige informatie".

Artikel 6

Kennisgeving van uitbesteding van de rapportageverplichtingen

1. Financiële entiteiten die de verplichting om ernstige ICT-gerelateerde incidenten te rapporteren, overeenkomstig artikel 19, lid 5, van Verordening (EU) 2022/2554 hebben uitbesteed, stellen hun bevoegde autoriteit in kennis van die uitbestedingsovereenkomst zodra de uitbestedingsovereenkomst is gesloten en vóór de indiening van de eerste kennisgeving of het eerste verslag.

2. Financiële entiteiten verstrekken de bevoegde autoriteit de naam, contactgegevens en identificatiecode van de derde partij die de kennisgevingen of verslagen van ernstige ICT-gerelateerde incidenten voor hen zal indienen.

3. Financiële entiteiten die hun rapportageverplichtingen als bedoeld in artikel 19, lid 5, van Verordening (EU) 2022/2554, niet meer uitbesteden, stellen hun bevoegde autoriteit daarvan onmiddellijk in kennis.

Artikel 7

Geaggregeerde rapportage

1. Een derde dienstverlener aan wie rapportageverplichtingen zijn uitbesteed als bedoeld in artikel 19, lid 5, van Verordening (EU) 2022/2554, kan het model in bijlage I bij deze verordening gebruiken om geaggregeerde informatie over een ernstig ICT-gerelateerd incident dat gevolgen heeft voor meerdere financiële entiteiten, in één kennisgeving of verslag te verstrekken, en kan die kennisgeving of dat verslag indienen bij de bevoegde autoriteit namens alle geraakte financiële entiteiten, mits aan elk van de volgende voorwaarden is voldaan:

a) het te rapporteren ernstige ICT-gerelateerde incident ontstond bij of werd veroorzaakt door een derde aanbieder van ICT-diensten;

b) die derde dienstverlener verleent de betrokken ICT-dienst aan meer dan één financiële entiteit of aan een groep;

c) het ICT-gerelateerde incident wordt door elke financiële entiteit die in de geaggregeerde kennisgeving of het geaggregeerde verslag wordt behandeld, als ernstig geclassificeerd;

d) het ernstige ICT-gerelateerde incident treft financiële entiteiten binnen één lidstaat en het geaggregeerde verslag heeft betrekking op financiële entiteiten die onder toezicht staan van dezelfde bevoegde autoriteit;

e) de bevoegde autoriteiten hebben deze soort financiële entiteiten uitdrukkelijk toegestaan hun rapportage te aggregeren.

2. Lid 1 is niet van toepassing op kredietinstellingen die als belangrijk worden aangemerkt als bedoeld in artikel 2, punt 16, van Verordening (EU) nr. 468/2014 van de Europese Centrale Bank ([8]), exploitanten van handelsplatformen en centrale tegenpartijen; zij gebruiken het model in bijlage I alleen om kennisgevingen of verslagen van ernstige ICT-gerelateerde incidenten op individuele basis in te dienen bij hun bevoegde autoriteit.

3. Indien de bevoegde autoriteiten informatie verlangen over de individuele gevolgen van het ernstige ICT-gerelateerde incident voor één financiële entiteit, dient de financiële entiteit op verzoek van de bevoegde autoriteit een individuele kennisgeving of een verslag in over het ernstige ICT-gerelateerde incident.

([8]) Verordening (EU) nr. 468/2014 van de Europese Centrale Bank van 16 april 2014 tot vaststelling van een kader voor samenwerking binnen het Gemeenschappelijk Toezichtsmechanisme tussen de Europese Centrale Bank en nationale bevoegde autoriteiten en met nationale aangewezen autoriteiten (GTM-kaderverordening) (ECB/2014/17) (PB L 141 van 14.5.2014, blz. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Artikel 8

Kennisgeving van significante cyberdreigingen

1. Financiële entiteiten die bevoegde autoriteiten overeenkomstig artikel 19, lid 2, van Verordening (EU) 2022/2554 in kennis stellen van significante cyberdreigingen, gebruiken het model van bijlage III bij deze verordening en volgen het glossarium van de gegevens en de instructies in bijlage IV bij deze verordening.

2. Financiële entiteiten zorgen ervoor dat de informatie in de kennisgeving van significante cyberdreigingen volledig en nauwkeurig is.

Artikel 9

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 23 oktober 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

MODELLEN VOOR DE RAPPORTAGE VAN ERNSTIGE INCIDENTEN

Nummer van het veld	Gegevensveld	
Algemene informatie over de financiële entiteit		
1.1	Soort indiening	
1.2	Identificatie van de entiteit die het verslag indient	
1.3	Identificatiecode van de entiteit die het verslag indient	
1.4	Soort getroffen financiële entiteit	
1.5	Naam van de getroffen financiële entiteit	
1.6	LEI-code van de getroffen financiële entiteit	
1.7	Naam van de voornaamste contactpersoon	
1.8	E-mail: van de voornaamste contactpersoon	
1.9	Telefoonnummer van de voornaamste contactpersoon	
1.10	Naam van de tweede contactpersoon	
1.11	E-mail: van de tweede contactpersoon	
1.12	Telefoonnummer van de tweede contactpersoon	
1.13	Naam van de uiteindelijke moederonderneming	
1.14	LEI-code van de uiteindelijke moederonderneming	
1.15	Rapportagevaluta	
Inhoud van de eerste kennisgeving		
2.1	Door de financiële entiteit toegekende incidentreferentiecode	
2.2	Datum en tijdstip van detectie van het ernstige ICT-gerelateerde incident	
2.3	Datum en tijdstip van classificatie van het ICT-gerelateerde incident als ernstig	
2.4	Beschrijving van het ernstige ICT-gerelateerde incident	
2.5	Classificatiecriteria die aanleiding hebben gegeven tot de rapportage van het incident	
2.6	Materialiteitsdrempels voor het classificatiecriterium “geografische spreiding”	
2.7	Ontdekking van het ernstige ICT-gerelateerde incident	

Nummer van het veld	Gegevensveld	
2.8	Vermelding of het ernstige ICT-gerelateerde incident ontstond bij een derde aanbieder of een andere financiële entiteit	
2.9	Activering van het bedrijfscontinuïteitsplan, indien geactiveerd	
2.10	Andere nuttige informatie	
Inhoud van het tussentijdse verslag		
3.1	Door de bevoegde autoriteit verstrekte incidentreferentiecode	
3.2	Datum en tijdstip waarop het ernstige ICT-gerelateerde incident zich heeft voorgedaan	
3.3	Datum en tijdstip waarop diensten, activiteiten of verrichtingen zijn hersteld	
3.4	Aantal getroffen cliënten	
3.5	Percentage getroffen cliënten	
3.6	Aantal getroffen financiële tegenpartijen	
3.7	Percentage getroffen financiële tegenpartijen	
3.8	Gevolgen voor relevante cliënten of financiële tegenpartijen	
3.9	Aantal getroffen transacties	
3.10	Percentage getroffen transacties	
3.11	Waarde van de getroffen transacties	
3.12	Informatie over de vraag of het om werkelijke cijfers of om ramingen gaat, of dat er geen gevolgen zijn geweest	
3.13	Reputatieschade	
3.14	Contextuele informatie over de reputatieschade	
3.15	Duur van het ernstige ICT-gerelateerde incident	
3.16	Uitvaltijd van de dienst	
3.17	Informatie over de vraag of de cijfers voor de duur en de uitvaltijd van de dienst werkelijke cijfers zijn of ramingen	
3.18	Soorten gevolgen in de lidstaten	
3.19	Beschrijving van de gevolgen van het ernstige ICT-gerelateerde incident in andere lidstaten	
3.20	Materialiteitsdrempels voor het classificatiecriterium “gegevensverliezen”	
3.21	Beschrijving van de gegevensverliezen	

Nummer van het veld	Gegevensveld	
3.22	Classificatiecriterium “getroffen kritieke diensten”	
3.23	Soort ernstig ICT-gerelateerde incident	
3.24	Andere soorten incidenten	
3.25	Door de dreigingsactor gebruikte dreigingen en technieken	
3.26	Andere soorten technieken	
3.27	Informatie over getroffen functionele gebieden en bedrijfsprocessen	
3.28	Getroffen infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen	
3.29	Informatie over de getroffen infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen	
3.30	Gevolgen voor de financiële belangen van cliënten	
3.31	Rapportage aan andere autoriteiten	
3.32	Specificatie van “andere” autoriteiten	
3.33	Tijdelijke acties/maatregelen die zijn genomen of gepland om van het incident te herstellen	
3.34	Beschrijving van eventuele tijdelijke acties en maatregelen die zijn genomen of gepland om van het incident te herstellen	
3.35	Indicatoren voor aantasting	
Inhoud van het eindverslag		
4.1	Classificatie op hoog niveau van de onderliggende oorzaken van het incident	
4.2	Gedetailleerde classificatie van de onderliggende oorzaken van het incident	
4.3	Aanvullende classificatie van de onderliggende oorzaken van het incident	
4.4	Andere soorten onderliggende oorzaken	
4.5	Informatie over de onderliggende oorzaken van het incident	
4.6	Samenvatting van de oplossing van het incident	
4.7	Datum en tijdstip waarop de onderliggende oorzaak van het incident is aangepakt	
4.8	Datum en tijdstip waarop het incident is opgelost	
4.9	Informatie als de datum van permanente afwikkeling van het incident verschilt van de oorspronkelijk geplande uitvoeringsdatum	
4.10	Beoordeling van het risico voor kritieke functies voor afwikkelingsdoeleinden	
4.11	Informatie die relevant is voor afwikkelingsautoriteiten	

Nummer van het veld	Gegevensveld	
4.12	Materialiteitsdrempel voor het classificatiecriterium “economische effecten”	
4.13	Bedrag van de bruto directe en indirecte kosten en verliezen	
4.14	Bedrag van de financiële terugvorderingen	
4.15	Informatie over de vraag of de niet-ernstige incidenten al dan niet van terugkerende aard zijn	
4.16	Datum en tijdstip waarop terugkerende incidenten zich hebben voorgedaan	

BIJLAGE II

GLOSSARIUM VAN GEGEVENS EN INSTRUCTIES VOOR DE RAPPORTAGE VAN ERNSTIGE INCIDENTEN

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
Algemene informatie over de financiële entiteit					
1.1. Soort indiening	Vermeld de soort kennisgeving van of verslag over een incident die bij de bevoegde autoriteit wordt ingediend.	Ja	Ja	Ja	Keuze: — eerste kennisgeving — tussentijds verslag — eindverslag — ernstig incident geherclassificeerd als niet-ernstig
1.2. Identificatie van de entiteit die het verslag indient	Volledige juridische naam van de entiteit die het verslag indient.	Ja	Ja	Ja	Alfanumeriek
1.3. Identificatiecode van de entiteit die het verslag indient	Identificatiecode van de entiteit die het verslag indient. Wanneer financiële entiteiten de kennisgeving/het verslag indienen, is de identificatiecode een LEI (Legal Entity Identifier) — een unieke code van twintig alfanumerieke tekens, die op ISO 17442-1:2020 berust. Een derde aanbieder die een verslag voor een financiële entiteit indient, kan gebruikmaken van een identificatiecode uit de technische uitvoeringsnormen die zijn vastgesteld op grond van artikel 28, lid 9, van Verordening (EU) 2022/2554.	Ja	Ja	Ja	Alfanumeriek
1.4. Soort getroffen financiële entiteit	Soort entiteit als bedoeld in artikel 2, lid 1, punten a) tot en met t), van Verordening (EU) 2022/2554, waarvoor het verslag wordt ingediend. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de te selecteren verschillende soorten financiële entiteiten waarop het geaggregeerde verslag betrekking heeft.	Ja	Ja	Ja	Keuze (meerkeuze): — kredietinstelling; — betalingsinstelling; — vrijgestelde betalingsinstelling; — aanbieder van rekeninginformatiediensten; — instelling voor elektronisch geld; — vrijgestelde instelling voor elektronisch geld; — beleggingsonderneming; — aanbieder van cryptoactivadiensten; — uitgever van activagerelateerde tokens; — centrale effectenbewaarinstelling; — centrale tegenpartij; — handelsplatform; — transactieregister;

