



2025/302

20.2.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/302

of 23 October 2024

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

(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 ⁽¹⁾, and in particular Article 20, fourth paragraph, thereof,

Whereas:

- (1) To ensure that financial entities report major incidents to their competent authorities in a consistent manner and to ensure that they provide those authorities with data of good quality, it should be specified which data fields financial entities need to provide at the various stages of the reporting referred to in Article 19(4) of Regulation (EU) 2022/2554. It is important that that information is presented in a way that allows for a single overview of the incident. It is therefore necessary to lay down a single reporting template for those purposes.
- (2) Financial entities should complete those data fields of the reporting template that correspond to the information requirements of the respective notification or report. However, financial entities that already have information which they are to provide at a later reporting stage, i.e. in the intermediate or final report, should be allowed to anticipate the submission of the data.
- (3) Since multiple or recurring incidents may constitute a major incident as referred to in Article 8 of Commission Delegated Regulation (EU) 2024/1772 ⁽²⁾, the design of the reporting template and of the data fields should enable financial entities to report such recurring incidents.
- (4) To ensure accurate and up to-date information, the reporting template should enable financial entities, when submitting the intermediate and final report, to update any information that was submitted previously, and where necessary reclassify major incidents as non-major.
- (5) The legal identification of entities should be aligned with the identifiers specified in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554.
- (6) Where financial entities outsource the major ICT-related incident reporting obligations to a third party, competent authorities should be aware of the identity of the third-party reporting on behalf of the financial entity prior to the submission of the first notification or reporting, in order to verify the legitimacy of the reporting third party.

⁽¹⁾ OJ L 333, 27.12.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

⁽²⁾ Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents (OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

- (7) To identify easily the impact of an incident that occurred at, or was caused by a third-party provider, and that affects multiple financial entities within a single Member State, and to reduce the reporting effort for financial entities, the reporting template should allow for the submission of an aggregated report covering aggregated information about the impact of the incident on all impacted financial entities that have classified the incident as major.
- (8) The reporting template should be designed in a technology neutral way to allow for its implementation into various incident reporting solutions that already exist or that may be developed for the implementation of the requirements of Regulation (EU) 2022/2554.
- (9) The design of the reporting template and data fields should facilitate the reporting of major ICT-related incidents by third parties to whom financial entities outsourced their reporting obligation in accordance with Article 19(5) of Regulation (EU) 2022/2554.
- (10) This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Supervisory Authorities.
- (11) The European Supervisory Authorities 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 ⁽³⁾, (EU) No 1094/2010 ⁽⁴⁾, (EU) No 1095/2010 ⁽⁵⁾ of the European Parliament and of the Council.
- (12) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ⁽⁶⁾ and delivered a positive opinion on 22 July 2024. Any processing of personal data within the scope of this Regulation should be performed in accordance with the applicable data protection principles and provisions set out in Regulation (EU) 2018/1725,

HAS ADOPTED THIS REGULATION:

Article 1

Template for reporting ICT-related major incidents

1. Financial entities shall use the template laid down in Annex I to submit the initial notification, the intermediate report, and the final report referred to in Article 19(4) of Regulation (EU) 2022/2554 as follows:
 - (a) financial entities that submit an initial notification shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 2 of Commission Delegated Regulation (EU) 2025/301 ⁽⁷⁾, and may, where they already have that information, complete those data fields the completion of which is not required for an initial notification but is required for an intermediate or final report;

⁽³⁾ Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12, ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

⁽⁴⁾ Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48, ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

⁽⁵⁾ Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84, ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

⁽⁶⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

⁽⁷⁾ Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats. (OJ L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

- (b) financial entities that submit an intermediate report shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 3 of Delegated Regulation (EU) 2025/301 and may, where they already have the relevant information, complete data fields the completion of which is not required for the intermediate report, but is required for the final report.
 - (c) financial entities that submit a final report shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 4 of Delegated Regulation (EU) 2025/301.
2. Financial entities shall ensure that the information contained in the initial notification, and in the intermediate and final report, is complete and accurate.
 3. Financial entities shall provide estimated values based on other available data and information, to the extent possible, where accurate data are not available at the time of reporting for the initial notification or the intermediate report.
 4. When submitting an intermediate or final report, financial entities shall use the template laid down in Annex I to submit all required information and update, where applicable, the information that was previously provided in the initial notification or in the intermediate report.
 5. Financial entities shall follow the data glossary and instructions set out in Annex II when completing the template laid down in Annex I.

Article 2

Joint submission of initial notification, intermediate and final reports

Financial entities may combine the submission of the initial notification, the intermediate report, and the final report to provide two or all of those at the same time, where regular activities have recovered or the root cause analysis has been completed and provided that the time limits set out in Article 5 of Delegated Regulation (EU) 2025/301 are met.

Article 3

Recurring ICT-related incidents

Financial entities that provide information on non-major recurring ICT-related incidents that cumulatively meet the conditions for one major ICT-related incident as set out in Article 8(2) of Delegated Regulation (EU) 2024/1772, shall provide that information in an aggregated form.

Article 4

Use of secure electronic channels

1. Financial entities shall use secure electronic channels as made available by their competent authority to submit the initial notification and the intermediate and final reports.
2. Financial entities that are unable to use the secure electronic channels as made available by their competent authority shall inform their competent authority about a major ICT-related incident through other secure means in agreement with the competent authority. If required by the competent authority, financial entities shall resubmit the initial notification, or intermediate or final report, through the secure electronic channel as made available by their competent authority once they are able to do so.

*Article 5***Reclassification of major ICT-related incidents**

Where after further assessment, the financial entity concludes that the ICT-related incident previously reported as major, at no time fulfilled the classification criteria and thresholds set out in Article 8 of Delegated Regulation (EU) 2024/1772, the financial entity shall notify to the competent authority that it has reclassified the ICT-related incident from major to non-major by providing the information about that reclassification in the template laid down in Annex II to this Regulation in relation to the fields 'type of report' and 'other information'.

