cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 25/892

Application of the Joint ESA Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554 (JC 2024 34)

Circular CSSF 25/892

Application of the Joint ESA Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554 (JC 2024 34)

To all financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of Regulation (EU) 2022/2554[1] on digital operational resilience for the financial sector (hereafter "DORA")

Luxembourg, 27 May 2025

Ladies and Gentlemen,

The purpose of this circular is to inform you that the CSSF, in its capacity as competent authority, applies the Joint Guidelines of the European Supervisory Authorities (ESAs) on the estimation of aggregated annual costs and losses caused by major ICT-related incidents referred to in Article 11(11) of DORA (i.e. JC/GL/2024/34; hereafter the "Guidelines").

This circular is divided into three chapters:

- Chapter 1 defines the scope of application;
- Chapter 2 clarifies the reporting obligation to the CSSF;
- Chapter 3 provides for the entry into force of this circular.

The guidelines are attached as an annex to this circular.

[1] 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

Chapter 1: Scope of application

1. The following entities, other than microenterprises as defined in Article 3(60) of DORA[2], are to be considered as financial entities in the framework of this circular:

   a) credit institutions, investment firms, market operators operating a trading venue and approved publication arrangements (APAs) with a derogation and authorised reporting mechanisms (ARMs) with a derogation within the meaning of the Law of 5 April 1993 on the financial sector (LFS);
   b) payment institutions, account information service providers and electronic money institutions within the meaning of the Law of 10 November 2009 on payment services (LPS);
   c) crypto-asset service providers and issuers of asset-referenced tokens within the meaning of Regulation (EU) 2023/1114;
   d) central securities depositories within the meaning of the Law of 6 June 2018 on central securities depositories (CSD Law);
   e) central counterparties within the meaning of the Law of 15 March 2016 on OTC derivatives, central counterparties and trade repositories;
   f) management companies incorporated under Luxembourg law and subject to Chapter 15 or Article 125-2 of Chapter 16, and Luxembourg branches of investment fund managers subject to Chapter 17, and investment companies which did not designate a management company within the meaning of Article 27 of the Law of 17 December 2010 relating to undertakings for collective investment;
   g) alternative investment fund managers authorised under Chapter 2 and internally managed alternative investment funds within the meaning of point (b) of Article 4(1) of the Law of 12 July 2013 on alternative investment fund managers (AIFM Law);
   h) institutions for occupational retirement provisions authorised in accordance with Article 2(2) of the Law of 13 July 2005 on institutions for occupational retirement provision in the form of pension savings companies with variable capital (SEPCAVs) and pension savings associations (ASSEPs);
   i) administrators of critical benchmarks within the meaning of point (b) of Article 20(1) of Regulation (EU) 2016/1011;
   j) crowdfunding service providers within the meaning of the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services;

2. Branches in Luxembourg of the financial entities that are part of a legal entity whose head office is located in a different Member State of the European Union (EU branches) are expected to report their estimations under DORA to the competent authority of that Member State (home Member State) upon its request and are therefore excluded from the scope of this circular.

[2] 'microenterprise' means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million.

Chapter 2: Reporting obligation to the CSSF

3. As required in Article 11(10) of DORA, financial entities shall, upon request, make available to the CSSF an estimation of aggregated annual costs and losses of major ICT-related incidents.
4. The CSSF, in its capacity as competent authority, applies in full the Guidelines and integrates them into its administrative practice and regulatory approach with a view to promoting supervisory convergence in this field at European level.
5. The estimation referred to in paragraph 3 above shall be done in line with the Guidelines and submitted by using the "reporting template for gross costs and losses and financial recoveries in the reference year" as defined in the Annex I of the Guidelines.

Chapter 3: Date of application

6. This circular shall apply as from 31 May 2025.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex Joint Guidelines of the European Supervisory Authorities (ESAs) on the estimation of aggregated annual costs and losses caused by major ICT-related incidents referred to in Article 11(11) of DORA (JC/GL/2024/34).

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 34

5 June 2024

Final Report

Joint Guidelines

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

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Executive Summary

Article 11(11) of Regulation 2022/2554 on digital operational resilience for the financial sector (DORA) mandates the European Supervisory Authorities (ESAs), to develop 'common guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents'. These Guidelines aim at harmonising the estimation by financial entities of their aggregated annual costs and losses caused by major information and communication technology (ICT)-related incidents according to Article 11(10) DORA.