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
					— beheerder van een alternatieve beleggingsinstelling; — beheermaatschappij; — aanbieder van datarapportagediensten; — verzekerings- en herverzekeringsonderneming; — verzekeringstussenpersoon, herverzekeringstussenpersoon en nevenverzekeringstussenpersoon; — instelling voor bedrijfspensioenvoorziening; — ratingbureau; — beheerder van kritieke benchmarks; — aanbieder van crowdfundingdiensten; — securitisatieregister.
1.5. Naam van de getroffen financiële entiteit	Volledige juridische naam van de financiële entiteit die door het ernstige ICT-gerelateerde incident is getroffen en die krachtens artikel 19 van Verordening (EU) 2022/2554 verplicht is het ernstige incident bij haar bevoegde autoriteit te rapporteren. In het geval van geaggregeerde rapportage: a) lijst van alle namen van de financiële entiteiten die door het ernstige ICT-gerelateerde incident zijn getroffen, gescheiden door een puntkomma. b) de derde aanbieder die een kennisgeving of verslag van een ernstig incident op geaggregeerde wijze indient als bedoeld in artikel 7 van deze verordening, vermeldt de namen van alle door het incident geraakte financiële entiteiten, gescheiden door een puntkomma.	Ja, als de door het incident getroffen financiële entiteit verschilt van de entiteit die het verslag indient en in geval van geaggregeerde rapportage	Ja, als de door het incident getroffen financiële entiteit verschilt van de entiteit die het verslag indient en in geval van geaggregeerde rapportage	Ja, als de door het incident getroffen financiële entiteit verschilt van de entiteit die het verslag indient en in geval van geaggregeerde rapportage	Alfanumeriek
1.6. LEI-code van de getroffen financiële entiteit	Identificatiecode (LEI) van de financiële entiteit die is getroffen door het ernstige ICT-gerelateerde incident, zoals toegewezen overeenkomstig de regels van de Internationale Organisatie voor normalisatie. In het geval van geaggregeerde rapportage: a) een lijst van alle LEI-codes van de financiële entiteiten die door het ernstige ICT-gerelateerde incident zijn getroffen, gescheiden door een puntkomma.	Ja, als de door het ernstige ICT-gerelateerde incident getroffen financiële entiteit verschilt van de entiteit	Ja, als de door het ernstige ICT-gerelateerde incident getroffen financiële entiteit verschilt van de entiteit die	Ja, als de door het ernstige ICT-gerelateerde incident getroffen financiële entiteit verschilt van de entiteit die	Unieke code van twintig alfanumerieke tekens, gebaseerd op ISO 17442-1:2020

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	b) de derde aanbieder die een kennisgeving of verslag van een ernstig incident op geaggregeerde wijze indient zoals bedoeld in artikel 7 van deze verordening, vermeldt de LEI-codes van alle door het incident geraakte financiële entiteiten, gescheiden door een puntkomma. De volgorde van LEI-codes en namen van financiële entiteiten is identiek.	die het verslag indient en in het geval van geaggre-geerde rapportage.	het verslag indient en in het geval van geaggregeerde rapportage.	het verslag indient en in geval van geaggregeerde rapportage.	
1.7. Naam van de voornaamste contactpersoon	Voor- en achternaam van de voornaamste contactpersoon van de financiële entiteit. In geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de naam van de voornaamste contactpersoon in de entiteit die het geaggregeerde verslag indient.	Ja	Ja	Ja	Alfanumeriek
1.8. E-mail: van de voornaamste contactpersoon	E-mailadres van de voornaamste contactpersoon dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie. In geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de e-mail van de voornaamste contactpersoon in de entiteit die het geaggregeerde verslag indient.	Ja	Ja	Ja	Alfanumeriek
1.9. Telefoonnummer van de voornaamste contactpersoon	Het telefoonnummer van de voornaamste contactpersoon dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie. In geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, het telefoonnummer van de voornaamste contactpersoon in de entiteit die het geaggregeerde verslag indient. Het telefoonnummer moet met alle internationale kengetallen (bv. +33 XXXXXXXXX) worden opgegeven.	Ja	Ja	Ja	Alfanumeriek
1.10. Naam van de tweede contactpersoon	Voor- en achternaam van de tweede contactpersoon of de naam van het verantwoordelijke team van de financiële entiteit of een entiteit die namens de financiële entiteit het verslag indient	Ja	Ja	Ja	Alfanumeriek
1.11. E-mail: van de tweede contactpersoon	E-mailadres van de tweede contactpersoon of een functioneel e-mailadres van het team dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie	Ja	Ja	Ja	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
1.12. Telefoonnummer van de tweede contactpersoon	Het telefoonnummer van de tweede contactpersoon of van een team dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie. Het telefoonnummer moet met alle internationale kengetallen (bv. +33 XXXXXXXXX) worden opgegeven.	Ja	Ja	Ja	Alfanumeriek
1.13. Naam van de uiteindelijke moederonderneming	Naam van de uiteindelijke moederonderneming van de groep waartoe de getroffen financiële entiteit behoort, indien van toepassing.	Ja, als de financiële entiteit tot een groep behoort.	Ja, als de financiële entiteit tot een groep behoort.	Ja, als de financiële entiteit tot een groep behoort.	Alfanumeriek
1.14. LEI-code van de uiteindelijke moederonderneming	LEI van de uiteindelijke moederonderneming van de groep waartoe de getroffen financiële entiteit behoort, indien van toepassing. Toegewezen overeenkomstig de regels van de Internationale Organisatie voor normalisatie.	Ja, als de financiële entiteit tot een groep behoort.	Ja, als de financiële entiteit tot een groep behoort.	Ja, als de financiële entiteit tot een groep behoort.	Unieke code van twintig alfanumerieke tekens, gebaseerd op ISO 17442-1:2020.
1.15. Rapportagevaluta	Valuta gebruikt voor de rapportage van incidenten	Ja	Ja	Ja	Valutacode invullen volgens ISO 4217.
Inhoud van de eerste kennisgeving					
2.1. Door de financiële entiteit toegekende incidentreferentiecode	Door de financiële entiteit uitgegeven unieke referentiecode waarmee het ernstige ICT-gerelateerde incident ondubbelzinnig wordt geïdentificeerd. In geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de door de derde aanbieder toegekende incidentreferentiecode.	Ja	Ja	Ja	Alfanumeriek
2.2. Datum en tijdstip van detectie van het ICT-gerelateerde incident	Datum en tijdstip waarop de financiële entiteit kennis heeft gekregen van het ICT-gerelateerde incident. Voor terugkerende incidenten, de datum en het tijdstip waarop het laatste ICT-gerelateerde incident werd ontdekt.	Ja	Ja	Ja	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
2.3. Datum en tijdstip van classificatie van het incident als ernstig	Datum en tijdstip waarop het ICT-gerelateerde incident is geclassificeerd als ernstig volgens de classificatiecriteria van Gedelegeerde Verordening (EU) 2024/1772.	Ja	Ja	Ja	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)
2.4. Beschrijving van het ICT-gerelateerde incident	Beschrijving van de meest relevante aspecten van het ernstige ICT-gerelateerde incident. Financiële entiteiten verstrekken een overzicht op hoog niveau van de volgende informatie, zoals mogelijke oorzaken, onmiddellijke gevolgen, getroffen systemen en andere informatie. Financiële entiteiten vermelden — indien dat bekend is of redelijkerwijs mag worden verwacht — of het incident gevolgen heeft voor derde aanbieders of andere financiële entiteiten, de soort aanbieder of financiële entiteit, hun naam, hun respectieve identificatiecodes en de soort identificatiecode (bv. LEI of EUID). In latere verslagen kan de veldinhoud mee evolueren met het voortschrijdende inzicht in het ICT-gerelateerde incident en kan deze andere informatie over het ICT-gerelateerde incident bevatten die niet in de gegevensvelden was opgenomen, met inbegrip van informatie over de intern door de financiële entiteit ingeschatte ernst van de situatie (bv. zeer laag, laag, gemiddeld, hoog, zeer hoog) en een indicatie van het niveau en de naam van de structuren op het hoogste besluitvormingsniveau die bij de respons op het ICT-gerelateerde incident betrokken waren.	Ja	Ja	Ja	Alfanumeriek
2.5. Classificatiecriteria die aanleiding hebben gegeven tot de rapportage van het incident	Classificatiecriteria op grond van Gedelegeerde Verordening (EU) 2024/1772 die aanleiding hebben gegeven tot de classificatie van het ICT-gerelateerde incident als ernstig en de daaropvolgende kennisgeving en rapportage. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de classificatiecriteria die aanleiding hebben gegeven tot de classificatie van het ICT-gerelateerde incident als ernstig voor ten minste één of meer financiële entiteiten.	Ja	Ja	Ja	Keuze (meervoudig): — getroffen cliënten, financiële tegenpartijen en transacties; — reputatieschade; — duur en uitvaltijd van de dienst; — geografische spreiding; — gegevensverliezen; — getroffen kritieke diensten; — economische effecten.
2.6. Materialiteits drempels voor het classificatiecriterium “geografische spreiding”	EER-lidstaten die geraakt zijn door het ernstige ICT-gerelateerde incident Bij de beoordeling van de gevolgen van het ernstige ICT-gerelateerde incident in andere lidstaten houden financiële entiteiten rekening met de artikelen 4 en 12 van Gedelegeerde Verordening (EU) 2024/1772.	Ja, als de drempel voor “geografische spreiding” wordt gehaald.	Ja, als de drempel voor “geografische spreiding” wordt gehaald.	Ja, als de drempel voor “geografische spreiding” wordt gehaald.	Keuze (meervoudig) ingevuld aan de hand van ISO 3166 ALPHA-2 van de getroffen landen

