JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 68

27 November 2023

Consultation paper on Joint Guidelines

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

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'. The apparent aim of these Guidelines is to harmonise 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 reported by financial entities, other than microenterprises, to their competent authority upon its request.

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 reduce the reporting burden for financial entities. All the criteria in the proposed 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 draft Guidelines therefore propose to

- apply the same approach as the forthcoming regulatory technical standard on major incident 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 net costs and losses of major ICT-related incidents;
- set the reference period for aggregating all costs and losses of major ICT-related incidents equal to the accounting year to facilitate the estimation based on available figures from the validated financial statements;
- 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 that accounting year, or submitted in previous years if it had an impact on the costs and losses of that accounting year; and
- report the breakdown of the gross costs and losses, financial recoveries and of the net costs and losses by major ICT-related incident to substantiate the aggregate figures.

Next steps

The consultation period will run until 04 March 2024. The final Guidelines will be published after the consultation period.

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] The apparent aim of these Guidelines is to harmonise 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 reported 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, this Consultation Paper (CP) sets out the ESAs' proposals for Guidelines addressed to financial entities on the estimation of aggregated annual costs and losses caused by major ICT-related incidents. The Rationale section below sets out the options that the ESAs assessed on how best to fulfil the mandate and the reasoning for the options eventually proposed in this CP. It then presents the proposal 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 reporting of gross and net costs and losses incurred across major ICT-related incidents.

Rationale

3. The ESAs arrived at the view that one of the objectives that these Guidelines should attain is to harmonise across financial sectors how financial entities estimate the aggregated annual costs and losses caused by major ICT-related incidents to be reported to CAs. This information will be used by CAs to complement the assessment of the overall financial impact of ICT-related incidents, beyond the individual notifications on major ICT-related incidents that they will receive.

4. Another objective of the Guidelines is to enable CAs to use the reported aggregated costs and losses to improve their assessment of the effectiveness of the ICT risk management framework of financial entities, thus contributing to the risk-based approach, and to make supervision more efficient as a whole.

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

Estimation of gross and net costs and losses in its interplay with other mandates under DORA

5. In the view of the ESAs, four ICT-related incident reporting mandates conferred on the ESAs under DORA are closely linked with one another, namely:

   - the Guidelines on the annual aggregation of costs and losses of major ICT-related incidents under Article 11(11) DORA that are being proposed in this CP,
   - the Regulatory Technical Standard (RTS) on the classification of ICT-related incidents under Article 18(3) DORA that was published for consultation on 19 June 2023, and
   - the RTS as well as the Implementing Technical Standard (ITS) on reporting of major ICT-related incidents under Article 20 DORA are being published for consultation in parallel with this CP.

6. All these mandates include a requirement related to costs and losses of ICT-related incidents, albeit for different purposes. The RTS on the classification of ICT-related incidents includes an overall assessment of the likely economic impact against a threshold of 100 000 EUR, which is used as a criterion for the classification of an ICT-related incident as major, where applicable. The RTS and ITS on reporting of ICT-related incidents, in turn, require the reporting of the materialised impact of major ICT-related incidents by indicating net costs and losses, including financial recoveries for each incident. The Guidelines on aggregated annual costs and losses proposed in this CP, in turn, require from a given financial entity the aggregation of estimated costs and losses of all its major ICT-related incidents within a one-year period, including the ones that do not meet the "economic impact" criterion of 100 000 EUR.

7. More specifically, the proposed RTS under Article 18(3) DORA on the classification of ICT-related incidents that was published for consultation, prescribes, inter alia, how financial entities shall classify ICT-related incidents as major.[2] One of the criteria that can affect the classification is the 'economic impact', which aims at assessing the costs and losses to the financial entity resulting from the ICT-related incident. To this end, the RTS includes the types of costs and the approach to apply when estimating the economic impact. As the classification of the incident has to be carried out in a timely manner after the detection of the incident, the ESAs are of the view that, in most cases, the economic impact can only be estimated, at that time, and on a best effort basis.

8. Furthermore, as this impact needs to be measured against a threshold, the ESAs proposed in said Consultation Paper to measure the costs and losses on a gross basis only, as it would be premature to provide estimates about possible financial recoveries at the time the incident occurs. All the criteria in the proposed RTS on classification, including, but not limited to, the one on 'economic impact', are designed to ensure proportionality, meaning that small financial

[2] Link to the Consultation Paper of the draft regulatory technical standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554

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.

