JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Consultation Paper

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. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 04 March 2024. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the EBA website.

2. 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).

In fulfilment of the mandates, the draft RTS presented in the consultation paper (CP) proposes time limits for reporting of the initial notification of 4 hours after classification and 24 hours after detection of the incident, 72 hours for reporting of the intermediate report and 1 month for the reporting of the final report. The proposed time limits have been aligned with NIS2 and have been set out in a way to be proportionate for the different types and size of FEs within the scope of DORA.

In addition, the draft RTS and ITS in the CP propose the types of information to be collected with the notification/reports for major incidents and significant cyber threats, with detailed description of these types of information and instructions how to populate them provided in the Annex to the draft ITS. These types of information include 101 data points and cover, inter alia, general information about the reporting entity, the impact of the incident, the classification criteria met, the handling the incident, the root cause of the incident and the measures taken to prevent similar incidents in the future.

To ensure a balanced and proportionate approach, the draft RTS and ITS propose that the essential data fields (46%) are mandatory and the remaining one conditional, depending on the type and nature of the incident. Moreover, the CP proposes that the majority of data fields and details to be reported in the intermediate and final reports, thus allowing FEs, in particular small ones, in focusing their resources in handling the incident in the early stages after its detection.

Taking into account the voluntary nature of reporting significant cyber threats, the CP proposes short and simple template covering only essential data fields, the majority of which are conditional.

Finally, the CP proposes in the draft ITS a single template for reporting major incidents, which covers the initial notification, intermediate and final reports.

Next steps

The consultation period will run until 04 March 2024. The final draft RTS and ITS will be published after the public consultation by 17 July 2024.

3. List of abbreviations

CP – Consultation paper

CSIRT - Computer Security Incident Response Team

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

ESAs – European Supervisory Authorities

EU – European Union

FE – financial entity

ITS – Implementing Technical Standards

NIS2 – Directive (EU) 2022/2555

RTS – Regulatory Technical Standards

TS – Technical Standards

4. Background and rationale

4.1 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 financial entities 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 financial entity, 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 publicly consulted on by 11 September 2023.

6. The following chapter sets out how the ESAs are proposing to fulfil this mandate and the underlying reasoning and considerations. In addition, the Impact assessment section at the end of the Consultation paper (CP) provides additional choices and options that have been considered by the ESAs.

4.2 Rationale

7. Given that DORA aims to harmonise and streamline incident reporting for all FEs in its scope, the ESAs have arrived at the view that the RTS and ITS requirements on (i) the content of the information to be reported for major incidents under DORA and significant cyber threats, (ii) the time limits for submitting the notification and reports, and (iii) the templates and process for reporting of such incidents should be harmonised and consistent for all FEs. With the view to ensure consistency with NIS2, the proposed timelines for reporting of major incidents and the content of the notifications and reports to be submitted have been aligned to the greatest extent possible between the two technical standards (TS) and NIS2.

8. To ensure continuity of reporting under existing incident reporting frameworks and cross-sectorial harmonisation, the ESAs have arrived at the view that the requirements of the TS will have - to the greatest extent possible – reflect the experience with the various related Guidelines issued by ENISA under NIS1 (and, where available, under NIS2), and other existing sectorial legal instruments, such as the revised EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)[1], Guidelines on periodic information and notification of material changes to be submitted to ESMA by Trade Repositories[2], and others.

9. In line with the mandate under Article 20a of DORA, the proposed draft RTS has the following distinct parts:

   - General reporting requirements and timelines; and
   - Content of major incident notifications and reports, and notifications of significant cyber threats.

10. In line with the mandate under Article 20b of DORA, the proposed ITS has the following parts:

    - Format and templates for reporting major incidents and significant cyber threats; and
    - Reporting requirements.

[1] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

[2] https://www.esma.europa.eu/press-news/esma-news/esma-publishes-guidelines-periodic-information-trade-repositories

11. The following sub-sections of the Rationale section provide the underlying reasoning, considerations and some options considered for the parts of the TS indicated in paragraphs 9 and 10 above.

4.2.1 Reporting timelines

12. In line with the objective of DORA of introducing a harmonised incident reporting framework and taking into account the need to ensure simple, clear and coherent reporting requirements, the ESAs have arrived at the view that the incident reporting timelines should be harmonised for all FEs within the scope of DORA. Further details on the options considered in that regard are available in the Impact assessment section contained in the last section of this CP.

13. With regard to the reporting timelines, the ESAs have considered various timelines for the initial notification and the intermediate and final report. On the initial notification, the ESAs considered timelines ranging from submitting a notification immediately after detection of the incident up to 72 hours after the detection of the incident. In order to balance well between the objectives of (i) providing incident information promptly to CAs allowing them to take actions, including to preventing spill-over effect to other FEs, and (ii) to ensure that FEs dedicate their resources in handling the incident and have sufficient time to prepare the information requested with the initial notification, the ESAs have arrived at the view that the initial notification shall be submitted four hours from the moment of classification of the incident as major, but no later than 24 hours from the time of detection of the incident after the FE has classified the incident as major.

14. When it comes to the intermediate report, Article 19(4)(b) of DORA already provides that FEs shall submit to their CAs an intermediate report 'as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority'. Complementary, the ESAs are mandated to develop timelines for the submission of the intermediate report. In that regard, the ESAs took into account the need of CAs to receive more detailed information about the incident (e.g. detailed information on the impact of the incident, classification criteria triggered and others) without undue delay and the need of FEs to have sufficient time to obtain and prepare this detailed information. Accordingly, the ESAs have considered timelines for submission of the intermediate report ranging from 1 day up to 1 month after the submission of the initial notification. Taking into account that the intermediate report will be the first substantial and detailed information that will allow CAs to assess properly the impact or potential impact of the incident in order to take informed supervisory actions, the ESAs have arrived at the view that the most appropriate timeline for submission of the intermediate report is 3 days (72 hours) after the classification of the incident as major. In addition, the ESAs have arrived at the view that regular activities of the FE can be recovered earlier and have specified in the RTS that FEs shall submit the intermediate report to CAs 'within 72 hours from the classification of the incident as major, or sooner when regular activities have been recovered and business is back to normal'.

15. The ESAs considered which will be the most appropriate starting point to count the timelines for submission of the intermediate report, namely the date of detection, date of classification of the incident as major or date of reporting and arrived at the view that the most appropriate one is the 'date of classification of the incident'. This will allow consistency with the calculation of the timelines for submission of the initial notification and with the approach taken in NIS2.

16. Accordingly, following the requirements of DORA and the RTS, an intermediate report shall be submitted by FEs as soon as one of the below triggers have been met:

- as soon as the status of the original incident has changed significantly (Art. 19.4 DORA);
- when the handling of the major ICT-related incident has changed based on new information available (Art. 19.4 DORA);
- when regular activities have been recovered and business is back to normal (Art. 6(1)(b) of the RTS); and
- within 72 hours of the classification of the incident as major (Art. 6(1)(b) of the RTS), if the previous conditions have not been met.

17. In addition, in accordance with Art. 19.4 DORA, FEs shall update the information provided by submitting a revised intermediate report:

- when relevant status update is available (Art. 19.4 DORA); and
- upon request from the CAs (Art. 19.4 DORA).

18. In relation to the final report, which will require additional level of detail to the intermediate report, including root cause analysis and information about the actions taken, the ESAs considered timelines for submission between two weeks and 3 months. The ESAs have arrived at the view that 1 month (30 days) will be the most appropriate timeline since it will provide sufficient time for FEs to obtain all relevant information, while allowing CAs to receive the information without significant delay after the submission of the intermediate report.

19. The ESAs have also envisaged cases where the FE may not be in a position to submit an initial notification, intermediate report or final report within the timelines set out in Article 2 of the draft RTS and have introduced in Article 4 of the draft ITS the possibility for FEs to submit the notification/report with a delay, in which case, FEs shall inform their competent authority without undue delay and shall explain the reasons why.