In view of the ESAs, this mandate is closely interlinked with the DORA mandates conferred to the ESAs under Article 18(3) on incident classification and under Article 20 on reporting of incidents as these also require an assessment of costs and losses of ICT-related incidents. Consequently, the ESAs seek to achieve consistency across these mandates to avoid contradictions, increase comparability of the reported figures under the different mandates and, in case the competent authorities request such information from the financial entities, reduce the reporting burden for financial entities. All the criteria in the RTS on classification, including, but not limited to, the one on 'economic impact', are designed to ensure proportionality, meaning that small financial entities are likely to classify ICT-related incidents as "major" less frequently than bigger financial entities. Proportionality is thereby embedded in all other mandates that build on the classification of ICT-related incidents as major, including these Guidelines.

In fulfilment of the mandate, the Guidelines therefore set out that financial entities:

- apply the same approach as the regulatory technical standard specifying the criteria for the classification of ICT-related incidents under Article 18(3) DORA for assessing gross costs and losses and to apply the same approach as the forthcoming technical standards on incident reporting under Article 20 DORA for assessing the financial recoveries of major ICT-related incidents;
- include only those ICT-related incidents that have been classified as major and for which the financial entity has provided a final incident report according to Article 19(4)(c) DORA in the reference year, or submitted in previous years if it had an impact on the costs and losses of that reference year; and
- report the breakdown of the gross costs and losses and financial recoveries by major ICT-related incident to substantiate the aggregate figures.

The ESAs conducted a public consultation on a draft version of the Guidelines from November 2023 to March 2024 and received seventy consultation responses. After assessing these responses, the ESAs decided to review their proposal how to set the reference year to allow for more flexibility for financial entities, that will also reduce their reporting burden. To further limit the reporting burden, the ESAs also decided to request only the estimation of gross costs and losses, not net costs and losses, as the competent authorities can calculate those by themselves.

Next steps

The Joint Guidelines will be translated into the official EU languages and published on the ESAs websites. The deadline for competent authorities to report whether they comply with the Guidelines will be two months after the publication of the translations. The Guidelines should apply from 17 January 2025.

2. Background and rationale

Background

1. Article 11(11) of Regulation 2022/2554 on digital operational resilience for the financial sector (DORA) mandates the European Supervisory Authorities (ESAs), which consist of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA), to develop 'common guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents'.[1] These Guidelines aim at harmonising the estimation by financial entities of their aggregated annual costs and losses caused by major information and communication technology (ICT)-related incidents according to Article 11(10) DORA, which are then to be submitted by financial entities, other than microenterprises, to their competent authority (CA) upon its request. Costs and losses incurred by the financial entities from non-major ICT-related incidents are not in the scope of these Guidelines.

2. In fulfilment of the aforementioned mandate and related provisions and recitals, the ESAs published on 27 November 2023 a Consultation Paper (CP), which set out the ESA's proposals for the Guidelines. The CP laid out the proposed content on how to estimate the annual costs and losses, how to define the one-year period and which figures to use for the estimation of costs and losses. It concludes with a proposal on the aggregation and estimation of gross and net costs and losses incurred across major ICT-related incidents. A public hearing was held on 23 January 2023 before the end of the consultation period on 4 March 2024, by which time the ESAs had received seventy responses which were assessed in detail, as presented in the feedback table in section 4.2 of this Final Report.

3. The Rationale section below provides an overview of the key changes that have been made after the public consultation of the draft Guidelines originally proposed.

Rationale

4. The respondents to the public consultation commented on all aspects of the proposed draft Guidelines. The key points raised that led to changes to the draft Guidelines are a) reviewing the reference year for which financial entities should provide an estimation to the competent authority; and b) limiting the costs and losses that should be reported to the competent authorities. These two points are discussed in this section. Further comments were received that led to clarifications in the Guidelines, but not to significant changes, as well as comments that did not lead to any changes. These comments and the ESAs' analyses of them are presented in detail in the feedback table in section 4.2.

[1] https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Reviewing the reference year for which financial entities should provide an estimation

5. Several respondents argued to allow for reporting by calendar year and based on supervisory reporting or internal risk management figures instead of reporting by financial year and based on financial statements, because:

   - Financial accounts do not include the types of costs that are listed in the RTS on classification while data on operational risk losses do;
   - Reporting requirements under the CRR operational risk framework and DORA should be harmonised;
   - Asset managers already use annual cost estimates for risk management purposes on a calendar-year basis. Reporting for the financial year would lead to an additional burden for them.

6. The ESAs' initial proposal in the Consultation Paper aimed at limiting the reporting burden for financial entities, as many of them are not subject to regular reporting requirements like credit institutions that report on operational risks. The responses to the public consultation confirmed that these entities overwhelmingly support the possibility to base the estimations on accounting figures, for which it is necessary to stick to the accounting year.