*Article 6***Notification of outsourcing of the reporting obligations**

1. Financial entities that have outsourced the obligation to report major ICT-related incidents in accordance with Article 19(5) of Regulation (EU) 2022/2554 shall inform their competent authority of that outsourcing arrangement as soon as the outsourcing arrangement has been concluded and at the latest prior to the first notification or reporting.
2. Financial entities shall provide the competent authority with the name, contact details, and identification code of the third-party that will submit the major ICT-related incident notifications or reports for them.
3. Financial entities shall inform their competent authority as soon as they no longer outsource their reporting obligations as referred to in Article 19(5) of Regulation (EU) 2022/2554.

*Article 7***Aggregated reporting**

1. A third-party service provider to whom reporting obligations have been outsourced as referred to in Article 19(5) of Regulation (EU) 2022/2554 may use the template set out in Annex I to this Regulation to provide aggregated information about a major ICT-related incident impacting multiple financial entities in one single notification or report, and submit that notification or report to the competent authority on behalf of all impacted financial entities, provided that all of the following conditions are met:
 - (a) the major ICT-related incident to be reported originates from or is being caused by a third-party ICT service provider;
 - (b) that third-party service provider provides the relevant ICT service to more than one financial entity, or to a group;
 - (c) the ICT-related incident is classified as major by each financial entity covered in the aggregated notification or report;
 - (d) the major ICT-related incident affects financial entities within a single Member State and the aggregated report relates to financial entities which are supervised by the same competent authority;
 - (e) competent authorities have explicitly permitted this type of financial entities to aggregate their reporting.
2. Paragraph 1 shall not apply to credit institutions that are considered to be of significant relevance as referred to in Article 2 point (16) of Regulation (EU) No 468/2014 of the European Central Bank ⁽⁸⁾, operators of trading venues, and central counterparties, which shall only use the template in Annex I to submit major ICT-related incident notifications or reports individually to their competent authority.
3. Where competent authorities require information on the individual impact of the major ICT-related incident on a single financial entity, upon request of the competent authority, the financial entity shall submit an individual notification or a report on the major ICT-related incident.

⁽⁸⁾ Regulation (EU) No 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (SSM Framework Regulation) (ECB/2014/17) (OJ L 141, 14.5.2014, p. 1, ELI: <http://data.europa.eu/eli/reg/2014/468/oj>).

*Article 8***Notification of significant cyber threats**

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

*Article 9***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, 23 October 2024.

For the Commission
The President
Ursula VON DER LEYEN

TEMPLATES FOR THE REPORTING OF MAJOR INCIDENTS

Number of field	Data field	
General information about the financial entity		
1.1	Type of submission	
1.2	Name of the entity submitting the report	
1.3	Identification code of the entity submitting the report	
1.4	Type of financial entity affected	
1.5	Name of the financial entity affected	
1.6	LEI code of the financial entity affected	
1.7	Primary contact person name	
1.8	Primary contact person email	
1.9	Primary contact person telephone	
1.10	Second contact person name	
1.11	Second contact person email	
1.12	Second contact person telephone	
1.13	Name of the ultimate parent undertaking	
1.14	LEI code of the ultimate parent undertaking	
1.15	Reporting currency	
Content of the initial notification		
2.1	Incident reference code assigned by the financial entity	
2.2	Date and time of detection of the major ICT-related incident	
2.3	Date and time of classification of the ICT-related incident as major	
2.4	Description of the major ICT-related incident	
2.5	Classification criteria that triggered the incident report	
2.6	Materiality thresholds for the classification criterion 'Geographical spread'	
2.7	Discovery of the major ICT-related incident	

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

Number of field	Data field	
3.22	Classification criterion 'Critical services affected'	
3.23	Type of the major ICT-related incident	
3.24	Other types of incidents	
3.25	Threats and techniques used by the threat actor	
3.26	Other types of techniques	
3.27	Information about affected functional areas and business processes	
3.28	Affected infrastructure components supporting business processes	
3.29	Information about affected infrastructure components supporting business processes	
3.30	Impact on the financial interest of clients	
3.31	Reporting to other authorities	
3.32	Specification of 'other' authorities	
3.33	Temporary actions/measures taken or planned to be taken to recover from the incident	
3.34	Description of any temporary actions and measures taken or planned to be taken to recover from the incident	
3.35	Indicators of compromise	
Content of the final report		
4.1	High-level classification of root causes of the incident	
4.2	Detailed classification of root causes of the incident	
4.3	Additional classification of root causes of the incident	
4.4	Other types of root cause types	
4.5	Information about the root causes of the incident	
4.6	Incident resolution summary	
4.7	Date and time when the incident root cause was addressed	
4.8	Date and time when the incident was resolved	
4.9	Information if the permanent resolution date of the incident differs from the initially planned implementation date	
4.10	Assessment of risk to critical functions for resolution purposes	
4.11	Information relevant for resolution authorities	

Number of field	Data field	
4.12	Materiality threshold for the classification criterion 'Economic impact'	
4.13	Amount of gross direct and indirect costs and losses	
4.14	Amount of financial recoveries	
4.15	Information on whether the non-major incidents have been recurring	
4.16	Date and time of occurrence of recurring incidents	

DATA GLOSSARY AND INSTRUCTIONS FOR THE REPORTING OF MAJOR INCIDENTS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
General information about the financial entity					
1.1. Type of submission	Indicate the type of incident notification or report being submitted to the competent authority.	Yes	Yes	Yes	Choice: — initial notification; — intermediate report; — final report; — major incident reclassified as non-major.
1.2. Name of the entity submitting the report	Full legal name of the entity submitting the report.	Yes	Yes	Yes	Alphanumeric
1.3. Identification code of the entity submitting the report	<p>Identification code of the entity submitting the report.</p> <p>Where financial entities submit the notification/report, the identification code shall be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.</p> <p>A third-party provider that submits a report for a financial entity can use an identification code as specified in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554.</p>	Yes	Yes	Yes	Alphanumeric
1.4. Type of the affected financial entity	<p>Type of the entity as referred to in Article 2(1), points (a) to (t), of Regulation (EU) 2022/2554 for whom the report is submitted.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation, the different types of financial entities covered in the aggregated report to be selected.</p>	Yes	Yes	Yes	Choice (multiselect): — credit institution; — payment institution; — exempted payment institution; — account information service provider; — electronic money institution; — exempted electronic money institution; — investment firm; — crypto-asset service provider; — issuer of asset-referenced tokens; — central securities depository; — central counterparty; — trading venue; — trade repository;