20. Finally, when considering the above timelines for reporting of major incidents, the ESAs have taken into account the timelines set out in Article 23(4) of NIS2 (which envisages the submission of early warning, incident notification and final report within 24 hours, 72 hours and 1 month respectively) and tried aligning to the greatest extent possible. In addition, the

Question 1 – Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

ESAs aimed at setting common and harmonised timelines for reporting of major incidents under DORA that suit all types and sizes of FEs. To ensure further proportionality, the ESAs have considered that certain FEs, in particular smaller institutions, could be exempted from reporting of intermediate and final reports for major incidents over the weekend or bank holidays if the institution is not significant or the incident does not have a systemic or a cross-border impact. In these cases, the proposed Article 2(4) of the draft RTS allows FEs to submit the report in the first hour of the next working day.

4.2.2 Content of major incident notifications and reports, and notifications of significant cyber threats

21. When developing the draft RTS, the ESAs have considered various data fields to be included in the reporting requirements ensuring a balanced approach in the reporting of incidents, where:

- CAs receive all essential information about the major incident that will be of their interest;
- FEs do not face unnecessary reporting burden; and
- The information collected is useful for NIS2 authorities and resolution authorities due to the *lex specialis* nature of DORA to other legislations, namely NIS2.

22. The ESAs have proposed that the incident reporting template cover 37 specific types of data, spread between general information about the reporting FE (7 types of data), initial notification (7 types of data), intermediate report (16 types of data) and final report (7 types of data). The incident reporting template includes the following data types split by notification/reports:

a) General information - Type of report; Name, type and LEI code of the reporting and/or affected financial entity under Article 2 of DORA; Contact details of responsible persons within the affected financial entity or a third party reporting on behalf of the affected financial entity; Identification of the parent undertaking of the group, where applicable; and Reporting currency.

b) Initial notification - Date and time of detection and classification of the incident; Description of the incident; Classification criteria that triggered or are likely to trigger the incident report in accordance with the RTS under Article 18(4) of Regulation (EU)2022/2554; Members States impacted or potentially impacted by the incident, where applicable; Information about the origin of the incident; Indication on the impact or potential impact on other financial entities and/or third party providers; Information whether the incident is recurring or relates to a previous incident, where applicable; and Indication of activation of business continuity plan.

c) Intermediate report - Date and time of occurrence of the incident; Date and time when regular activities have been recovered and business is back to normal; Incident reference code; Type of the incident; Information about the classification criteria that triggered or are likely to trigger the incident report; Information on how the incident has been discovered; Information on the impact or potential impact on other financial entities and/or third party providers; Information about affected functional areas and business processes; Information about affected infrastructure components supporting business processes; Indication on communication to clients and/or financial counterparts; Information about reporting to law enforcement and other authorities where applicable; Information on whether the incident is recurring or relates to a previous incident, where applicable; Temporary actions/measures taken or planned to be taken to recover from the incident; Indication whether the incident originates from a third party provider or other financial entity; Information on vulnerabilities exploited, where applicable; and Information on indicators of compromise, where applicable.

d) Final report - Date and time when the incident was resolved permanently; Information about direct and indirect costs and losses stemming from the incident and information about financial recoveries; Information about inability to comply with legal requirements; Information about breach of contractual arrangements/SLAs; Information on the measures and actions taken by the financial entity for the resolution of the incident and additional controls to prevent similar incidents in the future; Information relevant for resolution authorities; Information about the reclassification of a major incident to non-major, where applicable.

23. The 37 types of data have been further specified and described in the Annex to the ITS, which also covers basic reporting instructions. The data glossary in the Annex II to the ITS, therefore, contains 101 data points. To ensure the balanced and proportionate approach to the reporting of major incidents, the ESAs have decided that only the essential information should be mandatory to be provided (46 data points), with the remaining data fields being conditional (54) depending on the nature of the incident. The nature of the fields is indicated in Annex II to the ITS where mandatory fields can be indicated for each notification/report, while the conditional fields are indicated in the instructions for populating the relevant field (see table below) and also marked as 'mandatory, if applicable'.

Table 1: detailed breakdown of the nature of the data fields in the DORA incident reporting template

Report	Mandatory fields	Conditional fields
General information	10	8
Initial notification	9	8
Intermediate report	15	24
Final report	12	15
TOTAL	46	55

24. The ESAs have also strived at taking a proportionate approach, which is reflected in the nature of the data fields highlighted above where less than half of the fields are of mandatory nature, thus providing flexibility for FEs, with smaller entities most likely to benefit from it. In addition, to avoid reporting burden on the FEs, smaller entities in particular, the ESAs have proposed the more detailed fields to be reported with the intermediate and final reports since FEs will have more time to prepare these.

Question 2 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 3 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 4 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

25. When it comes to the data fields on the reporting of significant cyber threats, the ESAs have taken into account the voluntary nature of their reporting in accordance with Article 19 of DORA and that in order to encourage the reporting of such threats, the reporting template should not pose any burden to FEs to prepare and submit it to CAs. Accordingly, the ESAs have arrived at the view that the template should be short, simple, that it leverages on the data fields used for incident and reflecting the specificities of significant cyber threats as set out in the RTS on the criteria for classification of major incidents and significant cyber threats under DORA.

26. In that regard, the ESA have proposed in this CP the following data fields:

- general information about the FE;
- date and time of detection of the cyber threat
- description of the significant cyber threat;
- information about potential impact;
- potential incident classification criteria;
- status of the cyber threat;
- actions taken to prevent materialisation;
- notification to other stakeholders; and
- indicators of compromise.

Question 5 – Do you agree with the data fields proposed in the draft RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.

4.2.3 Format, templates and reporting requirements

27. The ESAs have assessed various ways of approaching the reporting of major incidents under DORA, namely:

    - submitting the notification and reports in an incremental manner;
    - having a structured intermediate and final report and a general free text field for the initial notification; and
    - introducing a single template covering the initial notification, intermediate and final reports.

28. The ESAs have considered various aspects related to the reporting template, such as ensuring good quality of the data received, standardisation of fields allowing automated processing of the data, providing flexibility to FEs by requiring a minimum set of mandatory fields and the possibility for covering additional data on voluntary basis, the technical implementation by FEs, CAs and ESAs. Based on these, the ESAs have arrived at the view that the approach that balances best between these aspects is to introduce a single template covering the initial notification, intermediate and final reports with data fields, which will clearly indicate which fields are expected to be submitted with the respective notification/report. With regard to updates of the information, the ESAs the draft ITS requires financial entities to update the information provided with previous notification/report (e.g. updating the information provided with the initial notification when submitting the intermediate report).

29. In addition, the ESAs have considered whether the reporting should be on solo basis only or whether it should take into account reporting on consolidated/aggregated basis, where possible. After having assessed the legal requirements of Chapter III of DORA, in particular Article 18, which focuses on the impact of the incident on the specific FE, the ESAs have arrived at the view that the reporting should be on solo basis only and have designed the reporting template accordingly.

30. 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. In that case, upon receipt of the notification envisaged in Article 6 of the draft ITS and 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.

31. In the cases where the incident impacts FEs in different Member States, the respective TPP, in line with DORA and the RTS, would need to submit the respective reports to the CA where the FE is established.

32. When composing the procedures and other reporting requirements for the purpose of the ITS, the ESAs have followed an approach where the draft ITS centers around the template for reporting and supporting technical details designed in the similar way as other prudential reporting requirements. The approach to major incidents and significant cyber threats reporting set out in the Annexes to the draft ITS in a technology agnostic way. The draft ITS provide a data glossary, instructions on how to populate the data fields, the key characteristics of the data fields, and a clear indication on the nature of the data fields (mandatory or conditional).

33. The ESAs have also introduced in Article 3 of the ITS standard reporting requirements aiming at ensuring the submitted information is complete, accurate and comprehensive. The ESAs have also envisaged provisions for the reclassification of incidents from major to non-major in cases where the FE has observed that the incident has not met at any time the classification criteria.

34. In addition, the ESAs have envisaged specific aspects to facilitate the incident reporting by financial entities, namely by allowing FEs to submit all notifications and reports with one template in one submission. This applies to the cases where the FE has identified, assessed and resolved the incident quickly enough.

Question 6 – Do you agree with the proposed approach to reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

5. 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 limites for reporting major incidents should be consistent for all types of financial entities. The time limits should also be consistent, to the greatest extent possible, with 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. 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 notificaiton, 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 or that do not provide services across different Member States, in particular over 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.