7. Nevertheless, the ESAs acknowledge that especially for credit institutions and other financial entities that have already established an operational risk framework, it makes more sense to provide the reporting on already existing reporting requirements for operational risk.

8. Consequently, the ESAs have decided to amend the Guidelines to allow financial entities to choose which reference year they intend to use. However, once they have decided whether they will report based on the calendar year or the accounting year, financial entities should also provide future annual reports on the same type of year. If a financial entity wanted to change its decision, it should notify the competent authority, who would have a 2-month period to object to the change of decision. This approach to provide flexibility on which year to use will make it simpler for financial entities to choose the most appropriate and easily accessible data source they have. This will especially benefit financial entities that have such information available via their supervisory reporting, for instance credit institutions.

Limiting the costs and losses that should be reported to the competent authorities

9. Some respondents argued to only include the gross costs while others argued to only include the net costs in the estimation. The same applies to the reporting of the gross and net costs and losses and to the reporting template. The gross costs are the costs or losses that the financial entity paid or booked. The net costs are a simple subtraction of financial recoveries from the gross costs and losses. As such, the ESAs are of the view that competent authorities can themselves calculate the net costs and losses. Consequently, the ESAs have arrived at the view that the requirement to include and report the net costs and losses can be deleted from

the Guidelines to simplify the reporting requirements for financial entities. However, the estimate of the financial recoveries has been maintained in the Guidelines, in addition to the gross costs and losses.

3. 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 1093/2010[2]; Article 16 of Regulation (EU) No 1094/2010 [3]; and Article 16 of Regulation (EU) No 1095/2010[4] - '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. 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).

[2] 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)

[3] 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)*

[4] 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) 2022/2554[5], 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.

[5] 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][6] 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][7];

[6]Commission 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/reg_del/2024/1772/oj*]

[7] 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

(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.

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/reg_impl/2025/302/oj*]

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	----------	----------		

4. Accompanying documents

4.1 Cost- Benefit Analysis / Impact Assessment

As per Article 16(2) of Regulation (EU) No 1093/2010 (EBA Regulation), 1093/2010 (EIOPA Regulation) and 1095/2010 (ESMA regulation), any guidelines and recommendations developed by the ESAs shall be accompanied by an Impact Assessment (IA) which analyses 'the potential related costs and benefits'.

This analysis presents the IA of the main policy options included in this Consultation Paper (CP) on Joint Guidelines (RTS) on the estimation of aggregated annual costs and losses caused by major ICT-related incidents.

A. Problem identification

According to Article 11 of the Regulation 2022/2554 (DORA), financial entities, other than microenterprises, shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents.

The costs and losses can be measured in various ways and also may be estimated differently across sectors and financial entities. Without further specifications, the data on costs and losses reported by financial entities may be based on different methodologies and assumptions. These divergences can lead to a lack of comparability of data across financial entities and would undermine the usefulness of this information for the Competent Authorities with respect to their supervisory role.

B. Policy objectives

The general objective of the guidelines is to harmonise across sectors the estimation of the aggregated annual costs and losses caused by major ICT-related incidents to be reported to the CAs.

More specific objectives of the guidelines are to enable CAs to use the reported aggregated costs and losses to improve their assessment of the efficiency of the ICT risk management framework of financial entities.

C. Baseline scenario

The baseline scenario is the situation when the current definitions and taxonomy is kept, without further changes or further harmonisation.

With the entry into force of DORA, financial entities must comply with Article 11 of DORA. The above legal requirements form the baseline scenario of the impact assessment, i.e. the impact caused by DORA is not assessed within this impact assessment, which focuses only on areas where further specifications have been provided in the Guidelines.

The following aspects have been considered when developing the Guidelines.

Policy issue 1: Start and end dates for aggregating costs and losses

Options considered

Option A: CAs can specify start and end date, which may have to be calculated on other figures than the profit and loss statements

Option B: Start and end date of accounting years, based on the profit and loss statement of that accounting year

Option C: The financial entities can decide themselves whether they want to set the start and end dates of the reference year according to the calendar year or according to their accounting year, but they would need to stick to that decision.

Option A, whereby the CA is free to specify the start and end date for the estimation, allows the CA to decide which period is most relevant for its purposes. The disadvantage of this approach is that depending on the CA request, the financial entities will need to recalculate the costs for the respective periods.