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
					<ul style="list-style-type: none"> — manager of alternative investment fund; — management company; — data reporting service provider; — insurance and reinsurance undertaking; — insurance intermediary, reinsurance intermediary and ancillary insurance intermediary; — institution for occupational retirement provision; — credit rating agency; — administrator of critical benchmarks; — crowdfunding service provider; — securitisation repository.
1.5. Name of the financial entity affected	<p>Full legal name of the financial entity affected by the major ICT-related incident and required to report the major incident to its competent authority under Article 19 of Regulation (EU) 2022/2554.</p> <p>In case of aggregated reporting:</p> <p>(a) list of all names of the financial entities affected by the major ICT-related incident, separated by a semicolon;</p> <p>(b) the third-party provider submitting a major incident notification or report in an aggregated manner as referred to in Article 7 of this Regulation, to list the names of all financial entities impacted by the incident, separated by a semicolon.</p>	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting	Alphanumeric
1.6. LEI code of the financial entity affected	<p>Legal Entity Identifier (LEI) of the financial entity affected by the major ICT-related incident assigned in accordance with the International Organisation for Standardisation.</p> <p>In case of aggregated reporting:</p> <p>(a) a list of all LEI codes of the financial entities affected by the major ICT-related incident, separated by a semicolon.</p>	Yes, if the financial entity affected by the major ICT-related incident is different	Yes, if the financial entity affected by the major ICT-related incident is different from the entity	Yes, if the financial entity affected by the major ICT-related incident is different from	Unique 20 alphanumeric character code, based on ISO 17442-1:2020

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(b) the third-party provider submitting a major incident notification or report in an aggregated manner as referred to in Article 7 of this Regulation to list the LEI codes of all financial entities impacted by the incident, separated by a semicolon.</p> <p>The order of appearance of LEI codes and financial entities names shall be identical.</p>	from the entity submitting the report and in case of aggregated reporting	submitting the report and in case of aggregated reporting	the entity submitting the report and in case of aggregated reporting	
1.7. Primary contact person name	<p>Name and surname of the primary contact person of the financial entity.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation, the name of the primary contact person in the entity submitting the aggregated report.</p>	Yes	Yes	Yes	Alphanumeric
1.8. Primary contact person email	<p>Email address of the primary contact person that can be used by the competent authority for follow-up communication.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation, the email of the primary contact person in the entity submitting the aggregated report.</p>	Yes	Yes	Yes	Alphanumeric
1.9. Primary contact person telephone	<p>The telephone number of the primary contact person that can be used by the competent authority for follow-up communication.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation, the telephone number of the primary contact person in the entity submitting the aggregated report.</p> <p>The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXXX)</p>	Yes	Yes	Yes	Alphanumeric
1.10. Second contact person name	<p>Name and surname of the second contact person or the name of the responsible team of the financial entity or an entity submitting the report on behalf of the financial entity</p>	Yes	Yes	Yes	Alphanumeric
1.11. Second contact person email	<p>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.</p>	Yes	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
1.12. Second contact person telephone	The telephone number of the second contact person, or of a team, that can be used by the competent authority for follow-up communication. The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXXX)	Yes	Yes	Yes	Alphanumeric
1.13. Name of the ultimate parent undertaking	Name of the ultimate parent undertaking of the group to which the affected financial entity belongs, where applicable.	Yes, if the FE belongs to a group	Yes, if the FE belongs to a group	Yes, if the FE belongs to a group	Alphanumeric
1.14. LEI code of the ultimate parent undertaking	LEI of the ultimate parent undertaking of the group to which the affected financial entity belongs, where applicable. Assigned in accordance with the International Organisation for Standardisation.	Yes, if the FE belongs to a group	Yes, if the FE belongs to a group	Yes, if the FE belongs to a group	Unique 20 alphanumeric character code, based on ISO 17442-1:2020
1.15. Reporting currency	Currency used for the incident reporting	Yes	Yes	Yes	Choice populated by using ISO 4217 currency codes

Content of the initial notification

2.1. Incident reference code assigned by the financial entity	Unique reference code issued by the financial entity unequivocally identifying the major ICT-related incident. In case of aggregated reporting as referred to in Article 7 of this Regulation, the incident reference code assigned by the third-party provider.	Yes	Yes	Yes	Alphanumeric
2.2. Date and time of detection of the ICT-related incident	Date and time at which the financial entity has become aware of the ICT-related incident. For recurring incidents, the date and the time at which the last ICT-related incident was detected.	Yes	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
2.3. Date and time of classification of the incident as major	Date and time when the ICT-related incident was classified as major according to the classification criteria established in Delegated Regulation (EU) 2024/1772	Yes	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
2.4. Description of the ICT-related incident	<p>Description of the most relevant aspects of the major ICT-related incident.</p> <p>Financial entities shall provide a high-level overview of the following information such as possible causes, immediate impacts, systems affected, and others. Financial entities, shall include, where known or reasonably expected, whether the incident impacts third-party providers or other financial entities, the type of provider or financial entity, their name, their respective identification codes and type of the identification code (e.g. LEI or EUID).</p> <p>In subsequent reports, the field content can evolve over time to reflect the ongoing understanding of the ICT-related incident and describe any other relevant information about the ICT-related incident not captured by the data fields, including the internal severity assessment by the financial entity (e.g. very low, low, medium, high, very high) and an indication of the level and name of most senior decision structures that has been involved in response to the ICT-related incident.</p>	Yes	Yes	Yes	Alphanumeric
2.5. Classification criteria that triggered the incident report	<p>Classification criteria under Delegated Regulation (EU) 2024/1772 that have triggered determination of the ICT-related incident as major and subsequent notification and reporting.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the classification criteria that have triggered determination of the ICT-related incident as major for at least one or more financial entities.</p>	Yes	Yes	Yes	<p>Choice (multiple):</p> <ul style="list-style-type: none"> — clients, financial counterparts and transactions affected; — reputational impact; — duration and service downtime; — geographical spread; — data losses; — critical services affected; — economic impact.
2.6. Materiality thresholds for the classification criterion 'Geographical spread'	<p>EEA Member States impacted by the major ICT-related incident</p> <p>When assessing the impact of the major ICT-related incident in other Member States, financial entities shall take into account Articles 4 and 12 of Delegated Regulation 2024/1772.</p>	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Choice (multiple) populated by using ISO 3166 ALPHA-2 of the affected countries

