

JC 2024 34

5 June 2024

Joint Guidelines

On the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554

These Guidelines contain references to EU Commission delegated and implementing regulations that have not yet been published in the EU Official Journal. Once these forthcoming Regulations will have been published in the Official Journal, these Guidelines will be finalised by including these references. The references will be inserted in the sections highlighted in yellow.

The date of application of these Guidelines can only be determined once these Guidelines are finalised. The expected date of application of these Guidelines is 17 January 2025. In case there is a delay in finalising these Guidelines, the latest day of application of these Guidelines will be two months following the date of the publication of the translations of these Guidelines in all official EU languages.

Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

Status of these Joint Guidelines

This document contains Joint Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010¹; Article 16 of Regulation (EU) No 1094/2010²; and Article 16 of Regulation (EU) No 1095/2010³ - ‘the ESAs’ Regulations’. In accordance with Article 16(3) of the respective ESAs’ Regulations, competent authorities and financial institutions must make every effort to comply with the Guidelines.

Joint Guidelines set out the ESAs’ view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities to whom the Joint Guidelines apply should comply by incorporating them into their supervisory practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where the Joint Guidelines are directed primarily at institutions.

Reporting Requirements

In accordance with Article 16(3) of the ESAs’ Regulations, competent authorities must notify the respective ESA whether they comply or intend to comply with these Joint Guidelines/Recommendations, or otherwise with reasons for non-compliance, by 19.05.2025 (two months after issuance). In the absence of any notification by this deadline, competent authorities will be considered by the respective ESA to be non-compliant. Notifications should be sent to compliance@eba.europa.eu, compliance@eiopa.europa.eu and DORA@esma.europa.eu with the reference ‘JC/GL/2024/34’. A template for notifications is available on the ESAs’ websites. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities.

Notifications will be published on the ESAs’ websites, in line with Article 16(3).

¹ Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12)

² Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC, (OJ L 331, 15.12.2010, p. 48–83)

³ Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC, (OJ L 331, 15.12.2010, p. 84–119)

Title I - Subject matter, scope, addressees, and definitions

Subject matter and Scope of application

1. These guidelines are aimed at fulfilling the mandate given to the ESAs under Article 11(11) of Regulation (EU) 2022/2554⁴, to develop common guidelines on the estimation of aggregated annual costs and losses of major ICT-related incidents referred to Article 11(10) of that Regulation. These guidelines also specify a common template for the submission of the aggregated annual costs and losses.

Addressees

2. These guidelines are addressed to competent authorities as defined in Article 46 of Regulation 2022/2554 and to financial institutions as defined in Article 4(1) of Regulation (EU) 1093/2010, Article 4(1) of Regulation (EU) 1094/2010 and Article 4(1) of Regulation (EU) 1095/2010 .

Definitions

3. Terms used and defined in Regulation (EU) 2022/2554 have the same meaning in these guidelines.

Title II- Implementation

Date of application

4. These Guidelines apply from 19.05.2025.

⁴ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, (OJ L 333, 27.12.2022, p. 1–79)

Title III- Provisions on the estimation of aggregated annual costs and losses of major ICT-related incidents

5. Financial entities should estimate the aggregate annual costs and losses of major ICT-related incidents by aggregating the costs and losses for major ICT-related incidents that fall within the reference year for which the competent authority requested the estimation. The financial entity may choose whether the reference year should correspond to either the completed calendar year, or to the completed accounting year of the financial entity for which the financial entity has finalised its financial statements. Once a financial entity has decided whether it will provide the estimation based on the calendar year or its accounting year, such a decision should be applied to future estimations of aggregated annual costs and losses. The financial entity may change that decision by notifying the competent authority, and provided that the competent authority does not object within two months of receiving the notification. Financial entities should not include costs and losses related to those incidents that fall before or after that reference year.

6. Financial entities should include in the estimation all ICT-related incidents that, irrespective of the reason, were classified as major in accordance with Commission Delegated Regulation [OJ L, 2024/1772, 25.6.2024]⁵ on incident classification and
 - (a) for which the financial entity has submitted a final report in accordance with Article 19(4)(c) Regulation (EU) 2022/2554 in the relevant reference year, or
 - (b) any incident for which the financial entity submitted in previous reference years a final report in accordance with Article 19(4)(c) of Regulation (EU) 2022/2554 that had a quantifiable financial impact on the financial entity in the relevant reference year.

7. Financial entities should estimate the aggregated annual costs and losses by applying the follow sequential steps:
 - (a) estimate the costs and losses of each major ICT-related incident as referred to in paragraph 6 individually. Those estimations should produce the gross costs and losses taking into account the types of costs and losses as set out in Article 7(1) and (2) of the Commission Delegated Regulation [OJ L, 2024/1772, 25.6.2024];
 - (b) for each major ICT-related incident, financial entities should also estimate the financial recoveries as specified in Annex II to Commission Implementing Regulation [OJ L, 2025/302, 20.2.2025]⁶;

⁵Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents [OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/req_del/2024/1772/oj]

⁶ Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat [OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/req_impl/2025/302/oj]

- (c) financial entities should aggregate the gross costs and losses and the financial recoveries across major ICT-related incidents.
8. As basis for the estimations, financial entities should refer to the costs, losses and financial recoveries that are reflected in their financial statements such as the profit and loss account, or where applicable in their supervisory reporting, of the relevant reference year. In their estimation, financial entities should also include accounting provisions that are reflected in their financial statements such as the profit and loss account of the relevant reference year. Where accurate data is not available, financial entities should base their estimation on other available data and information to the extent possible.
 9. Financial entities should include adjustments on the costs and losses of an estimation that it submitted for a previous year in the estimation of the relevant reference year in which the adjustments are made.
 10. Financial entities should include in the report of their estimation of the aggregated annual costs and losses also the breakdown of gross costs and losses and of financial recoveries for each major ICT-related incident that were included in the aggregation.
 11. Financial entities should use the template in the Annex to submit to the competent authority the estimation of their aggregated annual costs and losses for the reference year. For each item under paragraph 6 and 9 that is included in the estimation of the reference year, financial entities should use the same incident reference codes provided by the financial entity as the ones used in the final report in accordance with Article 19(4)(c) of Regulation (EU) 2022/2554.



Annex: Reporting template for gross costs and losses and financial recoveries in a reference year

Name of the financial entity				
Legal Entity Identifier				
Start and end date of the reference year of the financial entity				
Currency				
Number of incident	Date of the submission of the final incident report	Incident reference number	Gross costs and losses of the incident in the reference year (1000s of units)	Recoveries of the incident in the reference year (1000s of units)
1				
2				
...				
Total for reference year	-----	-----		