(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[3]

HAS ADOPTED THIS REGULATION:

Article 1
General provisions

Financial entities shall provide the content of the initial notification, the intermediate report or the final report 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 notifications, intermediate and final reports

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

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

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 which of those entities referred to in Article 2(1) of Regulation (EU)2022/2554 it is authorised or registered as;
c) Contact details of the contact person responsible for communicating with the competent authority;
d) The parent undertaking of the group, where applicable; and
e) 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) Date and time of detection and classification of the incident;
b) Description of the incident;
c) Classification criteria that triggered the incident report in accordance with [Articles 1 to 8 of Delegated Regulation [insert number once published in official journal];
d) Members States impacted or potentially impacted by the incident, where applicable;
e) Information on how the incident has been discovered;
f) Information about the source of the incident, where available;
g) Indication whether there has been impact or potential impact on other financial entities and any third party providers, where applicable;
h) Information whether the incident is recurring or relates to a previous incident, where applicable;
i) Indication whether a business continuity plan has been activated; and
j) Other information.

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;
b) Date and time of occurrence of the incident;
c) Date and time when regular activities have been recovered to levels as they were prior to the incident; and
d) Information about the classification criteria that triggered the incident report;
e) Type of the incident;
f) Information about affected functional areas and business processes;
g) Information about affected infrastructure components supporting business processes;

h) Indication whether a communication to clients or financial counterparts has taken place;
i) Information about reporting to other authorities, where applicable;
j) Temporary actions taken or planned to be taken to recover from the incident;
k) Information on vulnerabilities exploited, where applicable; 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 cause of the incident
b) Information about inability to comply with legal requirements;
c) Information about breach of contractual arrangements/SLAs;
d) Date and time when the incident was resolved and the root cause addressed;
e) Information on the measures and actions taken by the financial entity for the resolution of the incident and additional controls to prevent similar incidents in the future;
f) Information about the reclassification of a major incident to non-major, where applicable;
g) Information relevant for resolution authorities; and
h) Information about direct and indirect costs and losses stemming from the incident and information about financial recoveries.

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 time of detection of the incident.
    b) an intermediate report shall be submitted within 72 hours from the classification of the incident as major, or when regular activities have been recovered and business is back to normal.
    c) the final report shall be submitted no later than 1 month from the classification of the incident as major, unless the incident has not been resolved. In that latter case, the final report shall be submitted the day after the incident has been resolved permanently.
2. Where the deadline for submission of an intermediate report or a final report falls on a weekend day or a bank holiday in the Member State of the reporting financial entity,

financial entities may submit the intermediate or final reports within one hour following regular starting time of the next working day.

3. Paragraph 2 shall not apply where the major incident has an impact in another Member State or to another financial entity or that the financial entity is a significant credit institution, a financial market infrastructure or a financial entity deemed significant or systemic by the competent authority for the national market. In this case, the financial entities shall apply the time limits set out in paragraphs 1.

Article 7
Content of the notification of significant cyber threat

Financial entities shall provide to competent authorities with the following information in relation to significant cyber threats with the notification in accordance with Article 19(2) of Regulation (EU) 2022/2554:

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 materisalised;
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.

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

6. Draft implementing 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 identified 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[4] .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

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

throughout the reporting stages that should be used for the submission of the initial notification, the interim 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 interim 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 (EU) 2024/XXX [insert OJ number of RTS on classification of major incidents].

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

5. 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.

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

7. This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Supervisory Authorities (ESAs, European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA)).

8. 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, 1094/2014, 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 [insert OJ number of RTS on content of reports][5]. Financial entities may complete data fields which are required with submission of the interim or final report, where they have the relevant information.

(b) Where an interim 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 [insert OJ number of RTS on content of reports]. Financial entities may complete data fields which are be required with submission of the final report, where it has 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 [insert OJ number of RTS on content of reports].

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

3. Where accurate data is not available 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 shall be able to submit the information requested within the initial notification, intermediate report or final report, to competent authorities at the same time with one submission, where applicable.

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 16 of Commission Delegated Regulation (EU) 2024/XXX [insert number of RTS on classification of major incidents], financial entities shall provide aggregated information regarding such incidents.

[5] Full title plus OJ reference

Article 4

Use of secure channels and notification of competent authorities in case of deviation from established channels or time limits

1. Financial entities shall use secure electronic channels to submitting intimal notification and intermediate and final reports as agreed with the competent authorities.
2. Where financial entities are unable to use established channels to submit incident notifications or reports to the competent authorities, financial entities shall inform competent authorities about the major incident through other secure means, after consulting with or as previously agreed with the competent authority, in accordance with the time limits set out in Article 6 of Commission Delegated Regulation [insert OJ number of RTS on content of reports]. Financial entities shall resubmit the initial notification, intermediate or final report, as relevant, through the established channels once they are able to do so.
3. Where financial entities are unable to submit the initial notification, intermediate report or final report within the timelines as set out in Article 6(1) of Commission Delegated Regulation [insert OJ number of RTS on content of reports], financial entities shall inform the competent authority without undue delay, but no later than 24 hours, and shall explain the reasons for the delay.

Article 5

Reclassification of major incidents

Financial entities shall reclassify a major incident as non-major, 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 Delegated Regulation (EU) 2024/XXX [insert OJ number of RTS on classification of major incidents RTS]. In that case, financial entities shall submit a final report completing only the information related to the reclassification of the major incident as non-major.

Article 6

Outsourcing of the reporting obligation

1. Where financial entities outsource the incident reporting obligation in accordance with Article 19(5) of Regulation (EU) 2022/2554, they shall inform the competent authorities prior to any notification or reporting and indicate the name and contact details, including Legal Entity Identifier (LEI), of the third party that will submit the incident notification or report on their behalf. Financial entities shall also inform competent authorities where such outsourcing does no longer take place or has been cancelled.
2. Where outsourcing arrangements are of long-term or general nature, financial entities shall notify the competent authority prior to any notification or reporting and provide details, including the LEI codes, of the third party that will be submitting the incident notification of reports.

Article 7

Standard form for 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 to the extent possible.

Article 8

Data precision and information associated with submissions.

1. Financial entities shall submit the information referred to in this Regulation in the data exchange formats and representations specified by competent authorities and respecting the data point definition of the data point model and the validation formulas specified in Annex V as well as the following specifications:
   (a) numeric values shall be submitted as facts pursuant to the following conventions:
      i. data points with the data type 'Monetary' shall be reported using a minimum precision equivalent to thousands of units;
      ii. data points with the data type 'Percentage' shall be expressed as per unit with a minimum precision equivalent to two decimals;
      iii. data points with the data type 'Integer' shall be reported using no decimals and a precision equivalent to units.
2. Financial entities and third parties submitting data specified in this Regulation on behalf of the financial entities affected by the incident shall be identified by their Legal Entity Identifier (LEI).

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 Presiden

JOINT COMMITTEE OF THE EUROPEAN
SUPERVISORY AUTHORITIES

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	LEI of the entity submitting the report	
1.4	Type of the entity submitting the report	
1.5	Name of the financial entity affected	
1.6	Type of financial entity affected	
1.7	LEI code of the financial entity affected	
1.8	Primary contact person name	
1.9	Primary contact person email	
1.10	Primary contact person telephone	
1.11	Second contact person name	
1.12	Secondary contact person email	
1.13	Second contact person telephone	
1.14	Name of the ultimate parent undertaking	
1.15	LEI code of the ultimate parent undertaking	
1.16	Name of affected third party providers	
1.17	LEI code of affected third party providers	
1.18	Reporting currency	
Content of the initial notification		
2.1	Date and time of detection of the incident	

Number of field	Data field	
2.2	Date and time of classification of the incident as major	
2.3	Description of the incident	
2.4	Classification criteria that triggered the incident report	
2.5	Materiality thresholds for the classification criterion 'Geographical spread'	
2.6	Discovery of the incident	
2.7	Indication whether the incident originates from a third party provider or another financial entity	
2.8	Impact or potential impact on other financial entities and/or third-party providers	
2.9	Description of how the incident affects or could affect other financial entities	
2.10	Description of how the incident affects or could affect third-party providers	
2.11	Information whether the major incident has been recurring	
2.12	Number of occurrences of the same incident	
2.13	Information on whether the incident relates to a previous incident	
2.14	Activation of business continuity plan, if activated	
2.15	Business continuity plan: description	
2.16	Other information	
Content of the intermediate report		
3.1	Incident reference code provided by the financial entity	
3.2	Incident reference code provided by the competent authority	
3.3	Date and time of occurrence of the incident	
3.4	Date and time of occurrence of recurring incidents	
3.5	Date and time when services, activities and/or operations have been restored	
3.6	Number of clients affected	
3.7	Percentage of clients affected	
3.8	Number of financial counterparts affected	
3.9	Percentage of financial counterparts affected	
3.10	Impact on relevant clients or financial counterpart	