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
2.7. Discovery of the major ICT-related incident	Indication of how the major ICT-related incident has been discovered.	Yes	Yes	Yes	Choice: <ul style="list-style-type: none"> — IT Security; — staff; — internal audit; — external audit; — clients; — financial counterparts; — third-party provider; — attacker; — monitoring systems; — authority/agency/ law enforcement body; — other.
2.8. Indication whether the incident originates from a third-party provider or another financial entity	Indication whether the major ICT-related incident originates from a third-party provider or another financial entity. Financial entities shall indicate whether the major ICT-related incident originates from a third-party provider or another financial entity (including financial entities belonging to the same group as the reporting entity) and the name, identification code of the third-party provider or financial entity and type of the identification code (e.g. LEI or EUID).	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity	Alphanumeric
2.9. Activation of business continuity plan, if activated	Indication of whether there has been a formal activation of the business continuity response measures of the financial entity.	Yes	Yes	Yes	Boolean (Yes or No)
2.10. Other relevant information	Any further information not covered in the template. Financial entities that have reclassified a major ICT-related incident as non-major shall describe the reasons why the ICT-related incident does not fulfil, and is not expected to fulfil, the criteria to be considered as a major ICT-related incident.	Yes, if there is other information not covered in the template or	Yes, if there is other information not covered in the template or if the major	Yes, if there is other information not covered in the template or	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		if the major ICT-related incident has been reclassified as non-major.	ICT-related incident has been reclassified as non-major	if the major ICT-related incident has been reclassified as non-major	

Content of the intermediate report

3.1. Incident reference code provided by the competent authority	Unique reference code assigned by the competent authority at the time of receipt of the initial notification to unequivocally identify the major ICT-related incident.	No	Yes, if applicable	Yes, if applicable	Alphanumeric
3.2. Date and time of occurrence of the incident	Date and time at which the major ICT-related incident has occurred, if different from the time the financial entity has become aware of the major ICT-related incident. For recurring major ICT-related incidents, the date and the time at which the last major ICT-related incident has occurred.	No	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
3.3. Date and time when services, activities or operations have been recovered	Information on the date and time of the recovery of the services, activities or operations affected by the major ICT-related incident.	No	Yes, if data field 3.16. 'Service downtime' has been populated	Yes, if data field 3.16. 'Service downtime' has been populated	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
3.4. Number of clients affected	Number of clients affected by the major ICT-related incident that use the service provided by the financial entity. When assessing the number of clients affected, financial entities shall take into account Articles 1(1) and 9(1), point (b), of Delegated Regulation (EU) 2024/1772 in their assessment. A financial entity that cannot determine the actual number of clients impacted shall use estimates based on available data from comparable reference periods. In the case of aggregated reporting as referred to in Article 7 of this Regulation, the total number of clients affected across all financial entities.	No	Yes	Yes	Numerical integer

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.5. Percentage of clients affected	<p>Percentage of clients affected by the major 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, the services shall be provided in an aggregated manner.</p> <p>Financial entities shall take into account Article 1(1) and Article 9(1), point (a), of Delegated Regulation (EU) 2024/1772 in their assessment.</p> <p>A financial entity that cannot determine the actual percentage of clients impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, a financial entity shall divide the sum of all affected clients by the total number of clients of all impacted financial entities.</p>	No	Yes	Yes	Expressed as percentage – any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2,4 instead of 2,4 %). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up
3.6. Number of financial counterparts affected	<p>Number of financial counterparts affected by the major ICT-related incident that have concluded a contract with the financial entity.</p> <p>When assessing the number of financial counterparts affected, financial entities shall take into account Article 1(2) of Delegated Regulation (EU) 2024/1772 in their assessment. A financial entity that cannot determine the actual number of financial counterparts impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the total number of financial counterparts affected across all financial entities.</p>	No	Yes	Yes	Numerical integer

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.7. Percentage of financial counterparts affected	<p>Percentage of financial counterparts affected by the major ICT-related incident in relation to the total number of financial counterparts that have concluded a contract with the financial entity.</p> <p>When assessing the percentage of financial counterparts affected, financial entities shall take into account Articles 1(1) and 9(1), point (c) of Delegated Regulation (EU) 2024/1772 in their assessment.</p> <p>A financial entity that cannot determine the actual percentage of financial counterparts impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, indicate the sum of all affected financial counterparts divided by the total number of financial counterparts of all impacted financial entities.</p>	No	Yes	Yes	Expressed as percentage – any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2,4 instead of 2,4 %). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up
3.8. Impact on relevant clients or financial counterparts	Any identified impact on relevant clients or financial counterpart as referred to in Article 1(3) and Article 9(1), point (f), of Delegated Regulation (EU) 2024/1772.	No	Yes, if 'Relevance of clients and financial counterparts' threshold is met	Yes, if 'Relevance of clients and financial counterparts' threshold is met	Boolean (Yes or No)
3.9. Number of affected transactions	<p>Number of transactions affected by the major ICT-related incident.</p> <p>When assessing the impact on transactions, financial entities shall take into account Article 1(4) of Delegated Regulation (EU) 2024/1772, including all affected domestic and cross-border transactions containing a monetary amount that have at least one part of the transaction carried out in the Union.</p>	No	Yes, if any transaction has been affected by the incident	Yes, if any transaction has been affected by the incident	Numerical integer

