JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 34

5 juni 2024

Gemensamma riktlinjer

för uppskattning av totala årliga kostnader och förluster orsakade av allvarliga IKT-relaterade incidenter enligt förordning (EU) 2022/2554

Dessa riktlinjer innehåller hänvisningar till EU-kommissionens delegerade förordningar och genomförandeförordningar som ännu inte har offentliggjorts i Europeiska unionens officiella tidning. Så snart dessa kommande förordningar har offentliggjorts i Europeiska unionens officiella tidning kommer dessa riktlinjer att färdigställas genom att hänvisningarna uppdateras. Hänvisningarna kommer att införas i de gulmarkerade avsnitten.

Datum för ikraftträdande av dessa riktlinjer kan fastställas först när riktlinjerna har färdigställts. Det preliminära datumet för ikraftträdande av dessa riktlinjer är den 17 januari 2025. Om färdigställandet av dessa riktlinjer skulle försenas kommer den senaste dagen för ikraftträdande av dessa riktlinjer att vara den dag som infaller två månader efter offentliggörandet av översättningarna av dessa riktlinjer på alla officiella EU-språk.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Gemensamma riktlinjer för uppskattning av totala årliga kostnader och förluster orsakade av allvarliga IKT-relaterade incidenter

Status för dessa gemensamma riktlinjer

Detta dokument innehåller gemensamma riktlinjer som utfärdats i enlighet med artikel 16 i förordning (EU) nr 1093/2010 [1], artikel 16 i förordning (EU) nr 1094/2010 [2] och artikel 16 i förordning (EU) nr 1095/2010[3], nedan kallade *ESA-förordningarna*. I enlighet med artikel 16.3 i ESA-förordningarna ska behöriga myndigheter och finansinstitut med alla tillgängliga medel söka följa dessa riktlinjer.

I de gemensamma riktlinjerna beskrivs de europeiska tillsynsmyndigheternas syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen bör tillämpas inom ett särskilt område. De behöriga myndigheter som berörs av de gemensamma riktlinjerna bör följa dem genom att på lämpligt sätt införliva dem i sin tillsynspraxis (t.ex. genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när de gemensamma riktlinjerna i första hand är riktade till institut.

Rapporteringskrav

I enlighet med artikel 16.3 i ESA-förordningarna måste de behöriga myndigheterna meddela respektive europeisk tillsynsmyndighet om de följer eller avser att följa dessa gemensamma riktlinjer/rekommendationer, eller i annat fall ange skälen till att de inte följer dem, senast den 19.05.2025 (två månader efter utfärdandet av riktlinjerna). Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer respektive europeisk tillsynsmyndighet att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningarna ska skickas till compliance@eba.europa.eu, compliance@eiopa.europa.eu och DORA@esma.europa.eu med hänvisningen ”JC/GL/2024/34”. En mall för anmälan finns på de europeiska tillsynsmyndigheternas webbplatser. Anmälningarna bör lämnas av personer med befogenhet att på sina behöriga myndigheters vägnar rapportera om hur reglerna tillämpas.

[1] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

[2] Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten) och om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (*EUT L 331, 15.12.2010, s. 48–83*).

[3] Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84–119).

Anmälningarna kommer att offentliggöras på de europeiska tillsynsmyndigheternas webbplatser i enlighet med artikel 16.3.

Avdelning I – Syfte, tillämpningsområde, mottagare och definitioner

Syfte och tillämpningsområde

1. Dessa riktlinjer syftar till att fullgöra det mandat som tilldelats de europeiska tillsynsmyndigheterna (ESA) enligt artikel 11.11 i förordning (EU) 2022/2554[4], det vill säga att utarbeta gemensamma riktlinjer för uppskattning av totala årliga kostnader och förluster som orsakas av allvarliga IKT-relaterade incidenter, i enligt artikel 11.10 i den förordningen. I dessa riktlinjer ingår också en gemensam mall för inlämning av totala årliga kostnader och förluster.

Mottagare

2. Dessa riktlinjer gäller för behöriga myndigheter enligt definitionen i artikel 46 i förordning 2022/2554 och finansinstitut enligt definitionen i artikel 4.1 i förordning (EU 1093/2010), artikel 4.1 i förordning (EU) 1094/2010 och artikel 4.1 i förordning (EU) 1095/2010.

Definitioner

3. De termer som används och definieras i förordning (EU) 2022/2554 har samma betydelse i dessa riktlinjer.

Avdelning II – Genomförande

Datum för tillämpning

4. Dessa riktlinjer börjar gälla den 19.05.2025.

[4] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 *(EUT L 333, 27.12.2022, s. 1–79)*.

