JC 2024 34

5 juni 2024

Gemeenschappelijke richtsnoeren

voor de raming van de geaggregeerde jaarlijkse kosten en verliezen als gevolg van ernstige ICT-gerelateerde incidenten krachtens Verordening (EU) 2022/2554

Deze richtsnoeren bevatten verwijzingen naar gedelegeerde verordeningen en uitvoeringsverordeningen van de Europese Commissie die nog niet in het Publicatieblad van de EU zijn bekendgemaakt. Zodra deze toekomstige verordeningen in het Publicatieblad zijn bekendgemaakt, zullen deze richtsnoeren worden voltooid door deze verwijzingen erin op te nemen. De verwijzingen zullen worden opgenomen in de geel gemarkeerde delen.

De datum van toepassing van deze richtsnoeren kan pas worden vastgesteld wanneer deze richtsnoeren definitief zijn. De verwachte datum van toepassing van deze richtsnoeren is 17 januari 2025. Indien de definitieve versie van deze richtsnoeren vertraging oploopt, worden deze richtsnoeren uiterlijk twee maanden na de datum van publicatie van de vertaling van deze richtsnoeren in alle officiële EU-talen van toepassing.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Gemeenschappelijke richtsnoeren voor de raming van de geaggregeerde jaarlijkse kosten en verliezen als gevolg van ernstige ICT-gerelateerde incidenten

Status van deze gemeenschappelijke richtsnoeren

Dit document bevat gezamenlijke richtsnoeren die zijn uitgevaardigd krachtens artikel 16 van Verordening (EU) nr. 1093/2010[1]; artikel 16 van Verordening (EU) nr. 1094/2010[2]; en artikel 16 van Verordening (EU) nr. 1095/2010[3] – de zogeheten "ETA-verordeningen". Overeenkomstig artikel 16, lid 3, van de respectieve ETA-verordeningen moeten bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan de richtsnoeren te voldoen.

De gezamenlijke richtsnoeren beschrijven de visie van de ETA's op passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht of op de wijze waarop het recht van de Unie op een bepaald gebied moet worden toegepast. Bevoegde autoriteiten waarop de gemeenschappelijke richtsnoeren van toepassing zijn, dienen hieraan te voldoen door ze op passende wijze in hun toezichtpraktijken te integreren (bijvoorbeeld door hun wettelijk kader of hun toezichtprocessen aan te passen), ook wanneer de gemeenschappelijke richtsnoeren primair tot instellingen zijn gericht.

Rapportagevereisten

Overeenkomstig artikel 16, lid 3, van de ETA-verordeningen moeten de bevoegde autoriteiten uiterlijk 19.05.2025 (twee maanden na uitvaardiging) aan de respectieve ETA's meedelen of zij aan deze gezamenlijke richtsnoeren/aanbevelingen voldoen of voornemens zijn deze op te volgen, dan wel de redenen voor niet-naleving opgeven. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet aan de richtsnoeren te hebben voldaan. Kennisgevingen dienen te worden gestuurd naar compliance@eba.europa.eu, compliance@eiopa.europa.eu en DORA@esma.europa.eu met het kenmerk "JC/GL/2024/34". Een model voor kennisgevingen is beschikbaar op de websites van de ETA's. Kennisgevingen dienen te worden ingezonden door personen die gemachtigd zijn om namens hun bevoegde autoriteit mee te delen of deze al dan niet aan de richtsnoeren voldoet.

[1] 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)

[2] 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. 48-83*)

[3] 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. 84-119)

Kennisgevingen worden overeenkomstig artikel 16, lid 3, van de ETA-verordeningen op hun websites bekendgemaakt.

Titel I – Onderwerp, toepassingsgebied, adressaten en definities

Onderwerp en toepassingsgebied

1. Deze richtsnoeren zijn gericht op het vervullen van het mandaat dat aan de ETA's is gegeven op grond van artikel 11, lid 11, van Verordening (EU) 2022/2554 [4], om gemeenschappelijke richtsnoeren te ontwikkelen voor de raming van de geaggregeerde jaarlijkse kosten en verliezen van ernstige ICT-gerelateerde incidenten als bedoeld in artikel 11, lid 10, van die verordening. Deze richtlijnen specificeren eveneens een gemeenschappelijk model voor de indiening van de geaggregeerde jaarlijkse kosten en verliezen.

Adressaten

2. Deze richtsnoeren zijn gericht tot bevoegde autoriteiten als omschreven in artikel 46 van Verordening 2022/2554 en tot financiële instellingen als omschreven in artikel 4, lid 1, van Verordening (EU) 1093/2010, artikel 4, lid 1, van Verordening (EU) 1094/2010 en artikel 4, lid 1, van Verordening (EU) 1095/2010.

Definities

3. De termen die in Verordening (EU) 2022/2554 worden gebruikt en gedefinieerd, hebben in deze richtsnoeren dezelfde betekenis.