Option B would be to set the start and end date to be identical with the accounting year of the financial entity. The advantage of this approach is that it would allow financial entities to base their estimates on existing figures from the profit and loss statement. The reporting of costs on losses based on the profit and loss statement will thus be the easiest to implement for the financial entity. However, as some financial entities already calculate the figures for their operational risk management based on the calendar year, this option would impose that these financial entities re-calculate the figures for their accounting years, if that is not identical to the calendar year.

Option C would leverage on the most conveniently available data for financial entities as those that have already an operational risk management framework in place can re-use the data from that. Other financial entities that do not have such a framework in place could rely more on using their accounting figures, which will be a source of information for all financial entities. As financial entities should report consistently by calendar or accounting year over the years, this will ensure that the figures will be coherent for each financial entity over time, since it will rely on a similar established estimation methodology. As a result, in cases when data will be requested over several years, the information provided will be comparable and consistent over time.

Considering the above arguments, Option C is the preferred one.

Policy issue 2: Granularity of reported data

Options considered

Option A: Aggregated data per year only

Option B: Also report the breakdown of the data per year by incident

The mandate requires that financial entities report data on aggregated costs and losses, which would justify Option A. While this option entails reporting of one datapoint per financial entity per year, this figure may not be meaningful for the CA in case they would request the financial entities to report their estimations, since it may hide information on incidents of various sizes and incidents spanning over several years, for which the costs will be split across periods.

Option B, whereby costs and losses are reported at incident level, has several advantages:

- Costs and losses at incident level are more meaningful for the CA being reported separately for each incident;
- In case of incidents spanning over multiple years, the CA would be able to reconstruct the chain of losses from one single incident incurred over several periods.

Furthermore, Option B, despite requiring the reporting of disaggregated data, will not create additional material burden, since the raw data will be estimated at incident level, and therefore will already exist in a disaggregated form.

Option B is therefore preferred.

Cost and benefit analysis

Overall, the guidelines are expected to provide advantages to both financial entities and competent authorities by clarifying the way aggregated costs and losses should be reported, without adding any additional material burden.

	Advantages	**Disadvantages**
Financial entities	Clarity on the way data is estimated	None
Competent authorities	Ensuring comparability of data across sectors and Member States Ensuring the data is meaningful to the CA and usable	None

4.2 Feedback on the public consultation

The ESAs publicly consulted on the draft proposal contained in the Consultation paper.

The consultation period lasted for more than three months and ended on 4 March 2024. 70 responses were received.

This section presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary. In many cases several industry bodies made similar comments or the same body repeated its comments in the response to different questions. In such cases, the comments, and ESAs' analysis are included in the section of this paper where ESAs consider them most appropriate.

Changes to the draft Guidelines have been incorporated as a result of the responses received during the public consultation.

Summary of the responses to the consultation and the ESAs' analysis

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
Feedback on responses to question 1: Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.			
Comments relating to the RTS on major ICT-related incident classification	Several respondents raised issues that relate to - the types of costs to be analysed, such as how to define/ specify them, or whether opportunity costs can be included in the types of costs, or whether indirect costs can be excluded, or to remove certain types of costs and that there are too many types of costs to assess, - the approach to estimating these costs, such as whether estimates are acceptable, or that only external/exceptional costs should be considered, - that the threshold of 100,000 EUR for the economic impact criterion is too low, and - that the 'economic impact' should not be part of the classification criterions.	The comments raised do not relate to the Guidelines but to the RTS on the classification of major ICT-related incidents (JC 2023 83) and are consequently out of the scope of these Guidelines. The Guidelines refer to these RTS in order to ensure consistency.	No change.
Include either net or gross costs and losses, not both.	Some respondents argued to only include the gross costs while others argued to only include the net costs. The same applies to the reporting of the gross and net costs and losses and to the reporting template.	The gross costs are the costs or losses that the financial entity paid or booked. The net costs are a simple subtraction of financial recoveries from the gross costs and losses. As such, the competent authorities can themselves calculate the net costs and losses. Consequently, the ESAs have arrived at the view that the requirement to include and report the net costs and losses can be deleted from the Guidelines to simplify the reporting requirements for financial entities. However, the estimate of the financial recoveries has been maintained in the Guidelines, in addition to the gross costs and losses.	Paragraph 7 point (b) and (c) have been amended as follows: "b) for each major ICT-related incident, financial entities should also ~~calculate the net costs and losses by deducting from the estimated gross costs and losses~~ estimate the financial recoveries as specified ~~in row 4.24 of~~ the Annex II of the ~~implementing technical standards on~~ to Commission Implementing Regulation [OJ L, 2024/1772, 25.6.2024]; c) financial entities should aggregate the gross costs and losses~~,~~ and the financial recoveries ~~and the net costs and losses~~ across major ICT-related incidents."