Avdelning III – Regler för uppskattningen av totala årliga kostnader och förluster orsakade av allvarliga IKT-relaterade incidenter

5. Finansiella entiteter bör uppskatta de totala årliga kostnader och förluster som orsakas av allvarliga IKT-relaterade incidenter genom att aggregera de kostnader och förluster för allvarliga IKT-relaterade incidenter som bokförts under det referensår för vilket den behöriga myndigheten begärt uppskattningen. Den finansiella entiteten kan välja om referensåret ska motsvara det avslutade kalenderåret eller det avslutade räkenskapsåret för vilket den finansiella entiteten har färdigställt sina räkenskaper. När en finansiell entitet har beslutat huruvida den ska tillhandahålla uppskattningen baserat på kalenderåret eller räkenskapsåret bör det valda alternativet tillämpas även på framtida uppskattningar av totala årliga kostnader och förluster. Under förutsättning att den finansiella entiteten underrättar den behöriga myndigheten och att myndigheten inte gör några invändningar inom två månader efter mottagandet av underrättelsen har den finansiella entiteten möjlighet att ändra den typ av referensår som ska tillämpas. Finansiella entiteter bör inte inkludera kostnader och förluster orsakade av incidenter som infaller före eller efter det valda referensåret.

6. I uppskattningen bör de finansiella entiteterna inkludera alla IKT-relaterade incidenter som, oavsett orsak, klassificerades som allvarliga i enlighet med kommissionens delegerade förordning [OJ L, 2024/1772, 25.6.2024][5] om incidentklassificering och

   (a) för vilka den finansiella entiteten har lämnat in en slutrapport i enlighet med artikel 19.4 c i förordning (EU) 2022/2554 under det relevanta referensåret, eller

   (b) alla incidenter för vilka den finansiella entiteten under tidigare referensår har lämnat in en slutrapport i enlighet med artikel 19.4 c i förordning (EU) 2022/2554 och som hade en kvantifierbar ekonomisk inverkan på den finansiella entiteten under det relevanta referensåret.

7. Finansiella entiteter bör uppskatta de totala årliga kostnaderna och förlusterna genom att tillämpa dessa på varandra efterföljande steg:

   (a) Uppskatta kostnaderna och förlusterna för varje enskild allvarlig IKT-relaterad incident i enlighet med punkt 6. Dessa uppskattningar bör resultera i bruttokostnader och förluster med beaktande av de typer av kostnader och förluster som anges i artikel 7.1 och 7.2 i kommissionens delegerade förordning [OJ L, 2024/1772, 25.6.2024].

[5]Kommissionens delegerade förordning (EU) 2024/1772 av den 13 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar kriterierna för klassificering av IKT-relaterade incidenter och cyberhot, fastställande av väsentlighetströsklar och närmare uppgifter om rapporter om allvarliga incidenter, [*OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj*]

(b) För varje allvarlig IKT-relaterad incident bör de finansiella entiteterna också uppskatta återbetalningarnas storlek i enlighet med bilaga II till kommissionens genomförandeförordning [OJ L, 2025/302, 20.2.2025][6].

(c) De finansiella entiteterna bör aggregera bruttokostnaderna, förlusterna och de återbetalningar som härrör från allvarliga IKT-relaterade incidenter.

8. Som grund för uppskattningarna bör de finansiella entiteterna använda de kostnader, förluster och återbetalningar som anges i deras redovisning, exempelvis i resultaträkningen, eller i tillämpliga fall i deras tillsynsrapportering, för det relevanta referensåret. I uppskattningarna bör de finansiella entiteterna även ta hänsyn till de bokföringsmässiga avsättningar som förekommer i redovisningen för det relevanta referensåret, exempelvis i resultaträkningen. Om det saknas tillförlitliga uppgifter bör de finansiella entiteterna i den mån det är möjligt basera sin uppskattning på andra tillgängliga uppgifter.

9. Finansiella entiteter bör inkludera justeringar av kostnader och förluster för uppskattningar som de har lämnat in för ett tidigare år i uppskattningen av det relevanta referensår under vilket justeringarna görs.

10. I rapporten med uppskattningen av de totala årliga kostnaderna och förlusterna bör de finansiella entiteterna även ange hur bruttokostnader, förluster och återbetalningar fördelas per allvarlig IKT-relaterad incident som ingår i de aggregerade uppgifterna.

11. För att lämna in uppskattningen av de totala årliga kostnaderna och förlusterna för referensåret till den behöriga myndigheten bör finansiella entiteter använda mallen i bilagan. För varje post under punkterna 6 och 9 som ingår i uppskattningen för referensåret bör den finansiella entiteten använda samma incidensreferenskoder som de som används i slutrapporten i enlighet med artikel 19.4 c i förordning (EU) 2022/2554.

[6] Kommissionens genomförandeförordning (EU) 2025/302 av den 23 oktober 2024 om fastställande av tekniska genomförandestandarder för tillämpningen av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller standardformulär, mallar och förfaranden för att finansiella entiteter ska kunna rapportera allvarliga IKT-relaterade incidenter och anmäla betydande cyberhot, [*OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj*]

Bilaga: Rapporteringsmall för bruttokostnader, förluster och återbetalningar under ett referensår

Namn på den finansiella entiteten	
LEI-nummer (identifieringskod för juridisk person)	
Start- och slutdatum för den finansiella entitetens referensår	
Valuta	

Incidentens nummer	Datum för inlämnande av incidentslutrapporten	Incidentens referensnummer	Bruttokostnader och förluster för incidenten under referensåret (enhet, tusental)	Återbetalningar som härrör från incidenten under referensåret (enhet, tusental)
1				
2				
…				
Totalt för referensåret	----------	----------		