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
2.7. Ontdekking van het ernstige ICT-gerelateerde incident	Vermelding van de wijze waarop het ernstige ICT-gerelateerde incident is ontdekt.	Ja	Ja	Ja	Keuze: — IT-beveiliging; — personeel; — interne audit; — externe audit; — cliënten; — financiële tegenpartijen; — derde aanbieder; — aanvaller; — monitoringsystemen; — autoriteit/agentschap/ wetshandhavingsinstantie; — andere.
2.8. Vermelding of het incident ontstond bij een derde aanbieder of een andere financiële entiteit	Vermelding of het ernstige ICT-gerelateerde incident ontstond bij een derde aanbieder of een andere financiële entiteit. Financiële entiteiten geven aan of het ernstige ICT-gerelateerde incident ontstond bij een derde aanbieder of een andere financiële entiteit (met inbegrip van financiële entiteiten die tot dezelfde groep behoren als de rapporterende entiteit), en vermelden de naam, de identificatiecode van de derde aanbieder of de financiële entiteit en de soort identificatiecode (bv. LEI of EUID).	Ja, als het incident ontstond bij een derde aanbieder of een andere financiële entiteit	Ja, als het incident ontstond bij een derde aanbieder of een andere financiële entiteit	Ja, als het incident ontstond bij een derde aanbieder of een andere financiële entiteit	Alfanumeriek
2.9. Activering van het bedrijfscontinuïteitsplan, indien geactiveerd	Vermelding of er sprake is geweest van een formele activering van de bedrijfscontinuïteitsresponsmaatregelen van de financiële entiteit.	Ja	Ja	Ja	Booleaans (ja of nee)
2.10. Andere nuttige informatie	Verdere informatie die niet onder het model valt. Financiële entiteiten die een ernstig ICT-gerelateerd incident hebben geherclassificeerd als niet-ernstig, beschrijven waarom het ICT-gerelateerde incident niet beantwoordt en naar verwachting niet zal beantwoorden aan de criteria om als een ernstig ICT-gerelateerd incident te worden aangemerkt.	Ja, als er andere informatie is die niet in het model is opgenomen of indien het ernstige ICT-gerelateerde incident is	Ja, als er andere informatie is die niet in het model is opgenomen of indien het ernstige ICT-gerelateerde incident is	Ja, als er andere informatie is die niet in het model is opgenomen of indien het ernstige ICT-gerelateerde incident is	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
		geherclassificeerd als niet-ernstig.	geherclassificeerd als niet-ernstig	geherclassificeerd als niet-ernstig	
Inhoud van het tussentijdse verslag					
3.1. Door de bevoegde autoriteit verstrekte incidentreferentiecode	Unieke referentiecode die door de bevoegde autoriteit op het moment van ontvangst van de eerste kennisgeving wordt toegekend om het ernstige ICT-gerelateerde incident ondubbelzinnig te identificeren.	Nee	Ja, indien van toepassing	Ja, indien van toepassing	Alfanumeriek
3.2. Datum en tijdstip waarop het incident zich heeft voorgedaan	Datum en tijdstip waarop het ernstige ICT-gerelateerde incident zich heeft voorgedaan, indien verschillend van het tijdstip waarop de financiële entiteit kennis heeft gekregen van het ernstige ICT-gerelateerde incident. Voor terugkerende ernstige ICT-gerelateerde incidenten, de datum en het tijdstip waarop het laatste ernstige ICT-gerelateerde incident zich heeft voorgedaan.	Nee	Ja	Ja	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)
3.3. Datum en tijdstip waarop diensten, activiteiten of verrichtingen zijn hersteld	Informatie over de datum en het tijdstip van het herstel van de diensten, activiteiten of verrichtingen die door het ernstige ICT-gerelateerde incident zijn getroffen.	Nee	Ja, indien gegevensveld 3.16. “Uitvaltijd van de dienst” is ingevuld	Ja, indien gegevensveld 3.16. “Uitvaltijd van de dienst” is ingevuld	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)
3.4. Aantal getroffen cliënten	Aantal door het ernstige ICT-gerelateerde incident getroffen cliënten die gebruikmaken van de door de financiële entiteit verleende dienst. Bij de beoordeling van het aantal getroffen cliënten houden financiële entiteiten bij hun beoordeling rekening met artikel 1, lid 1, en artikel 9, lid 1, punt b), van Gedelegeerde Verordening (EU) 2024/1772. Een financiële entiteit die het werkelijke aantal geraakte cliënten niet kan bepalen, gebruikt ramingen op basis van beschikbare gegevens uit vergelijkbare referentieperioden. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, het totale aantal getroffen cliënten van alle financiële entiteiten.	Nee	Ja	Ja	Numeriek geheel getal

Gegevensveld		Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
3.5.	Percentage getroffen cliënten	Percentage cliënten dat door het ernstige ICT-gerelateerde incident wordt getroffen in verhouding tot het totale aantal cliënten dat gebruikmaakt van de getroffen dienst die door de financiële entiteit wordt verleend. In het geval van meer dan één getroffen dienst worden de diensten op geaggregeerde wijze vermeld. Financiële entiteiten houden bij hun beoordeling rekening met artikel 1, lid 1, en artikel 9, lid 1, punt a), van Gedelegeerde Verordening (EU) 2024/1772. Een financiële entiteit die het werkelijke percentage geraakte cliënten niet kan bepalen, gebruikt ramingen op basis van beschikbare gegevens uit vergelijkbare referentieperioden. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, deelt een financiële entiteit de som van alle getroffen cliënten door het totale aantal cliënten van alle geraakte financiële entiteiten.	Nee	Ja	Ja	Uitgedrukt als percentage — elke waarde van maximaal 5 numerieke tekens inclusief maximaal 1 decimaal uitgedrukt als percentage (bv. 2,4 in plaats van 2,4 %). Indien de waarde meer dan 1 cijfer achter de komma telt, moeten de rapporterende tegenpartijen naar boven afronden.
3.6.	Aantal getroffen financiële tegenpartijen	Aantal door het ernstige ICT-gerelateerde incident getroffen financiële tegenpartijen die een contract met de financiële entiteit hebben gesloten. Bij de beoordeling van het aantal getroffen financiële tegenpartijen houden financiële entiteiten rekening met artikel 1, lid 2, van Gedelegeerde Verordening (EU) 2024/1772. Een financiële entiteit die het werkelijke aantal geraakte financiële tegenpartijen niet kan bepalen, gebruikt ramingen op basis van beschikbare gegevens uit vergelijkbare referentieperioden. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, het totale aantal getroffen financiële tegenpartijen van alle financiële entiteiten.	Nee	Ja	Ja	Numeriek geheel getal

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
3.7. Percentage getroffen financiële tegenpartijen	Percentage financiële tegenpartijen dat door het ernstige ICT-gerelateerde incident is getroffen in verhouding tot het totale aantal financiële tegenpartijen dat een contract met de financiële entiteit heeft gesloten. Bij de beoordeling van het percentage getroffen financiële tegenpartijen houden financiële entiteiten rekening met artikel 1, lid 1, en artikel 9, lid 1, punt c), van Gedelegeerde Verordening (EU) 2024/1772. Een financiële entiteit die het werkelijke percentage geraakte financiële tegenpartijen niet kan bepalen, gebruikt ramingen op basis van beschikbare gegevens uit vergelijkbare referentieperioden. Vermeld in het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de som van alle getroffen financiële tegenpartijen gedeeld door het totale aantal financiële tegenpartijen van alle geraakte financiële entiteiten.	Nee	Ja	Ja	Uitgedrukt als percentage — elke waarde van maximaal 5 numerieke tekens inclusief maximaal 1 decimaal uitgedrukt als percentage (bv. 2,4 in plaats van 2,4 %). Indien de waarde meer dan 1 cijfer achter de komma telt, moeten de rapporterende tegenpartijen naar boven afronden.
3.8. Gevolgen voor relevante cliënten of financiële tegenpartijen	Alle geconstateerde gevolgen voor relevante cliënten of financiële tegenpartijen als bedoeld in artikel 1, lid 3, en artikel 9, lid 1, punt f), van Gedelegeerde Verordening (EU) 2024/1772.	Nee	Ja, als de drempel voor "relevantie van cliënten en financiële tegenpartijen" wordt gehaald	Ja, als de drempel voor "relevantie van cliënten en financiële tegenpartijen" wordt gehaald	Booleaans (ja of nee)
3.9. Aantal getroffen transacties	Aantal door het ernstige ICT-gerelateerde incident getroffen transacties. Bij de beoordeling van de gevolgen voor transacties houden financiële entiteiten rekening met artikel 1, lid 4, van Gedelegeerde Verordening (EU) 2024/1772, met inbegrip van alle getroffen binnenlandse en grensoverschrijdende transacties met een geldbedrag waarbij ten minste één deel van de transactie in de Unie wordt uitgevoerd.	Nee	Ja, als een transactie door het incident is getroffen	Ja, als een transactie door het incident is getroffen	Numeriek geheel getal

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	Een financiële entiteit die het werkelijke aantal geraakte transacties niet kan bepalen, gebruikt ramingen op basis van beschikbare gegevens uit vergelijkbare referentieperioden. Vermeld in het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, het totale aantal getroffen transacties van alle financiële entiteiten.				
3.10. Percentage getroffen transacties	Percentage van de getroffen transacties in verhouding tot het dagelijkse gemiddelde aantal binnenlandse en grensoverschrijdende transacties dat de financiële entiteit met betrekking tot de getroffen dienst heeft uitgevoerd. Financiële entiteiten houden rekening met artikel 1, lid 4, en artikel 9, lid 1, punt d), van Gedelegeerde Verordening (EU) 2024/1772. Een financiële entiteit die het werkelijke percentage van de geraakte transacties niet kan bepalen, gebruikt ramingen. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, telt een financiële entiteit het aantal getroffen transacties op en deelt zij de som door het totale aantal transacties van alle geraakte financiële entiteiten.	Nee	Ja, als een transactie door het incident is getroffen	Ja, als een transactie door het incident is getroffen	Uitgedrukt als percentage — elke waarde van maximaal 5 numerieke tekens inclusief maximaal 1 decimaal uitgedrukt als percentage (bv. 2,4 in plaats van 2,4 %). Indien de waarde meer dan 1 cijfer achter de komma telt, moeten de rapporterende tegenpartijen naar boven afronden.
3.11. Waarde van de getroffen transacties	De totale waarde van de door het ernstige ICT-gerelateerde incident getroffen transacties wordt beoordeeld overeenkomstig artikel 1, lid 4, en artikel 9, lid 1, punt e), van Gedelegeerde Verordening (EU) 2024/1772. Een financiële entiteit die de werkelijke waarde van de geraakte transacties niet kan bepalen, gebruikt ramingen op basis van beschikbare gegevens uit vergelijkbare referentieperioden. Een financiële entiteit rapporteert het geldbedrag als een positieve waarde. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de totale waarde van de getroffen transacties van alle financiële entiteiten.	Nee	Ja, als transacties door het incident zijn getroffen	Ja, als een transactie door het incident is getroffen	Monetair Financiële entiteiten rapporteren het gegevenspunt in eenheden met een nauwkeurigheid die ten minste overeenkomt met duizendtallen (bv. 2,5 in plaats van 2 500 EUR).