Titel II – Tenuitvoerlegging

Toepassingsdatum

4. Deze richtsnoeren zijn van toepassing met ingang van 19.05.2025.

[4] 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 *(PB L 333 van 27.12.2022, blz. 1-79)*

Titel III – Bepalingen voor de raming van de geaggregeerde jaarlijkse kosten en verliezen van ernstige ICT-gerelateerde incidenten

5. Financiële entiteiten dienen de geaggregeerde jaarlijkse kosten en verliezen van ernstige ICT-gerelateerde incidenten te ramen door de kosten en verliezen voor grote ICT-gerelateerde incidenten die binnen het referentiejaar vallen waarvoor de bevoegde autoriteit de raming heeft gevraagd, samen te voegen. De financiële entiteit kan kiezen of het referentiejaar dient overeen te stemmen met hetzij het voltooide kalenderjaar, hetzij het voltooide boekjaar waarvoor de financiële entiteit haar jaarrekening heeft afgesloten. Zodra een financiële entiteit heeft besloten of zij de raming zal verstrekken op basis van het kalenderjaar dan wel het boekjaar, dient dit besluit te worden toegepast op toekomstige ramingen van de geaggregeerde jaarlijkse kosten en verliezen. De financiële entiteit kan dat besluit wijzigen door de bevoegde autoriteit daarvan in kennis te stellen, mits de bevoegde autoriteit niet binnen twee maanden na ontvangst van de kennisgeving bezwaar maakt. Financiële entiteiten mogen geen kosten en verliezen opnemen in verband met incidenten die vóór of na dat referentiejaar plaatsvinden.

6. Financiële entiteiten moeten in de raming alle ICT-gerelateerde incidenten opnemen die, ongeacht de reden, als ernstig zijn geclassificeerd overeenkomstig Gedelegeerde Verordening [OJ L, 2024/1772, 25.6.2024][5] van de Commissie betreffende de classificatie van incidenten, en

   (a) waarvoor de financiële entiteit overeenkomstig artikel 19, lid 4, punt c), van Verordening (EU) 2022/2554 in het desbetreffende referentiejaar een eindverslag heeft ingediend, of

   (b) elk incident waarvoor de financiële entiteit in voorgaande referentiejaren overeenkomstig artikel 19, lid 4, punt c), van Verordening (EU) 2022/2554 een eindverslag heeft ingediend dat een kwantificeerbare financiële impact had op de financiële entiteit in het desbetreffende referentiejaar.

7. Financiële entiteiten dienen de geaggregeerde jaarlijkse kosten en verliezen te ramen door de volgende sequentiële stappen toe te passen:

   (a) afzonderlijke raming van de kosten en verliezen van elk ernstig ICT-gerelateerd incident als bedoeld in punt 6. Die ramingen dienen de brutokosten en -verliezen op te leveren, rekening houdend met de soorten kosten en verliezen als bedoeld in artikel 7, leden 1 en 2, van Gedelegeerde Verordening [OJ L, 2024/1772, 25.6.2024] van de Commissie;

[5] 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, [*OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj*]

(b) voor elk ernstig ICT-gerelateerd incident moeten financiële entiteiten ook een raming maken van de financiële terugvorderingen zoals gespecificeerd in bijlage II bij Uitvoeringsverordening [OJ L, 2025/302, 20.2.2025][6] van de Commissie;

(c) financiële entiteiten dienen de brutokosten en verliezen en de financiële terugvorderingen bij ernstige ICT-gerelateerde incidenten samen te voegen.

8. Als basis voor de ramingen dienen financiële entiteiten te verwijzen naar de kosten, verliezen en financiële terugvorderingen die zijn weergegeven in hun financiële overzichten zoals de winst- en verliesrekening, of indien van toepassing in hun toezichtrapportage, van het relevante referentiejaar. In hun raming dienen financiële entiteiten ook rekening te houden met boekhoudkundige voorzieningen die tot uitdrukking komen in hun financiële overzichten, zoals de winst- en verliesrekening van het betreffende referentiejaar. Als er geen nauwkeurige gegevens beschikbaar zijn, dienen financiële entiteiten hun raming zoveel mogelijk te baseren op andere beschikbare gegevens en informatie.

9. Financiële entiteiten dienen aanpassingen van de kosten en verliezen van een raming die zij voor een eerder jaar hebben ingediend op te nemen in de raming van het desbetreffende referentiejaar waarin de aanpassingen worden gedaan.

10. Financiële entiteiten dienen in het verslag van hun raming van de geaggregeerde jaarlijkse kosten en verliezen ook de uitsplitsing van brutokosten en verliezen en van financiële terugvorderingen op te nemen voor elk belangrijk ICT-gerelateerd incident dat in de samenvoeging is opgenomen.

11. Financiële entiteiten dienen de template in de bijlage te gebruiken om de raming van hun geaggregeerde jaarlijkse kosten en verliezen voor het referentiejaar bij de bevoegde autoriteit in te dienen. Voor elk item onder de punten 6 en 9 dat is opgenomen in de raming van het referentiejaar, dienen financiële entiteiten dezelfde door de financiële entiteit verstrekte referentiecodes voor incidenten te gebruiken als die welke zijn gebruikt in het eindverslag overeenkomstig artikel 19, lid 4, punt c), van Verordening (EU) 2022/2554.

[6] 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, [*OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj*]

Bijlage: Rapportagemodel voor brutokosten en -verliezen en financiële terugvorderingen in een referentiejaar

Naam van de financiële entiteit	
LEI-code	
Start- en einddatum van het referentiejaar van de financiële entiteit	
Valuta	

Aantal incidenten	Datum van indiening van het definitieve incidentenverslag	Referentienummer van het incident	Brutokosten en -verliezen van het incident in het referentiejaar (1 000 EUR)	Terugvorderingen van het incident in het referentiejaar (1 000 EUR)
1				
2				
…				
Totaal voor het referentiejaar	----------	----------		