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
			Paragraph 10 has been amended as follows: " Financial entities should include in the report of their estimation of the aggregated annual costs and losses also the breakdown of gross ~~and net~~ costs and losses and of financial recoveries for each major ICT-related incident that were included in the aggregation." The template in the annex has been amended to delete the column "Net costs and losses of the incident in the accounting year"
Adjustments to previous reports	Several respondents asked to clarify how the adjustments are to be conducted, for instance when costs or losses are wrongly calculated and in the case of costs and losses which become quantifiable at a later time or if the financial entity wants to update the annual report at a later point in time. One respondent also suggested to include a column in the annex to track the adjustments. One respondent argued that adjustments should only be made for incidents that occurred in the year prior to the reference year as "tracking" the incidents is burdensome.	The Guidelines require adjustments to be included in the following years so that annual reports do not need to be updated. Also, the reports of following years will only need to be submitted if the competent authority requests it. Also, paragraph 9 is clear that adjustments to reports of previous years should only be included in the report of the year in which the adjustments are made. The ESAs do not consider a separate column for the adjustments to be necessary. In case the economic impact of past incidents are adjusted during the following year(s), the FEs should have to include again the incidents in the breakdown for each major ICT-related incident in their template (with the same incident reference numbers as the ones used the first time they have been reported), but the value of gross costs and losses/recoveries would be limited to the value of the adjustments. To make this clear, the ESAs have amended paragraph 11. The ESAs have decided to clarify to which incident reference code from the final incident report the FE should refer to and also included in the Annex the LEI of the FEs to avoid any misunderstanding and for CAs to be capable of reconciling all the information provided across years. Considering the proposal to limit the time horizon for how long an entity should track an incident and include adjustments in the annual	Paragraph 11 has been amended as follows: „Financial entities should use the template in the Annex to ~~report~~ submit to the competent authority the estimation of ~~aggregated annual costs and losses~~ 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." The Annex has been amended to include the Legal Entity Identifier (LEI) of the financial entity.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
		report, the ESAs arrived at the view that one of the main advantages of the annual report for competent authorities is to understand the evolution of the costs and losses and financial recoveries over time. Furthermore, Article 17(2) DORA requires the financial entities to record all ICT-related incidents so such information should be available in any case. Consequently, the ESAs have rejected the proposal.	
Estimating costs by incidents is overly burdensome	Some respondents argued that estimating costs for each incident individually is overly burdensome since in the financial statements the costs and losses are already aggregated.	The ESAs do not agree with this assessment, as financial entities need to be able to track the costs of the incidents in any case as they are supposed to be able to assess the economic impact in accordance with Article 18(1) point (f) DORA.	No change.
Estimation of costs	Five respondents argued that several types of costs are difficult to estimate with reasonable accuracy and propose to allow determining the costs on a best effort basis. Three respondents asked for more guidance on the estimation of costs and losses. One respondent asked for further clarifications and examples on how the estimated costs have to be reflected. One respondent pointed to a discrepancy between Art. 11(10-11) of DORA and Paragraph 8 of the GL: DORA requires estimates, whereas the GL expects financial entities to refer to the amounts that are reflected in their financial statements such as the profit and loss account.	Since the Guidelines detail that the annual report represents an estimation of costs and losses, the ESAs are of the view that the Guidelines are sufficiently clear that an estimation is sufficient. Being more prescriptive may increase the burden for financial entities. Details of the elements to take into account in costs and losses estimations are given in Paragraph 7 of the GL, which also refers to the RTS on classification. Paragraph 8 of the GL only specifies the source of estimates. Where accurate data is not available for the valuation of some types of costs and losses, the financial entity should rely on estimated values based on other available data and information to the extent possible.	No change.
Accuracy of the data	One respondent argued that a statement on the accuracy of the data should be included, analogue to Article 8(1) point a)i) of the Draft RTS on major incident reporting under DORA which states that "data points with the data type 'Monetary' shall be reported using a minimum precision equivalent to thousands of units".	On the principle, the ESAs agree with the respondent that the annual aggregated report, which is an estimation, should not need to be more precise than the final incident report, which are the actual impact figures. However, the requirement from the ITS on major incident reports that the respondent refers to is not an alleviation of reporting accuracy but merely a reporting standard to be able to interpret the figures uniformly. This means that the level of precision of the figures is effectively different in dependency of the currency on which the financial entity reports the figures.	The Annex has been amended to specify that monetary values have to be reported in 1000s of units.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
		Consequently, in view of the ESAs, there is no need to specify the level of accuracy in the Guidelines as this will give CAs more flexibility in setting the level of necessary accuracy, also in consideration of the type of entity, its size and other relevant criteria. Nevertheless, to avoid a misunderstanding when filling out the template, the template has been amended to specify that monetary values have to be reported in 1000s of units.	
Group-level vs. entity-level reporting.	Three respondents stated that in capital groups, costs and losses are usually calculated at a group level. Therefore, the Draft Guidelines should allow for the estimates on costs and losses to be calculated at a group level.	Article 11(10) DORA requires the reporting at the level of the financial entity, not at group level.	No change.
Cross-country incidents	One respondent asked more details how to reflect on major incident covering two or more countries.	As the reporting should be done at the level of the financial entity, it should include all costs and losses, irrespective where they originated.	No change.
Feedback on responses to question 2: Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.			
Allow for estimation based on supervisory reporting, the operational risk framework and calendar year	Several respondents argued to allow for reporting by calendar year and based on supervisory reporting or internal risk management figures instead of reporting by financial year and based on financial statements, because: - Financial accounts do not include the types of costs that are listed in the RTS on classification while operational risk losses do. - Reporting requirements under the CRR operational risk framework and DORA should be harmonized. - Asset managers already use annual cost estimates for risk management purposes on a calendar year basis. Reporting for the financial year would lead to an additional burden for them.	The ESAs' initial proposal in the Consultation Paper aimed at limiting the reporting burden for financial entities, as many of them are not subject to regular reporting requirements like credit institutions that report on operational risks. These entities seem to overwhelmingly support the possibility to base the estimations on accounting figures, for which it is necessary to stick to the accounting year. Nevertheless, the ESAs acknowledge that especially for credit institutions and other financial entities that have already established an operational risk framework, it makes more sense to provide the reporting on already existing reporting of operational risk. Consequently, the ESAs have decided to amend the Guidelines to allow financial entities to choose which reference year they intend to use. However, once they have decided whether they will report based on the calendar year or the accounting year, financial entities should also provide future annual reports on the same type of year. If a	Paragraph 5 has been amended as follows: "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 period. The reference period should be the completed accounting 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