9. When it comes to the proposed RTS and ITS on reporting of major ICT-related incidents which is being published in parallel to this CP, if a financial entity has classified an ICT-related incident as "major", irrespective of whether the "economic impact" criterion has been met, or whether the incident has entailed costs and losses, the proposed RTS and ITS provide that a financial entity will have to provide information about the costs and losses related to that incident in the major ICT-related incident report submitted to competent authorities under Article 19 of DORA, and the technical standards under Article 20 DORA.

10. In particular, in the final incident report according to Article 19(4) c) of DORA, the financial entity will have to provide the actual impact of that incident, including associated costs and losses. By the time the financial entity submits the final incident report, the CA will be interested in assessing the impact on the financial entity which might be inferred from the net costs and losses associated with the incident. This is because the gross figures alone may give a skewed impression of the financial impact especially where financial recoveries, for instance through insurance claims or service provider contractual penalties, are not considered. To calculate the net costs and losses, the ITS introduces the concept of financial recoveries.

11. The estimation of aggregate annual costs and losses under the Guidelines under Article 11(11) DORA, in turn, relies on the classification of ICT-incidents as being "major" and the subsequent assessment of economic impact (represented as net costs and losses) of these incidents. Since the Guidelines aim at aggregating information for all major ICT-related incidents of a financial entity in the reporting period, the ESAs are of the view that the figures for each major ICT-related incident need to be comparable.

12. Since the estimation of costs and losses are part of all four mandates listed above, the different references to costs and losses, and their descriptions, should be consistent between mandates to facilitate synergies, and to minimise the introduced reporting burden for financial entities. Consequently, the ESA decided to propose a layered approach where all four mandates build on each other: Article 7 of the proposed RTS under Article 18(3) DORA includes a list of costs and losses for the assessment of gross economic impacts and the approach how to assess them, i.e., only to include those costs and losses that exceed the business-as-usual costs.[3] Said RTS requires the assessment of gross costs and losses only, so that the incident can be evaluated against a uniform threshold for the purpose of the classification. In the RTS and ITS on incident reporting, the ESAs proposed an approach to assess and report not only the gross costs of a major ICT-related incident, but also the net costs and losses, by taking financial

[3] The types of costs included in the RTS comprise expropriated funds or financial assets for which the financial entity is liable, including assets lost to theft; replacement or relocation costs of software, hardware or infrastructure; staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff; fees due to non-compliance with contractual obligations; customer redress and compensation costs; losses due to forgone revenues; costs associated to internal and external communication; advisory costs, including costs associated with legal counselling, forensic and remediation services.

recoveries into account. Finally, the Guidelines on aggregated annual costs and losses proposed in this CP provide an approach to aggregate and report the costs and losses across all major ICT-related incidents at a financial entity in a comparable manner, as detailed in the next paragraph.

13. In order to ensure a consistent approach to the assessment of gross and net costs and losses across the three mandates, the ESAs are therefore proposing that the Guidelines rely on the approach of the related RTSs rather than specifying a different approach for the assessment of gross and net costs and losses. As such, the ESAs propose referring to a) Article 7, paragraph 1 and 2 of the RTS on incident classification for the types of costs to be considered and the approach to estimating them only for those costs exceeding the business-as-usual costs, and b) the Annex II of the technical standard on reporting of major ICT-related incidents, row 4.24 on financial recoveries from those major ICT-related incidents.

14. Accordingly, the gross costs and losses are estimated by the sum of all of the below, which also includes accounting provisions for future costs and losses:

    - expropriated funds or financial assets for which the financial entity is liable, including assets lost to theft;
    - replacement or relocation costs of software, hardware or infrastructure;
    - staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff;
    - fees due to non-compliance with contractual obligations;
    - customer redress and compensation costs;
    - losses due to forgone revenues;
    - costs associated with internal and external communication;
    - advisory costs, including costs associated with legal counselling, forensic and remediation services.

15. The net costs and losses are calculated by subtracting the financial recoveries from the sum of the estimated gross costs and losses per major ICT-related incident.

Consultation 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.

Determining the timeframe and data source for the estimation of annual costs and losses

16. Article 11(10) of DORA provides that financial entities shall report to their competent authorities, upon request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents. Article 11(10) DORA does not specify how the "annual" costs and losses should be determined. Consequently, there is a lack of clarity on the start and end date of the one-year period and whether the reporting requirements can cover overlapping time periods. In view of the ESAs, the requirement should be such that for any given financial entity, sequential reports should not cover overlapping time periods, as otherwise two subsequent data requests addressed to a financial entity would not be distinctly comparable. The reporting period should also be consistent over time for the same reason, also as this should allow for a long-term, perennial assessment of costs and losses related to major ICT-related incidents and their remediation. Finally, the reporting period must be practically feasible to report and limit the reporting burden for the financial entity. The ESAs assessed three options how this could be achieved, which is summarised in the following paragraphs.