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
3.12. Informatie over de vraag of het om werkelijke cijfers of om ramingen gaat, of dat er geen gevolgen zijn geweest	Informatie over de vraag of de waarden in de gegevensvelden 3.4 tot en met 3.11 werkelijke of geraamde waarden zijn, of dat er geen gevolgen zijn geweest.	Nee	Ja	Ja	Keuze (meervoudig): — werkelijke cijfers voor de getroffen cliënten; — werkelijke cijfers voor de getroffen financiële tegenpartijen; — werkelijke cijfers voor de getroffen transacties; — ramingen voor de getroffen cliënten; — ramingen voor de getroffen financiële tegenpartijen; — ramingen voor de getroffen transacties; — geen gevolgen voor de cliënten; — geen gevolgen voor de financiële tegenpartijen; — geen gevolgen voor de transacties.
3.13. Reputatieschade	Informatie over de reputatieschade van het ernstige ICT-gerelateerde incident als bedoeld in de artikelen 2 en 10 van Gedelegeerde Verordening (EU) 2024/1772. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de categorieën reputatieschade die van toepassing zijn op ten minste één financiële entiteit.	Nee	Ja, als aan het criterium "reputatie-schade" is voldaan	Ja, als aan het criterium "reputatie-schade" is voldaan	Keuze (meervoudig): — over het ernstige ICT-gerelateerde incident is bericht in de media; — het ernstige ICT-gerelateerde incident heeft geleid tot herhaalde klachten van verschillende cliënten of financiële tegenpartijen over diensten of kritieke zakelijke relaties; — de financiële entiteit zal door het ernstige ICT-gerelateerde incident niet of wellicht niet in staat zijn om aan de wettelijke eisen te voldoen; — de financiële entiteit zal door het ernstige ICT-gerelateerde incident cliënten of financiële tegenpartijen verliezen of wellicht verliezen, met wezenlijke gevolgen voor haar bedrijfsactiviteiten.
3.14. Contextuele informatie over de reputatieschade	Informatie over de wijze waarop het ernstige ICT-gerelateerde incident de reputatie van de financiële entiteit heeft getroffen of kan treffen, met inbegrip van inbreuken op de wetgeving, regelgevingsvereisten waaraan niet is voldaan, het aantal klachten van cliënten en andere.	Nee	Ja, als aan het criterium "reputatie-schade" is voldaan	Ja, als aan het criterium "reputatie-schade" is voldaan	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	Het gaat onder meer om de soort media (bv. traditionele en digitale media, blogs, streamingplatforms) en berichtgeving in de media, met inbegrip van het bereik van de media (lokaal, nationaal, internationaal). Berichtgeving in de media betekent in dit verband niet een paar negatieve opmerkingen van volgers of gebruikers van sociale netwerken. De financiële entiteit geeft ook aan of de berichtgeving in de media significante risico's voor haar cliënten in verband met het ernstige ICT-gerelateerde incident aan het licht heeft gebracht, met inbegrip van het risico van insolventie van de financiële entiteit of het risico van verlies van middelen. Financiële entiteiten geven ook aan of zij informatie aan de media hebben verstrekt om het publiek op betrouwbare wijze te informeren over het ernstige ICT-gerelateerde incident en de gevolgen daarvan. Financiële entiteiten kunnen ook aangeven of er in de media sprake was van onjuiste informatie met betrekking tot het ICT-gerelateerde incident, met inbegrip van informatie die gebaseerd is op opzettelijke verspreiding van onjuiste informatie door dreigingsactoren, of informatie met betrekking tot of ter illustratie van de ongewenste verandering ("defacement") van de website van de financiële entiteit.				
3.15. Duur van het incident	Financiële entiteiten meten de duur van het ernstige ICT-gerelateerde incident vanaf het moment waarop het ernstige ICT-gerelateerde incident zich heeft voorgedaan tot het moment waarop het incident is opgelost. Financiële entiteiten die niet in staat zijn het moment te bepalen waarop het ernstige ICT-gerelateerde incident zich heeft voorgedaan, meten de duur van het ernstige ICT-gerelateerde incident op grond van wat het eerste valt: het moment waarop de financiële entiteit het incident heeft ontdekt, of het moment waarop de financiële entiteit het incident in netwerk- of systeemlogbestanden of andere gegevensbronnen heeft geregistreerd. Financiële entiteiten die nog niet weten op welk moment het ernstige ICT-gerelateerde incident zal worden afgewikkeld, passen ramingen toe. De waarde wordt uitgedrukt in dagen, uren en minuten. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, meten financiële entiteiten de langste duur van het ernstige ICT-gerelateerde incident in geval van verschillen tussen financiële entiteiten.	Nee	Ja	Ja	DD:UU:MM

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
3.16. Uitvaltijd van de dienst	De uitvaltijd van de dienst gemeten 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 ernstige ICT-gerelateerde incident werd verleend. Wanneer de uitvaltijd van de dienst een vertraging in de dienstverlening veroorzaakt nadat de geregelde activiteiten of verrichtingen zijn hersteld, wordt de uitvaltijd gemeten vanaf het begin van het incident tot het moment waarop die vertraagde dienst wordt verleend. Financiële entiteiten die niet in staat zijn het moment te bepalen waarop de uitvaltijd van de dienst is begonnen, meten de uitvaltijd van de dienst op grond van wat het eerste valt: het moment waarop het incident werd ontdekt, of het moment waarop het is geregistreerd. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, meten financiële entiteiten de langste duur van de uitvaltijd van de dienst in geval van verschillen tussen financiële entiteiten.	Nee	Ja, als het incident heeft geleid tot een uitvaltijd van de dienst	Ja, als het incident heeft geleid tot een uitvaltijd van de dienst	DD:UU:MM
3.17. Informatie over de vraag of de cijfers voor de duur en de uitvaltijd van de dienst werkelijke cijfers zijn of ramingen	Informatie over de vraag of de waarden in de gegevensvelden 3.15 en 3.16 werkelijke waarden of ramingen zijn.	Nee	Ja, als aan het criterium “duur en uitvaltijd van de dienst” is voldaan	Ja, als aan het criterium “duur en uitvaltijd van de dienst” is voldaan	Keuze: — werkelijke cijfers — ramingen — werkelijke cijfers en ramingen — geen informatie beschikbaar
3.18. Soorten gevolgen in de lidstaten	Soort gevolgen in de respectieve EER-lidstaten. Vermelding of het ernstige ICT-gerelateerde incident gevolgen heeft gehad in andere EER-lidstaten (dan de lidstaat van de bevoegde autoriteit waaraan het incident rechtstreeks wordt gerapporteerd), overeenkomstig artikel 4 van Gedelegeerde Verordening (EU) 2024/1772, en met name of het effect aanzienlijk is in verband met: a) cliënten en financiële tegenpartijen in andere lidstaten, of	Nee	Ja, als de drempel voor “geografische spreiding” wordt gehaald	Ja, als de drempel voor “geografische spreiding” wordt gehaald	Keuze (meervoudig): — cliënten — financiële tegenpartijen — bijkantoor van de financiële entiteit — financiële entiteiten binnen de groep die activiteiten verrichten in de respectieve lidstaat — financiëlemarktinfrastructuur — derde aanbieders die gemeenschappelijk kunnen zijn met andere financiële entiteiten