Number of field	Data field	
3.11	Number of affected transactions	
3.12	Percentage of affected transactions	
3.13	Value of affected transactions	
3.14	Information whether the numbers are actual or estimates	
3.15	Reputational impact	
3.16	Contextual information about the reputational impact	
3.17	Duration of the incident	
3.18	Service downtime	
3.19	Information whether the numbers for duration and service downtime are actual or estimates.	
3.20	Types of impact in the Member States	
3.21	Description of how the incident has an impact in other Member States	
3.22	Materiality thresholds for the classification criterion 'Data losses'	
3.23	Description of the data losses	
3.24	Materiality thresholds for the classification criterion 'Critical services affected'	
3.25	Comments to the classification criteria	
3.26	Type of the incident	
3.27	Threats and techniques used by the threat actor	
3.28	Other types of techniques	
3.29	Information about affected functional areas and business processes	
3.30	Affected infrastructure components supporting business processes	
3.31	Information about affected infrastructure components supporting business processes	
3.32	Communication to clients/financial counterparts	
3.33	Information about communication to clients/financial counterparts	
3.34	Reporting to other authorities	
3.35	Specification of 'other' authorities	

Number of field	Data field	
3.36	Temporary actions/measures taken or planned to be taken to recover from the incident	
3.37	Description of any temporary actions and measures taken or planned to be taken to recover from the incident	
3.38	Information on involvement of CSIRTs in dealing with the incident	
3.39	Information on involvement of CSIRTs in dealing with the incident	
3.40	Indicators of compromise	
3.41	Vulnerabilities exploited	
Content of the final report		
4.1	Root causes of the incident	
4.2	Other types of root cause types	
4.3	Information about the root causes of the incident	
4.4	Information about inability to comply with legal requirements	
4.5	Information about breach of contractual arrangement/SLAs	
4.6	Description of the measures and actions taken for the permanent resolution of the incident	
4.7	Assessment of the effectiveness of the actions taken and lessons learnt	
4.8	Date and time when the incident was resolved and the root caused addressed	
4.9	Information if the permanent resolution date of the incidents differs from the initially planned implementation date	
4.10	Information relevant for resolution authorities	
4.11	Reclassification of the incident from major to non-major	
4.12	Reasons for the reclassification	
4.13	Materiality threshold for the classification criterion ‘Economic impact’	
4.14	Amount of gross direct and indirect costs and losses	
4.15	Amount of expropriated funds or financial assets for which the financial entity is liable, including assets lost to theft	

Number of field	Data field	
4.16	Amount of replacement or relocation costs of software, hardware or infrastructure	
4.17	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	
4.18	Amount of fees due to non-compliance with contractual obligations	
4.19	Amount of customer redress and compensation costs	
4.20	Amount of losses due to forgone revenues	
4.21	Amount of costs associated with internal and external communication	
4.22	Amount of advisory costs, including costs associated with legal counselling, forensic and remediation services	
4.23	Amount of other costs and losses	
4.24	Amount of financial recoveries	
4.25	Details related to the economic impacts	

EBA EUROPEAN BANKING AUTHORITY eiopa ESMA European Securities and Markets Authority JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

ANNEX II

Data glossary and instructions for the reporting of major incidents

Data field	Description	Instructions	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: a) initial notification b) intermediate report c) final report
1.2. Name of the entity submitting the report	Full legal name of the entity submitting the report		Yes	Yes	Yes	Alphanumeric
1.3. LEI of the entity submitting the report	Legal Entity Identifier (LEI) of the entity submitting the report assigned in accordance with the International Organisation for Standardisation. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.		Yes	Yes	Yes	Alphanumeric
1.4. Type of the entity submitting the report	Type of the entity under Article 2.1(a)-(t) of DORA submitting the report		Yes	Yes	Yes	Choice (multiselect) from the pre-defined list of DORA financial entities.

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
						'Other' for entities not listed in Article 2.1 of DORA
1.5. Name of the financial entity affected	Full legal name of the financial entity affected by the major ICT-related incident.	Field mandatory if the financial entity affected by the incident is different from the entity submitting the report.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
1.6. Type of financial entity affected	Type of the financial entity under Article 2.1(a)-(t) of DORA affected by the major ICT-related incident.	Field mandatory if the financial entity affected by the incident is different from the entity submitting the report.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Choice (multiselect): Article 2.1 points (a) to (t) of DORA Regulation
1.7. 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. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.	Field mandatory if the financial entity affected by the incident is different from the entity submitting the report.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
1.8. Primary contact person name	Name and surname of the primary contact person of the financial entity		Yes	Yes	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
1.9. Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication		Yes	Yes	Yes	Alphanumeric (email format)
1.10. Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication		Yes	Yes	Yes	Number (telephone format)
1.11. Second contact person name	Name and surname of the second contact person of the financial entity or an entity submitting the report on behalf of the financial entity		Yes	Yes	Yes	Alphanumeric
1.12. Secondary 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 (email format)
1.13. Second contact person telephone	Telephone number of the second contact person that can be used by the competent authority for follow-up communication		Yes	Yes	Yes	Number (telephone format)
1.14. Name of the ultimate	Name of the ultimate parent undertaking of the group in which	Field mandatory if the FEs belongs to a group.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
parent undertaking	the affected financial entity belongs to, where applicable					
1.15. 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. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.	Field mandatory if the FEs belongs to a group.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
1.16. Name of affected third party providers	Name of the third party provider(s) affected by the incident, where applicable.	To be provided only where the third party provider is different from the entity submitting the report. Where there are multiple third party providers affected, the financial entity shall provide the names of all affected third party providers.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
1.17. LEI code of affected third party providers	LEI of the third party provider(s) affected by the incident. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.	To be provided only where the third party provider is different from the entity submitting the report.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		Where there are multiple third party providers affected, the financial entity shall provide the LEI of all affected third party providers.				
1.18. 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. Date and time of detection of the incident	Date and time at which the ICT-related incident was detected.	For recurring incidents, the data and time at which the last ICT-related incident was detected.	Yes	Yes	Yes	dd/mm/yyyy hh:mm
2.2. 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	dd/mm/yyyy hh:mm
2.3. 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. In subsequent reports, the field content can	Yes	Yes	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		evolve over time to reflect the ongoing understanding of the ICT-related incident. Description of any other relevant information about the incident not captured by the data fields, including the internal severity assessment by the financial entity. For recurring incidents, financial entities shall provide information about each recurring incident, including date and time of its occurrence.				
2.4. Classification criteria that triggered the incident report	RTS classification criteria that have triggered determination of the ICT-related incident as major and subsequent notification		Yes	Yes	Yes	Choice (multiple): (a) Clients, financial counterparts and transactions affected (b) Reputational impact (c) Duration and service downtime (d) Geographical spread (e) Data losses (f) Critical services affected (g) Economic impact
2.5. Materiality	EEA Member States impacted by the ICT-related incident	Financial entities shall have regard to Articles 4 and 12 of the RTS on	Yes, if applicable	Yes, if applicable	Yes, if applicable	Choice (multiple) populated by using ISO

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
thresholds for the classification criterion 'Geographical spread'		classification of ICT-related incident for more details). Mandatory to be reported with the initial notification and intermediate and final reports if 'Geographical spread' threshold is met.				3166 ALPHA-2 of the affected countries
2.6. Discovery of the incident	Indication of how the incident has been discovered.		Yes	Yes	Yes	Choice: (a) IT Security (b) Staff (c) Internal audit (d) Clients (e) Financial counter-parts (f) Third-party provider (g) Attacker (h) Other (specify)
2.7. Indication whether the incident originates from a third party provider or	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 or another financial entity (including financial entities belonging to the same group as the reporting entity).	Yes	Yes	Yes	Choice: (a) Third party provider (b) Financial entity (c) Not applicable