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
	- Nevertheless, other FEs support using the accounting year and financial statements, but request to specify that it is the accounting year of the FE, not of the CA.	financial entity wanted to change its decision, it should notify the competent authority, who would have a 2-month period to object to the change of decision. This approach to provide flexibility on which year to use will make it simpler for financial entities to choose the most appropriate and easily accessible data source they have. This will especially benefit financial entities that have such information available via their supervisory reporting, for instance credit institutions.	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 period year." Paragraph 6 has been amended as follows: "Financial entities should include in the estimation all ICT-related incidents that, irrespective of the reason, were classified as major in accordance with ~~the~~ Commission Delegated Regulation [OJ L, 2024/1772, 25.6.2024] 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 ~~accounting~~ reference year, or (b) any incident for which the financial entity submitted in previous ~~accounting~~ 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 ~~validated financial statements such as the~~

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
			~~profit and loss account of the~~ financial entity in the relevant ~~accounting~~ reference year." Paragraph 8 has been amended as follows: "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 ~~accounting~~ reference year~~, and that, if legally required, are validated by an independent entity~~. In their estimation, financial entities should also include accounting provisions that are reflected in their ~~validated~~ financial statements such as the profit and loss account of the relevant ~~accounting~~ reference year. Where accurate data is not available, financial entities should base their estimation on other available data and information to the extent possible." Paragraph 9 has been amended as follows: " Financial entities should include adjustments on the costs and losses ~~reported in the aggregated reporting~~ of an estimation that it submitted for a previous year in the ~~reporting~~ estimation of the relevant ~~accounting~~ reference year in which the adjustments are made."
Definition of the reference period	One respondent asked whether the word "annual" should be understood as "calendar" or "fiscal" year. Another respondent asked to clarify whether the accounting year can be specified by the financial entity or by the NCA. Two respondents said that internal financial accounting processes must be modified to meet the	Paragraph 5 of the GL says the reference period is the completed accounting year, which may also be known as the 'fiscal' or 'financial' year of the financial entity. It is already defined by the financial entities when submitting their annual accounts. Setting the start and end date to be identical with the accounting year of the financial entity creates the lowest administrative burden for many financial entities, because financial entities can use their	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
	reporting requirement and suggest to refer to the general ledger. One respondent said that Paragraph 5 is unclear ("The reference period should be the completed accounting year for which the competent authority requested the estimation") in the case an incident overlaps two accounting years.	financial statements that cover exactly that period as a source of information for the estimation. The last comment about an incident overlapping with several reference periods is addressed in paragraph 6(b).	
Limiting the number of years for which the CA can request the annual report.	One respondent requested to include a maximum number of 3 years backwards from the current for which the competent authority can request the annual report.	The ESAs are of the view that it is essential for competent authorities to be able to request the annual reports, where necessary, for several years. The added value of the Guidelines is to provide the CA a view of the development of the costs and losses over time and thus draw conclusions on the response and recovery actions of the FEs. Given that financial entities shall report the annual costs and losses to their competent authorities only upon the CAs' request, it should be already clear that the reporting is not automatic.	No change.
Frequency of reporting	One respondent asked to confirm that the annual report will only need to be submitted to the NCA upon its request and not automatically every year.	Article 11(10) DORA allows CAs to request this report, it does not require entities to provide this report even without being requested by the CA. The frequency of the reporting will depend on the supervisory needs and will be subject to the request from the CA.	No change.
