JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 33

17 July 2024

Final Report

Draft Regulatory Technical Standards

on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents

and

Draft Implementing Technical Standards

On the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Executive Summary

One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to harmonise and streamline the ICT-related incident reporting regime for financial entities (FEs) in the European Union (EU).

Article 20 of DORA mandates the European Supervisory Authorities (ESAs) to develop through the Joint Committee and in consultation with the European Central Bank and European Union Agency for Cybersecurity:

- Draft Regulatory Technical Standards (RTS) establishing the content of the reports for ICT-related incidents and the notification for significant cyber threats, and the time limits for FEs to report these incidents to competent authorities.
- Draft Implementing Technical Standards (ITS) establishing the standard forms, templates and procedures for FEs to report a major ICT-related incident or to notify a significant cyber threat.

Article 20 of DORA further requires the ESAs to ensure that the requirements of the draft RTS and ITS are proportionate and consistent with the approach for incident reporting under Directive (EU) 2022/2555 (NIS2).

The ESAs ran a public consultation between 8 December 2023 June and 4 March 2024. The ESAs received 109 responses to the Consultation paper. The ESAs assessed the concerns raised to decide what, if any, changes should be made to the draft RTS and ITS. In the light of the comments received, the ESAs agreed with some of the proposals and their underlying arguments and have introduced changes to the draft RTS and ITS. These changes are related to the time limits for reporting initial notification, intermediate report and final report, reporting over weekend and bank holidays, aggregated reporting and streamlining the content of the reporting template.

On the reporting time limits, the ESAs have extended the time limit for reporting the intermediate report with up to 24 hours and the final report with at least 72 hours by starting the calculation of the timelines from the submission of the previous notification/report, instead of the moment of classification of the incident as consulted.

On weekend and bank holiday reporting, the ESAs have reduced the scope of incidents that need to be reported, removed the obligation for smaller financial entities to report the initial notification, and have extended the time limit for submission of the notifications and reports by noon at the first working day, instead of within 1-hour as consulted.

In relation to the content of the incident template, the ESAs have streamlined it significantly, by reducing the number of reporting fields from 84 to 59. The ESAs have also simplified the initial notification 7 mandatory fields, so that FEs are able to focus their resources on handling the incident and report essential elements at this early stage of the incident.

Finally, ESAs have introduced aggregated reporting at national level for FEs supervised by a single competent authority, if certain conditions are met.

Next steps

The final draft RTS will be submitted to the Commission for adoption. Following the adoption, the RTS will be subject to scrutiny by the European Parliament and the Council and then will be published in the Official Journal of the European Union.

2. List of abbreviations

BRRD - Directive 2014/59/EU

CA – Competent authority

CSIRT – Computer Security Incident Response Team

DORA – Regulation EU 2022/2554 on digital operational resilience for the financial sector

ECB – European Central Bank

ENISA – European Union Agency for Cybersecurity

ESAs – European Supervisory Authorities

EU – European Union

FE – financial entity

FR – Final report

GDPR - Regulation (EU) 2016/679

IA – Impact assessment

ICT – Information and communication technology

IORP – Institutions for occupational retirement provision

ITS – Implementing Technical Standards

LEI – Legal Entity Identifier

NIS2 – Directive (EU) 2022/2555

PSD2 – Directive (EU) 2015/2366

RTS – Regulatory Technical Standards

TS – Technical Standards

TPP – third-party provider

3. Background and rationale

3.1 Background

1. One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to harmonise and streamline the ICT-related incident reporting regime for financial entities (FEs) in the EU. To that end, DORA introduces consistent requirements for FEs on management, classification and reporting of ICT-related incidents.

2. Article 19(1) of DORA prescribes that FEs 'shall report major ICT-related incidents to the relevant competent authority'. Article 19(4) of DORA, in turn, specifies that FEs 'may, on voluntary basis, notify significant cyber threats to the relevant competent authorities when they deem the threat to be of relevance to the financial system, service users or clients'.

3. In that regard, Article 20 of DORA mandates the European Supervisory Authorities (ESAs) to develop through the Joint Committee and in consultation with ENISA and the ECB:

    a) common draft regulatory technical standards (RTS) in order to:

        (i) establish the content of the reports for major ICT-related incidents in order to reflect the criteria laid down in Article 18(1) and incorporate further elements, such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident or not;

        (ii) determine the time limits for the initial notification and for each report referred to in Article 19(4);

        (iii) establish the content of the notification for significant cyber threats.

    b) common draft implementing technical standards (ITS) in order to establish the standard forms, templates and procedures for FEs to report a major ICT-related incident and to notify a significant cyber threat.

4. Article 20 of DORA also specifies that when developing the draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the FE, and the nature, scale and complexity of its services, activities and operations, and in particular, with a view to ensuring that, for the purposes of the reporting time limits, different time limits may reflect, as appropriate, specificities of financial sectors, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to DORA and to Directive (EU) 2022/2555 (NIS2).

5. These RTS and ITS are closely linked to the draft RTS 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, which was published by the ESAs on by 16 January 2024.

6. A Consultation paper (CP) on the draft RTS and ITS was published on 8 December for a three-month consultation period, which closed on 4 March 2024. The ESAs received 109 responses from a variety of market participants across the financial sector.

7. The ESAs have assessed the responses from the public consultation and have made changes to the draft RTS where relevant. The main issues raised by the stakeholders are presented in Section 7 of this report 'Accompanying documents' in the sub-section on feedback from the public consultation. The Rationale section provides an overview of the most prominent aspects raised during the consultation and/or those that resulted in more substantive changes to the draft RTS and ITS.

3.2 Rationale

8. The respondents to the public consultation commented on all aspects of the proposed draft RTS. The key points raised that led to changes to the draft RTS are reflected in this section, which focuses on:

   - Proportionality and entity specificities
   - Reporting timelines
   - Reporting over the weekend
   - Interplay between DORA and NIS2
   - Content of the reporting template
   - Aggregated reporting

9. The parts related to the body of the ITS, the significant cyber threats and the general information to be provided in the major incident initial notification, intermediate and final reports remain largely unchanged.

(i) Proportionality and entity specificities

10. Several respondents were of the view that the RTS and ITS do not fully incorporate the proportionality principle and suggested introducing different timelines reflecting the size and the overall risk profile of the FE, and the nature, scale and complexity of its services, activities and operations. Some of these respondents also highlighted that specificities and time-criticality of the services provided by FEs need to be taken into account in relation to the reporting timelines.

11. In particular, some of these respondents indicated that the timelines for the initial notification are too short for FEs in the insurance and pension sub-sectors, as well as savings banks, asset managers, investment firms and trade repositories. They indicated that the reporting timelines for the intermediate report should also be extended.

12. With regard to proportionality and entity-specificities, the ESAs would like to highlight that:

- In line with the objectives of DORA to introduce a harmonised and streamlined incident reporting framework and taking into account that often incidents within a group or originating from a TPP may affect different types of FEs, the ESAs have arrived at the view that retaining a harmonised timelines for reporting major incidents is preferrable and did not find compelling reasons why different timelines should apply to different FEs;

- Proportionality is embedded in the timelines set, which were designed to address to a great extent the specificities of different types of FEs and strike a good balance between the need to allow sufficient time for FEs to handle the incident, while at the same time providing CAs with relevant information about the major incident early enough; and

- Proportionality is embedded in the approach for classification of major ICT-related incidents set out in the RTS on criteria for classification of major incidents under DORA.

13. Nevertheless, the ESAs agree with some of the points raised on proportionality and, to ensure that the draft RTS and ITS are proportionate, introduced the following amendments:

- The ESAs have reduced the number of reporting fields in the reporting template, including by significantly streamlining the requested information in the initial notification to not put burden on entities while they will be handling the major incident.

- The ESAs have provided additional time for the reporting of the intermediate report and the final report due to the change in the start of calculating the time from the previous submitted notification/report, instead of the moment of classification of the incident. This means that FEs will have up to one additional day for reporting the intermediate report and up to 3 days (72 hours) more for reporting the final report;

- The ESAs have narrowed down the scope of mandatory weekend reporting by focusing only on credit institutions, trading venues, central counterparties, other FEs within the scope of NIS2 designated at national level, and entities with significant and systemic impact at national level (based on CAs' judgement), and by excluding the reporting of incidents having a cross-border impact or those affecting TPPs/FEs as a criterion for requiring reporting over the weekend.

- The ESAs have clarified the possibility for a few FEs to report major incidents in an aggregated way at national level, thus reducing the reporting effort for entities serviced by a single TPP or operating within a group.

(ii) Reporting timelines

14. Many respondents were of the view that the reporting timelines are too short and that they should be extended or that the data fields requested should be significantly reduced. The main argument presented is that FEs will be handling the incident at the time of reporting and that some of the information requested requires input from various functions. Some respondents also suggested aligning them further with existing frameworks such as NIS2 and PSD2 and avoiding introducing more stringent requirements than those already in place. In the subsections below, the ESAs have introduced the different views expressed and changes introduced as a result of the public consultation with respect to the initial notification, intermediate and final reports.

Initial notification

15. The majority of the respondents suggested extending the time limits for submission of the initial notification with some respondents finding the 4-hour reporting limit too short for non-critical services and suggested aligning with NIS2 (24h), or aligning with GDPR (72 hours), or that the reporting takes place in the next working day. Several respondents expressed concerns with having two separate deadlines (from the moment of classification and from the moment FEs become aware of the incidents). As part of the rationale provided, respondents highlighted that FEs will be handling the incident at the time of reporting and that some of the information requested requires input from various functions.

16. Finally, several respondents were of the view that introducing a time limit for submitting a notification after FEs become aware of the incident may lead to significant overreporting since FEs will be forced to report the incident. Some of them sought clarity on how to approach the reporting of incident that becomes major after 24 hours from detection.

17. The ESAs are of the view that the timelines for classification of an incident as major are appropriate since they provide the right balance between the need of CAs to receive information to address potential systemic issues and the need of FEs to focus their resource to handle the incident.

18. The ESAs would like to highlight that the envisaged timelines of submitting an initial notification within 4 hours from the classification of the incident but no later than 24 hours from the moment the FE has become aware of the incident provides sufficient flexibility to FEs, especially smaller ones with less complex business models and time criticality of the service, to submit the notification within the 24-hour period if they require more time to handle the incident.

19. Nevertheless, the ESAs also acknowledge the need for FEs to prioritise the handling of the incident and not facing reporting burden at these early stages of the incident and have, therefore, reduced the number of reporting fields in the initial notification from 17 to 10 with only 7 mandatory fields.

20. To reflect the difference in the time-criticality of the service, the ESAs have retained the two separate time limits (from moment of classification and from moment of becoming aware of the incident) for submission of the initial notification.

21. Finally, regarding the time limit for submission of initial notification after FEs become aware of the incident, the ESAs are of the view that this should not lead to overreporting since FEs will not be obliged to classify the incident as major if there is no indication it is such. Nevertheless, to acknowledge that there may be situations where an incident has not been classified as major within the first 24 hours after FEs become aware of it, but becomes major afterwards, the ESAs have introduced a new paragraph in Article 6 of the draft RTS.

Intermediate report

22. A large number of respondents were of the view that the proposed timelines of the intermediate report are too short and that they will introduce reporting burden, especially since they are more restrictive than any existing reporting framework. Many of these respondents suggested that the time limit for submitting the intermediate report should start counting from the submission of an initial notification and not from the moment of classification of the incident. The majority have suggested that 3 working days from the submission of the initial notification should work well. Several respondents (mainly from insurance and pension sub-sector) suggested even longer timelines.

23. A few respondents highlighted as a rationale for the extension of the timelines the large number of data fields, the need to coordinate between several functions and potential dependency on third-party providers introduce challenge to meet the reporting deadline.

24. In addition, some respondents indicated that it is impossible that FEs prepare an intermediate report immediately after the recovery of the activities and suggested that the ESAs introduce a specific time-limit (e.g. 4 hours) for the submission of the report.

25. The ESAs agree with the rationale provided and have amended Article 6(1)(b) of the draft RTS by referring to 72 hours from the submission of the initial notification. This should provide additional time for FEs to collect the requested information without posing burden to them while handling the incident.

26. In addition, the ESAs have clarified in the same paragraph that the submission of the intermediate report after the regular activities have been recovered should take place without undue delay to allow for time for FEs to prepare the report.

Final report

27. A large number of respondents were of the view that the timelines for submitting a final report should be one month after the submission of the intermediate report (rather than the moment of classification as set out in the Consultation paper). They also indicate that submitting the final

report a day after the permanent resolution is unrealistic due to the high number of data fields to be provided. Additional rationale provided by these respondents included that the permanent resolution of the incident takes normally longer than one month after classification of an incident, that there are procedural steps for preparing the report and coordinating internally (especially for large entities), dependencies on third-party providers and the time required for carrying out the root-cause analysis.

28. Some respondents also indicated that clarification is needed on the distinction between resolution and permanent resolution of the incident and which one is intended. Relatedly, a few respondents queried whether the final report should be updated in case the permanent resolution takes longer than 1 month. In addition, a few respondents suggested longer timelines since the root cause analysis can at times also take longer than one month.

29. The ESAs agree with the concerns expressed and the rationale provided by the respondents and have amended Article 6(1)(c) by requiring the submission of the final report no later than 1 month from the submission of the latest intermediate report and have deleted the reference to 'permanent' resolution of the incident to clarify that the aim is not covering problem management.

(iii) Reporting over the weekend

30. Many respondents were of the view that FEs should not report major incidents over the weekend but only during business hours. In addition, several respondents indicated that the intermediate and final report should be reported only during business hours. The rationale provided by the respondents was that reporting 24/7 will have a negative impact on the FEs and pose reporting burden by adding extra cost of maintaining operational staff at no apparent added value.

31. Moreover, many respondents viewed the 1-hour deadline for reporting the incident in the following working day as inadequate and posing unnecessary burden. Most of them suggested extending this deadline to 4 hours.

32. Finally, some respondents indicated that reporting over the weekend should apply to significant and large institutions only that have a systemic impact. They viewed that many incidents have a cross-border impact and/or affect another FE, thus posing the risk of very wide scope of the reporting obligation over the weekend.

33. The ESAs agree with the rationale provided by the respondents and have amended the draft RTS to address the issues raised, including ensuring a more proportionate approach, namely by:

- not requiring reporting of a final report over the weekend;

- extending the exemption to the initial notification so that not all FEs will be required to maintain a 24/7 incident reporting support function;
- requiring the submission of an initial notification and intermediate report over the weekend only by significant or systemic institutions at EU and national level, as well as critical or important entities under NIS2.
- removing the reference to 'from where the major incident has an impact in another Member State or to another financial entity' from Article 6(3) of the draft RTS to decrease the scope of weekend reporting for non-systemic and significant FEs; and
- increasing the time-limit for submission of an initial notification, intermediate and final reports in the working day following a weekend or a bank holiday from 1 hours after the start of business hours to 12:00 of the working day.

(iv) Interplay between DORA and NIS2

34. Several respondents suggested ensuring further consistency between DORA and NIS2 by ensuring the timelines for incident reporting are consistent and the information requested.

35. The ESAs would like to highlight that the proposed requirements for reporting major ICT-related incidents have already been much aligned and made consistent with NIS2 in line with the requirements of Article 20 of DORA. It should also be noted that Article 4 of NIS2 introduces the *lex specialis* regime of DORA (being a sector-specific legislation) over NIS2 and provides that the reporting requirements for major incidents under such sector-specific legislation should be 'at least equivalent in effect' to those laid down in NIS2. The ESAs would like to clarify that this does not mean that the requirements in relation to the timelines for reporting and the amount of information requested should be identical.

36. Following the public consultation, the ESAs assessed whether the proposed requirements in the Consultation paper and the amended requirements following the public consultation were aligned with NIS2. Accordingly, the ESAs arrived at the view that all provisions in the amended RTS and ITS are 'at least equivalent in effect' to the requirements in NIS2. In particular:

- the 24-hour timeline for submission of initial notification after the FE has become aware of the incident were deemed identical to NIS2, with the requirement to submit the initial notification 4 hours after classification being stricter for some larger and more systemic FEs;
- the timelines for reporting of the intermediate report at the latest within 72 hours from the submission of the initial report in DORA were deemed similar (slightly longer and more relaxed) compared to the requirement to submit incident notification within 72 hours from the moment of classification of the incident in NIS2 (as envisaged in the draft that was publicly consulted). However, since the key attributes required in the incident

notification in NIS2 will be required in a high-level way in the initial notification in DORA, which is submitted within 24 hours, and that the intermediate report under DORA requires more information compared to NIS2, in practice the DORA requirements are considered at least equivalent, if not slightly stricter in some aspects, than those set out in NIS2. Moreover, DORA envisages that FEs shall submit an intermediate report to the CA (i) as soon as the status of the original incident has changed significantly and (ii) as soon as the handling of the major ICT-related incident has changed based on new information available. In addition, the RTS envisage a submission of the intermediate report when the incident is resolved and business is back to normal. All these three scenarios allow a submission of an intermediate report before the 72-hour deadline; and

- the timelines for the submission of the final report of one month after the submission of the intermediate report (incident notification under NIS2) were deemed identical to those set out in NIS2.

(v) Content of the reporting template

37. Many of the respondents to the public consultation viewed the reporting template for major ICT-related incidents too long, detailed and posing burden to the industry at a time when they will need to be handling an incident. Accordingly, the ESAs have received specific proposals to delete or merge certain data fields, and to move some information requested to the later stages of the incident reporting. The specific and more detailed views are reflected in the Feeback table at the end of this Final report.

38. The ESAs have assessed all the points raised by the respondents and the rationale behind. Accordingly, the ESAs have arrived at the view that some changes to the reporting template for major ICT-related incidents should be introduced to avoid posing burden to the industry, especially at the early stages of reporting. In particular, the ESAs have reduced the data fields from the reporting template from 84 to 59 (or 30% decrease) making the reporting template simpler and more efficient. In particular, the ESAs have streamlined the initial notification by requiring only 10 fields, 7 of which mandatory, so that FEs are able to focus their resources on handling the incident and report only essential elements at this early stage of the incident. The table below provides an overview of the change in the data fields included in the template for major incidents.

Table 1: Changes made to the reporting fields in the template on major incidents

Report	Mandatory fields	Conditional fields
Initial notification	~~9~~ => 7	~~8~~ => 3
Intermediate report	~~16~~ => 14	~~24~~ => 21
Final report	~~12~~ => 7	~~15~~ => 7
TOTAL	**~~37~~ => 28**	**~~47~~ => 31**

(vi) Aggregated reporting

39. Many respondents were of the view that it should be possible for ICT third-party providers or for financial groups to submit one aggregated/consolidated report for all affected FEs. They argue that disallowing such aggregated or consolidated reporting will pose reporting burden since:

- ICT service providers would have to report the same incident multiple times or would have to answer many questions of FEs within the first hours such that they can fill out reports;
- FEs would need to collect all information about the incident from TPPs, including intragroup providers;
- Financial groups would need to report the same incident multiple times;
- CAs that have to analyse multiple reports of the same incident and face difficulties in aggregating the impact of the incident.

40. Some of these respondents were of the view that the information about the incident should also be reported in an aggregated way without including individual information for each FE. The respondents also proposed that TPPs and financial groups should be allowed to submit one consolidated report including a list of all affected FEs to reduce the burden and to make incident reporting more efficient.

41. The ESAs would like to highlight that the CP already envisaged the possibility that there may be cases where several FEs outsource the incident reporting activities to a third-party service provider, including members within a financial group, in accordance with Article 19(5) of DORA and that in these cases, subject to an agreement between the FEs and their CA, it may be possible for said third-party service providers to provide one report at national level for the FEs supervised by the same CA containing the relevant individual information for each FE that would classify the incident as major.

42. Having assessed the feedback from the respondents and the arguments presented, the ESAs have decided to introduce explicitly the possibility for submission by an ICT TPPs or intragroup TPPs of a single aggregate report for multiple FEs affected by the same incident. The main rationale for introducing such aggregated reporting is that it provides a holistic overview of the impact of the incident and whether it is of systemic relevance, and to decrease the reporting effort by FEs and CAs. The ESAs also took into account that most of the information about the incident is likely to be available to the TPP if the incident originates from it.

43. However, the ESAs have introduced the following conditions to ensure that such aggregated reporting is aligned with the requirements of DORA:

- The incident originates or is being caused by a TPP;

- The third-party provider provides relevant ICT services to more than one FE or to a group, in the Member State;
- The FEs impacted by the incident have outsourced the reporting obligations to a TPP in accordance with Art. 19(5) of DORA and Article 6 of the draft ITS;
- The impact of the incident is assessed for each FE and has been classified as major individually by each FE covered in the aggregated report;
- The incident has an impact in a single Member State and the aggregated report relates to FEs, which are supervised by the same competent authority (CA);
- The aggregated report should contain aggregated information about the impact of the incident on all FEs covered in the report;
- The aggregated report should not cover information about significant credit institutions and central counterparties, which should always report individually;
- CAs have explicitly permitted aggregated reporting to those financial entities;
- CAs can request the submission of an individual report from each FE; and
- The list of names and LEI codes need to be provided for all FEs covered by the aggregated report.