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>A financial entity that cannot determine the actual number of transactions impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, indicate the total number of transactions affected across all financial entities.</p>				
<p>3.10. Percentage of affected transactions</p>	<p>Percentage of affected transactions in relation to the daily average number of domestic and cross-border transactions carried out by the financial entity related to the affected service.</p> <p>Financial entities shall take into account Article 1(4) and Article 9(1), point (d), of Delegated Regulation (EU) 2024/1772.</p> <p>A financial entity that cannot determine the actual percentage of transactions impacted shall use estimates.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, a financial entity shall sum the number of all affected transactions and divide the sum by the total number of transactions of all impacted financial entities.</p>	<p>No</p>	<p>Yes, if any transaction has been affected by the incident</p>	<p>Yes, if any transaction has been affected by the incident</p>	<p>Expressed as percentage – any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2,4 instead of 2,4 %). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up</p>
<p>3.11. Value of affected transactions</p>	<p>Total value of the transactions affected by the major ICT-related incident shall be assessed in accordance with Article 1(4) and Article 9(1), point (e) of Delegated Regulation (EU) 2024/1772.</p> <p>A financial entity that cannot determine the actual value of transactions impacted shall use estimates based on available data from comparable reference periods.</p> <p>A financial entity shall report the monetary amount as a positive value.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the total value of the transactions affected across all financial entities.</p>	<p>No</p>	<p>Yes, if any transactions have been affected by the incident</p>	<p>Yes, if any transaction has been affected by the incident</p>	<p>Monetary Financial entities shall report the data point in units using a minimum precision equivalent to thousands of units (e.g. 2,5 instead of EUR 2 500).</p>

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.12. Information on whether the numbers are actual or estimates, or whether there has not been any impact	Information on whether the values reported in the data fields 3.4 to 3.11 are actual or estimates, or whether there has not been any impact.	No	Yes	Yes	Choice (multiple): <ul style="list-style-type: none"> — actual figures for clients affected; — actual figures for financial counterparts affected; — actual figures for transactions affected; — estimates for clients affected; — estimates for financial counterparts affected; — estimates for transactions affected; — no impact on clients; — no impact on financial counterparts; — no impact on transactions.
3.13. Reputational impact	Information about the reputational impact resulting from the major ICT-related incident as referred to in Articles 2 and 10 of Delegated Regulation (EU) 2024/1772. In the case of aggregated reporting as referred to in Article 7 of this Regulation, the reputational impact categories that apply to at least one financial entity.	No	Yes, if 'Reputational impact' criterion met	Yes, if 'Reputational impact' criterion met	Choice (multiple): <ul style="list-style-type: none"> — the major ICT-related incident has been reflected in the media; — the major ICT-related incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships — the financial entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the major ICT-related incident; — the financial entity will or is likely to lose clients or financial counterparts with a material impact on its business as a result of the major ICT-related incident.
3.14. Contextual information about the reputational impact	Information describing how the major ICT-related incident has affected or could affect the reputation of the financial entity, including infringements of law, regulatory requirements not met, number of client complaints, and other.	No	Yes, if 'Reputational impact' criterion met.	Yes, if 'Reputational impact' criterion met.	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>The contextual information shall include the type of media (e.g. traditional and digital media, blogs, streaming platforms) and media coverage, including reach of the media (local, national, international). Media coverage in this context shall not mean a few negative comments by followers or users of social networks.</p> <p>The financial entity shall also indicate whether the media coverage highlighted significant risks for its clients in relation to the major ICT-related incident, including the risk of the financial entity's insolvency or the risk of losing funds.</p> <p>Financial entities shall also indicate whether they have provided information to the media that served to reliably inform the public about the major ICT-related incident and its consequences.</p> <p>Financial entities may also indicate whether there was false information in the media in relation to the ICT-related incident, including information based on deliberate misinformation spread by threat actors, or information relating to or illustrating defacement of the financial entity's website.</p>				
3.15. Duration of the incident	<p>Financial entities shall measure the duration of the major ICT-related incident from the moment the major ICT-related incident occurred until the moment the incident was resolved.</p> <p>Financial entities that are unable to determine the moment when the major ICT-related incident has occurred shall measure the duration of the major ICT-related incident from the earlier between the moment the financial entity detected the incident and the moment when the financial entity recorded the incident in network or system logs or other data sources. Financial entities that do not yet know the moment when the major ICT-related incident will be resolved shall apply estimates. The value shall be expressed in days, hours, and minutes.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall measure the longest duration of the major ICT-related incident in case of differences between financial entities.</p>	No	Yes	Yes	DD:HH:MM

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.16. Service downtime	<p>Service downtime measured from the moment the service is fully or partially unavailable to clients, financial counterparts or other internal or external users, until the moment when regular activities or operations have been restored to the level of service that was provided prior to the major ICT-related incident.</p> <p>Where the service downtime causes a delay in the provision of service after regular activities or operations have been restored, financial entities shall measure the downtime from the start of the major ICT-related incident until the moment when that delayed service is provided. Financial entities that are unable to determine the moment when the service downtime has started, shall measure the service downtime from the earlier between the moment the incident was detected and the moment when it has been recorded.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall measure the longest duration of the service downtime in case of differences between financial entities.</p>	No	Yes, if the incident has caused a service downtime	Yes, if the incident has caused a service downtime	DD:HH:MM
3.17. Information on whether the numbers for duration and service downtime are actual or estimates	Information on whether the values reported in data fields 3.15 and 3.16 are actual or estimates.	No	Yes, if 'Duration and service downtime' criterion met	Yes, if 'Duration and service downtime' criterion met	Choice: <ul style="list-style-type: none"> — Actual figures; — Estimates; — Actual figures and estimates; — No information available.
3.18. Types of impact in the Member States	<p>Type of impact in the respective EEA Member States.</p> <p>Indication of whether the major ICT-related incident has had an impact in other EEA Member States (other than the Member State of the competent authority to which the incident is directly reported), in accordance with Article 4 of Delegated Regulation (EU) 2024/1772, and in particular with regard to the significance of the impact in relation to:</p> <p>(a) clients and financial counterparts affected in other Member States; or</p>	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Choice (multiple): <ul style="list-style-type: none"> — clients; — financial counterparts; — branch of the financial entity; — financial entities within the group carrying out activities in the respective Member State; — financial market infrastructure; — third-party providers that may be common to other financial entities.