Apply threshold for inclusion of incidents and time-limit for costs and losses	Some respondents argued that not all major ICT-related incidents should be included: Either a minimum threshold of the costs and losses should be included to disregard negligible costs and losses and keep the reporting burden low, or only include ICT-related incidents that met the "economic impact criterion" in the process of being classified as "major". Furthermore, some respondents argued that only include costs of incidents that occurred in the reporting year, and adjustments to incidents that occurred the year before that reporting year. Incidents from further in the past should not be considered to limit how long an incident needs to be "tracked".	The ESAs disagree with this proposal as it would a) be contrary to the level one requirement to provide an aggregate overview of costs and losses of major ICT-related incidents, which in the understanding of the ESAs is independent of the reason of classification and b) reduce the informative value of the annual report. Furthermore, under this proposal, financial entities will nevertheless need to estimate the costs and losses and only once they have done all the work they could establish whether to include the incidents or not. This would not reduce the reporting burden for financial entities. Regarding the proposal to limit the time, this contradicts the logic of the Guidelines to be able to understand the evolution of costs and losses over time.	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
Independent validation of financial statements	Some respondents stated that paragraph 8 "(...) and that, if legally required, are validated by an independent entity" is unnecessary and confusing. As not all elements referred to by paragraph 7 are reflected in financial statements, let alone independent validation. This could also cause additional, disproportionate costs of external validation of annual reports, especially given that only estimations are required by the Guidelines. One respondent asked whether the report on costs and losses needs external validation.	The reason for this provision is to give a trusted and ideally independent source for costs and losses estimation. The phrase "if legally required" is included to take into account the fact that some financial entities may not be subject to this requirement, while listed companies usually are subject to that requirement. This does not contradict accounting rules and does not impose a new requirement to validate the financial statements. Also, no external validation of the annual report on costs and losses itself is required. Nevertheless, the ESAs have decided to delete the reference and instead clarify in paragraph 5 of the Guidelines the reference year can be that completed accounting year of the financial entity for which the financial entity has finalised its financial statements.	Paragraph 5 has been amended as shown further above in this feedback table.
No financial statements reconciliation	Some respondents stated that the guidelines are not consistent with accounting rules. If changes to financial reporting are necessary, they should be determined under the framework of national accounting legislation. Therefore, the proposal is that FE provide prudent estimation of the aggregated costs and losses of the incidents of the past year, without reflecting them in the financial statements.	The ESAs emphasize that the Guidelines do not introduce any changes to financial reporting or accounting rules. The financial statements and accounting merely serve as a source of information for the estimation.	As explained further above in this feedback table, the amendments to paragraph 8 of the Guidelines clarify this further.
Feedback on responses to question 3: Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.			
Currency to use in the report	One respondent argued that the amounts to be reported if both EUR and non-EUR currencies should be taken into account.	If the official currency is not EUR, every costs should be indicated in local currency according to the principle already established in the RTS on incident reporting.	No change.
Scope of the template and breakdown by incident	One respondent stated that there is no legal basis for the additional report on costs per incident in Art. 11(10) and (11) DORA. Two respondents are of the view that the reporting of required data fields is too burdensome. While some respondents propose to focus reporting on gross cost and losses others suggest to just report aggregated net cost and losses.	The ESAs disagree with this view. The *RTS on classification of incidents* requires FEs to determine gross cost and losses to assess whether the *economic impact* criterion has been met. Thereby, gross cost and losses indicate the impact of the incident, not reflecting who is impacted. Furthermore, it requests reporting financial recoveries. However, as explained further above, the ESAs have decided to delete the requirement of reporting net costs and losses, as these can be simply calculated by CAs themselves.	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
		As explained in the CP of the GL, the breakdown by incident is also necessary to substantiate the aggregated figures.	
Distinction of incidents, which triggered the 'economic impact' criterion	Some respondents suggested making a distinction in the reporting template between incidents that have triggered the economic impact criterion according to the RTS on incident classification and those that have not in order to avoid misrepresentation of the financial entity's risk profile and operational resilience.	Incidents that do not trigger the economic impact criterion (100k EUR) can still be classified as major due to other factors, and that does not mean the incident is without an economic impact. As the annual report is non-public and the competent authority has in any case the information via the final incident report on the criteria that led to the classification of the incident as 'major', the ESAs do not consider this additional reporting requirement to be necessary. Nevertheless, the ESAs have decided to clarify paragraph 6.	Paragraph 6 has been amended as follows: "Financial entities should include in the estimation all ICT-related incidents that, irrespective of the reason, were classified as major in accordance with ~~the~~ Commission Delegated Regulation [OJ L, 2024/1772, 25.6.2024] on incident classification and […]"