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	b) bijkantoren of andere financiële entiteiten binnen de groep die activiteiten verrichten in andere lidstaten, of c) financiëlemarktinfrastructuren of derde aanbieders, die gevolgen kunnen hebben voor financiële entiteiten in andere lidstaten waaraan zij diensten verlenen.				
3.19. Beschrijving van de gevolgen van het incident in andere lidstaten	Beschrijving van de gevolgen en de ernst van het ernstige ICT-gerelateerde incident in elke getroffen lidstaat, met inbegrip van een beoordeling van de gevolgen en de ernst voor: a) cliënten; b) financiële tegenpartijen; c) bijkantoren van de financiële entiteit; d) andere financiële entiteiten binnen de groep die activiteiten verrichten in andere lidstaten; e) financiëlemarktinfrastructuren; f) derde aanbieders die gemeenschappelijk kunnen zijn met andere financiële entiteiten, zoals van toepassing in (een) andere lidsta(a)t(en).	Nee	Ja, als de drempel voor "geografische spreiding" wordt gehaald	Ja, als de drempel voor "geografische spreiding" wordt gehaald	Alfanumeriek
3.20. Materialiteits drempels voor het classificatiecriterium "gegevensverliezen"	Soort gegevensverliezen ten gevolge van het ernstige ICT-gerelateerde incident met betrekking tot beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens. Financiële entiteiten houden bij hun beoordeling rekening met de artikelen 5 en 13 van Gedelegeerde Verordening (EU) 2024/1772. In geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de gegevensverliezen waardoor ten minste één financiële entiteit wordt getroffen.	Nee	Ja, als aan het criterium "gegevensverliezen" is voldaan	Ja, als aan het criterium "gegevensverliezen" is voldaan	Keuze (meervoudig): — beschikbaarheid — authenticiteit — integriteit — vertrouwelijkheid
3.21. Beschrijving van de gegevensverliezen	Beschrijving van de gevolgen van het ernstige ICT-gerelateerde incident voor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van kritieke gegevens overeenkomstig de artikelen 5 en 13 van Gedelegeerde Verordening (EU) 2024/1772. Informatie over de gevolgen voor de uitvoering van de bedrijfsdoelstellingen van de financiële entiteit of voor de naleving van de regelgevingsvereisten. Financiële entiteiten geven onder meer aan of het bij de betrokken gegevens gaat om cliëntgegevens, om gegevens van andere entiteiten (bv. financiële tegenpartijen) of om gegevens van de financiële entiteit zelf.	Nee	Ja, als aan het criterium "gegevensverliezen" is voldaan	Ja, als aan het criterium "gegevensverliezen" is voldaan	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	De financiële entiteit kan ook aangeven welke soort gegevens bij het incident betrokken is, en met name of de gegevens vertrouwelijk zijn en om welke soort vertrouwelijkheid het gaat (bv. commerciële/zakelijke vertrouwelijkheid, persoonsgegevens, beroepsgeheim: bankgeheim, verzekeringsgeheim, geheimhouding van betalingsdiensten enz.). Ook kan worden vermeld welke risico's er mogelijk verbonden zijn aan de gegevensverliezen, bijvoorbeeld of de door het incident getroffen gegevens kunnen worden gebruikt om personen te identificeren of door de dreigingsactor kunnen worden gebruikt om zonder hun toestemming kredieten of leningen te verkrijgen, om gerichte phishingaanvallen uit te voeren of om informatie openbaar te maken. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, een algemene beschrijving van de gevolgen van het incident voor de getroffen financiële entiteiten. Indien er verschillen zijn in de gevolgen, worden in de beschrijving van de gevolgen duidelijk de specifieke gevolgen voor de verschillende financiële entiteiten vermeld.				
3.22. Classificatie criterium "getroffen kritieke diensten"	Informatie over het criterium "getroffen kritieke diensten". Financiële entiteiten houden bij hun beoordeling rekening met artikel 6 van Gedelegeerde Verordening (EU) 2024/1772, met inbegrip van informatie over: — de getroffen diensten of activiteiten waarvoor een vergunning of registratie vereist is of die onder toezicht staan van bevoegde autoriteiten, of — de ICT-diensten of netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen, en — de aard van de kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen van de financiële entiteit. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de gevolgen op kritieke diensten die van toepassing zijn op ten minste één financiële entiteit.	Nee	Ja	Ja	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
3.23. Soort incident	Classificatie van incidenten naar soort.	Nee	Ja	Ja	Keuze (meervoudig): — in verband met cyberbeveiliging — processtoring — systeemstoring — externe gebeurtenis — in verband met betalingen — andere (gelieve aan te geven wat)
3.24. Andere soorten incidenten	Andere soorten ICT-gerelateerde incidenten: financiële entiteiten die in 3.23 "andere" soort incidenten hebben geselecteerd, vermelden de soort ICT-gerelateerd incident.	Nee	Ja, als "andere" soort incidenten is geselecteerd in gegevensveld 3.23	Ja, als "andere" soort incidenten is geselecteerd in gegevensveld 3.23	Alfanumeriek
3.25. Door de dreigingsactor gebruikte dreigingen en technieken	Vermeld de bedreigingen en technieken die door de dreigingsactor worden gebruikt, met inbegrip van: a) social engineering, met inbegrip van phishing; b) (D)DoS; c) identiteitsdiefstal; d) gegevensversleuteling voor gevolgen, met inbegrip van ransomware; e) het kapen van hulpmiddelen; f) exfiltratie en manipulatie van gegevens, met uitzondering van identiteitsdiefstal; g) vernietiging van gegevens; h) ongewenste verandering van de website ("defacement"); i) aanval op de toeleveringsketen; j) andere (gelieve aan te geven wat).	Nee	Ja, als het bij de soort ICT-gerelateerd incident om "cyberveiligheid" is in veld 3.23 gaat	Ja, als het bij de soort ICT-gerelateerd incident om "cyberveiligheid" is in veld 3.23 gaat	Keuze (meervoudig): — social engineering (met inbegrip van phishing) — (D)DoS — identiteitsdiefstal — gegevensversleuteling voor effecten, met inbegrip van ransomware — het kapen van hulpmiddelen — exfiltratie en manipulatie van gegevens, met uitzondering van identiteitsdiefstal — vernietiging van gegevens — ongewenste verandering van de website ("defacement") — aanval op de toeleveringsketen — andere (gelieve aan te geven wat)
3.26. Andere soorten technieken	Andere soorten technieken Financiële entiteiten die in gegevensveld 3.25 "andere" soort technieken hebben geselecteerd, vermelden de soort techniek.	Nee	Ja, als "andere" soort technieken is geselecteerd in gegevensveld 3.25	Ja, als "andere" soort technieken is geselecteerd in gegevensveld 3.25	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
3.27. Informatie over getroffen functionele gebieden en bedrijfsprocessen	Vermelding van de functionele gebieden en bedrijfsprocessen die door het incident zijn getroffen, met inbegrip van producten en diensten. De functionele gebieden omvatten, maar zijn niet beperkt tot: a) marketing en bedrijfsontwikkeling; b) dienstverlening voor klanten; c) productbeheer; d) naleving van de regelgeving; e) risicobeheer; f) financieel beheer en boekhouding; g) HR en algemene diensten; h) informatietechnologie; De bedrijfsprocessen omvatten, maar zijn niet beperkt tot: — rekeninginformatie; — actuariële diensten; — acceptatie van betalingstransacties; — authenticatie/autorisatie; — onboarden van overheidsinstanties als klant; — uitkeringsadministratie; — beheer van uitkeringsbetalingen; — kopen en verkopen van verpakte verzekeringspolissen onder verzekeringen; — kaartbetalingen; — kasbeheer; — plaatsen of opnemen van contanten; — beheer van verzekeringsclaims; — claimproces verzekeringen; — clearing; — conglomeraten met bedrijfsleningen; — collectieve verzekeringen; — overmakingen; — bewaring van activa; — onboarden van klanten; — gegevensopname; — gegevensverwerking; — automatische afschrijving; — exportverzekeringen; — afronden van transacties/deals; — plaatsing van financiële instrumenten; — de boekhouding van het fonds; — vreemde valuta;	Nee	Ja	Ja	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	— beleggingsadvies; — beleggingsbeheer; — uitgifte van betaalinstrumenten; — beheer van leningverstrekking; — betalingsprocedures voor levensverzekeringen; — geldtransfers; — berekening van de nettoactiva; — order; — betaalinitiatie; — afsluiten van verzekeringen; — portefeuillebeheer; — het innen van premies; — ontvangst/doorgifte/uitvoering; — herverzekering; — afwikkeling; — monitoring van transacties. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, de getroffen functionele gebieden en bedrijfsprocessen in ten minste één financiële entiteit.				
3.28. Getroffen infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen	Informatie over de vraag of infrastructuurcomponenten (servers, besturingssystemen, software, applicatieservers, middleware, netwerkcomponenten, andere) die bedrijfsprocessen ondersteunen, getroffen zijn door het ernstige ICT-gerelateerde incident.	Nee	Ja	Ja	Keuze: — Ja — Nee — Informatie niet beschikbaar
3.29. Informatie over de getroffen infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen	Beschrijving van de gevolgen van het ernstige ICT-gerelateerde incident voor infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen, met inbegrip van hardware en software. Hardware omvat servers, computers, datacentra, schakelaars, routers en hubs. Software omvat besturingssystemen, toepassingen, databanken, beveiligingsinstrumenten, netwerkcomponenten, andere (gelieve aan te geven wat). In de beschrijvingen worden de getroffen infrastructuurcomponenten of -systemen beschreven of vermeld, en, indien beschikbaar: a) versiegegevens; b) interne infrastructuur/gedeeltelijk uitbesteed/volledig uitbesteed — naam derde aanbieder;	Nee	Ja, als het incident gevolgen heeft gehad voor infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen	Ja, als het incident gevolgen heeft gehad voor infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	c) of de infrastructuur wordt gebruikt of gedeeld over meerdere bedrijfsfuncties; d) relevante regelingen inzake veerkracht/continuïteit/herstel/substitueerbaarheid.				
3.30. Gevolgen voor de financiële belangen van cliënten	Informatie over de vraag of het ernstige ICT-gerelateerde incident de financiële belangen van cliënten heeft geraakt.	Nee	Ja	Ja	Keuze: — Ja — Nee — Informatie niet beschikbaar
3.31. Rapportage aan andere autoriteiten	Specificatie van de autoriteiten die zijn geïnformeerd over het ernstige ICT-gerelateerde incident. Rekening houdend met de verschillen die voortvloeien uit de nationale wetgeving van de lidstaten, wordt het begrip rechtshandhavingsautoriteiten door financiële entiteiten ruim opgevat, zodat het overheidsinstanties omvat die bevoegd zijn om cybercriminaliteit te vervolgen, met inbegrip van politie, rechtshandhavingsinstanties en openbare aanklagers.	Nee	Ja	Ja	Keuze (meervoudig): — Politie/rechtshandhaving — CSIRT — Gegevensbeschermingsautoriteit — Nationaal agentschap voor cyberbeveiliging — Geen — Andere (gelieve aan te geven wat)
3.32. Specificatie van “andere” autoriteiten	Specificatie van “andere” soorten autoriteiten die in kennis zijn gesteld van het ernstige ICT-gerelateerde incident. Indien geselecteerd in gegevensveld 3.31. “Andere”: de beschrijving bevat meer gedetailleerde informatie over de autoriteit waarbij de financiële entiteit informatie over het ernstige ICT-gerelateerde incident heeft ingediend.	Nee	Ja, als “andere” soorten autoriteiten door de financiële entiteit in kennis zijn gesteld van het ernstige ICT-gerelateerde incident.	Ja, als “andere” soorten autoriteiten door de financiële entiteit in kennis zijn gesteld van het ernstige ICT-gerelateerde incident	Alfanumeriek
3.33. Tijdelijke acties/maatregelen die zijn genomen of gepland om van het incident te herstellen	Vermelding of de financiële entiteit tijdelijke maatregelen heeft uitgevoerd (of van plan is uit te voeren) die zijn genomen (of gepland om te worden genomen) om te herstellen van het ernstige ICT-gerelateerde incident.	Nee	Ja	Ja	Booleaans (ja of nee)

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
3.34. Beschrijving van eventuele tijdelijke acties en maatregelen die zijn genomen of gepland om van het incident te herstellen	In de informatie worden de onmiddellijk genomen maatregelen beschreven, met inbegrip van de isolatie van het incident op netwerkniveau, de geactiveerde workaroundprocedures, geblokkeerde USB-poorten, de geactiveerde uitwijklocatie en eventuele andere tijdelijk ingestelde aanvullende beveiligingscontroles. Financiële entiteiten vermelden de datum en het tijdstip van de uitvoering van de tijdelijke acties en de verwachte datum van terugkeer naar de primaire locatie. Voor tijdelijke acties die niet zijn uitgevoerd maar nog gepland zijn, vermelding van de datum waarop de uitvoering ervan wordt verwacht. Indien er geen tijdelijke acties/maatregelen zijn genomen, geef dan de reden aan.	Nee	Ja, als er tijdelijke acties/ maatregelen zijn genomen of gepland zijn (gegevensveld 3.33)	Ja, als er tijdelijke acties/ maatregelen zijn genomen of gepland zijn (gegevensveld 3.33)	Alfanumeriek
3.35. Indicatoren voor aantasting	Informatie over het ernstige ICT-gerelateerde incident die kan helpen kwaadwillige activiteiten binnen een netwerk- of informatiesysteem (indicatoren voor aantasting) te identificeren, indien van toepassing. Het veld is alleen van toepassing op financiële entiteiten die binnen het toepassingsgebied van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([1]) vallen en financiële entiteiten die overeenkomstig de nationale regels tot omzetting van artikel 3 van Richtlijn (EU) 2022/2555 als essentiële of belangrijke entiteiten zijn aangemerkt, indien van toepassing. De door de financiële entiteit verstrekte indicatoren voor aantasting omvatten de volgende gegevenscategorieën: a) IP-adressen; b) URL-adressen; c) domeinen; d) bestandshashes; e) malwaregegevens (malwarenaam, -bestandsnamen en de locaties ervan, specifieke registratiesleutels in verband met malwareactiviteit); f) gegevens over netwerkactiviteiten (poorten, protocollen, adressen, referrers, gebruikersagenten, headers, specifieke logbestanden of onderscheidende patronen in het netwerkverkeer); g) gegevens van e-mailberichten (afzender, ontvanger, onderwerp, header, inhoud);	Nee	Ja, als cyberbeveiliging is geselecteerd als een soort incident in gegevensveld 3.23	Ja, als cyberbeveiliging is geselecteerd als een soort incident in gegevensveld 3.23	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	h) DNS-verzoeken en registerconfiguraties; i) activiteiten op het gebied van gebruikersaccounts (logins, activiteit op de account van geprivilegieerde gebruikers, privilege-escalatie); j) databankverkeer (lezen/schrijven), verzoeken aan hetzelfde bestand. In de praktijk kan het onder meer gaan om gegevens over indicatoren voor patronen in het netwerkverkeer die passen bij bekende aanvallen/botnetcommunicatie, IP-adressen van machines die besmet zijn met malware (bots), gegevens over door malware gebruikte "bedienings- en besturingsservers" (gewoonlijk domeinen of IP-adressen) en URL's van phishingsites of websites die malware hosten of kits exploiteren.				
Inhoud van het eindverslag					
4.1. Classificatie op hoog niveau van de onderliggende oorzaken van het incident	Classificatie op hoog niveau van de onderliggende oorzaak van het ernstige ICT-gerelateerde incident onder de soorten incidenten, met inbegrip van de volgende categorieën op hoog niveau: a) kwaadwillige handelingen; b) processtoring; c) storing/defect van het systeem; d) menselijke fout; e) externe gebeurtenis.	Nee	Nee	Ja	Keuze (meervoudig): — kwaadwillige handelingen; — processtoring; — storing/defect van het systeem; — menselijke fout; — externe gebeurtenis.
4.2. Gedetailleerde classificatie van de onderliggende oorzaken van het incident	Gedetailleerde classificatie van de onderliggende oorzaken van het ernstige ICT-gerelateerde incident onder de soorten incidenten, met inbegrip van de volgende gedetailleerde categorieën in verband met de categorieën op hoog niveau die in gegevensveld 4.1 worden gerapporteerd: 1. **Kwaadwillige handelingen** (indien geselecteerd, kies een of meer uit de volgende elementen): a) opzettelijke interne handelingen; b) opzettelijke fysieke beschadiging/manipulatie/diefstal; c) frauduleuze handelingen. 2. **Processtoring** (indien geselecteerd, kies een of meer van de volgende elementen): a) ontoereikende monitoring of geen monitoring en controle;	Nee	Nee	Ja	Keuze (meervoudig): — kwaadwillige handelingen: opzettelijke interne handelingen; — kwaadwillige handelingen: opzettelijke fysieke beschadiging/manipulatie/diefstal; — kwaadwillige handelingen: frauduleuze handelingen; — processtoring: ontoereikende monitoring of geen monitoring en controle; — processtoring: ontoereikende/onduidelijke rollen en verantwoordelijkheden; — processtoring: processtoring op het gebied van ICT-risicobeheer; — processtoring: ontoereikende of verstoorde ICT-activiteiten en ICT-beveiligingsoperaties;