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
another financial entity						
2.8. Impact or potential impact on other financial entities and/or third-party providers	Indicator as to whether the financial entity is aware of, or reasonably expects, a significant impact on other financial entities and/or third parties both at national level or in another Member State.		Yes	Yes	Yes	Choice: (a) Yes (b) No (c) No information available
2.9. Description of how the incident affects or could affect other financial entities	Description of how other financial entities have been affected by the incident, where known, or reasonably expected	Description of how other financial entities have been affected by the incident, where known, or reasonably expected. The description should include the following information about the other financial entities, if known: 1. name/group/activity/region, 2. entity type(s), 3. description of disruption incurred, 4. relationship (counterparty/service recipient/service provider).	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		Mandatory only if answer the incident has impacted or has the potential to impact other financial entities.				
2.10. Description of how the incident affects or could affect third-party providers	Description of how third-party providers have been affected by the incident where known, or reasonably expected	Description of how third-party providers have been affected by the incident where known, or reasonably expected. The description should include the following information about the third-party provider(s), if known: 1. name/group/activity/region, 2. service provided and their type, 3. criticality of service, 4. description of disruption incurred, 5. location of incident source if known Mandatory only if the incident has impacted or has the potential to impact third party providers	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
2.11. Information whether the major incident has	Information on whether the incident is being reported under Article 16 of RTS on criteria for classification of major incidents under DORA.		Yes	Yes	Yes	Boolean (Yes or No)

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
been recurring						
2.12. Number of occurrences of the same incident	Number of occurrences of previously reported incident	If Field ("Information on whether the incident relates to a previous incident") is populated with "yes", indicate the number of times the same incident occurred over the reference period referred to in Article 16(1) of RTS on criteria for classification of major incidents under DORA. Field mandatory if the major incident has been recurring.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Integer
2.13. Information on whether the incident relates to a previous incident	Incident reference code assigned by the competent authority of the previously notified incident	Where the incident relates to a previously reported incident, financial entities shall indicate the incident reference number of the previously notified incident	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
2.14. Activation of business continuity	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	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
plan, if activated						
2.15. Business continuity plan: description	The description of the elements of business continuity plan activated	The description shall include: • the plan element(s) activated (e.g. full DR, specific recovery playbook, crisis communications) • date and time of activation of this measure • the extent to which this activation has addressed or is expected to address the incident <full recovery in x hours, partial recovery of critical services in y hours with full service resumption in z hours> Data field mandatory if the business continuity plan has been activated.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
2.16. Other information	Any further information not covered in the template	Field mandatory if there is other information not covered in the template.	Yes, if applicable	Yes, if applicable	Yes, if applicable	Alphanumeric
Content of the intermediate report						
3.1. Incident reference code provided by	Unique reference code issued by the financial entity unequivocally identifying the major incident.		Yes	Yes	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
the financial entity						
3.2. 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	
3.3. Date and time of occurrence of the incident	Date and time at which the ICT-related incident has occurred, if different from the time of detection	For recurring incidents, the date and time at which the last ICT-related incident has occurred.	No	Yes	Yes	dd/mm/yyyy hh:mm
3.4. 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.	Data field is mandatory for recurring incidents	No	Yes, if applicable	Yes, if applicable	dd/mm/yyyy hh:mm
3.5. Date and time when services, activities and/or	Information on the date and time of the restoration of the services, activities and/or operations affected by the incident	Data field mandatory to be reported with the intermediate report if data field 3.17. 'Service downtime' has been populated.	No	Yes, if applicable	Yes, if applicable	dd/mm/yyyy hh:mm

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
operations have been restored		Data field mandatory where the incident has caused a service downtime.				
3.6. 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(c) of the RTS on classification of ICT-related incident 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.	No	Yes	Yes	Integer
3.7. 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 RTS on classification of ICT-related incident for more details).	No	Yes	Yes	Percentage
3.8. 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 RTS on classification of ICT-related incident for more details. Where the actual number of financial counterparts impacted cannot be	No	Yes	Yes	Integer

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		determined, the financial entity shall use estimates based on available data from comparable reference periods.				
3.9. 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(b) of the RTS on classification of ICT-related incident for more details.	No	Yes	Yes	Percentage
3.10. Impact on relevant clients or financial counterpart	Any identified impact on relevant clients or financial counterpart in accordance with Articles 1.3 9.1(f) of the RTS on classification of ICT-related incident.	Mandatory to be reported with the intermediate and final reports if 'Relevance of clients and financial counterparts' threshold is met.	No	Yes, if applicable	Yes, if applicable	Boolean (Yes or No)
3.11. Number of affected transactions	Number of transactions affected by the ICT-related incidents.	In accordance with article 1.4 of the RTS on classification of ICT-related incident, 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.	No	Yes, if applicable	Yes, if applicable	Integer

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		Field mandatory to be reported with the intermediate and final reports if any transactions have been affected by the incident.				
3.12. Percentage of affected transactions	Percentage of affected transactions in relation to the regular level 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 RTS on classification of ICT-related incident. Field mandatory to be reported with the intermediate and final reports if any transactions have been affected by the incident.	No	Yes, if applicable	Yes, if applicable	Percentage
3.13. Value of affected transactions	Total value of the transactions affected by the ICT-related incident in accordance with Article 1.4 and article 9.1(e) of the RTS on classification of ICT-related incident.	Field mandatory to be reported with the intermediate and final reports if any transactions have been affected by the incident.	No	Yes, if applicable	Yes, if applicable	Monetary
3.14. Information whether the numbers are actual or estimates	Information whether the values reported in the data fields 3.5. to 3.12. are actual or estimates.		No	Yes	Yes	Choice: (a) Actual figures (b) Estimates (c) Actual figures and estimates (d) No information available

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.15. Reputational impact	Information about the reputational impact resulting from the incident in accordance with Article 2 and Article 10 of the RTS on classification of ICT-related incident.	Mandatory to be reported with the intermediate and final reports if 'Reputational impact' criterion met.	No	Yes, if applicable	Yes, if applicable	Choice (multiple): (a) the incident has attracted media attention; (b) The financial entity has received complaints from different clients or financial counterparts; (c) Data exfiltrated from the financial entity has been disclosed without its consent (d) The financial entity will not be able to or is likely not to be able to meet regulatory requirements; (e) The financial entity is likely to lose clients or financial counterparts with an impact on its business as a result of the incident.)

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.16. 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 may include additional information, such as type of media (e.g. traditional, social media, blogs, social networks, 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	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		misinformation spread by threat actors, or information relating to or illustrating defacement of the financial entity's website. Field mandatory to be reported with the intermediate and final reports if 'Reputational impact' criterion met.				
3.17. 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 the incident will be resolved, they shall apply estimates. The value shall be expressed in days and hours.	No	Yes	Yes	DD:HH:MM
3.18. Service downtime	Service downtime measured from the moment the service(s)is fully or partially unavailable to clients and/or financial counterparts to the moment when regular activities/operations have been restored to the level of service(s)	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	No	Yes, if applicable	Yes, if applicable	DD:HH:MM

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	that was provided prior to the incident. Where multiple services are impacted, the service downtime should measure until all services are restored.	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. Field mandatory to be reported with the intermediate and final reports if the incident has caused a service downtime.				
3.19. Information whether the numbers for duration and service downtime are actual or estimates.	Information whether the values reported in data fields 3.16 and 3.17. are actual or estimates.	Mandatory to be reported with the intermediate and final reports if 'Duration and service downtime' criterion met.	No	Yes, if applicable	Yes, if applicable	Choice: (a) Actual figures (b) Estimates (c) Actual figures and estimates (d) No information available
3.20. Types of impact in the Member States:	Type of impact in the respective EEA Member States. Mandatory to be reported with the intermediate and final reports if 'Geographical spread' threshold is met.	Indication of whether the major ICT-related incident has had a significant 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 19 of the RTS on	No	Yes, if applicable	Yes, if applicable	Choice (multiple): (a) clients; (b) financial counterparts; (c) branch of the financial entity;