44. Accordingly, the ESAs have introduced in the ITS a new Article 7 on aggregated reporting. The ESAs have also introduced changes to the instruction fields in Annex II to the ITS clarifying how specific information about the incident should be reported in an aggregated manner.

4. Draft regulatory technical standards

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content of the reports and notifications for major ICT-related incidents and significant cyber threats and the time limits for reporting of these incidents

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,
Having regard to 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, and in particular Article 20(a) third subparagraph thereof,
Whereas:

(1) Given that Regulation (EU) 2022/2554 aims to harmonise and streamline incident reporting requirements, and to ensure that competent and other relveant authorities receive all necessary information about the major incident in order to take supervisory actions and to prevent potential spill-over effects, the reports for major incidents submitted from financial entities to competent authorities should provide essential and exhaustive information about the incident, in a consistent and standardised manner for all financial entities within the scope of Regulation (EU) 2022/2554.

(2) With a view to ensure the harmonisation of the reporting requirements for major incidents and to maintain a consistent approach with Directive (EU) 2022/2555, the time limits for reporting major incidents should be consistent for all types of financial entities. The time limits should also be consistent with, to the greatest extent possible, and at least equivalent in effect to the requirements set out in Directive (EU) 2022/2555.

(3) In order to take proper action, competent authorities need to receive information about the major incident at the very early stages after the incident has been classified as major. Consequently, the timeline for submitting the initial notification should be as short as possible after classification of the incident but also providing flexibility for financial entities, especially for non-time critical service business models, with a longer timeline after financial entities become aware of the incident in case financial entities require more time to handle the incident. To avoid imposing an undue reporting burden to the financial entity at a time when it will be handling with the incident, the content of such initial notification should be limited to the most significant information.

(4) Given that, after having received the initial notification, competent authorities will need more detailed information about the incident with the intermediate report and the full set of relevant information with the final report to further assess the situation and evaluate supervisory actions they may want to take, the reporting timelines should be such to allow competent authorities to receive the information timely, while ensuring financial entities have sufficient time to obtain complete and accurate information.

(5) In accordance with the proportionality requirement set out in Article 20(a), second sub-paragraph of Regulation (EU) 2022/2554, the reporting timelines should not pose burden to microenterprises and other financial entities that are not significant. Therefore, the reporting timelines should take into account, in particular weekends and bank holidays.

(6) Since significant cyber threats are to be reported on a voluntary basis, the requested information should not pose burden to financial entities to obtain and should be more limited than the information requested for major incidents.

(7) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Supervisory Authorities.

(8) The European Supervisory Authorities have conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the […] Stakeholder Group established in accordance with Article 37 of Regulations (EU) No 1093/2010, 1094/2010 and 1095/2010 of the European Parliament and of the Council[1]

HAS ADOPTED THIS REGULATION:

Article 1
General provisions

[1] Regulation (EU) No 109x/2010 of the European Parliament and of the Council ...[+*full title*] (OJ L [number], [date dd.mm.yyyy], [p.].).

Financial entities shall provide the initial notification, the intermediate report or the final report with the content as set out in this Regulation following the description and instructions as set out in the Implementing Regulation [insert reference once published in OJ].

Article 2
General information to be provided in the major incident initial notification, intermediate and final reports

When submitting the initial notification, the intermediate report and the final report, financial entities shall provide the following general information:

a) the type of report as referred to in Article 19(4) of Regulation (EU)2022/2554;
b) name, LEI code of the financial entity and specify, which of the type of entities referred to in Article 2(1) of Regulation (EU)2022/2554 it is authorised or registered as;
c) name and identification code of the entity submitting the report for the financial entity;
d) names and LEI codes of all financial entities covered in the aggregated report, where applicable.
e) contact details of the contact persons responsible for communicating with the competent authority;
f) identification of the parent undertaking of the group, where applicable; and
g) reporting currency.

Article 3
Content of initial notifications

Financial entities shall provide at least the following information about the incident in the initial notification:

a) incident reference code
b) date and time of detection and classification of the incident;
c) description of the incident;
d) classification criteria that triggered the incident report as set out in [Articles 1 to 8 of Delegated Regulation [insert number once published in official journal];
e) members States impacted by the incident, where applicable;
f) information on how the incident has been discovered;
g) information about the origin of the incident, where available;
h) indication whether a business continuity plan has been activated;
i) information about the reclassification of the incident from major to non-major, where applicable; and
j) other information, where available.

Article 4
Content of intermediate reports

Financial entities shall provide at least the following information about the incident in the intermediate report:

a) incident reference code provided by the competent authority, where applicable;
b) date and time of occurrence of the incident;
c) date and time when regular activities have been restored, where applicable;
d) information about the classification criteria that triggered the incident report;
e) type of the incident;
f) threats and techniques used by the threat actor, where applicable;
g) affected functional areas and business processes;
h) affected infrastructure components supporting business processes;
i) impact on the financial interest of clients;
j) information about reporting to other authorities;
k) temporary actions/measures taken or planned to be taken to recover from the incident; and
l) information on indicators of compromise, where applicable.

Article 5
Content of final reports

Financial entities shall provide the following information about the incident in the final report:

a) information about the root causes of the incident
b) dates and times when the incident was resolved and the root cause addressed;
c) information on the incident resolution;
d) information relevant for resolution authorities, where applicable;
e) information about direct and indirect costs and losses stemming from the incident and information about financial recoveries; and
f) information about recurring incidents, where applicable.

Article 6
Time limits for the initial notification and intermediate report and final reports referred to in Article 19(4) of Regulation (EU)2022/2554

1. The time limits for the submission of the initial notification and the intermediate and final reports as referred to in Article 19(4)(a) to (c) of Regulation (EU)2022/2554 shall be as follows:
    a) the initial report shall be submitted as early as possible within 4 hours from the moment of classification of the incident as major, but no later than 24 hours from the moment the financial entity has become aware of the incident;

b) An intermediate report shall be submitted the latest within 72 hours from the submission of the initial notification even where the status or the handling of the incident have not changed as referred to in Article 19(4)(b) of Regulation (EU) 2022/2554. Financial entities shall submit without undue delay an updated intermediate report, in any case, when regular activities have been recovered.
c) the final report shall be submitted no later than one month from the submission of the latest updated intermediate report.

2. Where an incident that has not been classified as major within the 24 hours is classified as major at a later stage, the financial entity shall submit the initial notification within the four-hours after the classification of the incident.
3. Where financial entities are unable to submit the initial notification, intermediate report or final report within the timelines as set out in paragraph 1, financial entities shall inform the competent authority without undue delay, but no later than the respective time limit for submission of the notification/report, and shall explain the reasons for the delay.
4. Where the time limit for submission of an initial notification, intermediate report or a final report falls on a weekend day or a bank holiday in the Member State of the reporting financial entity, the financial entity may submit the initial notification, intermediate or final reports by noon of the next working day.
5. Paragraph 4 shall not apply for the submission of an initial notification and an intermediate report by credit institutions, central counterparties, operators of trading venues, and other financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, or financial entities declared as significant or systemic by the competent authority. In this case, the financial entities shall apply the time limits set out in paragraph 1.

Article 7
Content of the voluntary notification of significant cyber threat

The content of the notification in relation to significant cyber threats in accordance with Article 19(2) of Regulation (EU) 2022/2554 shall cover:

a) general information about the reporting entity as set out in Article 4;
b) date and time of detection of the significant cyber threat and any other relevant timestamps related to the threat;
c) description of the significant cyber threat;
d) information about the potential impact of the cyber threat on the financial entity, its clients and/or financial counterparts;
e) the classification criteria that would have triggered a major incident report, if the cyber threat had materialised;
f) information about the status of the cyber threat and any changes in the threat activity;

g) description of the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, where applicable; and
h) information about notification of the cyber threat to other financial entities or authorities;
i) information on indicators of compromise, where applicable; and
j) other relevant information, where available.

Article 8
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union.*

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission

The President

5. Draft implementing technical standards

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down implementing technical standards for the application of [Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 and in particular Article 20 (b) thereof,

Whereas:

1. In order to ensure consistent reporting of major incidents and submission of good quality data, it should be specified which data fields need to be provided by financial entities at various stages of the reporting, when providing initial notification, intermediate and final reports as referred to in Article 19(4) of Regulation (EU) 2024/2554[2]. It is important that information provided over the different reporting stages until the final report is presented in a way that allows for a single overview. Therefore, there should be a single template which covers all necessary information

[2] 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)

throughout the reporting stages that should be used for the submission of the initial notification, the intermediate and final report.

2. Financial entities should complete those data fields of the template, which correspond to the information requirements of the respective notification or report. However, where financial entities have information which they are required to provide at a later reporting stage, i.e. the intermediate or final report as relevant, they should be allowed to anticipate that data and complete those data fields and provide to the competent authorities.

3. The design of the template and data fields should also enable the reporting of multiple or recurring incidents, since those incidents may constitute a major incident in accordance with Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.

4. In order to ensure accurate and up to date information, financial entities should update the previously submitted information when submitting the intermediate and final report, respectively, and should reclassify major incidents as non-major, where necessary.

5. The legal identification of entities within the scope of this Implementing Regulation should be aligned with the identifiers specified in the Commission Implementing Regulation specifying Art. 28(9) of Regulation (EU) 2022/2554.

6. To identify more easily the impact of an incident having occurred at or being caused by a third-party provider affecting multiple financial entities within a single Member State, and to reduce the reporting effort for financial entities, the reporting template should allow for the submission of an aggregated report covering aggregated information about the impact of the incident on all impacted financial entities that have classified the incident as major.

7. The design of the template should be technology and reporting format neutral to allow for its integration into various incident reporting solutions that already exist or may be developed for the implementation of the requirements of the Regulation (EU) 2022/2554.

8. The design of the reporting templates and data fields should facilitate the reporting of major ICT-related incidents by third parties to whom financial entities outsourced their reporting obligation in accordance with Article 19(5) of Regulation (EU) 2022/2554.

9. This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Supervisory Authorities (ESAs).

10. The ESAs have conducted open public consultations on the draft implementing technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulations (EU) No 1093/2010, 1094/2010, 1095/2010 of the European Parliament and of the Council,

HAS ADOPTED THIS REGULATION:

Article 1

Standard form for reporting of ICT-related major incidents

1. Financial entities shall use the template in Annex I to submit the initial notification, intermediate and final report as follows:

   (a) Where an initial notification is submitted, financial entities shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 3 of Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554. Financial entities may complete data fields, the completion of which is not required for an initial notification, but for an intermediate or final report, where they have the relevant information.

   (b) Where an intermediate report is submitted, financial entities shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 4 of Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554. Financial entities may complete data fields, the completion of which is not required for the intermediate report, but for the final report, where they have the relevant information.

   (c) Where a final report is submitted, financial entities shall complete the data fields of the template be completed which correspond to the information to be provided in accordance with Article 5 of Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554.

2. Financial entities shall ensure that the information contained in the initial notification, intermediate and final report is complete and accurate.

3. Where accurate data is not available at the time of reporting for the initial notification or the intermediate report, the financial entity shall provide estimated values based on other available data and information to the extent possible.

4. When submitting an intermediate or final report, financial entities shall update, where applicable, the information that was previously provided with the initial notification or the intermediate report.

5. Financial entities shall follow the data glossary and instructions set out in Annex II when completing the template in Annex I.

Article 2

Submission of initial notification, intermediate and final reports together

Financial entities may combine the submission of the initial notification, intermediate report and/or final report to provide two or all of those at the same time, where regular activities have been recovered and/or the root cause analysis has been completed, provided that the

timelines set out in Article 6 of the Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554 are met.

Article 3

Recurring incidents

Where the information is provided for recurring incidents, which do not individually meet the criteria for a major ICT related incident but do so cumulatively in accordance with Article 8(2) of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, financial entities shall provide aggregated information regarding such incidents.

Article 4

Use of secure channels in case of deviation from established channels or time limits

1. Financial entities shall use secure electronic channels set out by their competent authority to submit the initial notification and intermediate and final reports .
2. Where financial entities are unable to use established channels to submit incident notifications or reports to their competent authority, financial entities shall inform the competent authority about the major incident through other secure means, after consulting with or as previously agreed with the competent authority. If required by the competent authority, financial entities shall resubmit the initial notification, intermediate or final report through the established channels under paragraph 1 once they are able to do so.

Article 5

Reclassification of major incidents

Where after further assessment of the incident, the financial entity reaches the conclusion that the incident previously reported as major at no time fulfilled the classification criteria and thresholds in accordance with Article 18(4) of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, the financial entity shall indicate it has reclassified the incident from major to non-major and shall submit the information related to the reclassification of the major incident as non-major by completing the template in Annex II in relation to the fields ‘type of report’ and ‘other information’.

Article 6

Notification of outsourcing of the reporting obligation

Where financial entities intend to outsource the incident reporting obligation in accordance with Article 19(5) of Regulation (EU) 2022/2554, including where such outsourcing will be part of a general and/or long-term outsourcing arrangement, they shall inform their competent authority prior to the first notification or reporting under such an arrangement and the latest as soon as the outsourcing arrangement has been concluded. Financial entities shall

provide to the competent authority the name, contact details, and an identification code of the third-party that will submit the incident notifications or reports for them. Financial entities shall also inform their competent authority, where such outsourcing no longer takes place or has been cancelled.

Article 7

Aggregated reporting

1. A third-party provider, to whom reporting obligations have been outsourced, may aggregate the information about a major ICT-related incident impacting multiple financial entities in one single notification or report, and submit it to the competent authority for all impacted financial entities, provided that all of the following conditions are met:
   a) the major incidents to be reported originate from or is being caused by a third-party provider;
   b) this third-party provider provides the relevant ICT service to more than one financial entity, or to a group, in the Member State;
   c) the incident is classified as major individually by each financial entity covered in the aggregated report,
   d) the incident affects financial entities within a single Member State and the aggregated report relates to financial entities which are supervised by the same competent authority;
   e) the financial entities affected by the incident have outsourced reporting obligations to a third-party provider in accordance with Art. 19(5) of Regulation (EU) 2022/2554 and Article 6 of this Regulation, and
   f) competent authorities have explicitly permitted aggregated reporting to those financial entities.
2. Significant credit institutions in accordance with Article 6(4) of Regulation (EU) No 1024/2013, operators of trading venues and central counterparties shall be required to submit an incident notification or report at solo level to their competent authority.
3. Upon request by the competent authority, financial entities shall submit a separate individual incident notification or report.

Article 8

Standard form for voluntary reporting of notification of significant cyber threats

1. When notifying the competent authorities of significant cyber threats in accordance with Article 19(2) of Regulation (EU) 2022/2554, financial entities shall use the template in Annex III and follow the data glossary and instructions set out Annex IV.
2. Financial entities shall ensure that the information contained in the cyber threat notification is complete and accurate.

Article 9

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President

ANNEX I

Templates for the reporting of major incidents

Number of field	Data field	
General information about the financial entity		
1.1	Type of report	
1.2	Name of the entity submitting the report	
1.3	Identification code of the entity submitting the report	
1.4	Type of the affected financial entity	
1.5	Name of the financial entity affected	
1.6	LEI code of the financial entity affected	
1.7	Primary contact person name	
1.8	Primary contact person email	
1.9	Primary contact person telephone	
1.10	Second contact person name	
1.11	Second contact person email	
1.12	Second contact person telephone	
1.13	Name of the ultimate parent undertaking	
1.14	LEI code of the ultimate parent undertaking	
1.15	Reporting currency	
Content of the initial notification		
2.1	Incident reference code provided by the financial entity	
2.2	Date and time of detection of the incident	
2.3	Date and time of classification of the incident as major	
2.4	Description of the incident	

Number of field	Data field	
2.5	Classification criteria that triggered the incident report	
2.6	Materiality thresholds for the classification criterion 'Geographical spread'	
2.7	Discovery of the incident	
2.8	Indication whether the incident originates from a third-party provider or another financial entity	
2.9	Activation of business continuity plan, if activated	
2.10	Other information	
Content of the intermediate report		
3.1	Incident reference code provided by the competent authority	
3.2	Date and time of occurrence of the incident	
3.3	Date and time when services, activities and/or operations have been restored	
3.4	Number of clients affected	
3.5	Percentage of clients affected	
3.6	Number of financial counterparts affected	
3.7	Percentage of financial counterparts affected	
3.8	Impact on relevant clients or financial counterparts	
3.9	Number of affected transactions	
3.10	Percentage of affected transactions	
3.11	Value of affected transactions	
3.12	Information whether the numbers are actual or estimates, or whether there has not been any impact	
3.13	Reputational impact	
3.14	Contextual information about the reputational impact	
3.15	Duration of the incident	
3.16	Service downtime	
3.17	Information whether the numbers for duration and service downtime are actual or estimates.	
3.18	Types of impact in the Member States	

Number of field	Data field	
3.19	Description of how the incident has an impact in other Member States	
3.20	Materiality thresholds for the classification criterion 'Data losses'	
3.21	Description of the data losses	
3.22	Classification criterion 'Critical services affected'	
3.23	Type of the incident	
3.24	Other types of incidents	
3.25	Threats and techniques used by the threat actor	
3.26	Other types of techniques	
3.27	Information about affected functional areas and business processes	
3.28	Affected infrastructure components supporting business processes	
3.29	Information about affected infrastructure components supporting business processes	
3.30	Impact on the financial interest of clients	
3.31	Reporting to other authorities	
3.32	Specification of 'other' authorities	
3.33	Temporary actions/measures taken or planned to be taken to recover from the incident	
3.34	Description of any temporary actions and measures taken or planned to be taken to recover from the incident	
3.35	Indicators of compromise	
Content of the final report		
4.1	High-level classification of root causes of the incident	
4.2	Detailed classification of root causes of the incident	
4.3	Additional classification of root causes of the incident	
4.4	Other types of root cause types	
4.5	Information about the root causes of the incident	

Number of field	Data field	
4.6	Incident resolution summary	
4.7	Date and time when the incident root cause was addressed	
4.8	Date and time when the incident was resolved	
4.9	Information if the permanent resolution date of the incident differs from the initially planned implementation date	
4.10	Assessment of risk to critical functions for resolution purposes	
4.11	Information relevant for resolution authorities	
4.12	Materiality threshold for the classification criterion 'Economic impact'	
4.13	Amount of gross direct and indirect costs and losses	
4.14	Amount of financial recoveries	
4.15	Information whether the non-major incidents have been recurring	
4.16	Date and time of occurrence of recurring incidents	

ANNEX II

Data glossary and instructions for the reporting of major incidents

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
General information about the financial entity					
1.1. Type of report	Indicate the type of incident notification or report being submitted to the competent authority.	Yes	Yes	Yes	Choice: - initial notification - intermediate report - final report - major incident reclassified as non-major
1.2. Name of the entity submitting the report	Full legal name of the entity submitting the report.	Yes	Yes	Yes	Alphanumeric
1.3. Identification code of the entity submitting the report	Identification code of the entity submitting the report. Where financial entities submit the notification/report, the identification code is to be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020. Where a third-party provider submits a report for a financial entity, they can use an identification code as specified in the Commission Implementing Regulation specifying Art. 28(9) from Regulation (EU) 2022/2554.	Yes	Yes	Yes	Alphanumeric
1.4. Type of the affected	Type of the entity under Article 2.1(a)-(t) of DORA for whom the report is submitted.	Yes	Yes	Yes	Choice (multiselect): - credit institution

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
financial entity	In case of aggregated reporting in accordance with Article 7, the different types of financial entities covered in the aggregated report to be selected.				- payment institution - exempted payment institution - account information service provider - electronic money institution - exempted electronic money institution - investment firm - crypto-asset service provider - issuer of asset-referenced tokens - central securities depository - central counterparty - trading venue - trade repository - manager of alternative investment fund - management company - data reporting service provider