17. One option would be that a CA is free to specify the start and end date for the estimation, for instance by setting the start date at the date where the initial incident report or the final incident report of one specific major ICT-related incident of that financial entity was submitted to the CA. However, the ESAs discarded that option as not appropriate because the estimation is supposed to aggregate several ICT-related incidents within that year. And while the first major ICT-related incident may be fully captured within that one-year period, a second incident that was reported later may not be fully captured. It would also leave open which incident to choose for the start and end date with a view to requesting the estimation in future years for the same dates.

18. A second option would be to require the reporting for a given calendar year. This would have the advantage over the first option to set clear expectations for financial entities over which timeframe they need to estimate costs and losses, ensure that there is no overlap or gap between two reports by a financial entity and thus ensure that the full costs and losses of a major ICT-related incident can be captured in the long run by creating a chain of annual reports. Furthermore, the reports would become comparable between financial entities. However, the major drawback of this approach is that there is currently no reporting requirement in place that would allow for the calculation of costs and losses over a calendar year and would thus introduce a higher reporting burden for financial entities. This consideration leads to the third option described below.

19. The third option would be to set the start and end date to be identical with the accounting year of the financial entity. In view of the ESAs, this approach allows financial entities to base their estimates on ascertained and comparable figures from their relevant validated financial statements created in line with national law and the relevant accounting standards, most importantly the profit and loss account, and thus be the easiest to implement for the financial entities. While some costs and losses may not have materialised yet at the point in time of reporting, they are often represented in accounting provisions in the profit and loss account, which are an established form of a discrete annual estimation. Furthermore, financial recoveries are also normally reflected in the profit and loss account.

20. Furthermore, the provided figures would be coherent for each financial entity over time since it can rely on the timing and accuracy of the validated financial statements. The ESAs anticipate that the CAs are most likely to request this estimation for a number of years in a row for financial entities that have experienced several major ICT-related incidents. This means that in the long run, CAs will have a good overview of the estimated costs and losses attributed to a specific major ICT-related incident, broken down by their yearly development.

21. The third option bears the disadvantage that the reported annual figures may not be comparable between financial entities because they may cover different timeframes. However, if financial entities also report the breakdown of the figures by each major ICT-related incident, as proposed in the next section, then the CA can compare the costs, losses and financial recoveries evolution of major ICT-related incidents since their beginning, for instance by comparing after how many years the economic impact of an incident stops evolving and how much the remediation eventually cost. This allows to compare the costs and losses of incidents across financial entities. Furthermore, as the second option could not be implemented due to the lack of reported figures, this drawback seems unavoidable. Consequently, the ESAs propose that a) the estimation should cover a time period that is identical to the accounting year of a financial entity and b) that the estimation is based on the numbers from the validated financial statements such as the profit and loss account of that accounting year.

22. The ESAs point out that the figures reported in the final report under Article 19(4)(c) of DORA as set out in the proposed TS on incident reporting and the aggregated annual costs and losses reported under these Guidelines may differ, as the former is supposed to capture all the costs of losses of a specific incident, while the latter will capture the cost of all the major ICT-related incidents within a one-year period, irrespective whether these incidents started in that year or not.

23. The estimation of aggregated annual costs and losses should cover all major ICT-related incidents. However, Article 11(10) DORA does not specify whether these are incidents that were first reported in the one-year period, or if it should also include major ICT-related incidents that were first reported in previous years and that are having an economic impact on the financial entity across two or more years.

24. The ESAs expect that the annual aggregated reporting will not capture the whole lifecycle of all major ICT-related incidents that occurred within a year, especially for these incidents that were first reported close to the end of the accounting year, and that the CA should be able to obtain an estimation of the full economic impact of the incidents over time. For this to be possible, it is necessary to include in the aggregation the costs and losses all major ICT-related incidents, not only in the year in which they were first detected, but also in subsequent years. Consequently, the ESAs are proposing in paragraph 6 of the Guidelines in this CP that any major ICT-related incident should be included in the aggregation if that incident started in that year (even if the economic impact is zero) or if it had an impact on the relevant financial statement such as the profit and loss account in that year. Major ICT-related incidents that did not start

in that accounting year and that did not have an economic impact captured in that accounting year's profit and loss account should not be included in the aggregation as their impact is zero for that year. Should a cost or loss be incurred afterwards, it should be reflected in the next year's profit and loss account.