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		criteria for classification of major ICT-related incidents, including on: a) The clients and financial counterparts affected; or b) Branches of the financial entity or other financial entities within the group carrying out activities in the respective Member State; or c) Financial market infrastructures or third-party providers that may be common with other financial entities. Mandatory to be reported with the initial notification and intermediate and final reports if 'Geographical spread' threshold is met.				(d) financial entities within the group carrying out activities in the respective Member State; (e) financial market infrastructure; (f) third-party providers that may be common with other financial entities.
3.21. Description of how the incident has an impact in other Member States	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 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	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		f) Third-party providers that may be common with other financial entities as applicable in other member state(s). Mandatory to be reported with the intermediate and final reports if 'Geographical spread' threshold is met.				
3.22. 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 RTS on classification of ICT-related incident. Mandatory to be reported with the intermediate and final reports if 'Data losses' criterion is met.	No	Yes, if applicable	Yes, if applicable	Choice (multiple): (a) availability (b) authenticity (c) integrity; (d) confidentiality
3.23. 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 RTS on classification of ICT-related incident. Information about the impact on the implementation of the business objectives of the financial entity and/or on meeting regulatory requirements. As part of the information provided, financial entities shall indicate whether the data affected is client data, other entities'	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		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 spearphishing attacks, to disclose information publicly. Mandatory to be reported with the intermediate and final reports if 'Data losses' criterion is met.				
3.24. Materiality thresholds	Information related to the criterion 'Critical services affected'	In accordance with Articles 6 and 14 of the RTS on classification of ICT-related incident, including information about:	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
for the classification criterion 'Critical services affected'		- the affected services or activities that require authorisation; and/or - the ICT services that support critical or important functions of the financial entity; and - the escalation to senior management or management body outside any periodical notification procedure, including the date of escalation. Mandatory to be reported with the intermediate and final reports if 'Critical services affected' criterion met.				
3.25. Comments to the classification criteria	Any further information related to the classification criteria	Mandatory to be reported with the intermediate and final report if there is additional information available.	No	Yes, if applicable	Yes, if applicable	Alphanumeric
3.26. Type of the incident	Classification of incidents by type		No	Yes	Yes	Choice (multiple): (a) Cybersecurity (b) Process failure (c) System failure (d) External event (e) Other (please specify)

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.27. Threats and techniques used by the threat actor	Indicate the threats and techniques used by the threat actor.	The following threats and techniques shall be considered: 1. Social engineering, including phishing 2. (D)DoS 3. Data encryption for impact, including ransomware 4. Resource hijacking 5. Data exfiltration and manipulation, including identity theft 6. Data destruction 7. Defacement 8. Supply-chain attack 9. Other (please specify) Field mandatory if the type of the incident is 'cybersecurity' in field 3.26.	No	Yes, if applicable	Yes, if applicable	Choice (multiple): 1. Social engineering (including phishing) 2. (D)DoS 3. Data encryption for impact, including ransomware 4. Resource hijacking 5. Data exfiltration and manipulation, including identity theft 6. Data destruction 7. Defacement 8. Supply-chain attack 9. Other (please specify)
3.28. Other types of incidents and techniques	Other types of incidents and techniques	Where financial entities have selected 'other' type of techniques in data field 3.27, financial entities shall specify the type of root cause. Field mandatory to be reported with the intermediate report if 'other' type of	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		incidents or techniques is selected in data field 3.26 and 3.27.				
3.29. Information about affected functional areas and business processes	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: • 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	No	Yes	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		• Buying and selling packages insurances policies between insurances • Card payments • Cash management • Cash placement and/or withdrawals • Claim management • Claim process insurance • 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				

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		• Lending management • Life insurance payments process • Money remittance • Net asset calculation • Order • Payment initiation • Policy underwriting issuance • Portfolio management • Premium collection • Reception/transmission/execution • Reinsurance • Settlement • Transaction monitoring				
3.30. 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: (a) Yes (b) No (c) Information not available
3.31. Information about	Description on the impact of the incident on infrastructure components supporting business	Hardware includes servers, computers, data centres, switches, routers, hubs. Software includes operating systems,	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
affected infrastructure components supporting business processes	processes including hardware and software.	applications, databases, security tools, network components, others please specify. The descriptions should include the following the description or name of affected infrastructure components or systems, which may be complemented with the following information, where available: • Version information • Internal infrastructure/partially out-sourced/fully outsourced – third-party provider name • Whether the infrastructure is shared/dedicated across multiple busi-ness functions • Relevant resilience/continuity/recov-ery/ substitutability arrangements in place Mandatory to be reported with the intermediate report only if the incident has affected infrastructure components supporting business processes.				
3.32. Communicati	Information on whether financial entity has communicated to the		No	Yes	Yes	Choice: (a) Yes

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
on to clients/financial counterparts	clients and/or financial counterparts about the incident and about the measures that have been taken to mitigate the adverse effects					(b) No (c) Information not available
3.33. Information about communication to clients/financial counterparts	Description of the communication about the incident to clients or financial counterparts	The description shall include items such as the scope of the information contained in the communication, the means of communication with clients and/or financial counterparts, where possible, the categories of recipients and if communication was required under the financial entity's communication strategy. Mandatory to be reported with the intermediate report only if the financial entity has communicated with its clients and/or financial counterparts.	No	Yes, if applicable	Yes, if applicable	Alphanumeric
3.34. 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	No	Yes	Yes	Choice (multiple): (a) Police/Law Enforcement, (b) CSIRT, (c) Data Protection Authority, (d) National Cybersecurity Agency,

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		police, law enforcement agencies or public prosecutors				(e) None, (f) Other (please specify)
3.35. Specification of 'other' authorities	Specification of 'other' types of authorities informed about the incident	If selected in Data field 3.34. 'Other' the description shall include more detailed information about the authority to which the information about the incident was submitted. The field is mandatory to be reported with the intermediate report if 'other' type of authorities have been informed by the financial entity about the incident.	No	Yes, if applicable	Yes, if applicable	Alphanumeric
3.36. 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)
3.37. Description	Description of such temporary actions	The information shall include description of the immediate actions taken such as	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
of any temporary actions and measures taken or planned to be taken to recover from the incident		isolation of the incident at the network level, workaround procedures activated, USB ports blocked, Disaster Recovery site 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. Data field mandatory for the intermediate report if temporary actions/measures have been taken or are planned to be taken (data field 3.36.).				
3.38. Information on	Information on the involvement of CSIRTs in the handling of the incident, if applicable.	This description should include an indication of the nature of the CSIRT's involvement in handling the incident with	No	Yes, if applicable	Yes, if applicable	Choice (multiple): (a) Incident Report Acceptance

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
involvement of CSIRTs in dealing with the incident		reference to the following CSIRT incident management services. The 'Incident Report Acceptance' category covers the CSIRT's receipt, triage and processing of an initial notification or subsequent incident reports. It concerns the support of the CSIRT in the initial phase of incident handling. The 'Incident Analysis' category includes CSIRT support in the following areas: incident prioritisation and categorisation, information gathering, detailed analysis coordination, root cause analysis or cross-incident correlation. The 'Artifact and Forensic Evidence Analysis' category includes CSIRT involvement in media or surface analysis, reverse engineering, runtime or dynamic analysis, or comparative analysis. Both categories include the CSIRT's involvement in clarifying the causes and course of the incident and its impact on the financial entity in the next phase of incident handling.				(b) Incident Analysis (c) Artifact and Forensic Evidence Analysis (d) Mitigation and Recovery (e) Incident Coordination (f) Crisis Management Support (g) Other (please specify).