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
					- insurance and reinsurance undertaking - insurance intermediary, reinsurance intermediary and ancillary insurance intermediary - institution for occupational retirement provision - credit rating agency - administrator of critical benchmarks - crowdfunding service provider - securitisation repository
1.5. Name of the financial entity affected	Full legal name of the financial entity affected by the major ICT-related incident and required to report the major incident to their competent authority under Article 19 of Regulation (EU) 2022/2554. In case of aggregated reporting: (a) list of all names of the financial entities affected by the major ICT-related incident, separated by a semicolon. (b) the third-party provider submitting a major incident notification or in an aggregated manner in accordance with Article 7, to list the names	Yes, if the financial entity affected by the incident is different from the entity submitting	Yes, if the financial entity affected by the incident is different from the entity submitting the report	Yes, if the financial entity affected by the incident is different from the entity submitting	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	of all financial entities impacted by the incident, separated by a semicolon.	the report and in case of aggregated reporting.	and in case of aggregated reporting	the report and in case of aggregated reporting	
1.6. LEI code of the financial entity affected	Legal Entity Identifier (LEI) of the financial entity affected by the major ICT-related incident assigned in accordance with the International Organisation for Standardisation. In case of aggregated reporting (a) a list of all LEI codes of the financial entities affected by the major ICT-related incident, separated by a semicolon. (b) the third-party provider submitting a major incident notification or report in an aggregated manner in accordance with Article 7 to list the LEI codes of all financial entities impacted by the incident, separated by a semicolon. The order of appearance of LEI codes and FE names has to be the same so that it is possible to match name and LEI.	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting	Unique 20 alphanumeric character code, based on ISO 17442-1:2020
1.7. Primary contact person name	Name and surname of the primary contact person of the financial entity	Yes	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	In case of aggregated reporting in accordance with Article 7, the name of the primary contact person in the entity submitting the aggregated report.				
1.8. Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication In case of aggregated reporting in accordance with Article 7, the email of the primary contact person in the entity submitting the aggregated report.	Yes	Yes	Yes	Alphanumeric
1.9. Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication In case of aggregated reporting in accordance with Article 7, the telephone number of the primary contact person in the entity submitting the aggregated report. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Yes	Yes	Yes	Alphanumeric
1.10. Second contact person name	Name and surname of the second contact person or the name of the responsible team of the financial entity or an entity submitting the report on behalf of the financial entity	Yes	Yes	Yes	Alphanumeric
1.11. Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication	Yes	Yes	Yes	Alphanumeric
1.12. Second contact person telephone	Telephone number of the second contact person or a team that can be used by the competent authority for follow-up communication. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Yes	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
1.13. Name of the ultimate parent undertaking	Name of the ultimate parent undertaking of the group in which the affected financial entity belongs to, where applicable	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Alphanumeric
1.14. LEI code of the ultimate parent undertaking	LEI of the ultimate parent undertaking of the group in which the affected financial entity belongs to, where applicable. Assigned in accordance with the International Organisation for Standardisation.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Unique 20 alphanumeric character code, based on ISO 17442-1:2020.
1.15. Reporting currency	Currency used for the incident reporting	Yes	Yes	Yes	Choice populated by using ISO 4217 currency codes
Content of the initial notification					
2.1. Incident reference code provided by the financial entity	Unique reference code issued by the financial entity unequivocally identifying the major incident. In case of aggregated reporting in accordance with Article 7, the incident reference code assigned by the third-party provider.	Yes	Yes	Yes	Alphanumeric
2.2. Date and time of detection of the incident	Date and time at which the financial entity has become aware of the ICT-related incident. For recurring incidents, the data and time at which the last ICT-related incident was detected.	Yes	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
2.3. Date and time of classification of the incident as major	Date and time when the ICT-related incident was classified as major according to the classification criteria established in Regulation (EU) 2023/XXXX	Yes	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
2.4. Description of the incident	Description of the most relevant aspects of the major ICT-related incident. Financial entities shall provide a high-level overview of the following information such as possible causes, immediate impacts, systems affected, and others. Financial entities, shall include, where known or reasonably expected, whether the incident impacts third-party providers or other financial entities, the type of provider or financial entity, their name and their respective identification codes. In subsequent reports, the field content can evolve over time to reflect the ongoing understanding of the ICT-related incident and include also a description of any other relevant information about the incident not captured by the data fields, including the internal severity assessment by the financial entity (e.g. very low, low, medium, high, very high) and an indication of the level and name of most senior decision structures that has been involved in response to the incident.	Yes	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
2.5. Classification criteria that triggered the incident report	Classification criteria under Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 that have triggered determination of the ICT-related incident as major and subsequent notification and reporting. In the case of aggregated reporting in accordance with Article 7, the classification criteria that have triggered determination of the ICT-related incident as major for at least one or more financial entities.	Yes	Yes	Yes	Choice (multiple): - Clients, financial counterparts and transactions affected - Reputational impact - Duration and service downtime - Geographical spread - Data losses - Critical services affected Economic impact
2.6. Materiality thresholds for the classification criterion 'Geographical spread'	EEA Member States impacted by the ICT-related incident Financial entities shall have regard to Articles 4 and 12 of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details.	Yes, if 'Geographical spread' threshold is met.	Yes, if 'Geographical spread' threshold is met.	Yes, if 'Geographical spread' threshold is met.	Choice (multiple) populated by using ISO 3166 ALPHA-2 of the affected countries
2.7. Discovery of the incident	Indication of how the incident has been discovered.	Yes	Yes	Yes	Choice: - IT Security - Staff - Internal audit - External audit - Clients

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
					- Financial counterparts - Third-party provider - Attacker - Monitoring systems - Authority/agency/law enforcement body - Other
2.8. Indication whether the incident originates from a third-party provider or another financial entity	Indication whether the incident originates from a third-party provider or another financial entity Financial entities shall indicate whether the incident originates from a third-party provider or another financial entity (including financial entities belonging to the same group as the reporting entity) and the name and identification code of the third-party provider or financial entity.	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity	Alphanumeric
2.9. Activation of business continuity plan, if activated	Indication of whether there has been a formal activation of their business continuity response measures.	Yes	Yes	Yes	Boolean (Yes or No)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
2.10. Other information	Any further information not covered in the template. Where the incident has been reclassified as non-major, financial entities shall provide a description of the reasons why the incident does not fulfil the criteria to be considered as major and is not expected to fulfil them any longer before it is resolved.	Yes, if there is other information not covered in the template or if the incident has been reclassified as non-major.	Yes, if there is other information not covered in the template or if the incident has been reclassified as non-major	Yes, if there is other information not covered in the template or if the incident has been reclassified as non-major	Alphanumeric
Content of the intermediate report					
3.1. Incident reference code provided by the competent authority	Unique reference code assigned by the competent authority at the time of receipt of the initial notification to unequivocally identify the major incident.	No	Yes, if applicable	Yes, if applicable	Alphanumeric
3.2. Date and time of occurrence	Date and time at which the ICT-related incident has occurred, if different from the time of the financial entity has become aware of the incident	No	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
of the incident	For recurring incidents, the date and time at which the last ICT-related incident has occurred				
3.3. Date and time when services, activities and/or operations have been restored	Information on the date and time of the restoration of the services, activities and/or operations affected by the incident	No	Yes, if data field 3.16. 'Service downtime' has been populated	Yes, if data field 3.16. 'Service downtime' has been populated	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
3.4. Number of clients affected	Number of clients affected by the ICT-related incident, which may be natural or legal persons, that make use of the service provided by the financial entity Financial entities shall have regard of Articles 1.1 and 9.1(b) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual number of clients impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods. In the case of aggregated reporting in accordance with Article 7, the total number of clients affected across all financial entities.	No	Yes	Yes	Numerical integer

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.5. Percentage of clients affected	Percentage of clients affected by the ICT-related incident in relation to the total number of clients that make use of the affected service provided by the financial entity. In case of more than one service affected, these shall be provided in an aggregated manner. Financial entities shall have regard of Articles 1.1 and 9.1(a) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual percentage of clients impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods. In the case of aggregated reporting in accordance with Article 7, the sum of all affected clients divided by the total number of clients of all impacted financial entities.	No	Yes	Yes	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up
3.6. Number of financial counterparts affected	Number of financial counterparts affected by the ICT-related incident, that have concluded a contractual arrangement with the financial entity Financial entities shall have regard to Article 1.2 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual number of financial counterparts impacted cannot be determined, the financial entity shall	No	Yes	Yes	Numerical integer

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	use estimates based on available data from comparable reference periods. In the case of aggregated reporting in accordance with Article 7, the total number of financial counterparts affected across all financial entities.				
3.7. Percentage of financial counterparts affected	Percentage of financial counterparts affected by the ICT-related incident, in relation to the total number of financial counterparts that have concluded a contractual arrangement with the financial entity Financial entities shall have regard to see Articles 1.1 and 9.1(c) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual percentage of financial counterparts impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods. In the case of aggregated reporting in accordance with Article 7, indicate the sum of all affected financial counterparts divided by the total number of financial counterparts of all impacted financial entities.	No	Yes	Yes	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.8. Impact on relevant clients or financial counterpart	Any identified impact on relevant clients or financial counterpart in accordance with Articles 1.3 and 9.1(f) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.	No	Yes, if 'Relevance of clients and financial counterparts ' threshold is met	Yes, if 'Relevance of clients and financial counterparts' threshold is met	Boolean (Yes or No)
3.9. Number of affected transactions	Number of transactions affected by the ICT-related incidents. In accordance with article 1.4 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, the financial entity shall take into account all affected domestic and cross-border transactions containing a monetary amount that have at least one part of the transaction carried out in the EU. Where the actual number of transactions impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods. In the case of aggregated reporting in accordance with Article 7, indicate the total number of transactions affected across all financial entities.	No	Yes, if any transaction has been affected by the incident	Yes, if any transaction has been affected by the incident	Numerical integer

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.10. Percentage of affected transactions	Percentage of affected transactions in relation to the daily average number of domestic and cross-border transactions carried out by the financial entity related to the affected service Financial entities shall have regard of Article 1.4 and article 9.1(d) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554. Where the actual percentage of transactions impacted cannot be determined, the financial entity shall use estimates. In the case of aggregated reporting in accordance with Article 7, the sum of the number of all affected transactions divided by the total number of transactions of all impacted financial entities.	No	Yes, if any transaction has been affected by the incident	Yes, if any transaction has been affected by the incident	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up
3.11. Value of affected transactions	Total value of the transactions affected by the ICT-related incident in accordance with Article 1.4 and article 9.1e of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554. Where the actual value of transactions impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods. The monetary amount is to be reported as a positive value.	No	Yes, if any transactions have been affected by the incident	Yes, if any transaction has been affected by the incident	Monetary The data point shall be reported in units using a minimum precision equivalent to thousands of units (e.g. 2.5 instead of EUR 2500).

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	In the case of aggregated reporting in accordance with Article 7, the total value of the transactions affected across all financial entities.				
3.12. Information whether the numbers are actual or estimates, or whether there has not been any impact	Information whether the values reported in the data fields 3.4. to 3.11. are actual or estimates, or whether there has not been any impact.	No	Yes	Yes	Choice (multiple): - Actual figures for clients affected - Actual figures for financial counterparts affected - Actual figures for transactions affected - Estimates for clients affected - Estimates for financial counterparts affected - Estimates for transactions affected - No impact on clients - No impact on financial counterparts - No impact on transactions
3.13. Reputational impact	Information about the reputational impact resulting from the incident in accordance with Article 2 and Article 10 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.	No	Yes, if 'Reputational	Yes, if 'Reputational impact'	Choice (multiple): - the incident has been reflected in the media;

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	In the case of aggregated reporting in accordance with Article 7, the reputational impact categories that apply to at least one financial entity.		impact' criterion met	criterion met	- the incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business relation-ships - the financial entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the incident - the financial entity will or is likely to lose clients or financial counterparts with a material impact on its business as a result of the incident
3.14. Contextual information about the reputational impact	Information describing how the ICT-related incident has affected or could affect the reputation of the financial entity, such as infringements of law, regulatory requirements not met, number of client complaints and others. The contextual information Include additional information, such as type of media (e.g. traditional, social media, blogs, social networks,	No	Yes, if 'Reputational impact' criterion met.	Yes, if 'Reputational impact' criterion met.	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	streaming platforms) and media coverage, including reach of the media (local, national, international). It should be noted that media coverage in this context does not mean only a few negative comments by followers or users of social networks. The financial entity shall also indicate whether the media coverage highlighted significant risks for its clients in relation to the incident, such as the risk of the financial entity's insolvency or the risk of losing funds. Financial entities shall also indicate whether it has provided information to the media that served to reliably inform the public about the incident and its consequences. Financial entities may also indicate whether there was false information in the media in relation to the incident, including information based on deliberate misinformation spread by threat actors, or information relating to or illustrating defacement of the financial entity's website.				
3.15. Duration of the incident	The duration of the ICT-related incident shall be measured from the moment the incident occurs until the moment when the incident is resolved Where financial entities are unable to determine the moment when the incident has occurred, they shall measure the duration of the incident from the earlier between the moment it was detected and the moment when it has been recorded in network or system logs or other data sources. Where financial entities do not yet know the moment when	No	Yes	Yes	DD:HH:MM

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	the incident will be resolved, they shall apply estimates. The value shall be expressed in days, hours and minutes. In the case of aggregated reporting in accordance with Article 7, the longest duration of the incident in case of differences between financial entities.				
3.16. Service downtime	Service downtime measured from the moment the service is fully or partially unavailable to clients, financial counterparts or other internal or external users to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident. Where the service downtime causes a delay in the provision of service after regular activities/operations have been restored, the downtime shall be measured from the start of the incident to the moment when that delayed service is provided. Where financial entities are unable to determine the moment when the service downtime has started, they shall measure the service downtime from the earlier between the moment it was detected and the moment when it has been recorded. In the case of aggregated reporting in accordance with Article 7, the longest duration of the service downtime in case of differences between financial entities.	No	Yes, if the incident has caused a service downtime	Yes, if the incident has caused a service downtime	DD:HH:MM
3.17. Information whether the numbers for	Information whether the values reported in data fields 3.15 and 3.16. are actual or estimates.	No	Yes, if 'Duration and service	Yes, if 'Duration and service downtime'	Choice: - Actual figures - Estimates

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
duration and service downtime are actual or estimates.			downtime' criterion met	criterion met	- Actual figures and estimates - No information available
3.18. Types of impact in the Member States	Type of impact in the respective EEA Member States. Indication of whether the major ICT-related incident has had an impact in other EEA Member States (other than the Member State of the competent authority to which the incident is directly reported), in accordance with Article 4 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, and in particular with regard to the significance of the impact in relation to: a) clients and financial counterparts affected in other Member States; or b) Branches or other financial entities within the group carrying out activities in other Member States; or c) Financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services.	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Choice (multiple): - clients - financial counterparts - branch of the financial entity - financial entities within the group carrying out activities in the respective Member State - financial market infrastructure - third-party providers that may be common with other financial entities
3.19. Description of how the incident has an impact in	Description of the impact and severity of the incident in each affected Member State Information should include the assessment of impact and severity on: a) clients; or	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
other Member States	b) financial counterparts; or c) Branches of the financial entity; or d) Other financial entities within the group carrying out activities in the respective Member State; or e) Financial market infrastructures; or f) Third-party providers that may be common with other financial entities as applicable in other member state(s).				
3.20. Materiality thresholds for the classification criterion 'Data losses'	Type of data losses that the ICT-related incident entails in relation to availability, authenticity, integrity and confidentiality of data. In accordance with Articles 5 and 13 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554. In case of aggregated reporting in accordance with Article 7, the data losses affecting at least one financial entity.	No	Yes, if 'Data losses' criterion is met	Yes, if 'Data losses' criterion is met	Choice (multiple): - availability - authenticity - integrity - confidentiality
3.21. Description of the data losses	Description of the impact of the incident on availability, authenticity, integrity and confidentiality of critical data In accordance with Articles 5 and 13 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554. Information about the impact on the implementation of the business objectives of the financial entity and/or on meeting regulatory requirements.	No	Yes, if 'Data losses' criterion is met	Yes, if 'Data losses' criterion is met	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	As part of the information provided, financial entities shall indicate whether the data affected is client data, other entities' data (e.g. financial counterparts) or data of the financial entity itself. The financial entity may also indicate the type of data involved in the incident - in particular, whether the data is confidential and what type of confidentiality was involved (e.g. commercial/business confidentiality, personal data, professional secrecy: banking secrecy, insurance secrecy, payment services secrecy, etc.). The information may also include possible risks associated with the data losses, such as whether the data affected by the incident can be used to identify individuals and could be used by the threat actor to obtain credit or loans without their consent, to conduct spear phishing attacks, to disclose information publicly. In the case of aggregated reporting in accordance with Article 7, a general description of the impact of the incident on the affected financial entities. Where there are differences of the impact, the description of the impact should clearly indicate the specific impact on the different financial entities.				
3.22. Classification criterion 'Critical services affected'	Information related to the criterion 'Critical services affected'. In accordance with Articles 6 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, including information about:	No	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	- the affected services or activities that require authorisation, registration or that are supervised by competent authorities; and/or - the ICT services or network and information systems that support critical or important functions of the financial entity; and - the nature of the malicious and unauthorised access to the network and information systems of the financial entity. In the case of aggregated reporting in accordance with Article 7, the impact on critical services that apply to at least one financial entity.				
3.23. Type of the incident	Classification of incidents by type.	No	Yes	Yes	Choice (multiple): - Cybersecurity-related - Process failure - System failure - External event - Payment-related - Other (please specify)
3.24. Other types of incidents	Other types of incidents, where financial entities have selected 'other' type of incidents in the data field 3.23, financial entities shall specify the type of incident.	No	Yes, if 'other' type of incidents is selected in data field 3.23	Yes, if 'other' type of incidents is selected in data field 3.23	Alphanumeric
3.25. Threats and	Indicate the threats and techniques used by the threat actor.	No	Yes, if the type of the	Yes, if the type of the	Choice (multiple):

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
techniques used by the threat actor	The following threats and techniques shall be considered: 1. Social engineering, including phishing 2. (D)DoS 3. Identity theft 4. Data encryption for impact, including ransomware 5. Resource hijacking 6. Data exfiltration and manipulation, excluding identity theft 7. Data destruction 8. Defacement 9. Supply-chain attack 10. Other (please specify)		incident is 'cybersecurity-related' in field 3.23	incident is 'cybersecurity-related' in field 3.23	- Social engineering (including phishing) - (D)DoS - Identity theft - Data encryption for impact, including ransomware - Resource hijacking - Data exfiltration and manipulation, including identity theft - Data destruction - Defacement - Supply-chain attack - Other (please specify)
3.26. Other types of techniques	Other types of techniques Where financial entities have selected 'other' type of techniques in data field 3.25, financial entities shall specify the type of technique.	No	Yes, if other' type of techniques is selected in data 3.25	Yes, if other' type of techniques is selected in data 3.25	Alphanumeric
3.27. Information about affected	Indication of the functional areas and business processes that are affected by the incident, including products and services. The functional areas may include but are not limited to:	No	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
functional areas and business processes	• Marketing and business development • Customer service • Product management • Regulatory compliance • Risk management • Finance and accounting • HR and general services • Information Technology Business processes The business processes may include but are not limited to: • Account information • Actuarial services • Acquiring of payment transactions • Authentication/authorization • Authority/client on-boarding • Benefit administration • Benefit payment management • Buying and selling packages insurances policies between insurances • Card payments • Cash management • Cash placement and/or withdrawals • Claim management • Claim process insurance				

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	• Clearing • Corporate loans conglomerates • Collective insurances • Credit transfers • Custody and asset safekeeping • Customer onboarding • Data ingestion • Data processing • Direct debits • Export insurances • Finalizing trades/deals trade floors • Financial instruments placing • Fund accounting • FX money • Investment advice • Investment management • Issuing of payment instruments • Lending management • Life insurance payments process • Money remittance • Net asset calculation • Order • Payment initiation • Policy underwriting issuance				