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(b) branches or other financial entities within the group carrying out activities in other Member States; or</p> <p>(c) financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services.</p>				
3.19. Description of how the incident has an impact in other Member States	<p>Description of the impact and severity of the major ICT-related incident in each affected Member State, including an assessment of the impact and severity on:</p> <p>(a) clients;</p> <p>(b) financial counterparts;</p> <p>(c) branches of the financial entity;</p> <p>(d) other financial entities within the group carrying out activities in the respective Member State;</p> <p>(e) financial market infrastructures;</p> <p>(f) third-party providers that may be common to other financial entities as applicable in other Member State(s).</p>	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Alphanumeric
3.20. Materiality thresholds for the classification criterion 'Data losses'	<p>Type of data losses that the major ICT-related incident entails in relation to availability, authenticity, integrity, and confidentiality of data.</p> <p>Financial entities shall take into account Articles 5 and 13 of Delegated Regulation (EU) 2024/1772 in their assessment.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation, the data losses affecting at least one financial entity.</p>	No	Yes, if 'Data losses' criterion is met	Yes, if 'Data losses' criterion is met	Choice (multiple): — availability; — authenticity; — integrity; — confidentiality.
3.21. Description of the data losses	<p>Description of the impact of the major ICT-related incident on availability, authenticity, integrity, and confidentiality of critical data in accordance with Articles 5 and 13 of Delegated Regulation (EU) 2024/1772.</p> <p>Information about the impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements.</p> <p>As part of the information provided, financial entities shall indicate whether the data affected are client data, other entities' data (e.g. financial counterparts), or data of the financial entity itself.</p>	No	Yes, if 'Data losses' criterion is met	Yes, if 'Data losses' criterion is met	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>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.).</p> <p>The information may also include possible risks associated with the data losses, such as whether the data affected by the incident can be used to identify individuals and could be used by the threat actor to obtain credit or loans without their consent, to conduct spear phishing attacks, to disclose information publicly.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, a general description of the impact of the incident on the affected financial entities. Where there are differences of the impact, the description of the impact shall clearly indicate the specific impact on the different financial entities.</p>				
3.22. Classification criterion 'Critical services affected'	<p>Information related to the criterion 'Critical services affected'.</p> <p>Financial entities shall take into account Articles 6 of Delegated Regulation (EU) 2024/1772 in their assessment, including information about:</p> <ul style="list-style-type: none"> — the affected services or activities that require authorisation, registration or that are supervised by competent authorities; or — the ICT services or network and information systems that support critical or important functions of the financial entity; and — the nature of the malicious and unauthorised access to the network and information systems of the financial entity. <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the impact on critical services that apply to at least one financial entity.</p>	No	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.23. Type of the incident	Classification of incidents by type.	No	Yes	Yes	Choice (multiple): <ul style="list-style-type: none"> — Cybersecurity-related; — Process failure; — System failure; — External event; — Payment-related; — Other (please specify).
3.24. Other types of incidents	Other types of ICT-related incidents: financial entities that have selected 'other' type of incidents in the data field 3.23, shall specify the type of ICT-related incident.	No	Yes, if 'other' type of incidents is selected in data field 3.23	Yes, if 'other' type of incidents is selected in data field 3.23	Alphanumeric
3.25. Threats and techniques used by the threat actor	Indicate the threats and techniques used by the threat actor, including: (a) social engineering, including phishing; (b) (D)DoS; (c) identity theft; (d) data encryption for impact, including ransomware; (e) resource hijacking; (f) data exfiltration and manipulation, excluding identity theft; (g) data destruction; (h) defacement; (i) supply-chain attack; (j) other (please specify).	No	Yes, if the type of the ICT-related incident is 'cybersecurity-related' in field 3.23	Yes, if the type of the ICT-related incident is 'cybersecurity-related' in field 3.23	Choice (multiple): <ul style="list-style-type: none"> — Social engineering (including phishing); — (D)DoS; — Identity theft; — Data encryption for impact, including ransomware; — Resource hijacking; — Data exfiltration and manipulation, including identity theft; — Data destruction; — Defacement; — Supply-chain attack; — Other (please specify).
3.26. Other types of techniques	Other types of techniques Financial entities that have selected 'other' type of techniques in data field 3.25 shall specify the type of technique.	No	Yes, if other' type of techniques is selected in data field 3.25	Yes, if other' type of techniques is selected in data field 3.25	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.27. Information about affected functional areas and business processes	<p>Indication of the functional areas and business processes that are affected by the incident, including products and services.</p> <p>The functional areas shall include but are not limited to:</p> <ul style="list-style-type: none"> (a) marketing and business development; (b) customer service; (c) product management; (d) regulatory compliance; (e) risk management; (f) finance and accounting; (g) HR and general services; (h) information Technology. <p>The business processes shall include but are not limited to:</p> <ul style="list-style-type: none"> — account information; — actuarial services; — acquiring of payment transactions; — authentication/authorization; — authority; — client on-boarding; — benefit administration; — benefit payment management; — buying and selling packaged insurances policies between insurances; — card payments; — cash management; — cash placement or withdrawals; — insurance 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; — financial instruments placing; — fund accounting; 	No	Yes	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<ul style="list-style-type: none"> — FX money; — investment advice; — investment management; — issuing of payment instruments; — lending management; — life insurance payments process; — money remittance; — net asset calculation; — order; — payment initiation; — insurance underwriting; — portfolio management; — premium collection; — reception/transmission/execution; — reinsurance; — settlement; — transaction monitoring. <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the affected functional areas and business processes in at least one financial entity.</p>				
3.28. Affected infrastructure components supporting business processes	Information on whether infrastructure components (servers, operating systems, software, application servers, middleware, network components, others) supporting business processes have been affected by the major ICT-related incident.	No	Yes	Yes	Choice: — Yes; — No; — Information not available.
3.29. Information about affected infrastructure components supporting business processes	<p>Description on the impact of the major ICT-related incident on infrastructure components supporting business processes including hardware and software.</p> <p>Hardware includes servers, computers, data centres, switches, routers, hubs. Software includes operating systems, applications, databases, security tools, network components, others please specify. The descriptions shall describe or name affected infrastructure components or systems, and, where available:</p> <ul style="list-style-type: none"> (a) version information; (b) internal infrastructure/partially outsourced/fully outsourced – third-party provider name; 	No	Yes, if the incident has affected infrastructure components supporting business processes	Yes, if the incident has affected infrastructure components supporting business processes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	(c) whether the infrastructure is used or shared across multiple business functions; (d) relevant resilience/continuity/recovery/ substitutability arrangements in place.				
3.30. Impact on the financial interest of clients	Information on whether the major ICT-related incident has impacted the financial interest of clients.	No	Yes	Yes	Choice: — Yes; — No; — Information not available.
3.31. Reporting to other authorities	Specification of which authorities were informed about the major ICT-related incident. Taking into account the differences resulting from the national legislation of the Member States, the concept of law enforcement authorities shall be understood by financial entities broadly to include public authorities empowered to prosecute cybercrime, including police, law enforcement agencies, and public prosecutors.	No	Yes	Yes	Choice (multiple): — Police/Law Enforcement; — CSIRT; — Data Protection Authority; — National Cybersecurity Agency; — None; — Other (please specify).
3.32. Specification of 'other' authorities	Specification of 'other' types of authorities informed about the major ICT-related incident. If selected in Data field 3.31 'Other', the description shall include more detailed information about the authority to which the financial entity has submitted information about the major ICT-related incident.	No	Yes, if 'other' type of authorities have been informed by the financial entity about the major ICT-related incident.	Yes, if 'other' type of authorities have been informed by the financial entity about the major ICT-related incident	Alphanumeric
3.33. Temporary actions/measures taken or planned to be taken to recover from the incident	Indication of whether financial entity has implemented (or plan to implement) any temporary actions that have been taken (or planned to be taken) to recover from the major ICT-related incident.	No	Yes	Yes	Boolean (Yes or No)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
<p>3.34. Description of any temporary actions and measures taken or planned to be taken to recover from the incident</p>	<p>The information shall describe the immediate actions taken, including the 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.</p> <p>Financial entities shall 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 expected.</p> <p>If no temporary actions/measures have been taken, please indicate the reason.</p>	<p>No</p>	<p>Yes, if temporary actions/ measures have been taken or are planned to be taken (data field 3.33)</p>	<p>Yes, if temporary actions/ measures have been taken or are planned to be taken (data field 3.33)</p>	<p>Alphanumeric</p>
<p>3.35. Indicators of compromise</p>	<p>Information related to the major ICT-related incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.</p> <p>The field applies only to those financial entities that fall within the scope of Directive (EU) 2022/2555 of the European Parliament and of the Council (*) and those financial entities financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, where relevant.</p> <p>The IoC provided by the financial entity shall include the following categories of data:</p> <ul style="list-style-type: none"> (a) IP addresses; (b) URL addresses; (c) domains; (d) file hashes; (e) malware data (malware name, file names and their locations, specific registry keys associated with malware activity); (f) network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); (g) email message data (sender, recipient, subject, header, content); 	<p>No</p>	<p>Yes, if cybersecurity-related is selected as a type of incident in data field 3.23</p>	<p>Yes, if cybersecurity-related is selected as a type of incident in data field 3.23</p>	<p>Alphanumeric</p>