Reporting tool	Four respondents suggested using an online platform where FEs can report estimates and where they can access previous reports.	In view of the ESAs, CAs can decide independently about the application of the reporting requirements as well as about the implementation of reporting platforms and methods in their jurisdiction. In addition, the mandate of Article 11(10) DORAis about the estimation of aggregated annual costs and losses, not about the reporting conditions.	No change.
Feedback on responses to question 4: Any other comment			
Purpose of the report	Six respondents questioned the benefit of reporting aggregated annual cost and losses due to various reasons: Data is only available long after the incident; the reporting of incidents should just focus on the impact on clients and customers and not on FEs; data on cost and losses of major ICT-related incident should already been submitted as part of final incident reports under Article 19(4) (c) DORA.	DORA sets out the legal mandate for the reporting of aggregated annual cost and losses upon request by CAs in Article 11(10).	No change.
Proportionality	Three respondents stated that smaller financial entities will not be able to make accurate estimations of gross and net losses. The application of the principle of proportionality is based on incorrect assumptions, since smaller entities are more likely to classify an incident as major, due to	The annual report should be an estimation and does not aim at being fully accurate. Furthermore, smaller financial entities are less likely to be requested to provide such a report, both because the classification of major ICT-related incidents already provides for proportionality, given many criteria defined in the draft RTS on incident classification are relative and criteria in absolute values are high. In addition, CAs will request the reporting for the various types of financial entities	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the GL
	more Single Point of Failures and to fewer incident mitigation measures	under their responsibility, in line with their general supervisory practices, which is generally risk-based. Also, Article 11(10) DORA exempts microenterprises from reporting annual costs and losses.	
Reconciliation of the annual report with final incident report	One respondent stated that more clarity is needed on whether financial entities will have to reconcile the content of the cost and losses reports with the final incident reports. In particular, the Guidelines should clarify whether financial entities will be expected to correct both the closed final incident report and cost and losses reports to make sure they reconcile, in the event where additional recoveries are made after submitting a final incident report.	The annual report is independent of the final incident reports given they will not be reported at the same time. The final incident reports will not need to be updated or adjusted. The annual report will also not need to be updated: adjustments only have to be included in the annual cost and losses reports of the following year, in case the CA requests that report, too.	No change.
Comments relating to the final incident report	Several respondents raised comments that do not relate to the Guidelines themselves, but rather to the obligation to submit a final incident report, such as: - the costs and losses should only be provided in the annual report, - The costs and losses cannot be provided within 30 days of the incident in the final incident report.	DORA mandates the reporting of the economic impact in the final incident report. This has to be provided in all cases, irrespective whether the 'economic impact' criterion has been met for classification of the incident as 'major'. The annual report is an additional requirement that only has to be provided upon request of the competent authority and has no impact on the submission and the content of the final incident report. The 30-day deadline is established in the ITS on incident reporting according to Article 20 DORA. A deferred reporting of the costs and losses to update the final incident report is not foreseen by DORA.	
Comparable data	Two respondents disagreed with the sentence on paragraph 11 in the rationale section of the CP, stating that "the ESAs are of the view that the figures for each major ICT-related incident need to be comparable". For the respondents this suggests that all major incidents are similar, which is not the case and the ESAs need to carefully consider what exactly is being compared and to what effect.	The ESAs are conscious of the fact that not all ICT major incidents are the same. The meaning of the paragraph 11 was mainly due to the fact that the GLs, since they aim to aggregate information for all major ICT-related incidents of FE in the reporting period, need to take into account figures that are comparable as far as possible.	No change.