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	• Portfolio management • Premium collection • Reception/transmission/execution • Reinsurance • Settlement • Transaction monitoring In the case of aggregated reporting in accordance with Article 7, the affected functional areas and business processes that have been impacted in at least one financial entity.				
3.28. Affected infrastructure components supporting business processes	Information on whether infrastructure components (servers, operating systems, software, application servers, middleware, network components, others) supporting business processes have been affected by the incident.	No	Yes	Yes	Choice: - Yes - No - Information not available
3.29. Information about affected infrastructure components	Description on the impact of the incident on infrastructure components supporting business processes including hardware and software. Hardware includes servers, computers, data centres, switches, routers, hubs. Software includes operating systems, applications, databases, security tools, network components, others please specify. The descriptions should include the description or name of affected	No	Yes, if the incident has affected infrastructure components supporting	Yes, if the incident has affected infrastructure component	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
supporting business processes	infrastructure components or systems, which may be complemented with the following information, where available: • Version information • Internal infrastructure/partially outsourced/fully outsourced – third-party provider name • Whether the infrastructure is shared/dedicated across multiple business functions • Relevant resilience/continuity/recovery/ substitutability arrangements in place		business processes	s supporting business processes	
3.30. Impact on the financial interest of clients	Information on whether the incident has impacted financial interest of clients	No	Yes	Yes	Choice: - Yes - No - Information not available
3.31. Reporting to other authorities	Specification of what authorities were informed about the incident. Taking into account the differences resulting from the national legislation of the Member States, the concept of law enforcement authorities should be understood broadly to include public authorities empowered to prosecute cybercrime, including but not limited to police, law enforcement agencies or public prosecutors	No	Yes	Yes	Choice (multiple): - Police/Law Enforcement - CSIRT - Data Protection Authority - National Cybersecurity Agency - None - Other (please specify)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.32. Specification of 'other' authorities	Specification of 'other' types of authorities informed about the incident If selected in Data field 3.31. 'Other' the description shall include more detailed information about the authority to which the information about the incident was submitted.	No	Yes, if 'other' type of authorities have been informed by the financial entity about the incident	Yes, if 'other' type of authorities have been informed by the financial entity about the incident	Alphanumeric
3.33. Temporary actions/measures taken or planned to be taken to recover from the incident	Indication of whether financial entity has implemented (or plan to implement) any temporary actions that have been taken (or planned to be taken) to recover from the incident.	No	Yes	Yes	Boolean (Yes or No)
3.34. Description of any temporary	The information shall include description of the immediate actions taken such as isolation of the incident at the network level, workaround procedures activated, USB ports blocked, Disaster Recovery site	No	Yes, if temporary actions/measures have	Yes, if temporary actions/measures have	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
actions and measures taken or planned to be taken to recover from the incident	activated, any other additional security controls temporarily put in place. Financial entities shall also indicate the date and the time of the implementation of the temporary actions and the expected date of return to the primary site. For any temporary actions that have not been implemented but are still planned, indication of the date by when their implementation is foreseen. If no temporary actions/measures have been taken, please indicate the reason.		been taken or are planned to be taken (data field 3.33)	been taken or are planned to be taken (data field 3.33)	
3.35. Indicators of compromise	Information related to the incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable. The field applies only to the financial entities within the scope of Directive (EU) 2022/2555 and those financial entities financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, where relevant. The IoC provided by the financial entity may include, but not be limited to, the following categories of data: • IP addresses; • URL addresses; • Domains;	No	Yes, if cybersecurity-related is selected as a type of incident in data field 3.23s	Yes, if cybersecurity-related is selected as a type of incident in data field 3.23	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	• File hashes; • Malware data (malware name, file names and their locations, specific registry keys associated with malware activity); • Network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); • E-mail message data (sender, recipient, subject, header, content); • DNS requests and registry configurations; • User account activities (logins, privileged user account activity, privilege escalation); • Database traffic (read/write), requests to the same file. In practice, this type of information may include data relating to, for example, indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to "command and control" servers used by malware (usually domains or IP addresses), URLs relating to phishing sites or websites observed hosting malware or exploit kits, etc				
Content of the final report					
4.1. High-level classification of root	High-level classification of root cause of the incident under the incident types. The following high-level categories shall be considered:	No	No	Yes	Choice (multiple): - Malicious actions - Process failure

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
causes of the incident	1. Malicious actions 2. Process failure 3. System failure/malfunction 4. Human error 5. External event				- System failure/malfunction - Human error - External event
4.2. Detailed classification of root causes of the incident	Detailed classification of root causes of the incident under the incident types. The following detailed categories shall be considered linked to the high-level categories that are reported in data field 4.1: **1. Malicious actions** (if selected, choose one or more the following) a. Deliberate internal actions b. Deliberate physical damage/manipulation/theft c. Fraudulent actions **2. Process failure** (if selected, choose one or more the following): a. Insufficient and/or failure of monitoring and control b. Insufficient/unclear roles and responsibilities c. ICT risk management process failure:	No	No	Yes	Choice (multiple): - Malicious actions: deliberate internal actions - Malicious actions deliberate physical damage/manipulation/theft - Malicious actions: fraudulent actions - Process failure: insufficient and/or failure of monitoring and control - Process failure: insufficient/unclear roles and responsibilities

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	d. Insufficient and/or failure of ICT operations and ICT security operations e. Insufficient and/or failure of ICT project management f. Inadequate of internal policies, procedures and documentation g. Inadequate ICT Systems Acquisition, Development, and Maintenance h. Other (please specify) **3.System failure/malfunction** (if selected, choose one or more the following) a. Hardware capacity and performance: incidents caused by hardware resources which prove inadequate in terms of capacity or performance to fulfil the applicable legislative requirements. b. Hardware maintenance: incidents resulting from inadequate or insufficient maintenance of hardware components, other than "Hardware obsolescence/ageing" as defined below. c. Hardware obsolescence/ageing: This root cause type involves incidents resulting from outdated or aging hardware components. d. Software compatibility/configuration: incidents caused by software components that are incompatible with other software or system configurations. It includes, but it is not limited to, incidents resulting from software conflicts, incorrect settings, or misconfigured parameters that impact the overall system functionality.				- Process failure: ICT risk management process failure: - Process failure: insufficient and/or failure of ICT operations and ICT security operations - Process failure: insufficient and/or failure of ICT project management - Process failure: inadequate of internal policies, procedures and documentation - Process failure: inadequate ICT Systems Acquisition, Development, and Maintenance - Process failure: other (please specify) - System failure: hardware capacity and performance - System failure: hardware maintenance

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	e. Software performance: incidents resulting from software components that exhibit poor performance or inefficiencies, for reasons other than those defined under "Software compatibility/configuration" above. It includes incidents caused by slow response times, excessive resource consumption, or inefficient query execution impacting the performance of the software or system. f. Network configuration: incidents resulting from incorrect or misconfigured network settings or infrastructure. It includes but it is not limited to incidents caused by network configuration errors, routing issues, firewall misconfigurations, or other network-related problems affecting connectivity or communication. g. Physical damage: incidents caused by physical damage to ICT infrastructure which lead to system failures. h. Other (please specify) **4.Human error** (if selected, choose one or more the following) a. Omission (unintentional) b. Mistake c. Skills & knowledge: incidents resulting from a lack of expertise or proficiency in handling ICT systems or processes, that may be caused by inadequate training, insufficient knowledge, or gaps in skills required to perform specific tasks or address technical challenges				- System failure: hardware obsolescence/ageing - System failure : software compatibility/configuration - System failure: software performance - System failure: network configuration - System failure: physical damage - System failure: other (please specify) - Human error**:** omission - - Human error: mistake - Human error: skills & knowledge - Human error: inadequate human resources - Human error miscommunication - Human error: other (please specify)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	d. Inadequate human resources: incidents caused by a lack of necessary resources, such as hardware, software, infrastructure, or personnel. It includes but it is not limited to situations where insufficient resources lead to operational inefficiencies, system failures, or an inability to meet business demands e. Miscommunication f. Other (please specify) **5.External event** (if selected, choose one or more the following) a. Natural disasters/force majeure b. Third-party failures c. Other (please specify) Financial entities shall take into account that for recurring incidents, the specific apparent root cause of the incident.				- External event: natural disasters/force majeure - External event: third-party failures - External event: other (please specify)
4.3. Additional classification of root causes of the incident	Additional classification of root causes of the incident under the incident types. The following additional classification categories shall be considered linked to the detailed categories that reported in data field 4.2. The field is mandatory for the final report if specific values required additional classification listed below are reported in data field 4.2. 2(a) Insufficient and/or failure of monitoring and control:	No	No	Yes	Choice (multiple): - Monitoring of policy adherence - Monitoring of third-party service providers - Monitoring and verification of remediation of vulnerabilities

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	- Monitoring of policy adherence - Monitoring of third-party service providers - Monitoring and verification of remediation of vulnerabilities - Identity and access management - Encryption and cryptography - Logging 2(c) ICT risk management process failure: - Failure in defining accurate risk tolerance levels - Insufficient vulnerability and threat assessments - Inadequate risk treatment measures - Poor management of residual ICT risks 2(d) Insufficient and/or failure of ICT operations and ICT security operations: - Vulnerability and patch management - Change management - Capacity and performance management - ICT asset management and information classification - Backup and restore - Error Handling 2(g) Inadequate ICT Systems Acquisition, Development, and Maintenance: - Inadequate ICT Systems Acquisition, Development, and Maintenance Insufficient and /or failure of software testing				- Identity and access management - Encryption and cryptography - Logging - Failure in defining accurate risk tolerance levels - Insufficient vulnerability and threat assessments - Inadequate risk treatment measures - Poor management of residual ICT risks - Vulnerability and patch management - Change management - Capacity and performance management - ICT asset management and information classification - Backup and restore - Error Handling

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
					- Inadequate ICT Systems Acquisition, Development, and Maintenance - Insufficient and /or failure of software testing
4.4. Other types of root cause types	Financial entities shall specify other types of root cause types where they have selected 'other' type of root cause in data field 4.2.	No	No	Yes, if 'other' type of root causes is selected in data field 4.2.	Alphanumeric
4.5. Information about the root causes of the incident	Description of the sequence of events that led to the incident and description of how the incident has a similar apparent root cause if the incident is classified as a recurring incident. This includes a concise description of all underlying reasons and primary factors that contributed to the occurrence of the incident. Where there were malicious actions, description of the modus operandi of the malicious action, including the tactics, techniques and procedures used, as well as the entry vector of the incident. Includes description of the investigations and analysis that led to the identification of the root causes, if applicable.	No	No	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
4.6. Incident resolution	Additional information regarding the actions/measures taken/planned to permanently resolve the incident and to prevent that incident from happening again in the future. Lessons learnt from the incident. The description shall include the following points in your answer (non-exhaustive list): A) Resolution actions description • Actions taken to permanently resolve the incident (excluding any temporary actions); • For each action taken, indicate the potential involvement of a third-party provider and of the financial entity; • Indicate if procedures have been adapted, following the incident; • Indicate any additional controls that were put in place or that are planned with related implementation timeline. Potential issues identified regarding the robustness of the IT systems impacted and/or in terms of the procedures and/or controls in place, if applicable. Financial entities shall clearly indicate how the envisaged remediation actions will address the identified root causes and when the incident is expected to be resolved permanently.	No	No	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	B) Lessons learnt Financial entities shall describe findings from the post-incident review.				
4.7. Date and time when the incident root cause was addressed	Date and time when the incident root cause was addressed.	No	No	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
4.8. Date and time when the incident was resolved	Date and time when the incident was resolved.	No	No	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
4.9. Information if the permanent resolution date of the incidents differs from the initially planned implementation date	Descriptions of the reason for the permanent resolution date of the incidents being different from the initially planned implementation date, if applicable.	No	No	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
4.10. Assessment of risk to critical functions for resolution purposes	Assessment on whether the incident poses a risk to critical functions within the meaning of Article 2(1), point (35) of Directive 2014/59/EU . Entities referred to in Art. 1(1) of the Directive 2014/59/EU shall indicate whether the incident poses a risk to critical functions within the meaning of Article 2(1), point (35) of the BRRD, and reported in Template Z07.01 of Commission Implementing Regulation (EU) 2018/1624 and mapped to the specific entity in Template Z07.02.	No	No	Yes, if the incident poses a risk to critical functions of financial entities under Art. 2(1), point 35 of Directive 2014/59/EU	Alphanumeric
4.11. Information relevant for resolution authorities	Description of whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group. Entities referred to in Art. 1(1) of the Directive 2014/59/EU shall provide information on whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group. The entities shall also indicate whether the incident affects the solvency or liquidity of the financial entity and the potential quantification of the impact.	No	No	Yes, if the incident has affected the resolvability of the entity or the group.	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	The entities shall also provide information on the impact on operational continuity, impact on resolvability of the entity, any additional impact on the costs and losses from the incident, including on the financial entity's capital position, and whether the contractual arrangements on the use of ICT services are still robust and fully enforceable in the event of resolution of the institution.				
4.12. Materiality threshold for the classification criterion 'Economic impact'	Detailed information about thresholds eventually reached by the incident in relation to the criterion 'Economic impact' in accordance with articles 7 and 14 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.	No	No	Yes	Alphanumeric
4.13. Amount of gross direct and indirect costs and losses	Total amount of gross direct and indirect costs and losses incurred by the financial entity stemming from the major incident, including: Amount of expropriated funds or financial assets for which the financial entity is liable Amount of replacement or relocation costs of software, hardware or infrastructure.	No	No	Yes	Monetary

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	Amount of staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff. Amount of fees due to non-compliance with contractual obligations. Amount of customer redress and compensation costs. Amount of losses due to forgone revenues. Amount of costs associated with internal and external communication. Amount of advisory costs, including costs associated with legal counselling, forensic and remediation services. Amount other costs and losses, including: • direct charges, including impairments and settlement charges, to the Profit and Loss account and write-downs due to the major ICT-related incident; • provisions or reserves accounted for in the Profit and Loss account against probable losses related to the major ICT-related incident; • pending losses, in the form of losses stemming from the major ICT-related incident, which are temporarily booked in transitory or suspense accounts and are not yet reflected in the Profit and Loss which are planned to be included within a time period commensurate to the size and age of the pending item;				

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	• material uncollected revenues, related to contractual obligations with third parties, including the decision to compensate a client following the major ICT-related incident, rather than by a reimbursement or direct payment, through a revenue adjustment waiving or reducing contractual fees for a specific future period of time; • timing losses, where they span more than one financial accounting year and give rise to legal risk. In accordance with article 7(1) and (2) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, before taking into account financial recoveries of any type. The monetary amount is to be reported as a positive value. In the case of aggregated reporting in accordance with Article 7, the total amount of costs and losses across all financial entities. The data point shall be reported in units using a minimum precision equivalent to thousands of units.				
4.14. Amount of financial recoveries	Total amount of financial recoveries. Financial recoveries cover the occurrence related to the original loss that is independent of that loss and that is separate in time, in which funds or inflows of economic benefits are received from first or third parties.	No	No	Yes	Monetary The data point shall be reported in units using a minimum precision

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	The monetary amount is to be reported as a positive value. In the case of aggregated reporting in accordance with Article 7, the total amount of financial recoveries across all financial entities.				equivalent to thousands of units
4.15. Information whether the non-major incidents have been recurring	Information on whether more than one non-major incident have been recurring and are considered a major incident within the meaning of Article 8(2) of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554. Financial entities shall indicate whether the non-major incidents have been recurring and are considered as one major incident. Financial entities shall also indicate the number of occurrences of these non-major incidents.	No	No	Yes, if the major incident comprises more than one non-major recurring incidents.	Alphanumeric
4.16. Date and time of occurrence of recurring incidents	Where recurring incidents are being reported, date and time at which the first ICT-related incident has occurred.	No	No	Yes, for recurring incidents	ISO 8601 standard UTC (YYYY-MM-DD Thh:mm:ss)

JOINT COMMITTEE OF THE EUROPEAN
SUPERVISORY AUTHORITIES

ANNEX III

Templates for notification of significant cyber threats

Number of field	Data field	
1	Name of the entity submitting the notification	
2	Identification code of the entity submitting the notification	
3	Type of the financial entity submitting the notification	
4	Name of the financial entity	
5	LEI code of the financial entity	
6	Primary contact person name	
7	Primary contact person email	
8	Primary contact person telephone	
9	Second contact person name	
10	Second contact person email	
11	Second contact person telephone	
12	Date and time of detection of the cyber threat	
13	Description of the significant cyber threat	
14	Information about potential impact	
15	Potential incident classification criteria	
16	Status of the cyber threat	
17	Actions taken to prevent materialisation	
18	Notification to other stakeholders	
19	Indicators of compromise	
20	Other relevant information	

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

ANNEX IV

Data glossary and instructions for notification of significant cyber threats

Data field	Description	Mandatory field	Field type
1. Name of the entity submitting the notification	Full legal name of the entity submitting the notification.	Yes	Alphanumeric
2. Identification code of the entity submitting the notification	Identification code of the entity submitting the notification. Where financial entities submit the notification/report, the identification code is to be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020. Where a third-party provider submits a report for a financial entity, they can use an identification code as specified in the Commission Implementing Regulation specifying Art. 28(9) from Regulation (EU) 2022/2554.	Yes	Alphanumeric
3. Type of financial entity submitting the report	Type of the entity under Article 2.1(a)-(t) of DORA submitting the report.	Yes, if the report is not provided by the affected financial entity directly.	Choice (multiselect): - credit institution - payment institution - exempted payment institution - account information service provider - electronic money institution - exempted electronic money institution - investment firm

Data field	Description	Mandatory field	Field type
			- crypto-asset service provider - issuer of asset-referenced tokens - central securities depository - central counterparty - trading venue - trade repository - manager of alternative investment fund - management company - data reporting service provider - insurance and reinsurance undertaking - insurance intermediary, reinsurance intermediary and ancillary insurance intermediary - institution for occupational retirement provision - credit rating agency - administrator of critical benchmarks - crowdfunding service provider

Data field	Description	Mandatory field	Field type
			- securitisation repository
4. Name of the financial entity	Full legal name of the financial entity notifying the significant cyber threat.	Yes, if the financial entity is different from the entity submitting the notification.	Alphanumeric
5. LEI code of the financial entity	Legal Entity Identifier (LEI) of the financial entity notifying the significant cyber threat, assigned in accordance with the International Organisation for Standardisation.	Yes, if the financial entity notifying the significant cyber threat is different from the entity submitting the report	Unique alphanumeric 20 character code, based on ISO 17442-1:2020
6. Primary contact person name	Name and surname of the primary contact person of the financial entity.	Yes	Alphanumeric
7. Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication.	Yes	Alphanumeric (
8. Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Yes	Alphanumeric
9. Second contact person name	Name and surname of the second contact person of the financial entity or an entity submitting the notification on behalf of the financial entity, where available.	Yes, if name and surname of the second contact person of the financial entity or an entity submitting the notification for the financial entity is available.	Alphanumeric

Data field	Description	Mandatory field	Field type
10. Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication, where available.	Yes, if email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication is available.	Alphanumeric
11. Second contact person telephone	Telephone number of the second contact person that can be used by the competent authority for follow-up communication, where available. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX).	Yes, if telephone number of the second contact person that can be used by the competent authority for follow-up communication is available.	Alphanumeric
12. Date and time of detection of the cyber threat	Date and time at which the financial entity has become aware of the significant cyber threat.	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
13. Description of the significant cyber threat	Description of the most relevant aspects of the significant cyber threat. Financial entities shall provide: - a high-level overview of the most relevant aspects of the significant cyber threat; - the related risks arising from it, including potential vulnerabilities of the systems of the financial entity that can be exploited;	Yes	Alphanumeric

Data field	Description	Mandatory field	Field type
	- information about the probability of materialisation of the significant cyber threat; and - Information about the source of information about the cyber threat.		
14. Information about potential impact	Information about the potential impact of the cyber threat on the financial entity, its clients and/or financial counterparts if the cyber threat has materialised	Yes	Alphanumeric
15. Potential incident classification criteria	The classification criteria that could have triggered a major incident report if the cyber threat had materialised.	Yes	Choice (multiple): - Clients, financial counterparts and transactions affected - Reputational impact - Duration and service downtime - Geographical spread - Data losses - Critical services affected - Economic impact
16. Status of the cyber threat	Information about the status of the cyber threat for the financial entity and whether there have been any changes in the threat activity. Where the cyber threat has stopped communicating with the financial entity's information systems, the status can be marked as inactive. If the financial entity has information that the threat remains active against other parties or the financial system as a whole, the status should be marked as active.	Yes	Choice: - active - inactive

Data field	Description	Mandatory field	Field type
17. Actions taken to prevent materialisation	High-level information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if applicable.	Yes	Alphanumeric
18. Notification to other stakeholders	Information about notification of the cyber threat to other financial entities or authorities.	Yes, if other financial entities or authorities have been informed about the cyber threat).	Alphanumeric
19. Indicators of compromise	Information related to the significant threat that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable. The IoC provided by the financial entity may include, but not be limited to, the following categories of data: • IP addresses; • URL addresses; • Domains; • File hashes; • Malware data (malware name, file names and their locations, specific registry keys associated with malware activity); • Network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); • E-mail message data (sender, recipient, subject, header, content); • DNS requests and registry configurations; • User account activities (logins, privileged user account activity, privilege escalation);	Yes, if information about indicators of compromise connected with the cyber threat are available.)	Alphanumeric

Data field	Description	Mandatory field	Field type
	• Database traffic (read/write), requests to the same file. In practice, this type of information may include data relating to, for example, indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to "command and control" servers used by malware (usually domains or IP addresses), URLs relating to phishing sites or websites observed hosting malware or exploit kits, etc.		
20. Other relevant information	Any other relevant information about the significant cyber threat	Yes, if applicable and if there is other information available, not covered in the template.	Alphanumeric

6. Accompanying documents

6.1. Draft cost-benefit analysis / impact assessment

According to Articles 10 of Regulations (EU) No 1093/2010, 1094/2010 and 1095/2010 of the European Parliament and of the Council (ESAs' Regulations), the ESAs shall analyse the potential costs and benefits of draft Regulatory Technical Standards (RTS) developed by the ESAs. The RTS and the Implementing Technical Standards (ITS) developed by the ESAs shall therefore 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 Final report (FR) on RTS and the ITS on the content and timing of incident reports under Article 20 of the DORA Regulation.