25. Regarding the starting date of an incident, the ESAs assessed which would be the most suitable cut-off date for including a major ICT-related incident in the estimation of aggregated annual costs and losses. The ESAs reasoned that if the initial notification of the incident according to Article 19(4)a) DORA was the cut-off date, financial entities might find themselves in the situation that for an incident they need to not only identify the root causes of the incident, remediate it, and provide the final reports according to Article 19(4)c) CORA to the CA, but also at the same time provide the estimated aggregated annual costs and losses according to these Guidelines. This may put an unnecessary reporting burden on them at that time.

26. To avoid such a situation, the ESAs are proposing in paragraph 6a of this CP that the cut-off date for including a major ICT-related incident in the estimation should be the submission of the final incident report according to Article 19(4)c) DORA. This approach should facilitate the reporting for financial entities and put them in the position to provide a more informed estimation of costs and losses. This approach will in any case allow to capture all major ICT-related incidents in the aggregated annual figures in the long run, as an incident that was detected in a given accounting year, but for which the final incident report was not submitted in that same year, would be captured in the following year's annual report.

Consultation 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.

Reporting of annual costs and losses

27. Furthermore, the CA may not be able to deduce sufficient information from one aggregated figure for gross costs and losses and one for net costs and losses for a financial entity if that financial entity faced more than one major ICT-related incident in that period. The ESAs see merit that the aggregation should be substantiated by an estimation of the costs and losses for each major ICT-related incident individually, too. Considering that financial entities need to identify individually the costs and losses for each major ICT-related incident in any given year to be able to aggregate over all major ICT-related incidents in that year, it would not pose an

inappropriate burden for those financial entities to provide more granularity in the reported figures.

28. Consequently, the ESAs are proposing in paragraph 10 of this CP that financial entities should report the annual aggregated gross costs and losses and annual aggregated net costs and losses of all major ICT-related incidents, as well as the annual gross and net figures for each major ICT-related incident individually a) for which the financial entity submitted the final report in that accounting year (even if its economic impact was zero) or that b) had an economic impact that is not zero in that accounting year. The template in the annex aims at ensuring that the incidents can be clearly identified and linked to each other across years.

Consultation 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.

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[4]; Article 16 of Regulation (EU) No 1094/2010 [5]; and Article 16 of Regulation (EU) No 1095/2010[6] - '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 dd.mm.yyyy (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 compliance@esma.europa.eu] with the reference 'JC/GL/201x/xx'. 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).

[4] 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)

[5] 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)*

[6] 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[7], 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 dd.mm.yyyy

[7] 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 period. The reference period should be the completed accounting year for which the competent authority requested the estimation. Financial entities should not include costs and losses related to those incidents that fall before or after that reference period.

6. Financial entities should include in the estimation all ICT-related incidents that were classified as major in accordance with the RTS 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 year, or

   (b) any incident for which the financial entity submitted in previous accounting 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 profit and loss account of the financial entity in the relevant accounting 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 RTS on incident classification;

   (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 the financial recoveries as specified in row 4.24 of the Annex II of the implementing technical standards on incident reporting;

   (c) financial entities should aggregate the gross costs and losses, the financial recoveries and the net costs and losses 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 of the relevant accounting 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 year.

9. Financial entities should include adjustments on the costs and losses reported in the aggregated reporting of a previous year in the reporting of the relevant accounting year in which the adjustments are made.

10. Financial entities should include in the report of the estimation of the aggregated annual costs and losses the breakdown of gross and net costs and losses for each major ICT-related incident that were included in the aggregation.

11. Financial entities should use the template in the Annex to report the estimation of aggregated annual costs and losses.

Annex: Reporting template for gross and net costs and losses in an accounting year

Name of the financial entity					
Start and end date of accounting year of the financial entity					
Reporting 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 accounting year	Recoveries of the incident in the accounting year	Net costs and losses of the incident in the accounting year
1					
2					
…					
Aggregated annual costs and losses	----------	----------			

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 way, 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 lack of comparability of data across financial entities and will 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 harmonize 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 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 disadvantages 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 advantages of this approach is that it would allow financial entities to base its 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.

In addition, using Option B, will ensure that the figures will be coherent for each financial entity over time, since it will rely on a similar established estimation methodology, and will also include information on recoveries, that are also reflected in the profit and loss statement. 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 B 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, 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 cost sand 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 Overview of questions for consultation

Consultation 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.

Consultation 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.

Consultation 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.