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		The 'Mitigation and Recovery' category may be reported by the financial entity if the CSIRT was involved in ad hoc response and containment, system restoration or other mitigation and recovery support. If the CSIRT has been involved in activities related to the coordination of incident handling, the financial entity should indicate on 'Incident Coordination' category. This includes support from the CSIRT related to: communication, notification distribution, relevant information distribution, activities coordination, reporting or media communication. If the CSIRT provided support in the area of crisis management, the category 'Crisis Management Support' should be indicated. Financial entities shall select 'Other' if the CSIRT's involvement in the incident handling is none of the above. In this case, further details can be also provided in the free text field				

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		The field is mandatory to be reported with the intermediate report if CSIRTs have been informed by the financial entity about the incident.				
3.39. Information on involvement of CSIRTs in dealing with the incident	Additional information about the extent the CSIRT was involved in handling of the reported incident and the specific area, where the category 'other' is selected in Data field 28.1.	The field is mandatory to be reported with the intermediate report if the category 'other' is selected in Data field 3.38.	No	Yes, if applicable	Yes, if applicable	Alphanumeric
3.40. 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 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);	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		• 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				

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		observed hosting malware or exploit kits, etc. Data field is mandatory for the intermediate and final report if cybersecurity is selected as a type of incident in data field 3.26.				
3.41. Vulnerabilities exploited	Description of the vulnerabilities exploited during the incident, including weaknesses, susceptibility or flaw of ICT products or ICT services.	The description should include an indication of whether any vulnerabilities have been exploited in connection with the incident and, if so, to provide the relevant information, including, but not limited to: • Information about the affected products, their versions, configurations, patches and extensions • Information about the affected platforms and operating systems (including their configuration) • Information about the manufacturer or provider of the vulnerable ICT products or ICT services • Description of the vulnerability, including information about the exploitation	No	Yes, if applicable	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		of the vulnerability – for unpublished vulnerabilities • Own assessment of criticality: low/medium/high/critical –for unpublished vulnerabilities • Applied mitigation measures (workarounds or hot fixes) Information about the manufacturer or provider of the vulnerable ICT products or ICT services may include, in particular, the name or other data identifying the ICT third-party service provider. If the provider is not also the manufacturer of the ICT product affected by the vulnerability, it is also important to provide information that allows identification of the manufacturer of such a product. When providing information on how the vulnerability was exploited, the effects/impacts of the vulnerability may be considered in the first place. The description should include also the assessment of the criticality of the				

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		vulnerability by using common industry standards and may consult the European Vulnerability database established as per NIS2 Art. 12. The description should also include whether other authorities have been notified of the vulnerability and whether the provider/manufacturer has been contacted. Data field is mandatory for the intermediate and final report if cybersecurity is selected as a type of incident in data field 3.26.				
Content of the final report						
4.1. Root causes of the incident	Classification of root cause of the incident under the incident types.	The following categories shall be considered: **1.Malicious actions** (if selected, choose one or more the following) a. Deliberate internal actions b. Deliberate physical damage/manipulation/theft c. Fraudulent actions	No	No	Yes	Choice (**multiple)**: **1. Malicious actions** (if selected, choose one or more the following) a. Deliberate internal actions

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		d. Cybersecurity **2. Process failure** a. Insufficient and/or failure of monitoring and control a. Monitoring of policy adherence; b. Monitoring of third-party service providers; c. Monitoring and verification of remediation of vulnerabilities; d. Identity and access management; e. Encryption and cryptography: f. Logging. b. Insufficient/unclear roles and responsibilities c. ICT risk management process failure: a. Failure in defining accurate risk tolerance levels b. Insufficient vulnerability and threat assessments c. Inadequate risk treatment measures				b. Deliberate physical damage/manipulation/theft c. Fraudulent actions d. Cybersecurity **2. Process failure** a. Insufficient and/or failure of monitoring and control i. Monitoring of policy adherence; ii. Monitoring of third-party service providers; iii. Monitoring and verification of remediation of vulnerabilities; iv. Identity and access management; v. Encryption and cryptography:

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		d. Poor management of residual ICT risks . d. Insufficient and/or failure of ICT operations and ICT security operations a. Vulnerability and patch management; b. Change management; c. Capacity and performance management; d. ICT asset management and information classification; e. Backup and restore; f. Error Handling; 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 a. Inadequate ICT Systems Acquisition, Development, and Maintenance b. Insufficient and /or failure of software testing a				vi. Logging. b. Insufficient/unclear roles and responsibilities c. ICT risk management process failure: i. Failure in defining accurate risk tolerance levels ii. Insufficient vulnerability and threat assessments iii. Inadequate risk treatment measures iv. Poor management of residual ICT risks . d. Insufficient and/or failure of ICT operations and ICT security operations

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		h. Other (please specify) **3.System failure/malfunction** 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				i. Vulnerability and patch management; ii. Change management; iii. Capacity and performance management; iv. ICT asset management and information classification; v. Backup and restore; and vi. Error Handling. e. Insufficient and/or failure of ICT project management f. Inadequate of internal policies, procedures and documentation

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		resulting from software conflicts, incorrect settings, or misconfigured parameters that impact the overall system functionality. 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 prob-				g. Inadequate ICT Systems Acquisition, Development, and Maintenance i. Inadequate ICT Systems Acquisition, Development and Maintenance ii. Insufficient and /or failure of software testing a h. Other (please specify) **3. System failure** a. Hardware capacity and performance b. Hardware maintenance c. Hardware obsolescence/ageing d. Software compatibility/configuration

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		lems affecting connectivity or communication. Physical damage: incidents caused by physical damage to ICT infrastructure which lead to system failures. g. Other (please specify) **4.Human error** 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 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				e. Software performance f. Network configuration g. Physical damage h. Other (please specify) **4. Human error** a. Omission b. Mistake c. Skills & knowledge d. Inadequate human resources e. Miscommunication f. Other (please specify) **5. External event** a. Natural disasters/force majeure

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		insufficient resources lead to operational inefficiencies, system failures, or an inability to meet business demands e. Miscommunication f. Other (please specify) **5. External event** a. Natural disasters/force majeure b. Third-party failures c. Other (please specify)				b. Third-party failures Other (please specify)
4.2. Other types of root cause types	Other types of root cause types	Where financial entities have selected 'other' type of root cause in data field 4.1., financial entities shall specify the type of root cause Field mandatory for the final report if 'other' type of root causes is selected in data field 4.1.	No	No	Yes, if applicable	Alphanumeric
4.3. Information about the root causes	Description of the sequence of events that led to the incident	Description of the sequence of events that led to the incident including a concise description of all underlying reasons and primary factors that contributed to the occurrence of the incident.	No	No	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
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.				
4.4. Information about inability to comply with legal requirements	Information on whether or not and, if so, how legal requirements have not been complied with, or are likely not to be complied with, as a result of the major incident, including information on what requirements are affected.		No	No	Yes	Alphanumeric
4.5. Information about breach of contractual arrangement /SLAs	Information on whether or not and, if so, how contractual arrangements and service level agreements with financial counterparts have been breached or are likely to be breached leading to non-compliance with contractual obligations as a result of the major incident.		No	No	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
4.6. Description of the measures and actions taken for the permanent resolution of the incident	Additional information regarding the actions/measures taken/planned to permanently resolve the incident and to prevent that incident from happening again in the future.	The description shall include the following points in your answer (non-exhaustive list): • 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	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
4.7. Assessment of the effectiveness of the actions taken and lessons learnt	Assessment of the effectiveness action(s) taken to remediate and select one of the below	Financial entities shall choose between the following: • Highly Effective: Appropriate actions were taken in a timely manner and the incident was remedied and its impact significantly limited. • Moderately Effective: Actions were taken in a progressive manner and the incident was remedied and its impact limited. • Not Effective: The incident was remedied after a great impact on the entity. • Not yet available: The actions taken did not lead to the remediation of the incident so far. In case this option is selected, the supervised entities should provide an updated version of the notification when the incident is remedied.	No	No	Yes	Choice: (a) Highly effective (b) Moderately effective (c) Not effective (d) Not yet available
4.8. Date and time when the incident was resolved and the root	Date and time when the incident was resolved and the root caused addressed		No	No	Yes	dd/mm/yyyy hh:mm

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
caused addressed						
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
4.10. Information relevant for resolution authorities	Description of on whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group.	Financial entities shall provide information on whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group. Financial entities shall also indicate whether the incident affects the solvency or liquidity of the financial entity and the potential quantification of the impact. Financial entities shall also provide information on the impact on operational	No	No	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		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.				
4.11. Reclassification of the incident from major to non-major	Information on whether the incident has been reclassified as non-major if it does not fulfil the criteria to be considered as major after initially being considered as major.	The data field is mandatory if the incident has been reclassified as non-major. If the field is selected, all other data fields are non-mandatory.	No	No	Yes, if applicable	Boolean (Yes or No)
4.12. Reasons for the reclassification	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.	The data field is mandatory if the incident has been reclassified as non-major.	No	No	Yes, if applicable	Alphanumeric
4.13. Materiality threshold for the classification	Detailed information about thresholds eventually reached by the incident in relation to the criterion 'Economic impact' in accordance		No	No	Yes	Alphanumeric