A. Problem identification

DORA (Art. 19) requires financial entities (FEs) to report major ICT-related incidents to competent authorities (CAs). CAs, in turn, will forward the received incident reports to EBA, ESMA, EIOPA and/or ECB. Article 20a of DORA mandates the ESAs to develop through the Joint Committee the content of the incident reports for major ICT-related incidents, the timelines for submitting incident reports and notification, and the content of the voluntary cyber threats notifications.

The information is to be reported for major ICT-related incidents across 20 types of FEs within the scope of DORA. Accordingly, the requirements of the RTS will impact more than 20 000 FEs. DORA requires that FEs provide both initial notifications and intermediate and final reports on major incidents.

The reporting exercise is complex and requires alignment of reporting practices across many types of FEs, to ensure a smooth data collection, transmission and processing.

B. Policy objectives

The main objective of the RTS and ITS on the content and timing of incident reports is that CAs obtain sufficient and good quality information about major ICT-related and security and operational payment-related incidents and significant cyber threats in a timely manner, while avoiding the imposition of a disproportionate operational burden on reporting FEs and ensuring proportionality for all types of FEs within the scope of DORA. In addition, the RTS aims to have data fields that are simple, concise, and clear.

C. Baseline scenario

The baseline scenario is the situation where the current reporting requirements are kept, without further changes or further harmonisation. This includes:

- ENISA taxonomy, NIS 2

- PSD2 payment-related major incidents

The Directive (EU) 2022/2555 or Network and Information Security (NIS2) Directive was adopted on 17 January 2023, at the same time as DORA. It is an expansion of NIS Directive, which was the first piece of EU-wide legislation on cybersecurity aiming to achieve a high common level of cyber security across the EU. NIS1, and subsequently NIS2, are considered as the horizontal framework for cybersecurity in the EU and serves as a baseline standard for a minimum harmonisation of all sectoral legislation in this field.

Policy issue 1: general approach on timelines for reporting major ICT-related incidents

Option 1A - a harmonised set of reporting timelines applicable to all FEs, embedding proportionality within the common timelines

Option 1B - a harmonised timelines for two groups of FEs (smaller and larger firms) reflecting proportionality

Option 1C - separate timelines for the different types of FEs within the scope of DORA.

Option 1A ensures harmonisation and streamlining of requirements, in line with the objectives of DORA. It will also be simpler to apply, as the rules will be the same for all FEs.

Option 1B will provide proportionality along the size dimension. However, it may be difficult to achieve a single classification by size that would be meaningful for all the types of FEs covered by DORA. Providing multiple classifications depending on the type of FEs would add complexity and fragmentation to the framework.

Finally, Option 1C, would also be proportionate, but would require tailored timelines for each type of FEs covered under DORA. Such an approach would be very complex to implement, apply and monitor. Due to its low level of harmonisation, it might determine unjustified differences in treatment among FEs.

Options 1B and 1C risk loosing situational awareness of CAs in times of crisis, as many of the underlying technologies which may be impacted are ubiquitous across FEs.

Given the above benefits and costs, Option 1A is preferred. It also appears the one most in line with the overarching harmonisation and simplification objectives of DORA.

Policy issue 2: Timelines for reporting of major ICT-related incidents'

Information on major ICT-related incident is provided in 3 stages: initial notification, intermediate report and final report that are to be submitted to the CAs within specific timelines. When reviewing the timelines for each of these submissions, the following options were considered:

Option 2a: replicate NIS2 reporting requirements.

Option 2b: align to the extent possible with NIS2, with adjustments to consider DORA specificities.

Option 2c: introduce separate DORA-specific requirements

Alignment with NIS2 (i.e. Option 2a or 2b) is generally preferred as NIS2 provides a horizontal framework that has been applied over many years. Moreover, some FEs within the scope of DORA are covered in NIS2, therefore synergies between the frameworks will be desirable. Finally, NIS2 indicates that sector-specific legislation that are lex specialis should be at least as stringent as the requirements set out in NIS2.

However certain aspects are specific to DORA, and therefore had to be adjusted:

- While initial notification from the time of FEs become aware of the incident is 24h in line with the early warning under NIS2, the submission deadline from the moment of classification is not covered under NIS2, and therefore has been assessed separately. In particular, potentially shorter timelines will be applied for the reporting of the initial notification from the moment of classification of the incident as major, adequate even for most time critical notifications (4 hours). Thus DORA being more stringent than NIS2.
- The intermediate report (incident notification) under NIS2 is submitted without undue delay and in any event within 72 hours of becoming aware of the significant incident. The timeline envisaged under DORA is the latest within 72 hours from the submission of the initial notification, which gives additional hours for FEs. However, it should be noted that most of the information requested under NIS2 is required in a high-level way in the initial notification. Moreover, the current reporting template for intermediate report is more detailed compared to NIS2.

Option 2b therefore is preferred.

Policy issue 3: Data fields of the notifications and reports for incident reports and cyber threats

Option 3a: minimalistic approach, asking only for essential data to classify an incident and understand its nature and impact

Option 3b: a balanced approach, asking immediately for essential data fields, and allowing FEs to provide other relevant fields that may be helpful to the NCAs in a scattered manner

Option 3c: Comprehensive approach, asking for all the data that may be needed for supervisory, regulatory or statistical purposes

Option 3a ensures that the FEs' focus on what is essential, envisages less resources and costs related to filling in template and data processing by NCAs. However, with this approach, there is the risk of some important information missing. Moreover, there may be a lack of (i) situational awareness by CAs to identify where a supervisory response is required; (ii) unnecessary increase of communications between the CA and FE during time of stress and (iii) missing statistical information to allow for the awareness and learning in the financial system on an ongoing basis.

Option 3c, by contrast ensures that all data is available, so that the CAs can have a good understanding of the situation, including the detailed specificities of each incident. This would allow the CAs to conduct additional data processing, such as statistical analysis, to get additional insights into the patterns of the reported incidents. The drawback of this approach is that it would involve higher costs and resources related to filling the templates on the FEs side and processing the data on the CAs' (and ESAs') side.

Option 3b achieves a good balance between essential and comprehensive information, and hence is the preferred option. It would allow the CAs to get more information, but without overburdening the FEs with the need to provide too much data. In addition, it will allow meeting the needs of other authorities and bodies, such as resolution authorities, CSIRTs and others. Furthermore, FEs are permitted to correct information submitted in an initial notification and intermediate report and use estimates when initially submitting these.

Option 3b is therefore preferred.

Policy issue 4: ITS on the format and process of reporting major incidents

The ITS centres around the template for reporting and supporting technical details designed in the similar way as other prudential reporting requirements. Three options were considered on the way the templates are structured

> Option 4a: Submit the notification and reports in an incremental manner (current PSD2 approach)
>
> Option 4b: Structured intermediate and final reports and a general free text field for the initial notification
>
> Option 4c: Single template with data fields, which will clearly indicate which fields are expected to be submitted with the initial notification, the intermediate report and final report respectively.

Option 4a, while currently applied as part of PSD2 approach for reporting major payment-related incidents, would not allow FEs to easily submit additional information about the incident that may be available, if this information is required by a report to be submitted at a later stage (e.g. receiving with the initial notification information that is requested only with the final report). Such information, if available early could be useful to the CAs.

Option 4b allows the submission of the initial notification in a general free text format. This approach acknowledges the importance of submitting in a flexible and simple manner the initial notification as soon as possible, even when data is incomplete. This approach would be easy to implement, as it would not require a template. However, the absence of structured data will lead to issues for CAs and the ESAs in assessing the information received and automatically processing it, especially in cases where the report needs to be forwarded to other authorities.

Finally, Option 4c, is more complex to implement technically. However, it provides a good balance between the flexibility for the FEs on the one hand, as FEs can populate also fields that are not necessarily expected to be submitted with the respective notification/intermediate report in the cases where FEs possess this information, and, on the other hand, it ensures that the CAs get all the available data in a structured form.

Considering, the above advantages and drawbacks, option 4c is preferred.

Policy issue 5: Optionality of data fields

Option 5a: All data fields optional

Option 5b: All data fields mandatory

Option 5c: Specific fields mandatory and others conditional

Option 5d: Data fields for the initial notification optional, the other data fields mandatory

Option 5a envisages that all the fields are optional. This approach would provide flexibility and would ensure that the FEs will submit the major ICT-incident report even when not all data is available. It will also mean less burden and costs for the FEs to fill in the templates. On the drawbacks side, this approach may lead to low data quality, missing out on essential information, lack of harmonisation, as well as inability for the CAs and ESAs to assess the data provided in a consistent, efficient and structured manner. Moreover, it will not be legally sound and reflective of the mandatory and binding nature of Regulatory Technical Standards.

Option 5b, which requires all data fields to be mandatory, has the benefit of having all data available for the CAs and would ensure full consistency and harmonisation of data. On the other hand, such a strict approach may result in missing information being an obstacle to submission. Alternatively, the data may be filled in by the FEs with irrelevant or inaccurate information, just to fulfil the mandatory requirement, and to be able to submit the report. Finally, this option would be burdensome for the FEs to fill in the templates and will introduce additional cost.

Both Option 5a and 5b are seen as either too lax or too restrictive, so are not preferred. Option 5c and 5d represent a hybrid approach, combining both optional, conditional and/or mandatory fields.

Option 5c requires that the FEs fill in only the essential information (as defined in this draft CP), ensuring that NCAs have the essential information, while at the same time giving flexibility to FEs to provide more information should they wish to, while not being an obstacle to submission of the

report swiftly. This approach allows the FEs to tailor the response based on the nature and impact of the incident, and represents a smaller reporting burden. While this approach does not ensure the consistency and harmonisation of all the information, it ensures consistency and harmonisation of essential information for the CAs to process it in a more efficient and automatic manner. The drawback of this approach is that some incident=specific fields may be missing, but it should be acceptable, since CAs can identify these and request an update to the incident report so that CAs can conduct their core assessment.

Option 5d, which requires that the data in the initial notification only is optional, has the benefit of allowing the initial notification to be submitted swiftly. This gives the FEs flexibility, and ensures a lower reporting burden at a time when it is most crucial to manage the incident. The drawback of this option is that the initial notification includes some essential information that should be provided to the CAs. Lack of such information in the first submission may lead to incomplete assessment of the situation by supervisors, and the potential inability to identify spill-over effects to other FEs. Moreover, it will not be legally sound and reflective of the mandatory and binding nature of the RTS.

Given the above arguments, Option 5c is preferred, as it provides sufficient flexibility to the FEs and ensures that the CAs have all the essential information in a timely manner.

D. Cost-benefit analysis

When comparing with the baseline scenario (where the FEs subject to existing incident reporting frameworks, such as NIS and PSD2) keep reporting using these), the RTS and the ITS are expected to bring benefits by achieving a higher level of harmonisation of reporting templates, timelines, data fields and definitions, which will increase data comparability and quality. This in turn will contribute to more effective supervision and monitoring of the major ICT-related incidents by the NCAs and ESAs, in line with the DORA requirements. In that way, these RTS and ITS contribute to ensuring the safety and soundness of the European financial system.

The RTS is expected to lead to moderate costs to FEs in relation to the adjustment of the infrastructure and process to align with the new reporting requirements. CAs will incur one-off costs related to implementation of the infrastructure and processes, as well as incurring costs related to processing of data. These costs are expected to be moderate, given that the costs of the RTS are only incremental to the costs for implementing the existing reporting requirements set out in DORA.

6.2. Feedback on the public consultation and on the opinion of the ESAs stakeholder groups

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

The consultation period lasted for 3 months and ended on 4 March 2024. 109 responses were received.

This paper 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 considers them most appropriate.

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

Views of the ESAs Stakeholder Groups and ESAs' analysis

General comments

The SGs welcome and support the ESAs' general approach of aligning the requirements of these RTS and ITS, to the greatest extent possible, with existing sectoral legal instruments, such as the revised EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2), and the various related Guidelines issued by ENISA under Directive (EU) 2022/2555 (NIS2). The SGs agree that cross-sectoral harmonisation is essential given that ICT incidents and cyber-threats are not inherently sector-specific and should therefore be addresses in a consistent manner that concentrates on the nature and significance of the incident or threat rather than the place where it originates or is first detected. Within the financial sector, a degree continuity of reporting requirements with existing, proven incident reporting frameworks is, of course, highly desirable to reduce implementation costs and capitalise on existing investments in infrastructure, systems. skills and experience.

Response from the ESAs

The ESAs have acknowledge the preference of the ESAs Stakeholder Groups of aligning the RTS and ITS with existing sectorial legal instruments and for ensuring cross-sectorial harmonization and consistency. The ESAs have retained this approach in the draft RTS and ITS following the public consultation.

Q1. Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

The SGs largely agree with the ESAs proposal to introduce harmonised timelines for all FEs across all sectors (policy option 1a).

While the SGs acknowledge that some of the sectors covered by DORA operate in very different ways – including, in particular, the architecture and use of ICT systems and the frequency and 'cycle time' of transactions – they appreciate that ICT-related risks are capable of propagating rapidly and across sectors. It is of critical importance, therefore, for financial institutions – as much as for other providers of essential services that are subject to similar obligations, e.g. under Directives (EU) 2022/2555 (NIS2) and 2022/2557 (CER2) – to adhere to consistent, harmonised timelines. Moreover, some entities subject to incident reporting under DORA may be in scope of more than one regulator; different timelines could create uncertainty and needlessly complicate the implementation process for these entities.

From a sectoral perspective, however, some members of the SGs observe that the proposed timelines may not be feasible to implement for the insurance sector, in particular. They note that these deadlines are stricter than any comparable legislation that applies to the sector – e.g. 72 hours under GDPR or 24 hours for an 'early warning' under NIS 2. They suggest that a more appropriate timeline would be for an initial notification to be submitted, at the latest, within 24

hours after classification, or on the next working day if the due date a major incident is detected on a weekend or bank holiday. They propose that the intermediate report could be submitted within ten working days of the initial notification, and the final report within 30 working days from the permanent resolution of the incident.

The SGs emphasise that proportionality must be maintained in order not to overload smaller entities which may have limited capacities and may therefore be less capable of detecting, analyzing and reporting on ICT incidents than their larger peers. The SGs therefore welcome the provisions in Article 6(2) and 6(3) RTS, which exempt FEs from the obligation to file intermediate and final reports for major incidents over the weekend or bank holidays if they are not classified as 'significant' or the incident does not have a systemic or a cross-border impact. The SGs are satisfied, moreover, that a significant degree of proportionality is already reflected in the criteria for classifying an incident as 'major' and refer to their comments to the ESAs' earlier consultation on this matter.

The SGs note that the ability of FEs which rely on third-party providers (TPPs) to operate some or all of their ICT services to report on major incidents in a timely manner critically depends on the alertness and responsiveness of these TPPs. An incident that occurs within the sphere of the TPP and affects the operations of a FE may not immediately be detected by the FE. Instead, the FE may be reliant upon the TPP to issue an alert. The responsibility for timely reporting, however, still lies with the FE unless incident reporting itself has been outsourced (Article 6 ITS). It is important, in any event, that the relevant service-level agreements are consistent with FEs' obligations under DORA. It may be helpful, in this context, for the incident reporting framework to provide additional transparency on the effectiveness of these arrangements so that regulation and supervision can be designed and calibrated more effectively.

The SGs agree with the principle of aligning the reporting framework under DORA as much as possible with that of NIS2, subject to adjustments for financial-sector DORA specificities (policy option 2b).

Given the interconnectedness of the financial sector, and the potential systemic risk arising from a major incident, the introduction of a shorter notification period (24 hours from detection) and of an additional criterion (4 hours after the incident has been classified as 'major') appears appropriate and prudent. The SGs notes, however, that the rationale for extending the deadline for submission of the final report from 20 days (under NIS2) to one month is not well explained in the draft RTS. The SGs appreciate that a balance needs to be struck between the objectives of incentivising entities to report, resolve, and analyse major incidents rapidly, on the one hand, and the need to allow for a thorough forensic analysis and ex-post assessment, on the other. The draft RTS appears to prioritise the latter – if so, the argument should be spelt out more clearly.

Response from the ESAs

The ESAs agree with the views to ensure harmonised and consistent incident reporting framework, including timelines.

Regarding the points on sector-specificities for the insurance sector, the ESAs view this would bring divergent approaches, fragmentation and unlevel-playing field. Accordingly, the ESAs have not introduced such changes. However, to address on some of the points about additional time, the ESAs extended slightly the time for submission of intermediate report and final report by having the timeline counted from the submission of the initial notification or the latest intermediate report (when regular activities have been recovered) respectively, instead of the moment of classification. The ESAs have also exempted smaller entities from weekend reporting, which should bring further proportionality and address further the concerns expressed by the insurance stakeholders. Moreover, it is worth highlighting that the classification criteria for major ICT-related incidents already embed proportionality.

The ESAs also welcome the positive assessment of the ESAs Stakeholder Groups on the level of proportionality ensured with the reporting timelines and weekend reporting. The ESAs would like to highlight that they have introduced further proportionality by reducing the number of reporting fields in the reporting template, including by significantly streamlining the requested information in the initial notification to not put burden on entities while they will be handling the major incident.

On the service-level agreements between FEs and TPPs, the ESAs would like to highlight that it goes beyond the legal mandate conferred by DORA. Furthermore, the ESAs are not able to address requirements directly to TPPs.

The timeline for submission of the final report under the draft RTS is aligned with the one month deadline set out in NIS2.

Q2. Do you agree with the data fields proposed in the draft RTS and the Annex (I and II) to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree with the ESAs approach to differentiate between essential, mandatory data fields and additional, optional data fields that provide valuable information for supervisory, regulatory or statistical purposes (policy option 3b).

The SGs agree, in principle, with the proposed format and data fields of the initial report, subject to the following observation:

- As mentioned previously (Q1.), additional information on the circumstances of the detection of a major incident could be useful for supervisory authorities to evaluate the effectiveness of outsourcing arrangements, and the attendant sharing of monitoring and incident reporting responsibilities. With respect to fields 1.16 and 1.17 it may be of considerable relevance for the assessment of the incident by supervisory authorities to include information on whether the

incident was detected by the affected TPP or by the FE. An additional, optional data field could be added for that purpose.

- Some members of the SGs observe, however, that certain data points, in particular items (d), (e), (g) and (h) from Article 3, might be included more appropriately in the intermediate or final notification as this information may be too burdensome to collect at the time of the initial notification, or might not yet be available.

Response from the ESAs

The ESAs welcome the broad support for the approach with the data fields. Regarding the proposal to add a field in the general information on whether the incident is detected by the TPP or the FE, the ESAs would like to clarify that such fields exist in the initial notification.

The fields proposed to be moved to the intermediate or final report related to the discovery of the incident, classification criteria, impact in other Member States and information about impact on TPPs or other FEs, the ESAs would like to clarify that the first three are high-level and should be available to the FE at the time of submission of the initial notification. The impact on TPPs or other FEs has been deleted and covered in the description of the incident, if applicable. Regarding the impact in other Member States, this information is critical to enable timely assessment of the need to forward notifications to CAs in other Member States where the incident has an impact.

Q3. Do you agree with the data fields proposed in the draft RTS and the Annex (I and II) to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree, in principle, with the proposed format and data fields of the intermediate report, subject to the following observations:

- For the purposes of completing fields 3.8 to 3.10, FEs are required to make an assessment of the number/percentage of financial counterparties affected by the incident and the impact of the incident on these counterparties. The SGs agree with the intended purpose of this information, i.e. to alert supervisors to potential spillover effects and any risk of cross-border contagion. FEs may find it difficult, however, to provide accurate, factual information on these points at the time when the intermediate report is due, i.e. most likely before a comprehensive forensic analysis could have been completed. The draft RTS should therefore be amended to clarify that the reporting entity would only be expected to provide a preliminary assessment on this stage, based on available information and reasonable assumptions. This preliminary assessment should then be updated and completed in the final report.

- Some members of the SGs expressed concerns that the timeline of 72 hours may not allow sufficient time for companies to provide material updates. They suggest that reporting should be reduced so as to not pose an excessive burden while the incident is ongoing. In particular, they suggest that information already covered by the initial notification (items (d) and (e) of

Article 4) should be limited, and non-essential information that will require more time to be collected (items (b), (k) and (l) of Article 4) should be moved to the final report.