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(h) DNS requests and registry configurations; (i) user account activities (logins, privileged user account activity, privilege escalation); (j) database traffic (read/write), requests to the same file.</p> <p>In practice, this type of information may include data relating to, inter alia, 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), and URLs relating to phishing sites or websites observed hosting malware or exploit kits.</p>				

Content of the final report

4.1. High-level classification of root causes of the incident	<p>High-level classification of root cause of the major ICT-related incident under the incident types, including the following high-level categories:</p> <p>(a) malicious actions; (b) process failure; (c) system failure/malfunction; (d) human error; (e) external event.</p>	No	No	Yes	<p>Choice (multiple):</p> <ul style="list-style-type: none"> — malicious actions; — process failure; — system failure / malfunction; — human error; — external event.
4.2. Detailed classification of root causes of the incident	<p>Detailed classification of root causes of the major ICT-related incident under the incident types, including the following detailed categories linked to the high-level categories that are reported in data field 4.1:</p> <p>1. Malicious actions (if selected, choose one or more the following): (a) deliberate internal actions; (b) deliberate physical damage/manipulation/theft; (c) fraudulent actions.</p> <p>2. Process failure (if selected, choose one or more the following): (a) insufficient monitoring or failure of monitoring and control;</p>	No	No	Yes	<p>Choice (multiple):</p> <ul style="list-style-type: none"> — malicious actions: deliberate internal actions; — malicious actions: deliberate physical damage/manipulation/theft; — malicious actions: fraudulent actions; — process failure: insufficient monitoring or failure of monitoring and control; — process failure: insufficient/unclear roles and responsibilities; — process failure: ICT risk management process failure; — process failure: insufficient or failure of ICT operations and ICT security operations;

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(b) insufficient/unclear roles and responsibilities; (c) ICT risk management process failure; (d) insufficient or failure of ICT operations and ICT security operations; (e) insufficient or failure of ICT project management; (f) inadequate internal policies, procedures and documentation; (g) inadequate ICT systems acquisition, development, or maintenance; (h) other (please specify).</p> <p>3. System failure/malfunction (if selected, choose one or more the following):</p> <p>(a) hardware capacity and performance: major ICT-related incidents caused by hardware resources which prove inadequate in terms of capacity or performance to fulfil the applicable legislative requirements;</p> <p>(b) hardware maintenance: major ICT-related incidents resulting from inadequate or insufficient maintenance of hardware components, other than 'Hardware obsolescence/ageing';</p> <p>(c) hardware obsolescence/ageing: this root cause type involves major ICT-related incidents resulting from outdated or aging hardware components;</p> <p>(d) software compatibility/configuration: major ICT-related incidents caused by software components that are incompatible with other software or system configurations, including major ICT-related incidents resulting from software conflicts, incorrect settings, or misconfigured parameters that impact the overall system functionality;</p> <p>(e) software performance: major ICT-related incidents resulting from software components that exhibit poor performance or inefficiencies, for reasons other than those specified under 'Software compatibility/configuration', including major ICT-related incidents caused by slow response times, excessive resource consumption, or inefficient query execution impacting the performance of the software or system;</p>				<ul style="list-style-type: none"> — process failure: insufficient or failure of ICT project management; — process failure: inadequacy of internal policies, procedures and documentation; — Process failure: inadequate ICT systems acquisition, development, and maintenance; — process failure: other (please specify); — system failure: hardware capacity and performance; — system failure: hardware maintenance; — system failure: hardware obsolescence/ageing; — system failure: software compatibility/configuration; — system failure: software performance; — system failure: network configuration; — system failure: physical damage; — system failure: other (please specify); — human error: omission; — human error: mistake; — human error: skills & knowledge; — human error: inadequate human resources; — human error miscommunication; — human error: other (please specify); — external event: natural disasters/force majeure; — external event: third-party failures; — external event: other (please specify).