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	b) ontoereikende/onduidelijke rollen en verantwoordelijkheden; c) processtoring op het gebied van ICT-risicobeheer; d) ontoereikende of verstoorde ICT-activiteiten en ICT-beveiligingsoperaties; e) ontoereikend of verstoord ICT-projectbeheer; f) ontoereikend(e) intern beleid, procedures en documentatie; g) ontoereikend(e) aanschaf, ontwikkeling en onderhoud van ICT-systemen; h) andere (gelieve aan te geven wat). 3. **Processtoring/defect** (indien geselecteerd, kies een of meer van de volgende elementen): a) hardwarecapaciteit en -prestaties: ernstige ICT-gerelateerde incidenten veroorzaakt door hardwaremiddelen die ontoereikend blijken te zijn wat betreft capaciteit of prestaties om aan de toepasselijke wettelijke eisen te voldoen; b) onderhoud van hardware: ernstige ICT-gerelateerde incidenten die het gevolg zijn van niet-passend of ontoereikend onderhoud van hardwarecomponenten, met uitzondering van "achterhaalde/verouderde hardware"; c) achterhaalde/verouderde hardware: deze soort onderliggende oorzaak betreft ernstige ICT-gerelateerde incidenten die het gevolg zijn van gedateerde of verouderde hardwarecomponenten; d) compatibiliteit/configuratie van software: ernstige ICT-gerelateerde incidenten die worden veroorzaakt door softwarecomponenten die incompatibel zijn met andere software- of systeemconfiguraties, met inbegrip van ernstige ICT-gerelateerde incidenten die het gevolg zijn van softwareconflicten, onjuiste instellingen of verkeerd geconfigureerde parameters die van invloed zijn op de algemene systeemfunctionaliteit; e) softwareprestaties: ernstige ICT-gerelateerde incidenten die het gevolg zijn van softwarecomponenten die slechte prestaties of inefficiënties vertonen om andere dan de onder "softwarecompatibiliteit/configuratie" vermelde redenen, met inbegrip van ernstige ICT-gerelateerde incidenten als gevolg van trage responstijden, buitensporig hulpbronnenverbruik of inefficiënte uitvoering van zoekopdrachten die van invloed zijn op de prestaties van de software of het systeem;				— processtoring: ontoereikend of verstoord ICT-projectbeheer; — processtoring: ontoereikende interne gedragslijnen, procedures en documentatie; — processtoring: ontoereikend(e) aanschaf, ontwikkeling en onderhoud van ICT-systemen; — processtoring: andere (gelieve aan te geven wat); — systeemstoring: hardwarecapaciteit en -prestaties; — systeemstoring: onderhoud van hardware; — systeemstoring: achterhaalde/verouderde hardware; — systeemstoring: compatibiliteit/configuratie van software; — systeemstoring: softwareprestaties; — systeemstoring: netwerkconfiguratie; — systeemstoring: fysieke beschadiging; — systeemstoring: andere (gelieve aan te geven wat); — menselijke fout: nalatigheid; — — menselijke fout: vergissing; — menselijke fout: kennis en vaardigheden; — menselijke fout: onvoldoende personele middelen; — menselijke fout: miscommunicatie; — menselijke fout: andere (gelieve aan te geven wat); — externe gebeurtenis: natuurrampen/overmacht; — externe gebeurtenis: storingen bij derden; — externe gebeurtenis: andere (gelieve aan te geven wat).

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	f) netwerkconfiguratie: ernstige ICT-gerelateerde incidenten die het gevolg zijn van onjuiste of verkeerd geconfigureerde netwerkinstellingen of -infrastructuur, met inbegrip van ernstige ICT-gerelateerde incidenten als gevolg van fouten in de netwerkconfiguratie, routeringsproblemen, misconfiguraties van de firewall of andere netwerkgerelateerde problemen die van invloed zijn op connectiviteit of communicatie; g) fysieke beschadiging: ernstige ICT-gerelateerde incidenten veroorzaakt door fysieke beschadiging aan ICT-infrastructuur die tot systeemstoringen leiden; h) andere (gelieve aan te geven wat). 4. **Menselijke fout** (indien geselecteerd, kies een of meer van de volgende elementen): a) nalatigheid (onopzettelijk); b) vergissing; c) kennis en vaardigheden: ernstige ICT-gerelateerde incidenten die het gevolg zijn van een gebrek aan deskundigheid of bekwaamheid in de omgang met ICT-systemen of -processen, die kunnen worden veroorzaakt door ontoereikende opleiding, ontoereikende kennis of lacunes in vaardigheden die nodig zijn om specifieke taken uit te voeren of technische uitdagingen aan te pakken; d) onvoldoende personele middelen: ernstige ICT-gerelateerde incidenten die worden veroorzaakt door een gebrek aan noodzakelijke middelen, waaronder hardware, software, infrastructuur of personeel, en met inbegrip van situaties waarin onvoldoende middelen leiden tot operationele inefficiënties, systeemstoringen of een onvermogen om aan de bedrijfsbehoeften te voldoen; e) miscommunicatie; f) andere (gelieve aan te geven wat). 5. **Externe gebeurtenis** (indien geselecteerd, kies een of meer van de volgende elementen) a) natuurrampen/overmacht; b) storingen bij derden;				

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	c) andere (gelieve aan te geven wat). Financiële entiteiten moeten erop letten dat bij terugkerende ernstige ICT-gerelateerde incidenten rekening wordt gehouden met de specifieke kennelijke onderliggende oorzaak van het incident en niet met de brede categorieën die in dit veld zijn opgenomen.				
4.3. Aanvullende classificatie van de onderliggende oorzaken van het incident	Aanvullende classificatie van de onderliggende oorzaken van het ernstige ICT-gerelateerde incident onder de soorten incidenten, met inbegrip van de volgende aanvullende classificatiecategorieën in verband met de gedetailleerde categorieën die in gegevensveld 4.2 moeten worden gerapporteerd. Het veld is verplicht voor het eindverslag als in gegevensveld 4.2 specifieke categorieën worden gerapporteerd die verdere granulariteit vereisen. 2 **a) Ontoereikende of geen monitoring en controle:** a) monitoring van de naleving van het beleid; b) monitoring van derde aanbieders van diensten; c) monitoring en verificatie het verhelpen van kwetsbaarheden; d) identiteits- en toegangsbeheer; e) encryptie en cryptografie; f) bijhouden van logbestanden. 2 **c) Processtoring op het gebied van ICT-risicobeheer:** a) niet-aangeven van nauwkeurige risicotolerantieniveaus; b) ontoereikende kwetsbaarheids- en dreigingsevaluaties; c) ontoereikende risicobehandelingsmaatregelen; d) slecht beheer van resterende ICT-risico's. 2 **d) Ontoereikende of verstoorde ICT-activiteiten en ICT-beveiligingsoperaties:** a) kwetsbaarhedenbeheer en patchmanagement; b) wijzigingsbeheer; c) capaciteits- en prestatiebeheer; d) ICT-vermogensbeheer en classificatie van de informatie;	Nee	Nee	Ja	Keuze (meervoudig): — monitoring van de naleving van het beleid; — monitoring van derde aanbieders van diensten; — monitoring en verificatie het verhelpen van kwetsbaarheden; — identiteits- en toegangsbeheer; — encryptie en cryptografie; — bijhouden van logbestanden; — niet-aangeven van nauwkeurige risicotolerantieniveaus; — ontoereikende kwetsbaarheids- en dreigingsevaluaties; — ontoereikende risicobehandelingsmaatregelen; — slecht beheer van resterende ICT-risico's; — kwetsbaarhedenbeheer en patchmanagement; — wijzigingsbeheer; — capaciteits- en prestatiebeheer; — ICT-vermogensbeheer en classificatie van de informatie; — back-up en herstel; — behandeling van fouten; — ontoereikend(e) aanschaf, ontwikkeling en onderhoud van ICT-systemen; — onvoldoende of mislukte softwaretests