- Some FEs also expressed concerns about the breadth of the requested information on affected infrastructure components (field 3.31). They argue that the list of components is too detailed, bearing in mind that many components may be affected in a major incident. The SGs are of the view that the relevance of this information depends materially on the nature of the incident. Reporting at the proposed level of granularity appears justified if this information appears relevant to assess, in particular, the potential cause, scope, or systemic risk, i.e. the speed and scale of propagation, of the incident. A detailed list should be provided in the final report, in any event.

- For the purposes of correctly determining the time for submission of the intermediate report (item. b. of Article 6(1) RTS), it would be helpful to define in more detail when *"regular activities"* are deemed to "*have been recovered and business is back to normal"*. In particular, it appears unclear if all services have to be restored to or whether a partial resumption of services would be considered sufficient. Similarly, it is not entirely clear if services should be considered as having been restored as long as 'temporary actions' (field 3.37) are still in place.

Response from the ESAs

Regarding the information about clients, financial counterparts and transactions affected, the ESAs would like to highlight that the instructions of the fields clearly envisage the possibility for provision of estimates if actual numbers are not available. Accordingly, the ESAs have not amended the draft ITS.

On the proposal to delete the fields on type of incident or the detailed information about the classification criteria, the ESAs disagree since this information is crucial for the assessment of the incident by CAs.

Regarding the comments to move specific data fields to the final report (vulnerabilities exploited, indicators of compromise), the ESAs have deleted the field vulnerabilities exploited due to concerns raised by various stakeholders (see also the Feedback table in the next sub-section). The ESAs have retained the indicators of compromise, where applicable, in the intermediate report to ensure alignment with NIS2.

On the information on infrastructure components, the ESAs view the level of detail of the information requested sufficient and not burdensome, especially since the mandatory requirement is to provide the description or name of affected infrastructure components or systems, with any additional information being complementary.

The ESAs have introduced minor changes to reflect on the clarifications sought on different terminology with more details available in the feedback table.

Q4. Do you agree with the data fields proposed in the draft RTS and the Annex (I and II) to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree, in principle, with the proposed format and data fields of the final report, subject to the following observations:

- As for the intermediate report, the conditions for submission of the final report (*"the incident has been resolved permanently";* item. c. of Article 6(1) RTS) should be defined more precisely. The SGs are mindful that the problem management process may be complex and time-consuming, and may not be completed within one month even though normal operations may have been fully restored by then. Arguably, the final report should be submitted at the earliest possible time, but not until the root cause of the incident has been identified and analysed, and a permanent fix has been applied.

- In the present draft ITS, FEs are required to provide a description of data losses associated with the incident (field 3.23). According to the current wording, "the FE may also indicate the type of data involved in the incident." The SGs are of the view that this wording suggests a degree of optionality that does not correspond to either the classification of the item in this ITS (as 'mandatory' for both the intermediate and final report) or the separate, but related legal obligation to report a 'personal data breach' to the CA under Article 33(1) of Regulation (EU) 2016/679 (GDPR) within 72 hours of its detection. In the interest of legal consistency, transparency, and procedural efficiency, the SGs would suggest to add clear instructions in this field that any loss of personal data in the context of the incident would be have to be notified, assessed and, if appropriate, notified to the CAs.

- Some members of the SGs are of the view that the current deadline for the final report –one month after the incident or one day after closing – may not be feasible, especially in the insurance sector, as FEs will be focused on resolving the incident and not have sufficient time to gather the necessary data.

Response from the ESAs

On the reference to permanent resolution as a reference point for the submission of the final report, the ESAs agree with the comments made and have amended the draft RTS by focusing on the root cause analysis only.

The data breaches as type of incident fall within the scope of the draft RTS on incident classification, which was published in January 2024.

Regarding the timeline of the final report, it is consistent with NIS2 and provides sufficient time for FEs to obtain the necessary information (one month after the business has been recovered). It should also be noted that the ESAs have extended the timeline for submission of the final report

(from the submission of the intermediate report, rather than the moment of classification of the incident).

Q5. Do you agree with the data fields proposed in the RTS and the Annex (III and IV) to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree with the ESAs approach of creating a simple, low-barrier template to encourage FEs to report cyber threats, which is voluntary. In the interest of making this data usable, e.g. for sectoral/cross-sectoral threat analysis and statistical purposes, a broad categorisation, in addition to the threat description (field 14), may be useful. These broad categories could be based, for instance, on the list used by ENISA in its periodic Threat Landscape (ETL) report. This categorisation may require inserting an additional, mandatory data field.

Response from the ESAs

To incentivize FEs to submit notifications about significant cyber threats and not posing burden to FEs, the ESAs would like to keep the mandatory fields to a minimum. Moreover, the information may be captured by the description of the cyber threat. Finally, the mandate has been developed in consultation with ENISA. Accordingly, the ESAs have not introduced any changes to the draft RTS and ITS.

Q6. – Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

The SGs agree in principle with the ESAs proposed approach. They note, however that if an incident affects several FEs within a consolidated group, it should be possible for them to file one consolidated report, by the parent company, provided that all affected entities are supervised by the same CA. Some members of the SGs suggest that it should be possible for FEs to submit the reports in any of the official EU languages, including English, as the need to translate them for the regulator prior to submission may cause delays.

Response from the ESAs

The ESAs agree with the views expressed by the ESAs stakeholder groups and have amended the draft ITS by introducing a new Article (7) with specific requirement about aggregated reporting. Additional information about the rationale and the changes introduced are available in the Rationale section, the Feedback table, Article 7 of the draft ITS and Annex II to the draft ITS.

On the language of reporting, the ESAs would like to clarify that the RTS and ITS cannot impose a specific language of reporting.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Summary of responses to the consultation and the EBA's analysis

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Feedback on the general comments			
DORA-NIS2 interplay	Several respondents suggested ensuring further consistency between DORA and NIS2 by ensuring the timelines for incident reporting and the information requested are consistent.	The ESAs would like to highlight that the proposed requirements for reporting major ICT-related incidents have already been much aligned and made consistent with NIS2 in line with the requirements of Article 20 of DORA. It should also be noted that Article 4 of NIS2 introduces the *lex specialis* regime of DORA (being a sector-specific legislation) over NIS2 and provides that the reporting requirements for major incidents under such sector-specific legislation should be 'at least equivalent in effect' to those laid down in NIS2. The ESAs would like to clarify that this does not mean that the requirements in relation to the timelines for reporting and the amount of information requested should be identical. Following the public consultation, the ESAs assessed whether the proposed requirements in the Consultation paper and the amended requirements following the public consultation were aligned with NIS2. Accordingly, the ESAs arrived at the view that all provisions in the amended RTS and ITS are 'at least equivalent in effect' to the requirements in NIS2. In particular: • the 24-hour timeline for submission of initial notification after the FE has become aware of the incident were deemed identical to NIS2, with the requirement to submit the initial notification 4 hours after classification being stricter for some larger and more systemic FEs;	No specific change but related amendments introduced with regard to the submission of the intermediate report.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
		• the timelines for reporting of the intermediate report at the latest within 72 hours from the submission of the initial notification in DORA were deemed similar (slightly longer and more relaxed) compared to the requirement to submit incident notification within 72 hours from the moment of becoming aware of the significant incident in NIS2 (as envisaged in the draft that was publicly consulted). However, since the key attributes required in the incident notification in NIS2 will be required in a high-level way in the initial notification in DORA, which is submitted within 24 hours, and that the intermediate report under DORA requires more information compared to NIS2, in practice the DORA requirements are considered at least equivalent, if not slightly stricter in some aspects, than those set out in NIS2. Moreover, DORA envisages that FEs shall submit an intermediate report to the CA (i) as soon as the status of the original incident has changed significantly and (ii) as soon as the handling of the major ICT-related incident has changed based on new information available. In addition, the RTS envisage a submission of the intermediate report when the incident is resolved and business is back to normal. All these three scenarios allow a submission of an intermediate report before the 72-hour deadline; and • the timelines for the submission of the final report of one month after the submission of the intermediate report (incident notification under NIS2) were deemed identical to those set out in NIS2.	
Transitional period for implementing the technical standards	A few respondents were of the view that the application date of 17 Jan 2025 is very challenging to the industry and propose extending.	The ESAs understand the potential implementation challenge for the industry. However, it should be noted that DORA has not envisaged a transitional period for the implementation of the incident reporting requirements and the related technical standards. Accordingly, the ESAs do not have a mandate to introduce such a transitional provision in the RTS/ITS.	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Alignment with the Financial Stability Board work on Format for Incident Reporting Exchange (FIRE)	A few respondents suggested the ESAs to take into account the work carried out by the Financial Stability Board on FIRE and to ensure alignment.	The ESAs are very supportive of alignment with international initiatives, which will bring synergies and efficiencies for FEs operating worldwide. However, it should be noted that the FIRE framework is not finalised yet and is not publicly available in order for the ESAs to align with it. Nevertheless, due to participation of some of the ESA CAs in the discussions on the development of the FIRE framework, the ESAs took into account some aspects and slightly amended particular aspects of the reporting template in the Annex to the ITS (e.g. retaining the collecting information on internal escalation, entity internal severity assessment of the incident, lessons learnt, and slightly adjusting the description and in relation to discovery of the incident, description of the measures taken for the permanent resolution of the incident, aligning the approach for the data fields with ISO 8601). In addition, the ESAs have amended the TS in line with the feedback received during the public consultation.	Minor amendments to various fields in the Annex to the template (Fields 2.2, 2.3, 2.4, 3.2, 3.3, 4.4, 4.5, 4.6, 4.14, in Annex II and field 13 in Annex IV)
Secure reporting channels	Several respondents were of the view that the RTS should ensure confidentiality and security of reported data when receiving incident reporting data. A few of them suggested that access to the data, which includes sensitive data, need to take place on a need-to-know basis and receiving CAs to have professional secrecy obligations	The transmission of data on incidents through the use of secure electronic channels is already addressed in Article 4(1) of the draft ITS. It should also be noted that any shared information falls under general professional secrecy requirements and confidential handling in accordance with Article 55 of DORA, as well as the general professional secrecy requirements of CAs based on their statutory mandate. The ESAs duly take note of these concerns and are fully aware of them and will take them into account for the incident reporting process set out in Article 19 of DORA, including by ensuring security and confidentiality of the transmitted data.	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Reclassification of incidents from major to non-major	Several respondents suggested being able to re-classify major incidents to non-major (in cases where FE arrive at the view that the incident does not meet the classification criteria as initially thought) at an early stage of the reporting process.	The ESAs would like to clarify that in the cases where FEs reclassify a major incident to non-major (which is expected to be an exception), the only additional information to be provided should be the reasons for reclassification. To address the concerns expressed, the ESAs have removed the fields on the reclassification of the incident from the final report and introduced the following amendments to the template in Annex II to the ITS to capture this information: • introduced the respective option to indicate the reclassification of an incident in field 1.1. 'Type of report' • amended the description and instructions of field 2.10 'Other information' to clarify that the information for the reclassification of the incident is expected to be provided in that field.	Changes to data fields 1.1. and 2.10 of Annex II.
Identification of payment-related incidents	Several respondents suggested introducing a field to identify payment-related incidents.	The ESAs have amended the ITS by introducing a new type of incident in field 3.23 of the template in Annex II by adding a type of incident - 'payment-related'. This will allow the identification of payment-related incidents.	Change in field 3.23 of Annex II to the ITS.
Significant changes	Several respondents sought clarification on the term significant changes and suggested that the ESAs should introduce time limits for reporting of significant changes.	The ESAs would like to clarify that the term 'significant change' is used in Article 19(4)(b) of DORA and is not covered by the mandate conferred on the ESAs in Article 20. Accordingly, the proposed clarification goes beyond the scope of the RTS, which need to set-out the time limits and content for incident reporting.	No change.
Solo vs consolidated reporting	Several respondents queried whether the incident reporting should be carried out by the FEat individual (solo) level or whether it can also be done at group level. In addition, these respondents queried how should	The ESAs would like to clarify that in accordance with the requirements of DORA (e.g. Article 19), the reporting of major incidents is a responsibility of the FE at solo level. Nevertheless, the ESAs have envisaged specific cases where FEs can report in an aggregated way at national level in accordance with DORA	Change to field 2.8 of Annex II.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	intragroup service agreements be considered. in this context? A few of these respondents also sought clarification on how field 2.8 (Indication whether the incident originates from a third-party provider or another FE) should be filled in for intra-group service provider whose services are affected.	(see point 'aggregated reporting' in the feedback on the responses to question 6). The ESAs amended field 2.8 to alphanumeric to provide for flexibility on the reporting of different types of providers, including intra-group service provider (who is a third-party provider from the perspective of the FE). It will also allow capturing the LEI code of said third-party provider.	
Data fields: types and character limitations	Many respondents requested information on the size limitation of the alphanumeric fields, with a few of them suggesting introducing good practices examples. Several respondents also suggested that some fields can be populated by CAs. Several respondents proposed to change all alphanumeric fields with multiselect. A few respondents proposed some data fields to be optional/recommended.	The responses to the questions depend on the type of the incident and its impact on the FE. Accordingly the ESAs have not provided any examples of good reporting practices for each field. With regard to the population of the fields, this falls within the responsibility of the FE, not the CA. In addition, the requested information cannot be known to the CA. Regarding the proposal not to use alphanumeric fields, the ESAs would like to clarify that choice and multiselect fields were used to the greatest extent possible. The remaining alphanumeric fields either require qualitative information or aim at providing flexibility and reducing burden to FEs (in particular where a multiselect may cover 20+ entries, such as functional areas affected). Finally, it should be noted that data fields in the RTS cannot be optional, which is the reason why the ESAs have used mandatory fields and 'conditional', with the latter depending on the type of incident.	No change
Financial entities subject to incident reporting	A few respondents queried whether FEs are obliged to submit incident reports also in the case when an incident occurs in subsidiaries outside the EU, i.e. outside jurisdictions covered by Regulation (EU) 2022/2554.	The ESAs would like to clarify that according to Article 19 of DORA, all FEs within the scope of DORA shall report major ICT-related incidents to their CA. Accordingly, FEs shall report any incident that affects the FEs within the EU, including cases where the incident originates from a subsidiary outside the EU.	No change

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Feedback on responses to question 1 (reporting timelines)			
Reporting timelines	Many respondents were of the view that the reporting timelines are too short and that they should be extended or that the data fields requested significantly reduced. The main argument presented is that FEs will be handling the incident at the time of reporting and that some of the information requested requires input from various functions. Some of the respondents also indicated that the proposed timelines, in particular for the intermediate report, are more stringent than any existing framework. Finally, several respondents were of the view that the reporting timelines should be aligned with NIS2 Directive.	The ESA agree with the concerns expressed by the respondents to the public consultation and the arguments provided. Accordingly, the ESAs have introduced changes to the RTS to address these, by both extending the reporting timelines for the intermediate and final reports, and by removing certain data fields or moving them to subsequent reports. On the latter point, the ESAs in particular streamlined the data fields requested with the initial report to not pose burden on FEs while they handle incidents. With regard to the timelines and the interplay with NIS2, the ESAs leveraged between several objectives of retaining a harmonised approach for all FEs, retaining the effect of the requirements to at least equivalent effect to NIS2 (in line with Art 4 of NIS2) and to reduce the required efforts by FEs while handling an incident. Accordingly, the ESAs have amended only the intermediate and final report within the boundaries set out by NIS2.	See specific changes covered in the entire feedback table.
Proportionality and sector specificities	Several respondents were of the view that the RTS and ITS do not fully incorporate the proportionality principle and suggested introducing different timelines reflecting the size and the overall risk profile of the FE, and the nature, scale and complexity of its services, activities and operations. Some of these respondents highlighted that specificities and time-criticality of the services provided by FEs need to be taken into account in relation to the reporting timelines and requested the timelines to be extended. In particular, these respondents indicated that the timelines for the initial notification are too short,	With regard to proportionality and sector/entity-specificities, the ESAs would like to clarify that: • In line with the objectives of DORA and taking into account that often incidents within a group or originating from a TPP may affect different types of FEs, the ESAs have arrived at the view that retaining a harmonised timelines for reporting major incidents is preferrable and did not find compelling reasons why different timelines should apply to different FEs;	Various changes applied in the draft RTS and ITS

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	especially for FEs in the insurance and pension sub-sectors, as well as savings banks, asset managers, investment firms and trade repositories. They indicated that the reporting timelines for the intermediate report should also be extended also be extended.	• Proportionality is embedded in the timelines set, which were designed to address to a great extent the specificities of different types of FEs leveraging between the need to allow sufficient time for FEs to handle the incident, while at the same time providing CAs with relevant information about the major incident early enough. • Proportionality is embedded in the approach for classification of major ICT-related incidents set out in the RTS on criteria for classification of major incidents under DORA. Nevertheless, the ESAs agree with some of the points raised on proportionality and, to ensure that the draft RTS and ITS are proportionate, introduced the following amendments: • The ESAs have reduced the number of reporting fields in the reporting template, including by significantly streamlining the requested information in the initial notification to not put burden on entities while they will be handling the major incident. • The ESAs have provided additional time for the reporting of the intermediate report (with up to one day more) and the final report (with close to 72 hours or more) due to the change in the start of calculating the time from the previous submitted notification/report, instead of the moment of classification of the incident. • The ESAs have narrowed down the scope of weekend reporting by focusing only on credit institutions, operators of trading venues, central counterparties, other FEs within the scope of NIS2 designated at national level and entities with significant and systemic impact at national level (based on CAs' judgement), and by excluding the reporting of incidents having a	