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
criterion 'Economic impact'	with articles 7 and 15 of the RTS on classification of ICT-related incident.					
4.14. Amount of gross direct and indirect costs and losses	Total amount of gross direct and indirect costs and losses stemming from the major incidents of which:	In accordance with article 7(1) and (2) of the RTS on classification of ICT-related incident, before taking into account financial recoveries of any type.	No	No	Yes	Monetary
4.15. Amount of expropriated funds or financial assets for which the financial entity is liable, including assets lost to theft	amount of expropriated funds or financial assets for which the financial entity is liable	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
4.16. Amount of replacement or relocation costs of software, hardware or infrastructure	amount of replacement or relocation costs of software, hardware or infrastructure	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary
4.17. Amount of staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or	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	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
impaired skills of staff						
4.18. Amount of fees due to non-compliance with contractual obligations	amount of fees due to non-compliance with contractual obligations	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary
4.19. Amount of customer redress and compensation costs	amount of customer redress and compensation costs	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary
4.20. Amount of losses due to forgone revenues	amount of losses due to forgone revenues	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary
4.21. Amount of costs	amount of costs associated with internal and external communication	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
associated with internal and external communication						
4.22. Amount of advisory costs, including costs associated with legal counselling, forensic and remediation services	amount of advisory costs, including costs associated with legal counselling, forensic and remediation services	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary
4.23. Amount of other costs and losses	other costs and losses, including: • direct charges, including impair-ments and settlement charges, to the Profit and Loss account and write-downs due to the major ICT-related incident;	Mandatory to be reported with the final report if the data is available.	No	No	Yes, if applicable	Monetary

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	• 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; • 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					

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	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.					
4.24. 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
4.25. Details related to the economic impacts	Any further information related to the classification criterion 'economic impact'	Mandatory to be reported with the final report if there is additional information available.	No	No	Yes, if applicable	Alphanumeric

ANNEX III

Templates for notification of significant cyber threats

Number of field	Data field	
1	Name of the entity submitting the notification	
2	LEI of the entity submitting the notification	
3	Type of the entity submitting the report	
4	Name of the financial entity	
5	Type of financial entity	
6	LEI code of the financial entity	
7	Primary contact person name	
8	Primary contact person email	
9	Primary contact person telephone	
10	Second contact person name	
11	Secondary contact person email	
12	Second contact person telephone	
13	Date and time of detection of the cyber threat	
14	Description of the significant cyber threat	
15	Information about potential impact	
16	Potential incident classification criteria	
17	Status of the cyber threat	
18	Actions taken to prevent materialisation	
29	Notification to other stakeholders	
20	Indicators of compromise	
21	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	Instructions	Mandatory field	Field type
1. Name of the entity submitting the notification	Full legal name of the entity submitting the notification		Yes	Alphanumeric
2. LEI of the entity submitting the notification	Legal Entity Identifier (LEI) of the entity submitting the notification assigned in accordance with the International Organisation for Standardisation. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.		Yes	Alphanumeric
3. Type of the entity submitting the report	Type of the entity under Article 2.1(a)-(t) of DORA submitting the report	To be provided only where the report is not provided by the affected financial entity directly.	Yes, if appliable	Choice (multiselect) from the pre-defined list of DORA financial entities. 'Other' for entities not listed in Article 2.1 of DORA
4. Name of the financial entity	Full legal name of the financial entity notifying the significant cyber threat.	Field mandatory if the financial entity is different from the entity submitting the notification.	Yes, if appliable	Alphanumeric
5. Type of financial entity	Type of the financial entity under Article 2.1(a)-(t) of DORA notifying the significant cyber threat.	Field mandatory if the financial entity affected by the incident is different from the entity submitting the notification.	Yes, if appliable	Choice (multiselect): Article 2.1 points (a) to (t) of DORA Regulation

Data field	Description	Instructions	Mandatory field	Field type
6. 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. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.	Field mandatory if the financial entity notifying the significant cyber threat is different from the entity submitting the report.	Yes, if appliable	Alphanumeric
7. Primary contact person name	Name and surname of the primary contact person of the financial entity		Yes	Alphanumeric
8. 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 (email format)
9. Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication		Yes	Number (telephone format)
10. 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		Yes	Alphanumeric
11. Secondary 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	Alphanumeric (email format)
12. Second contact person telephone	Telephone number of the second contact person that can be used by the competent authority for follow-up communication		Yes	Number (telephone format)

Data field	Description	Instructions	Mandatory field	Field type
13. Date and time of detection of the cyber threat	Date and time at which the significant cyber threat was detected.		Yes	dd/mm/yyyy hh:mm
14. 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; - information about the probability of materialisation of the significant cyber threat; and - information about the probability of materialisation of the significant cyber threat.	Yes	Alphanumeric
15. 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
16. Potential incident classification criteria	The classification criteria that could have triggered a major incident report if the cyber threat had materisalised.		Yes	Choice (multiple): (to be aligned with the RTS on classification of major incidents

Data field	Description	Instructions	Mandatory field	Field type
17. Status of the cyber threat	Information about the status of the cyber threat and whether there has been any changes in the threat activity.		Yes	Choice: a) active b) inactive
18. Actions taken to prevent materialisation	Information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if applicable.		Yes	Alphanumeric
19. Notification to other stakeholders	Information about notification of the cyber threat to other financial entities or authorities		Yes, if applicable	Alphanumeric
20. 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;	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory field	Field type
		• 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.		
21. Other relevant information	Any other relevant information about the significant cyber threat		Yes, if applicable	Alphanumeric

ANNEX V

Part I: Single Data Point Model

All data items set out in the Annexes to this Regulation shall be transformed into a single data point model, which is the basis for uniform IT systems of institutions and competent authorities.

The single data point model shall meet the following criteria:

a) it provides a structured representation of all data items set out in Annex I to IV
b) it identifies all the business concepts set out in Annexes I to IV;
c) it provides a data dictionary identifying table labels, ordinate labels, axis labels, domain labels, dimension labels and member labels;
d) it provides metrics, which define the property or amount of data points;
e) it provides data point definitions that are expressed as a composition of characteristics that univocally identify the concept;
f) it contains all the relevant technical specifications necessary for developing IT reporting solutions producing uniform supervisory data.

Part II: Validation rules

The data items set out in the Annexes to this Regulation shall be subject to validation rules ensuring data quality and consistency.

The validation rules shall meet the following criteria:

a) they define the logical relationships between relevant data points;
b) they include filters and preconditions that define a set of data to which a validation rule applies;
c) they check the consistency of the reported data;
d) they check the accuracy of the reported data;
e) they set default values, which shall be applied where the relevant information has not been reported.

7. Accompanying documents

7.1 Draft cost-benefit analysis / impact assessment

According to Articles 10 of Regulation (EU) No 1093/2010 (EBA Regulation), the EBA shall analyse the potential costs and benefits of draft regulatory standards (RTS) developed by the EBA. The RTS and the ITS developed by the EBA 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 Consultation Paper (CP) on regulatory technical standards (RTS) and the Implementing Technical Standards (ITS) on the content and timing of incident reports under Article 20 of the DORA Regulation.

A. Problem identification

DORA (Art. 19) requires 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 financial entities, 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 competent authorities obtain exhaustive 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 financial entities and ensuring proportionality for all types of financial entities 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 (NIS 2) Directive3 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 financial entities, 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 financial entities covered by DORA. Providing multiple classifications depending on the type of FEs would add complexity 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.

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 competent authorities 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 entities within the scope of DORA are covered in NIS2, therefore synergies between the frameworks will be desirable.

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

- While initial notification from the time of detection is 24h in line with 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).
- The final report is to be submitted under NIS 2 in 20 working days. Under DORA the preference was to choose 30 days which gives more flexibility in terms of reporting, given that many incident-related function operate 24 hours, 7 days a week, both in case of FEs and CAs.

Option 1b 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.

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.

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 field 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.

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 and 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 non-essential fields may be missing, but it should acceptable, as by definition they are not crucial for the CAs to 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.

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 keep reporting using the existing frameworks of NIS2 and PSD2), 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.

7.2 Overview of questions for consultation

Question 1 – Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

Question 2 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 3 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 4 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 5 – Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.

Question 6 – Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.