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	e) back-up en herstel; f) behandeling van fouten. 2 **g) Ontoereikend(e) aanschaf, ontwikkeling en onderhoud van ICT-systemen:** a) ontoereikend(e) aanschaf, ontwikkeling en onderhoud van ICT-systemen; b) onvoldoende softwaretests of mislukte softwaretests.				
4.4. Andere soorten onderliggende oorzaken	Financiële entiteiten die in gegevensveld 4.2 “andere” soort onderliggende oorzaak hebben geselecteerd, vermelden de andere soorten onderliggende oorzaken	Nee	Nee	Ja, als “andere” soort onderliggende oorzaken is geselecteerd in gegevensveld 4.2.	Alfanumeriek
4.5. Informatie over de onderliggende oorzaken van het incident	Beschrijving van de volgorde van gebeurtenissen die tot het ernstige ICT-gerelateerde incident hebben geleid en een beschrijving van de wijze waarop het ernstige ICT-gerelateerde incident een vergelijkbare kennelijke onderliggende oorzaak heeft indien dat incident als een terugkerend incident wordt geclassificeerd, met inbegrip van een beknopte beschrijving van alle onderliggende redenen en primaire factoren die hebben bijgedragen tot het optreden van het ernstige ICT-gerelateerde incident. Indien er kwaadwillige handelingen waren, een beschrijving van de modus operandi van de kwaadwillige handeling, met inbegrip van de gebruikte tactieken, technieken en procedures, alsmede de instapvector van het ernstige ICT-gerelateerde incident, met inbegrip van een beschrijving van de onderzoeken en analysen waarmee de onderliggende oorzaken konden worden achterhaald, indien van toepassing.	Nee	Nee	Ja	Alfanumeriek
4.6. Afwikkeling van incidenten	Aanvullende informatie over de acties/maatregelen die zijn genomen/gepland om het ernstige ICT-gerelateerde incident permanent af te wikkelen en te voorkomen dat dat incident zich opnieuw voordoet. Lessen die zijn getrokken uit het ernstige ICT-gerelateerde incident.	Nee	Nee	Ja	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	De beschrijving bevat de volgende punten: 1. **Beschrijving van de afwikkelingsmaatregelen** a) maatregelen die zijn genomen om het ernstige ICT-gerelateerde incident permanent af te wikkelen (met uitzondering van tijdelijke maatregelen); b) vermeld voor elke ondernomen actie de mogelijke betrokkenheid van een derde aanbieder en van de financiële entiteit; c) vermeld of de procedures zijn aangepast naar aanleiding van het ernstige ICT-gerelateerde incident; d) vermeld eventuele aanvullende controles die zijn ingevoerd of gepland met het bijbehorende tijdschema voor de uitvoering. Mogelijke problemen met betrekking tot de robuustheid van de geraakte IT-systemen of met betrekking tot de bestaande procedures of controles, indien van toepassing. Financiële entiteiten geven duidelijk aan hoe de beoogde herstelmaatregelen de geconstateerde onderliggende oorzaken zullen aanpakken en wanneer het ernstige ICT-gerelateerde incident naar verwachting permanent zal worden afgewikkeld. 2. **Lessen uit het verleden** Financiële entiteiten beschrijven de bevindingen van de evaluatie na het incident.				
4.7. Datum en tijdstip waarop de onderliggende oorzaak van het incident is aangepakt	Datum en tijdstip waarop de onderliggende oorzaak van het incident is aangepakt.	Nee	Nee	Ja	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)
4.8. Datum en tijdstip waarop het incident is opgelost	Datum en tijdstip waarop het incident is opgelost.	Nee	Nee	Ja	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
4.9. Informatie als de datum van permanente afwikkeling van de incidenten verschilt van de oorspronkelijk geplande uitvoeringsdatum	Beschrijving van de reden waarom de permanente afwikkelingsdatum van de ernstige ICT-gerelateerde incidenten verschilt van de oorspronkelijk geplande uitvoeringsdatum, indien van toepassing.	Nee	Nee	Ja	Alfanumeriek
4.10. Beoordeling van het risico voor kritieke functies voor afwikkelingsdoeleinden	Beoordeling of het ernstige ICT-gerelateerde incident een risico vormt voor kritieke functies in de zin van artikel 2, lid 1, punt 35, van Richtlijn 2014/59/EU van het Europees Parlement en de Raad ([2]). Entiteiten zoals bedoeld in artikel 1, lid 1, van Richtlijn 2014/59/EU, geven aan of het incident een risico vormt voor de kritieke functies in de zin van artikel 2, lid 1, punt 35, van Richtlijn 2014/59/EU, en zoals gerapporteerd in template Z07.01 van Uitvoeringsverordening (EU) 2018/1624 van de Commissie ([3]) en gemapt met een specifieke entiteit in template Z07.02.	Nee	Nee	Ja, als het incident een risico vormt voor kritieke functies van financiële entiteiten in de zin van artikel 2, lid 1, punt 35, van Richtlijn 2014/59/EU	Alfanumeriek
4.11. Informatie die relevant is voor afwikkelingsautoriteiten	Beschrijving van de vraag of en, zo ja, hoe het ernstige ICT-gerelateerde incident de afwikkelbaarheid van de entiteit of de groep heeft beïnvloed. Entiteiten als bedoeld in artikel 1, lid 1, van Richtlijn 2014/59/EU, verstrekken informatie over de vraag of en, zo ja, hoe het ernstige ICT-gerelateerde incident de afwikkelbaarheid van de entiteit of de groep heeft beïnvloed. Die entiteiten vermelden ook of het ernstige ICT-gerelateerde incident gevolgen heeft voor de solvabiliteit of liquiditeit van de financiële entiteit en voor de potentiële kwantificering van de gevolgen. Die entiteiten verstrekken ook informatie over de gevolgen voor de operationele continuïteit, de gevolgen voor de afwikkelbaarheid van de entiteit, eventuele aanvullende gevolgen voor de kosten en verliezen van het ernstige ICT-gerelateerde incident, met inbegrip van de kapitaalpositie van de financiële entiteit, en over de vraag of de contractuele regelingen voor het gebruik van ICT-diensten nog steeds robuust en volledig afdwingbaar zijn in geval van afwikkeling van de entiteit.	Nee	Nee	Ja, als het incident de afwikkelbaarheid van de entiteit of de groep heeft beïnvloed.	Alfanumeriek

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
4.12. Materialiteits drempel voor het classificatiecriterium “economische effecten”	Gedetailleerde informatie over de drempels die uiteindelijk door het ernstige ICT-gerelateerde incident zijn bereikt met betrekking tot het criterium “economische gevolgen” als bedoeld in de artikelen 7 en 14 van Gedelegeerde Verordening (EU) 2024/1772.	Nee	Nee	Ja	Alfanumeriek
4.13. Bedrag van de bruto directe en indirecte kosten en verliezen	Totaalbedrag van de bruto directe en indirecte kosten en verliezen die de financiële entiteit heeft gemaakt als gevolg van het ernstige ICT-gerelateerde incident, met inbegrip van: a) het bedrag aan onteigende gelden of financiële activa waarvoor de financiële entiteit aansprakelijk is; b) het bedrag van de kosten voor de vervanging of verplaatsing van software, hardware of infrastructuur; c) het bedrag van de personeelskosten, met inbegrip van 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) het bedrag van de vergoedingen wegens niet-naleving van contractuele verplichtingen; e) het bedrag van de kosten voor verhaal en compensatie voor klanten; f) het bedrag van de verliezen als gevolg van gederfde inkomsten; g) het bedrag van de kosten voor interne en externe communicatie; h) het bedrag van de advieskosten, met inbegrip van kosten in verband met juridisch advies, forensische diensten en saneringsdiensten; i) het bedrag van de overige kosten en verliezen, waaronder: i) directe kosten voor de winst-en-verliesrekening, inclusief waardeverminderingen en afwikkelingskosten, en afschrijvingen als gevolg van het ernstige ICT-gerelateerde incident; ii) voorzieningen of reserves die in de winst- en verliesrekening zijn opgenomen tegen waarschijnlijke verliezen in verband met het ernstige ICT-gerelateerde incident;	Nee	Nee	Ja	Monetair

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	iii) te verwachten verliezen, in de vorm van verliezen die voortvloeien uit het ernstige ICT-gerelateerde incident, die tijdelijk op tussenrekeningen of wachtrekeningen worden geboekt en nog niet in de winst-en-verliesrekening worden weerspiegeld, maar die zullen worden opgenomen binnen een termijn die in verhouding staat tot de omvang en de leeftijd van de te verwachten verliespost; iv) materiële gederfde inkomsten in verband met contractuele verplichtingen met derden, inclusief de beslissing om een cliënt na het ernstige ICT-gerelateerde incident niet met een terugbetaling of rechtstreekse betaling schadeloos te stellen maar door een aanpassing van de inkomsten waarbij voor een bepaalde periode in de toekomst geheel of gedeeltelijk wordt afgezien van contractuele vergoedingen; v) timingverliezen, wanneer zij zich uitstrekken over meer dan één boekjaar en aanleiding geven tot juridisch risico. Financiële entiteiten houden bij hun beoordeling rekening met artikel 7, leden 1 en 2, van Gedelegeerde Verordening (EU) 2024/1772. Financiële entiteiten nemen in dit cijfer niet enigerlei financiële terugvordering op. Financiële entiteiten rapporteren het geldbedrag als een positieve waarde. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, houden financiële entiteiten rekening met het totale bedrag van de kosten en verliezen van alle financiële entiteiten. Financiële entiteiten rapporteren het gegevenspunt in eenheden met een nauwkeurigheid die ten minste overeenkomt met duizendtallen.				
4.14. Bedrag van de financiële terugvorderingen	Totaalbedrag van de financiële terugvorderingen. Financiële terugvorderingen hebben betrekking op het oorspronkelijke verlies als gevolg van het incident, ongeacht het moment waarop de financiële terugvorderingen in de vorm van middelen of de instroom van economische voordelen worden ontvangen.	Nee	Nee	Ja	Monetair Financiële entiteiten rapporteren het gegevenspunt in eenheden met een nauwkeurigheid die ten minste overeenkomt met duizendtallen.

Gegevensveld	Omschrijving	Verplicht voor eerste kennisgeving	Verplicht voor tussentijds verslag	Verplicht voor eindverslag	Veldtype
	Financiële entiteiten rapporteren het geldbedrag als een positieve waarde. In het geval van geaggregeerde rapportage als bedoeld in artikel 7 van deze verordening, houden financiële entiteiten rekening met het totale bedrag aan financiële terugvorderingen van alle financiële entiteiten.				
4.15. Informatie over de vraag of de niet-ernstige incidenten al dan niet van terugkerende aard zijn	Informatie over de vraag of meer dan één niet-ernstig ICT-gerelateerd incident zich herhaaldelijk heeft voorgedaan en die incidenten samen worden aangemerkt als een ernstig incident in de zin van artikel 8, lid 2, van Gedelegeerde Verordening (EU) 2024/1772. Financiële entiteiten geven aan of de niet-ernstige ICT-gerelateerde incidenten zich herhaaldelijk hebben voorgedaan en samen als één ernstig ICT-gerelateerd incident worden aangemerkt. Financiële entiteiten vermelden ook het aantal gevallen van deze niet-ernstige ICT-gerelateerde incidenten.	Nee	Nee	Ja, als het grote incident meer dan één niet-ernstig terugkerend incident omvat.	Alfanumeriek
4.16. Datum en tijdstip waarop terugkerende incidenten zich hebben voorgedaan	Wanneer financiële entiteiten terugkerende ICT-gerelateerde incidenten rapporteren, datum en tijdstip waarop het eerste ICT-gerelateerde incident zich heeft voorgedaan.	Nee	Nee	Ja, voor terugkerende incidenten	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)

([1]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-Richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([2]) Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen en tot wijziging van Richtlijn 82/891/EEG van de Raad en de Richtlijnen 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU en 2013/36/EU en de Verordeningen (EU) nr. 1093/2010 en (EU) nr. 648/2012 van het Europees Parlement en de Raad (PB L 173 van 12.6.2014, blz. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Uitvoeringsverordening (EU) 2018/1624 van de Commissie van 23 oktober 2018 tot vaststelling van technische uitvoeringsnormen met betrekking tot procedures, standaardformulieren en templates ten behoeve van de informatieverstrekking voor de opstelling en uitvoering van afwikkelingsplannen voor kredietinstellingen en beleggingsondernemingen overeenkomstig Richtlijn 2014/59/EU van het Europees Parlement en de Raad, en tot intrekking van Uitvoeringsverordening (EU) 2016/1066 van de Commissie (PB L 277 van 7.11.2018, blz. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