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
		cross-border impact or those affecting TPPs/FEs as a criterion for requiring reporting over the weekend. • The ESAs have clarified the possibility for a few FEs to report major incidents in an aggregated way at national level, thus reducing the reporting effort for entities serviced by a single TPP or operating within a group.	
Reporting over the weekend / bank holidays	Many respondents were of the view that FEs shall not report major incidents over the weekend but only during business hours. In addition, several respondents indicated that the intermediate and final report should be reported only during business hours. The rationale provided by the respondents was that reporting 24/7 will have a negative impact on the FEs and pose reporting burden by adding extra cost of maintaining operational staff at no apparent added value. Moreover, many respondents viewed the 1-hour deadline for reporting the incident in the following working day as inadequate and posing unnecessary burden. Most of them suggested extending this deadline to 4 hours. Finally, some respondents indicated that reporting over the weekend should apply to significant and large institutions only that have a systemic impact. They viewed that many incidents have a cross-border impact and/or affect another FE, thus posing the risk of very wide scope of the reporting obligation over the weekend.	The ESAs agree with the arguments of the respondents and have amended the RTS to address the issues raised, including ensuring a more proportionate approach, namely by: • Not requiring reporting of a final report over the weekend. • Extending the exemption to initial notifications so that not all FEs will be required to maintain a 24/7 incident reporting support function. • Requiring the submission of an initial notification and intermediate report over the weekend only by significant or systemic institutions at EU and national level, as well as critical or important entities under NIS2. • Removing the reference to 'from where the major incident has an impact in another Member State or to another FE' from Article 6(3) of the draft RTS since it increased the scope of weekend reporting significantly. • Increasing the time-limit for submission of an initial notification, intermediate and final reports in the working day following a weekend or a bank holiday from 1 hours after the start of business hours to 12:00 of the working day.	Insert changes in Article 6, paragraphs 4 and 5 of the draft RTS.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Initial notification	The majority of the respondents suggested extending the time limits for submission of the initial notification. As mentioned in the issue related to proportionality, some respondents found the 4-hour reporting limit too short for non-critical services and suggested aligning with NIS2 (24h), or aligning with GDPR (72 hours), or that the reporting takes place in the next working day. Several respondents expressed concerns with having two separate deadlines. As part of the rationale provided, respondents highlighted that FEs will be handling the incident at the time of reporting and that some of the information requested requires input from various functions. Finally, several respondents were of the view that introducing a time limit for submitting a notification after FEs become aware of the incident may lead to significant overreporting since FEs will be forced to report the incident. Some of them sought clarity on how to approach the reporting of incident that becomes major after 24 hours from detection.	The ESAs are of the view that the timelines for classification of an incident as major are appropriate since they provide the right balance between the need of CAs to receive information to address potential systemic issues and the need of FEs to focus their resource to handle the incident. The ESAs would like to highlight that the envisaged timelines of submitting an initial notification within 4 hours from the classification of the incident but no later than 24 hours from the moment the FE has become aware of the incident provides sufficient flexibility to FEs, especially smaller ones with less complex business models and time criticality of the service, to submit the notification within the 24-hour period if they require more time to handle the incident. Nevertheless, the ESAs also acknowledge the need for FEs to prioritise the handling of the incident and not to face reporting burden at these early stages of the incident and have, therefore, reduced the number of reporting fields in the initial notification from 17 to 10 with only 7 mandatory fields. To reflect the difference in the time-criticality of the service, the ESAs have retained the two separate time limits (from moment of classification and from moment of becoming aware of the incident) for submission of the initial notification. Finally, regarding the time limit for submission of initial notification after FEs become aware of the incident, the ESAs are of the view that this should not lead to overreporting since FEs will not be obliged to classify the incident as major if there is no indication it is such. Nevertheless, to acknowledge that there may be situations where an incident has not been classified as major within the first 24 hours after FEs become aware of it, but	New proposed paragraph (2) in Article 6: '*Where an incident that has not been classified as major within the 24 hours is classified as major at a later stage, the financial entity shall submit the initial notification within the 4-hour timeline set out in paragraph 1*.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
		becomes major afterwards, the ESAs have introduced a new paragraph in Article 6.	
Intermediate report	A large number of respondents were of the view that the proposed timelines of the intermediate report are too short and that they will introduce reporting burden, especially since they are more restrictive than any existing reporting framework. Many of these respondents suggested that the time limit for submitting the intermediate report should start counting from the submission of an initial notification and not from the moment of classification of the incident. The majority have suggested that 3 working days from the submission of the initial notification should work well. Several respondents (mainly from insurance and pension sub-sector) suggested even longer timelines. A few highlighted as a rationale for the extension of the timelines that the large number of data fields, the need to coordinate between several functions and potential dependency on third-party providers introduce challenge to meet the reporting deadline. In addition, some respondents indicated that it is impossible that FEs prepare an intermediate report immediately after the recovery of the activities and suggested that the ESAs introduce a specific time-limit (e.g. 4 hours) for the submission of the report.	The ESAs agree with the rationale provided and have amended Article 6(1)(b) of the draft RTS by referring to 72 hours from the submission of the initial notification and clarifying that in any case FEs shall submit the intermediate report without undue delay after the regular activities have been recovered. This should provide additional time for FEs to collect the requested information and to prepare the report without posing burden to them while handling the incident.	Change in Article 6.1.b. of the draft RTS
Final report	A large number of respondents were of the view that the timelines for submitting a final report should be one month after the submission of the intermediate report (rather than the moment of classification). They also indicate that submitting the final report a day after the	The ESAs agree with the concerns expressed and the rationale provided by the respondents and have amended Article 6(1)(c) by requiring the submission of the final report within 1 month from the submission of the latest intermediate report and have deleted the reference to 'permanent' resolution of the incident to clarify that the aim is not covering problem management.	Change in Article 6(1)(c) of the draft RTS. Article 4(3) of the draft ITS was moved to Article 6(3) of the draft RTS.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	permanent resolution is unrealistic due to the high number of data fields to be provided. Additional rationale provided by these respondents include that the permanent resolution of the incident takes normally longer than one month after classification of an incident, that there are procedural steps for preparing the report and coordinating internally (especially for large entities), dependencies on third-party providers and the time required for carrying out the root-cause analysis. The proposed timelines for submitting the final report ranged from a few days up to 3 months after the last intermediate report. Some respondents also indicated that clarification is needed on the distinction between resolution and permanent resolution of the incident and which one is intended. Relatedly, a few respondents queried whether the final report should be updated in case the permanent resolution takes longer than 1 month. In addition a few respondents suggested longer timelines since the root cause analysis can at times also take longer than one month. A few respondents suggested moving Article 4(3) of the draft ITS in relation to informing CAs about delays in submission of the notifications/reports to Article 6 of the RTS.	The ESAs have also moved Article 4(3) of the ITS in relation to informing CAs about delays in submission of the notifications/reports to Article 6 of the RTS as suggested by the few respondents for consistency purposes.	'Where financial entities are unable to submit the initial notification, intermediate report or final report within the timelines as set out in paragraph 1, financial entities shall in-form the competent authority without undue delay, but no later than the respective time limit for submission of the notification/report, and shall explain the reasons for the delay.
Business hours / Time zones	Several respondents requested clarification on the applicable time zone for reporting of the incident.	The ESAs would like to clarify that since FEs are required to notify/report to the CA in the home Member State, it should be noted that the time zone is the one of that Member State. No changes are required in the RTS and ITS to reflect that.	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Detection of the incident	Several respondents requested a clarification of the term detection. Some of these, highlighted that there should be a distinction between incidents 'detected' by the FE and incidents reported to the FE by a TPP. Several respondents suggested referring to the moment the FE has become aware of the incident instead of the moment of detection. Some respondents also suggested clarifying who should carry out the classification of the incident in case it is detected by a third-party provider.	The ESA agree with the rationale presented in relation to the starting point of calculation of the timeline for submission of the intermediate report and have amended Article 6(1)(a) of the draft RTS by referring to the 'moment the FE has become aware of the incident' instead of the 'time of detection of the incident'. With regard to the classification of the incident, while DORA is clear that the FE is responsible for the classification, the ESAs have amended article 6(1)(a) to bring about greater clarity that it is within the responsibility of the FE.	Proposal to change article 6.1.a by referring to the 'moment the financial entity has become aware of the incident' 'the initial report shall be submitted as early as possible within 4 hours from the moment the financial entity classifies the incident as major, but no later than 24 hours from the moment the financial entity has become aware of the incident.'
Feedback on responses to question 2 (initial notification)			
Streamlining, simplifying and clarifying the initial notification	Many respondents were of the view that the initial notification should not include much detail since FEs will be handling the incident at that time and should not face reporting burden. Several respondents suggested moving the initial reference code provided by the FE to the initial notification in Annex II to the ITS in order to be consistent with the RTS. Several respondents suggested to allow the FEs to provide the contact details related to a function (e.g. function/group mailbox) instead of specific persons. A few others suggested to remove these fields or make them	To address the concerns expressed on the level of detail, the ESAs have deleted some data fields (e.g. description of the business continuation plan), moved certain fields to subsequent reports (e.g. recurring incidents) or merged fields (e.g. impact on TPPs or other FEs included in the general description of the incident). On the business continuity plan, the ESAs viewed that where such a plan is activated, the CAs may request it from the supervised entity, if needed. The ESAs have moved the incident reference code provided by the FE to the initial notification (part of Annex II to the ITS) to ensure consistency with the RTS.	The ESAs have moved data fields on recurring incidents to the final report. The ESAs have deleted the data fields on impact of the incident on TPP and FEs and included them in the field on description of the incident.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	optional as the NCAs are supposed to already have this type of information. A few respondents suggested using alternative identification codes (e.g. tax ID) instead of LEIs. A few respondents suggested adding an option 'Monitoring systems' in the field discovery of the incident. Several respondents also suggested aligning the field with the ECB and PSD2 terminology. Relatedly, some respondents suggested removing the field from the initial notification as the information may not be known or be accurate at the time of reporting. Many respondents suggested that the field on 'origination of the incident' should be either removed, made optional, or included only in the intermediate or final report as this information might not be known or sufficiently accurate at the time of the initial report. Many respondents suggested deleting the field related to information about the activation of the business continuity plan. Some of the respondents were of the view that the information may not be available during the time of submission of the initial notification, while others questioned the relevance of a full description of the information about the business continuity plans and suggested providing a high-level summary.	Regarding the contact details, the ESAs, in line with the suggestion by the respondents, included a functional team contact details in the contact details of the second contact person. However, the ESAs viewed it crucial to retain a specific person responsible as a primary contact person. The ESAs would like to highlight that LEIs allow for unequivocal identification of FEs However, to ensure consistency with the Implementing Regulation based on the DORA ITS on the register of information, the ESAs have amended the RTS and ITS by allowing TPPs reporting for FEs to provide an LEI code or any other identification code specified in the implementing technical standard specifying Art. 28(9) from Regulation (EU) 2022/2554. The ESAs have included an option 'monitoring systems', 'external audit' and 'Authority/agency/law enforcement body' in the field discovery of the incident, to address the proposals from the respondents. The ESAs do not find sufficient rationale for removing the field on 'discovery of the incident' since this information should be known to the FEs. Regarding the field 'origination of the incident' the ESAs agree that the field can be made conditional since it will depend on the type of the incident. In addition, to provide more flexibility to FEs in providing information to the CAs, the ESAs have converted the field to alphanumeric.	The ESAs have deleted the field on description of the business continuity plan. Data field on incident reference code provided by the financial entity moved to the initial notification, part of Annex II to the ITS. Additional identification code added for the fields related to TPPs reporting for FEs. Contact details of a functional team added in the fields related to the second contact person. Three additional options added in Field 2.7 Discovery of the incident. Change of the field 2.8. to conditional and alphanumeric.
Information on impacted TPP and FEs	The majority of the respondents suggested that the fields on impact on TPP and/or FEs should be either removed, made optional, or included only in the intermediate or final report as this information will likely not be known at	To address the concerns expressed by the respondents, the ESAs have included all information relevant to affected TPPs and affected FEs in the description of the incident and have indicated that this information is to be provided where known or	The specific data fields related to the impact on third-party providers and other financial entities

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	the time of the initial notification, as the FEs primarily focus on resolving the incident internally or are relying on the third-party provider to get the information. Some of these respondents proposed specific changes to the data format of the data fields, including a suggestion to combine them. A few respondents highlighted that, in practice, it will be impossible or too time-consuming for FEs to know with certainty, or to list, all affected third-party providers within the timeframe for the initial report. Therefore, they suggested to add "known affected third-party providers" in the field names and to amend the description and the instruction accordingly.	reasonably expected. This includes deleting data fields related to the Impact or potential impact on other FEs and/or TPPs and Description of how the incident affects or could affect other FEs/TPPs. Data fields 1.16 and 1.17 from the Consultation paper were deleted from the reporting template. The following text was included in the instruction of the data field 2.4 'Description of the incident': FEs, shall include, where known or reasonably expected, whether the incident impacts third-party providers or other FEs, the type of provider or FE, their name and identification codes.	have been removed and covered in data field 2.4 'Description of the incident'.
Recurring incidents	Almost half of the respondents suggested that the fields related to recurring incidents should be either removed, made optional, or included only in the intermediate or final report. The main reason put forward is that the root cause analysis is generally finalised at a later stage and, therefore, the information will not be available at the time of the initial notification. Others argued that this requirement will lead to a burdensome classification and compilation of all the minor ICT-related incidents to detect when the thresholds for reporting are reached. Finally, some respondents viewed these fields disproportionate to be submitted with the initial notification. Some of these respondents proposed specific changes to the type of data fields (multiple choice) or to be reported via a separate template. In addition, some clarification was sought on when an incident should be considered as a recurring incident, what period should be taken into account and what is a	To address the concerns expressed by the respondents, the ESAs have moved the information requested for recurring incidents to the final report. Regarding the clarifications sought, it should be noted that the reporting of recurring incidents covers non-major incidents that together are considered as one major incidents. Due to the nature of the incidents and the requirement to assess whether the incidents have the same apparent root cause, the ESAs expect that the FEs would normally become aware of such as part of their root cause analysis incidents. It should be noted that a final report should be submitted directly for such incidents, comprising all the information requested in the initial notification and intermediate report. The additional clarification sought on how to classify a recurring incident and the assessment period have been set out in the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554. In particular, the non-major incidents should have occurred at least twice within 6 months,	The data fields related to recurring incidents have been moved to the Final report. Minor changes introduced to clarify the nature of the recurring incidents.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	recurring incident. Additional clarification was sought on when and how recurring incidents should be reported.	have the same apparent root cause, and collectively qualify as a major incident.	
Feedback on responses to question 3 (intermediate report)			
Proportionality and level of detail	Many respondents commented on the level of detail of the intermediate report and proposed to decrease the number of fields or the prescriptiveness of some of the fields. Some of the respondents proposed to take a more proportionate approach by excluding certain data fields (e.g. impact in other Member States and description of the impact) from the scope of reporting for specific FEs, IORPs in particular. Some of the respondents suggested deleting the fields related to information to CSIRTS since they will not be useful for CAs. Some respondents have also indicated that particular data fields may not be available within 72 hours after classification of the incident (e.g. data and time when regular activities have been recovered, affected business areas and processes, infrastructure affected). A few respondents suggested introducing a flag in the intermediate report when services have been restored. Several respondents suggested that the fields related to communication to clients should be deleted. The main rationale provided relates to the confidentiality of some of the information, especially since parts may need to be anonymised. It was also questioned the use of this	As a general remark, the ESAs have tried to streamline and simplify the template by removing or combining data fields, or moving them to the final report. Regarding the point on proportionality, the ESAs would like to highlight that proportionality does not only focus on not applying requirements but also encompasses application of the requirements in a proportionate way. Accordingly, this should be taken into account when submitting incident reports. It should also be noted that if certain data fields are not applicable to specific FEs, they should not report on them (e.g. the fields on impact in other Member States and description of the impact). In addition, the ESAs assessed the relevance of fields for all FEs and decided to narrow down the scope of particular fields that may not apply to all FEs. In particular, the ESAs have clarified that field 3.35 'indicators of compromise' applies to FEs within the scope of NIS2 only and 4.9 on information relevant for resolution authorities applies to entities referred to in Directive 2014/59/EU. Regarding the information to CSIRTS, the ESAs agree with the respondents and have deleted the field. Moreover, the information can also be covered in field 3.31 Reporting to other authorities.	The ESAs have deleted the fields related to the information to CSIRTS and the information about communication to clients. The ESAs have changed the field on whether FEs have communicated to clients with a field on the 'Impact on the financial interest of clients'. Field on vulnerabilities exploited has been deleted. Scope of the field on indicators of compromise narrowed down to FEs within the scope of NIS2.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	information. A few respondents suggested moving it to the final report and a few others that the field should be clarified. Some respondents viewed the fields related to the infrastructure components affected as too detailed and proposed moving it to the final report. Several respondents suggested that the fields related to indicators of compromise and vulnerabilities exploited should be deleted since they contain sensitive and confidential information. The respondents also expressed concerns on sharing this information. Some respondents suggested that the field could be moved to the final report.	In relation to the availability of the information requested, the ESAs are of the view that it should be feasible for FEs to provide it, especially taking into account that the timeline for submission of intermediate report was extended with up to 24 hours by requiring the submission of the intermediate report 72 from the submission of the initial notification or when regular activities have been restored. Moreover, it should be noted that the information provided can be an estimate if no actual and final data is available. On the indication when services have been restored, the ESAs are of the view that the submission of the intermediate report and filling in field 3.3 'Date and time when services, activities and/or operations have been restored' already address this point. Accordingly, no change in the RTS and ITS is needed. In relation to communication to clients, the ESAs agree with the arguments presented and have deleted the fields and introduced a new one focusing on the impact on the financial interest of clients to be better aligned with Article 19(3) of DORA, which anyway requires FEs to inform impacted clients about the incident. On the information about specific infrastructure components being affected, the ESAs are of the view that the information is likely to be available before the final report. Even at an early stage of incident handling, the FE may be able to identify the affected infrastructure components supporting business processes when analysing the impact of the incident on its business. The level of granularity of the data in this data field serves to provide CAs with the information necessary to assess the nature of the incident and its impact and consequences on FE. This type	

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
		of information may also be relevant from NIS2 perspective. Accordingly, no change has been introduced. Regarding the field on vulnerabilities exploited, the ESAs agree with the concerns expressed and have deleted the field. On the indicators of compromise, this information cannot be deleted since DORA is lex specialis to NIS2 and NIS2 requires it at the intermediate report stage. However, the ESAs narrowed down the scope of the data field by making it applicable to FEs within the scope of NIS2 only.	
Classification criteria	Many respondents provided comments on the information requested for the classification criteria. Some of these respondents proposed that information about the classification criteria is simplified by requesting only a yes/no answer on whether the respective thresholds have been met or that information is provided in the final report. A few of these proposed changes in the catalogue of options provided in some of the criteria. Several respondents were of the view that the information on some criteria (e.g. reputational impact, clients affected) may not be available within 72 hours. Relatedly, some respondents suggested that the fields are made optional in case information is not available or difficult to calculate (e.g. impact on clients/transactions). Several respondents proposed that all data fields related to the classification criterion clients/financial counterparts/transactions affected should allow for provision of estimates. A few respondents proposed to add the following text to the instruction of the field related to value of the	The ESAs would like to highlight that the information about the classification criteria is key for assessing the impact of the incident by CAs and whether other FEs may be impacted. In relation to the remarks on the difficult to provide information about certain criteria, the ESAs would like to clarify that FEs can provide estimates in case the actual numbers are not available. Accordingly, to increase data precision and to address the related specific proposal from a few respondents, the ESAs have amended field 3.12 to indicate whether the figures are actual, estimates or whether there is no impact. The ESAs have also amended field 3.11 on the value of the transactions affected to envisage the provision of estimates. Regarding the change in the catalogue of information for the classification criteria, the ESAs would like to highlight that these are aligned with the RTS on criteria for classification of major ICT-related incidents and are not subject to change. The RTS and ITS on incident reporting merely replicate these classification criteria. Regarding the impact in other Member States, which information is crucial to understanding if additional CAs need to be informed of the incident under the forwarding set out in DORA article 19(7)	Change to field 3.12 to indicate whether the figures for clients, financial counterparts and transactions affected are actual, estimates or whether there is no impact. Change to field 3.11 to allow for the provision of estimates in relation to value of transactions affected. The ESAs have deleted the field 'comments to the classification criteria' from the template in Annex II to the ITS.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	transactions affected: 'Where the actual value of transactions impacted cannot be determined, the FE shall use estimates'. Several respondents indicated that FEs will not be able to determine how an incident has affected a third-party within another member state. They proposed that the impact in other Member States is removed or that a clarification 'if known' is included in the instructions. Some respondents did not see value added in the field 'comments to the classification criteria'. Some respondents highlighted a few typos and suggestions to align with the RTS on criteria for classification of major incidents under DORA.	the ESAs have arrived at the view that no change is needed. It should be noted that the fields are conditional since they depend on whether there has been an impact in two or more Member States. In addition, regarding the concern that impact on other FEs or TPPs may not be known, the descriptive fields provides sufficient flexibility to FEs to highlight this. On the data field 'comments to the classification criteria', the ESAs agree that the field will not add much to the descriptive information requested for each classification criterion and have removed it from the template. The ESAs would also like to highlight that the classification criteria have been amended to align with the changes made to the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554	
Types of incidents, threats and techniques	Some respondents suggested that the data fields on types of incidents is more relevant for the final report, as the type of incident may not be fully available/known during the intermediate reporting phase. A few of the respondents suggested deleting the field altogether. Some respondents also highlighted the overlap between the type of incident 'cybersecurity' and the same field covered as a malicious action in the final report template as a type of root cause. Some respondents were of the view that additional clarification is needed to distinguish between different incident types in data field 3.26, as they are often interconnected. They highlighted that a "process failure" could lead to a "cybersecurity" incident, and "external events" can cause both "cybersecurity" and "system failures". Additionally, it was highlighted that the term	The ESAs do not find compelling reasons to remove the fields on type of incidents and threats and techniques used. This fields will provide useful information to supervisors and allow ESAs to deliver on their mandate under Article 20(2) of DORA to develop a report covering the number of major ICT-related incidents, their nature and their impact on the operations of FEs or clients, remedial actions taken and costs incurred. The ESAs are also of the view that the timelines for reporting an intermediate report would allow sufficient time for FE to provide that information. It should also be noted that, in line with the RTS and ITS, the information provided can be updated with the final report in case of inaccuracies. With regard to the interdependence and partial overlap of the types of incidents and the types of root causes, it should be noted that it is not possible to delimit them precisely because of the variety of events that may lead to occurrence of the incident. For	Change in data field 3.23 on types of incidents, by amending the type 'cybersecurity' to 'cybersecurity-related'. The field other types of incidents and threats and techniques used split into two fields.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	"cybersecurity" in this context is misused. A more appropriate term would be "cyber breach" as it better aligns with the intended meaning of protecting against cyber-attacks. With regard to the threats and techniques used, some respondents highlighted that detailed information on threats and techniques used, as well as other types of incidents and techniques, may not be available at the intermediate stage and should be moved to the final report. Other respondents proposed to align the threats and techniques with other known frameworks, such as MITRE ATT&CK for better clarity.	this reason, this data field has a multiple-choice character. There is also the possibility of ticking the 'other' option, which allows FEs to indicate other options and provide an explanation about the potential other type of the incident. In order to clarify what the ESAs understand by the term "cybersecurity" within the data field on type of incident, it should be noted that DORA only refers to cybersecurity in its recitals. Accordingly, the term should be understood within the meaning of the definition in Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity), in particular 'activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'. Accordingly, the ESAs have changed the type of incidents to 'cybersecurity-related', which would include, inter alia, the term "cyber breach" (although DORA uses the term "cyber-attack" in this context). The ESAs do not consider that further clarification of the other terms from the data field 'type of incident' is needed. The terms of 'process failure', 'system failure' and 'external event' are general and broad, and the possibility to tick more than one and provide additional context is sufficient. With regard to the proposal to align the template with the MITRE ATT&CK framework, the ESAs would like to highlight that key attributes from the MITRE ATT&CK framework have already been reflected in the template. The ESAs, for proportionality reasons, do not find merit in fully aligning with said framework, to avoid posing burden on smaller entities. Finally, to ensure clarity for the industry and better quality data, the ESAs have split the field on other types of incidents and other threats and techniques used into two..	

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Clarifications of data fields	Some respondents suggested introducing various clarifications to the data fields. One group of respondents suggested clarifying how the incident reference number provided by the CA will be communicated to the FE. A few respondents suggested that the field data and time of occurrence of recurring incidents should be conditional. A few respondents sough clarity on the fields related to reporting to other authorities and highlighted that the template does not cover authorities outside of the EU. In addition, it was highlighted that communication with authorities can be confidential. A few respondents sought clarification on what is meant by 'temporary actions' and whether the relevant field would include manual workarounds for business or temporary IT/security fixes.	In relation to the incident reference number, the ESAs are of the view that CAs have discretion on how to assign it and provide it to the FE. That is the reason why the field is optional since not all CAs have the practice to appoint such numbers. On the field 'data and time of occurrence of recurring incidents', the ESAs agree it would not apply to all incidents and have amended the field as 'conditional' and not 'mandatory'. In addition, as indicated in other points, the field was moved to the Final report. On the communication with authorities, it should be noted that the information is relevant for CAs to assess the actions that need to be taken and whether and, if so, what information should be shared. No changed have been introduced to the RTS. In relation to the request for more detail around 'temporary actions', the ESAs are of the view that the instructions provided are sufficient for the reporting purposes. It should be noted that the include 'manual workarounds for business or temporary IT/security fixes'.	Change the nature of the field 'data and time of occurrence of recurring incidents' from mandatory to conditional.
Feedback on responses to question 4 (final report)			
Root cause	Some respondents questioned whether root cause analysis should be covered within the incident reporting framework. Some of these respondents also indicated that the term 'cybersecurity' has been interchangeably across different reporting fields (e.g. type of incidents, techniques used and root cause) and requested clarification on its use to avoid misunderstandings.	The ESAs would like to highlight that reporting information about the root cause is of paramount importance to supervisors to ensure effective incident management. In addition, DORA itself envisages the submission of the information by linking in Article 19(4)(c) the completion of the root cause analysis to the submission of the final report. Regarding the reference to 'cybersecurity', the ESAs agree with the comment and have removed the reference to cybersecurity from the root cause (fields 4.1 of Annex II to the ITS), to avoid	Clarification about the root cause of recurring incidents has been introduced in the instructions to field 4.1. The reference to 'cybersecurity' as a type of root cause has been deleted.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	Some respondents also expressed concerns about the potential security risks associated with the detailed disclosure of descriptive information about the root cause in field 4.3 (as well as the fields related to the description of the actions take and the assessment of their effectiveness), which may require security controls while sharing of information and adjustment of the reporting timelines. Finally, in relation to the root cause of recurring non-major incidents that together would qualify as one major incidents, several respondents expressed concerns that there is no detailed specification for identifying the root cause of these recurring incidents.	misalignment between incident type and cause. In addition, the ESAs have changed the type of incident 'cybersecurity' to cybersecurity-related' in the respective field of the intermediate report. On the comment related to security concerns for sharing information, please refer to the relevant row in the General feedback part of this Feedback table. Finally, in relation to the root cause of recurring incidents, the ESAs would like to clarify that the assessment should be performed against a specific apparent root cause of the incident and not against the broad category level. The ESAs cannot specify it further since the same apparent (and specific) root cause depends on the incident.	
Streamlining, simplifying and clarifying the final report	Many respondents suggested specific changes to the template of the final report, including deleting and clarifying specific fields. Several respondents indicated that they are not comfortable providing information, or hypothesising, about their inability to comply with legal requirements. Some of them also highlighted that providing this information would require involvement of the compliance team. Accordingly, they propose removing the field. Several other respondents sought clarify and asked for examples. Several respondents indicate that, with regards to the information about breach of contractual arrangements/ service level agreements (SLAs), it is unclear regarding how the information in the data field will be used by CAs and how the information correlates to the incident and its impact. In addition, they are of the view that contractual	The ESAs understand the concerns raised by the respondents on inability to comply with legal requirements and breach of SLAs, and agree with most of the rationale presented. Accordingly, the ESAs have decided to remove these fields. Regarding the provisions of estimates in the final report, the ESAs disagree. In line with the legal mandate, the final report shall include values that are final amounts (at the time of reporting). The ESAs agree with the proposal to split the data and time when the root cause was addressed from the data and time the incident was resolved. Regarding the field 4.9 from the template of the final report on 'Information relevant for resolution authorities', the ESAs agree with the respondents and have amended the field by focusing the scope of reporting to the FEs referred to in BRRD and have made the field conditional (if applicable). In addition, following a proposal by the Single Resolution Board, the ESAs have added a	The ESAs have removed the data fields on inability to comply with legal requirements and breach of SLAs from the final reporting template (In Annex II to the draft ITS). The ESAs have separated one data field by splitting data and time when the root cause was addressed and the data and time when the incident was resolved. The ESAs have made the field information relevant for resolution authorities

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	arrangements and SLAs are confidential and include client information that a FE will be uncomfortable in disclosing. This could place legal risk on the FE if costs were able to be linked directly to a client. Accordingly, these stakeholders proposed removing the data field. Some respondents suggest having the possibility to provide estimates of the financial information in the final report, the same as for the initial and intermediate reports. Several respondents indicated that the date and time when the incident was resolved should be distinguished from the date and time when the root cause is addressed. They recommend this data field is split into two data fields. Several respondents indicated that the incidents that would require the need to contact the Resolution Authority are rare. In addition, a few of them highlighted that some FEs are exempted from the requirements of Directive 2014/59/EU establishing a framework for the recovery and resolution of credit institutions and investment firms (BRRD). Accordingly, these respondents recommended the field to be made conditional (if applicable). Some respondents indicated that the description of measures and actions taken for the permanent resolution of the incidents should usually be covered in the problem management process and are also part of the long-term action plan, and not the incident resolution. In their view, it would in practice include change, which can be a long-tailed process and is part of other level 1 obligations under DORA that do not require reporting. They suggest limiting	complementary conditional field on the assessment of risk to critical functions for resolution purposes, which should serve to identify incidents that are relevant to resolution authorities. Regarding the field on resolution of the incident, in line with the description of the data field, it requires what are the measures the FE put in place to permanently resolve the incident and to prevent that incident from happening again in the future. With the use of the term "permanent", the ESAs aim to differentiate these "permanent" measures from the "temporary" measures that are usually linked to work-around and fall-back procedures as well BCP activation. The ESAs consider that after 1 month from the incident, the FE have sufficient information to indicate what are the measures that can permanently solve the incident, this does not mean that these measures have to necessary be implemented at the time of the reporting of the final report. In addition, the ESAs would like to underline that where FEs identify additional actions that can be implemented after having sent the final report, there is no need to provide such information through an incident report. For clarity the ESAs have amended the field name to incident resolution summary and included the lessons learnt. The ESAs also agreed with the arguments provided for removing the field on the assessment of the effectiveness of the measures taken and have removed it from the template.	conditional and have narrowed down the scope of reporting FEs. The ESAs have added a field on the assessment of risk to critical functions for resolution purposes. The ESAs have merged the fields on actions taken to resolve the incident and lessons learnt under the field 'incident resolution overview'. The ESAs have removed the data field 'effectiveness of the measures taken'.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	to the measures and actions taken to restore business service and identify root cause. Several respondents expressed concerns on the reporting of the assessment of the effectiveness of the measures taken. In their view, this information is subjective, may expose confidential information and is sensitive to report. Accordingly, they proposed removing the field.		
Information on costs and losses	Many respondents expressed concerns on the provision of detailed breakdown on the costs and losses from the incident. These respondents stressed on the reporting burden posed to FEs and on the unclear use of the detailed information by CAs, they suggested providing the total number of costs and losses or streamlining the fields significantly. Several respondents indicated that the costs and losses figures cannot be provided within 1 month following the detection of the incident. Several respondents suggested changing the type of fields from mandatory, to conditional.	The ESAs agree with the respondents and taking into account that individual information about the costs and losses can be requested by CAs in the course of their supervisory engagement with FEs, if needed, the ESAs have decided not requiring detailed breakdown of the amounts of each type of cost and loss. However, to retain clarity on what should be taken into account by FEs when calculating the costs and losses, the ESAs have moved the description and instructions fields for each type of costs and losses in a single field 4.11 on the 'Amount of gross direct and indirect costs and losses'. The ESAs would like to stress that the information about the amount of costs and losses incurred by the incident is crucial and have retained it mandatory. In the cases where the FE has not incurred costs, they can indicate '0'.	The ESAs have deleted the fields requesting detailed breakdown on the amounts of different types of costs and losses from the final report.
Feedback on responses to question 5 (significant cyber threats)			
Optional data fields	Several respondents suggested to change particular data fields (fields 10, 11, 12, 18, 19, 20 in Annex IV) from mandatory to optional, as a threat report without these fields is still valuable and each field adds time to prepare the report.	The reporting of significant cyber threats is of a voluntary nature and the provided template is very simple and streamlined requesting the very basic information about the cyber threats. Accordingly, to ensure data quality and receive meaningful	Change of data fields 10, 11 and 12 of Annex IV from mandatory to conditional (where the information is available)

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	Several respondents also suggested that all fields should be optional, except three: information about the FE, description of the threat including causes, and information on remediation. Many respondents supported the approach taken with the consultation paper.	information, the ESAs have retained the mandatory nature of most fields. Nevertheless, to simplify further the template, the ESAs have amended data fields 10-12 of Annex IV that relate to secondary contact person from mandatory to conditional (where the information is available).	
Confidentiality of data	A few respondents suggested reassuring FEs about the confidentiality of information provided by FEs in cyber threat reports, for instance by specifying where the data will be stored. Two respondents suggested to add a paragraph to Article 7 of the ITS with requirements for secure electronic channels for reporting, and a possibility for FEs to evaluate this channel.	This proposal goes beyond the scope of the legal mandate conferred by DORA to the ESAs. Regarding the confidentiality of some data fields, the ESAs would like to clarify that requesting such information is in line with DORA. As already articulated in the general section of this feedback table, the ESAs envisage that the information will be exchanged securely, ensuring data confidentiality, and that receiving authorities are subject to professional secrecy requirements. Finally, reporting channels used by the ESAs have appropriate security measures and controls in place. They are not subject to assessment of FEs.	No change.
Significant cyber threat definition	Two respondents asked for a clear definition of significant cyber threats. Two other respondents asked to clarify the difference between incident and threat.	The ESAs would like to clarify that significant cyber threat is defined in DORA. The Commission Delegated Regulation, which will be based on the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 provides further information about the nature of these cyber threats. Relatedly, the definition of a major ICT-related incident is provided in DORA and the approach for classifying major incidents set out in the aforementioned Commission Delegated Regulation. Accordingly, no changes have been introduced in the draft RTS and ITS.	No change

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
Description of the significant cyber threat"	A few respondents suggested requesting information about the modus operandi of the threat, if known. A few respondents suggested removing the risks arising from the threat, as the topic is already covered in data field 15 "Information about potential impact". Several respondents suggested removing the information about vulnerabilities, which in their view are confidential. Several respondents suggested that the information on vulnerabilities be requested only at an abstract level, to avoid risk of leakage of the notification. A few respondents suggested adding a data field for the source of information about the threat. One respondent identified a typo (duplicative entry and suggested deleting it)	The ESAs would like to clarify that data field 14 covers the most relevant parts of information about the significant cyber threat related to the FE. The ESAs disagree that the 'probability' of materialisation, which is part of the risk assessment, is important since together with data field 15 about the 'impact' define the risk with its two dimensions. The ESAs agree with the proposal to capture information about the 'source of information about the threat' and included it in Data dield 14 of Annex IV accordingly. Finally, the ESAs have deleted the duplicative entry related to the 'information about the probability of materialisation of the significant cyber threat'	Changes to data field 14 of Annex IV.
Feedback on responses to question 6 (process and format of reporting)			
Aggregated reporting	Many respondents were of the view that it should be possible for ICT third-party providers or for financial groups to submit one aggregated/consolidated report for all affected FEs. They argue that disallowing such aggregated or consolidated reporting will pose reporting burden since: - ICT service providers would have to report the same incident multiple times or would have to answer many questions of FEs within the first hours such that they can fill out reports; - FEs would need to collect all information about the incident from TPPs, including intragroup providers;	The ESAs would like to highlight that the CP already envisaged the possibility that there may be cases where several FEs outsource the incident reporting activities to a third-party service provider, including members within a financial group, in accordance with Article 19(5) of DORA and that in these cases, subject to an agreement between the FEs and their CA, it may be possible for said third-party service providers to provide one report at national level for the FEs supervised by the same CA containing the relevant individual information for each FE that would classify the incident as major. Having assessed the feedback from the respondents and the arguments presented the ESAs have decided to introduce explicitly the possibility for submission by an ICT TPPs or	The ESAs have introduced in the ITS a new Article 7 on aggregated reporting. The ESAs have introduced changes to the instructions fields in Annex II to the ITS clarifying how specific information about the incident should be reported in an aggregated manner.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
	- Financial groups would need to report the same incident multiple times; - CAs that have to analyse multiple reports of the same incident and face difficulties in aggregating the impact of the incident. Some of these respondents were of the view that the information about the incident should also be reported in an aggregated way without including individual information for each FE. The respondents propose that TPPs and financial groups should be allowed to submit one consolidated report including a list of all affected FEs to reduce the burden and to make incident reporting more efficient.	intragroup TPPs of a single aggregate report for multiple FEs affected by the same incidents. The main rationale for introducing such aggregated reporting is that it provides a holistic overview of the impact of the incident and whether it is of systemic relevance and to decrease the reporting effort by FEs and CAs. The ESAs also took into account that most of the information about the incident is likely to be available to the TPP if the incident originates from it. However, the ESAs have introduced the following conditions to ensure that such aggregated reporting is aligned with the requirements of DORA: - The incident originates or is being caused by a TPP; - The third-party provider provides relevant ICT services to more than one Fem or to a group, in the Member State; - The FEs impacted by the incident have outsourced the reporting obligations to a TPP in accordance with Art. 19(5) of DORA and Article 6 of the draft ITS; - The impact of the incident is assessed for each FE and has been classified as major individually by each FE covered in the aggregated report; - The incident has an impact in a single Member State and the aggregated report relates to FEs, which are supervised by the same CA; - The aggregated report should contain aggregated information about the impact of the incident on all FEs covered in the report;	

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
		- The aggregated report should not cover information about significant credit institutions and central counterparties, which should always report individually; - CAs have explicitly permitted aggregated reporting to those FEs; - CAs can request the submission of an individual report from each FE; and - The list of names and LEI codes need to be provided for all FEs covered by the aggregated report. Accordingly, the ESAs have introduced in the ITS a new Article 7 on aggregated reporting. The ESAs have also introduced changes to the instructions fields in Annex II to the ITS clarifying how specific information about the incident should be reported in an aggregated manner.	
Outsourcing of incident reporting	Many respondents pointed out that it should be sufficient if FEs inform CAs just once about existing outsourcing arrangement as well as of any changes but not in case of submission of each incident. One respondent was of the view that the initial notification/general information about the FE provides information about outsourcing arrangements such that further information are not necessary. One respondent is of the view that the ITS should provide clarifications on whether FEs need an authorisation from their CA on the delegation of reporting requirements to third-party service providers and whether this delegation is just based on the contractual relationship between FE and the service provider.	The ESAs agree that it is sufficient to inform CAs ones about name and contact and identification details of the third-party that will submit the report in accordance with Article 19(5) Regulation (EU) 2022/2554. This information must be submitted to the corresponding CA prior to the first report submitted by the specific third-party. The ESAs have amended Article 6 of the draft ITS to reflect on that point better. Regarding the information about the reporting TPP on behalf of the FEs in the initial notification, the ESAs would like to highlight that it serves for identification of the correct submitted of the incident report. Accordingly, provision of prior information about existing outsourcing arrangements is needed whenever a third-	The ESAs have amended Article 6 of the draft ITS by merging the existing paragraphs and clarifying that the outsourcing notification to CAs should happen only once.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
		party should submit the incident notification or report on behalf of the FE. No change required in the draft ITS. On the prior agreement of CAs with the outsourcing of the reporting of major incidents, it should be noted that CAs are responsible to identity and access management (IAM) for the reporting of major ICT-related incidents. This affects the reporting by any FEs but also the reporting of a third-party, which reports on behalf of any FE under Article 2(2) Regulation (EU) 2022/2554. This has also been reflected in Article 6 of the draft ITS.	
Data accuracy	Some respondents suggest taking into account that data accuracy is not always possible and should only be based on the information at the time of the submission of the reporting since information can be fluid and variable especially in the beginning of an incident. They suggest: - Modify article 1.2 to account for FEs providing complete and accurate information "on a best effort basis" or "to the extent possible", based on available information at the time of report submission - Delete "accurate" in article 1.3 and refer just to data being not available. One respondent proposes to amend ITS article 1.3 that estimates should be used only when data is not available, rather than "accurate data".	ESAs want to highlight that Article 1 of the ITS on major incident reporting is developed in such a way that takes into account possible difficulties in providing accurate data at the time of the submission of an incident notification or report. In particular, Article 1(2) requires that the information provided in the incident notification as well as in the intermediate and final reports to be complete and accurate. Article 1(3), however, states if accurate data is not available, which includes cases where no data is available or data is not exact enough to provide accurate information, at the time of the initial notification or the intermediate report, FEs are allowed to refer to estimates based on available data and information to the extent possible. At the latest when the final report is submitted, accurate data must be provided. Accordingly, no changes to the ITS are necessary.	No change.
Reporting language	Some respondents point out that English is the default language in many FEs, which is why a possible necessity to translate information into the language of the corresponding national CA may delay reporting.	ESAs want to underline that the technical standards will be translated into all EU official languages. The ESAs cannot impose a single language for reporting major ICT-related incidents under DORA.	No change.

Topic	Summary of responses received	ESAs' analysis	Proposed amendments to the RTS&ITS
		In addition, it should be noted that CAs are responsible for the application of the requirements in their jurisdiction, which includes, among others, defining reporting flows and specifications for FEs reporting to CAs, including the language of reporting. Accordingly, no changes to the draft ITS are required.	
Standardisation reporting process	A few respondents propose a standardised reporting template and reporting portal and ask for information on the reporting format. They suggest having one centralised reporting channel instead of multiple per Member State. Moreover, respondents are of the view that reporting should not be technologically neutral. Standardised specifications for reporting format and interfaces or a common solution for reporting major incidents across all Member States should be established. Furthermore, some respondent expresses concerns that XBRL may be too complex as reporting format and prefers a CSV or JSON solution.	The ESAs want to highlight that the reporting data flow are set out in DORA. The technical solution for reporting of major incidents from FEs to CAs and from CAs to the ESAs and related requirements are outside of the scope of the mandate. The possibility of further harmonisation of reporting is explored in a separate feasibility study concerning the establishment of a single EU Hub for major ICT-related incident reporting according to Article 21 of DORA. Accordingly, the ESAs have not introduced changes to the ITS.	No change.
Data precision	Respondent suggested to better align the approach to precision and reporting of numerical values across other DORA standards, notably ITS on Registers of Information of contractual arrangements with ICT third-party providers. Furthermore, respondents suggested to limit data precision to just one decimal for data points with the data type 'percentage'.	ESAs have aligned the requirements for data precision to align with the DORA ITS on Registers of Information, including by deleting Annex V and reviewed the approach to setting precisions in the reporting of numeric values. In particular it was clarified that (1) all monetary values shall be reporting in units with a possibility to round precision to thousands of units, e.g. a value of 5680 EUR shall be reported as 5680 or 6000, and (2) the precision of 'percentage' data points has been reduced to equivalent of one decimal. For clarity, below is an example on how to provide percentage values to provide more clarity on this question. 'Example: if 30.35% are affected, data submitted should be equal to 0.30'	Article 8(1)(a)(i) of the draft ITS has been revised and Annex V has been deleted.

JOINT COMMITTEE OF THE EUROPEAN
SUPERVISORY AUTHORITIES