BIJLAGE III

MODELLEN VOOR DE KENNISGEVING VAN SIGNIFICANTE CYBERDREIGINGEN

Nummer van het veld	Gegevensveld	
1	Naam van de entiteit die de kennisgeving doet	
2	Identificatiecode van de entiteit die de kennisgeving doet	
3	Soort financiële entiteit die de kennisgeving doet	
4	Naam van de financiële entiteit	
5	LEI-code van de financiële entiteit	
6	Naam van de voornaamste contactpersoon	
7	E-mail: van de voornaamste contactpersoon	
8	Telefoonnummer van de voornaamste contactpersoon	
9	Naam van de tweede contactpersoon	
10	E-mail: van de tweede contactpersoon	
11	Telefoonnummer van de tweede contactpersoon	
12	Datum en tijdstip van detectie van de cyberdreiging	
13	Beschrijving van de significante cyberdreiging	
14	Informatie over de mogelijke gevolgen	
15	Classificatiecriteria voor potentiële incidenten	
16	Status van de cyberdreiging	
17	Genomen maatregelen om te voorkomen dat de dreiging werkelijkheid wordt	
18	Kennisgeving aan andere belanghebbenden	
19	Indicatoren voor aantasting	
20	Andere nuttige informatie	

BIJLAGE IV

GLOSSARIUM VAN GEGEVENS EN INSTRUCTIES VOOR DE KENNISGEVING VAN SIGNIFICANTE CYBERDREIGINGEN

Gegevensveld	Omschrijving	Verplicht veld	Veldtype
1. Naam van de entiteit die de kennisgeving doet	Volledige juridische naam van de entiteit die de kennisgeving doet.	Ja	Alfanumeriek
2. Identificatie code van de entiteit die de kennisgeving doet	Identificatiecode van de entiteit die de kennisgeving doet. Wanneer financiële entiteiten de kennisgeving/het verslag indienen, is de identificatiecode een LEI (Legal Entity Identifier) — een unieke code van twintig alfanumerieke tekens, die op ISO 17442-1:2020 berust. Wanneer een derde aanbieder een verslag indient voor een financiële entiteit, mag deze gebruikmaken van een identificatiecode uit de technische uitvoeringsnormen die zijn vastgesteld op grond van artikel 28, lid 9, van Verordening (EU) 2022/2554.	Ja	Alfanumeriek
3. Soort financiële entiteit die het verslag indient	Soort entiteit als bedoeld in artikel 2, lid 1, punten a) tot en met t), van Verordening (EU) 2022/2554, die het verslag indient.	Ja, als het verslag niet rechtstreeks door de getroffen financiële entiteit wordt verstrekt.	Keuze (meerkeuze): — kredietinstelling; — betalingsinstelling; — vrijgestelde betalingsinstelling; — aanbieder van rekeninginformatiediensten; — instelling voor elektronisch geld; — vrijgestelde instelling voor elektronisch geld; — beleggingsonderneming; — aanbieder van cryptoactivadiensten; — uitgever van activagerelateerde tokens; — centrale effectenbewaarinstelling; — centrale tegenpartij; — handelsplatform; — transactieregister; — beheerder van een alternatieve beleggingsinstelling; — beheermaatschappij; — aanbieder van datarapportagediensten;

Gegevensveld	Omschrijving	Verplicht veld	Veldtype
			— verzekerings- en herverzekeringsonderneming; — verzekeringstussenpersoon, herverzekeringstussenpersoon en nevenverzekeringstussenpersoon; — instelling voor bedrijfspensioenvoorziening; — ratingbureau; — beheerder van kritieke benchmarks; — aanbieder van crowdfundingdiensten; — securitisatieregister.
4. Naam van de financiële entiteit	Volledige juridische naam van de financiële entiteit die kennisgeving doet van de significante cyberdreiging.	Ja, als de financiële entiteit een andere is dan de entiteit die de kennisgeving doet.	Alfanumeriek
5. LEI-code van de financiële entiteit	Identificatiecode (LEI) van de financiële entiteit die van de significante cyberdreiging kennisgeving doet, zoals toegewezen overeenkomstig de regels van de Internationale Organisatie voor Normalisatie.	Ja, als de financiële entiteit die van de significante cyberdreiging kennisgeving doet, verschilt van de entiteit die het verslag indient	Unieke code van 20 alfanumerieke tekens, gebaseerd op ISO 17442-1:2020
6. Naam van de voornaamste contactpersoon	Voor- en achternaam van de voornaamste contactpersoon van de financiële entiteit.	Ja	Alfanumeriek
7. E-mail: van de voornaamste contactpersoon	E-mailadres van de voornaamste contactpersoon dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie.	Ja	Alfanumeriek
8. Telefoon nummer van de voornaamste contactpersoon	Het telefoonnummer van de voornaamste contactpersoon dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie. Het telefoonnummer moet met alle internationale kengetallen (bv. +33 XXXXXXXXX) worden opgegeven.	Ja	Alfanumeriek
9. Naam van de tweede contactpersoon	Voor- en achternaam van de tweede contactpersoon van de financiële entiteit of een entiteit die de kennisgeving namens de financiële entiteit doet, indien beschikbaar.	Ja, als de voor- en achternaam van de tweede contactpersoon van de financiële entiteit of een entiteit die de kennisgeving voor de financiële entiteit doet, beschikbaar is.	Alfanumeriek

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Gegevensveld	Omschrijving	Verplicht veld	Veldtype
10. E-mail: van de tweede contactpersoon	E-mailadres van de tweede contactpersoon of een functioneel e-mailadres van het team dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie, indien beschikbaar.	Ja, als het e-mailadres van de tweede contactpersoon of een functioneel e-mailadres van het team dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie, beschikbaar is.	Alfanumeriek
11. Telefoon nummer van de tweede contactpersoon	Het telefoonnummer van de tweede contactpersoon dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie, indien beschikbaar. Het telefoonnummer moet met alle internationale kengetallen (bv. +33 XXXXXXXXX) worden opgegeven.	Ja, als het telefoonnummer van de tweede contactpersoon dat door de bevoegde autoriteit kan worden gebruikt voor follow-upcommunicatie, beschikbaar is.	Alfanumeriek
12. Datum en tijdstip van detectie van de cyberdreiging	Datum en tijdstip waarop de financiële entiteit zich bewust is geworden van de significante cyberdreiging.	Ja	Standaard-UTC volgens ISO 8601 (JJJJ-MM-DD Tuu: mm:ss)
13. Beschrijving van de significante cyberdreiging	Beschrijving van de meest relevante aspecten van de significante cyberdreiging. Financiële entiteiten verstrekken: a) een overzicht op hoog niveau van de meest relevante aspecten van de significante cyberdreiging; b) de daaraan verbonden risico's die eruit voortvloeien, met inbegrip van potentiële kwetsbaarheden van de systemen van de financiële entiteit die kunnen worden geëxploiteerd; c) informatie over de kans dat de significante cyberdreiging werkelijkheid wordt, en d) informatie over de bron van de informatie over de cyberdreiging.	Ja	Alfanumeriek
14. Informatie over de mogelijke gevolgen	Informatie over de mogelijke gevolgen van de cyberdreiging voor de financiële entiteit, haar cliënten of financiële tegenpartijen indien de cyberdreiging werkelijkheid wordt	Ja	Alfanumeriek
15. Classificatie criteria voor potentiële incidenten	De classificatiecriteria die aanleiding hadden kunnen geven tot de rapportage van een ernstig incident indien de cyberdreiging werkelijkheid was geworden.	Ja	Keuze (meervoudig): — getroffen cliënten, financiële tegenpartijen en transacties; — reputatieschade; — duur en uitvaltijd van de dienst; — geografische spreiding; — gegevensverliezen; — getroffen kritieke diensten; — economische effecten.

Gegevensveld		Omschrijving	Verplicht veld	Veldtype
16.	Status van de cyberdreiging	Informatie over de status van de cyberdreiging voor de financiële entiteit en over de vraag of de dreigingsactiviteit is gewijzigd. Wanneer de cyberdreiging niet langer communiceert met de informatiesystemen van de financiële entiteit, kan de status als inactief worden aangemerkt. Indien de financiële entiteit over informatie beschikt dat de dreiging actief blijft ten aanzien van andere partijen of het financiële stelsel als geheel, wordt de status als actief aangemerkt.	Ja	Keuze: — actief — inactief
17.	Genomen maatregelen om te voorkomen dat de dreiging werkelijkheid wordt	Informatie op hoog niveau over de maatregelen die de financiële entiteit heeft genomen om te voorkomen dat de significante cyberdreigingen werkelijkheid worden, indien van toepassing.	Ja	Alfanumeriek
18.	Kennisgeving aananderebelanghebbenden	Informatie over de kennisgeving van de cyberdreiging aan andere financiële entiteiten of autoriteiten.	Ja, als andere financiële entiteiten of autoriteiten in kennis zijn gesteld van de cyberdreiging.	Alfanumeriek
19.	Indicatoren voor aantasting	Informatie over de significante dreiging die kan helpen kwaadwillige activiteiten binnen een netwerk- of informatiesysteem (indicatoren voor aantasting) te identificeren, indien van toepassing. De door de financiële entiteit verstrekte indicatoren voor aantasting omvatten, maar zijn niet beperkt tot, de volgende categorieën gegevens: a) IP-adressen; b) URL-adressen; c) domeinen; d) bestandshashes; e) malwaregegevens (malwarenaam, -bestandsnamen en de locaties ervan, specifieke registratiesleutels in verband met malwareactiviteit); f) gegevens over netwerkactiviteiten (poorten, protocollen, adressen, referrers, gebruikersagenten, headers, specifieke logbestanden of onderscheidende patronen in het netwerkverkeer); g) gegevens van e-mailberichten (afzender, ontvanger, onderwerp, header, inhoud); h) DNS-verzoeken en registerconfiguraties; i) activiteiten op het gebied van gebruikersaccounts (logins, activiteit op de account van geprivilegieerde gebruikers, privilege-escalatie); j) databankverkeer (lezen/schrijven), verzoeken aan hetzelfde bestand. Het kan gaan om gegevens over indicatoren voor patronen in het netwerkverkeer die passen bij bekende aanvallen/botnetcommunicatie, IP-adressen van machines die besmet zijn met malware (bots), gegevens over door malware gebruikte "bedienings- en besturingsservers" (gewoonlijk domeinen of IP-adressen) en URL's van phishingsites of websites die malware hosten of kits exploiteren.	Ja, als er informatie beschikbaar is over indicatoren voor aantasting in verband met de cyberdreiging.	Alfanumeriek
20.	Andere nuttige informatie	Alle andere relevante informatie over de significante cyberdreiging	Ja, indien van toepassing en indien er andere informatie beschikbaar is, die niet onder het model valt.	Alfanumeriek