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(f) network configuration: major ICT-related incidents resulting from incorrect or misconfigured network settings or infrastructure, including major ICT-related incidents caused by network configuration errors, routing issues, firewall misconfigurations, or other network-related problems affecting connectivity or communication;</p> <p>(g) physical damage: major ICT-related incidents caused by physical damage to ICT infrastructure which lead to system failures;</p> <p>(h) other (please specify).</p> <p>4. Human error (if selected, choose one or more the following):</p> <p>(a) omission (unintentional);</p> <p>(b) mistake;</p> <p>(c) skills & knowledge: major ICT-related 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;</p> <p>(d) inadequate human resources: major ICT-related incidents caused by a lack of necessary resources, including hardware, software, infrastructure, or personnel, and including situations where insufficient resources lead to operational inefficiencies, system failures, or an inability to meet business demands;</p> <p>(e) miscommunication;</p> <p>(f) other (please specify).</p> <p>5. External event (if selected, choose one or more the following):</p> <p>(a) natural disasters/force majeure;</p> <p>(b) third-party failures;</p>				

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(c) other (please specify).</p> <p>Financial entities shall consider that for recurring major ICT-related incidents, the specific apparent root cause of the incident is taken into account and not the broad categories included in this field.</p>				
<p>4.3. Additional classification of root causes of the incident</p>	<p>Additional classification of root causes of the major ICT-related incident under the incident type, including the following additional classification categories linked to the detailed categories that are to be reported in data field 4.2.</p> <p>The field is mandatory for the final report if specific categories that require further granularity are reported in data field 4.2.</p> <p>2(a) Insufficient or failure of monitoring and control:</p> <ul style="list-style-type: none"> (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. <p>2(c) ICT risk management process failure:</p> <ul style="list-style-type: none"> (a) failure in specifying accurate risk tolerance levels; (b) insufficient vulnerability and threat assessments; (c) inadequate risk treatment measures; (d) poor management of residual ICT risks. <p>2(d) Insufficient or failure of ICT operations and ICT security operations:</p> <ul style="list-style-type: none"> (a) vulnerability and patch management; (b) change management; (c) capacity and performance management; (d) ICT asset management and information classification; 	<p>No</p>	<p>No</p>	<p>Yes</p>	<p>Choice (multiple):</p> <ul style="list-style-type: none"> — monitoring of policy adherence; — monitoring of third-party service providers; — monitoring and verification of remediation of vulnerabilities; — identity and access management; — encryption and cryptography; — logging; — failure in specifying accurate risk tolerance levels; — insufficient vulnerability and threat assessments; — inadequate risk treatment measures; — poor management of residual ICT risks; — vulnerability and patch management; — change management; — capacity and performance management; — ICT asset management and information classification; — backup and restore; — error handling; — inadequate ICT systems acquisition, development, and maintenance; — insufficient or failure of software testing.

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(e) backup and restore; (f) error handling.</p> <p>2(g) Inadequate ICT Systems acquisition, development, and maintenance: (a) inadequate ICT Systems acquisition, development, and maintenance; (b) insufficient software testing or failure of software testing.</p>				
4.4. Other types of root cause types	Financial entities that have selected 'other' type of root cause in data field 4.2 shall specify other types of root cause types	No	No	Yes, if 'other' type of root causes is selected in data field 4.2.	Alphanumeric
4.5. Information about the root causes of the incident	<p>Description of the sequence of events that led to the major ICT-related incident and description of how the major ICT-related incident has a similar apparent root cause if that incident is classified as a recurring incident, including a concise description of all underlying reasons and primary factors that contributed to the occurrence of the major ICT-related incident.</p> <p>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 major ICT-related incident, including a description of the investigations and analysis that led to the identification of the root causes, if applicable.</p>	No	No	Yes	Alphanumeric
4.6. Incident resolution	<p>Additional information regarding the actions/measures taken/planned to permanently resolve the major ICT-related incident and to prevent that incident from happening again.</p> <p>Lessons learnt from the major ICT-related incident.</p>	No	No	Yes	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>The description shall contain the following points:</p> <ol style="list-style-type: none"> 1. Resolution actions description <ol style="list-style-type: none"> (a) Actions taken to permanently resolve the major ICT-related incident (excluding any temporary actions); (b) for each action taken, indicate the potential involvement of a third-party provider and of the financial entity; (c) indicate whether procedures have been adapted following the major ICT-related incident; (d) indicate any additional controls that were put in place or that are planned with related implementation timeline. <p>Potential issues identified regarding the robustness of the IT systems impacted /or in terms of the procedures or controls in place, if applicable.</p> <p>Financial entities shall clearly indicate how the envisaged remediation actions will address the identified root causes and when the major ICT-related incident is expected to be resolved permanently.</p> <ol style="list-style-type: none"> 2. Lessons learnt <p>Financial entities shall describe findings from the post-incident review.</p>				
4.7. Date and time when the incident root cause was addressed	Date and time when the incident root cause was addressed.	No	No	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
4.8. Date and time when the incident was resolved	Date and time when the incident was resolved.	No	No	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
4.9. Information if the permanent resolution date of the incidents differs from the initially planned implementation date	Descriptions of the reason why the permanent resolution date of the major ICT-related incidents is different from the initially planned implementation date, where applicable.	No	No	Yes	Alphanumeric
4.10. Assessment of risk to critical functions for resolution purposes	<p>Assessment of whether the major ICT-related incident poses a risk to critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU of the European Parliament and of the Council ⁽²⁾.</p> <p>Entities as referred to in Article 1(1) of Directive 2014/59/EU shall indicate whether the incident poses a risk to the critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU, and as reported in Template Z07.01 of Commission Implementing Regulation (EU) 2018/1624 ⁽³⁾ and mapped to the specific entity in Template Z07.02.</p>	No	No	Yes, if the incident poses a risk to critical functions of financial entities under Article 2(1), point 35, of Directive 2014/59/EU	Alphanumeric
4.11. Information relevant for resolution authorities	<p>Description of whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group.</p> <p>Entities as referred to in Article 1(1) of Directive 2014/59/EU shall provide information on whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group.</p> <p>Those entities shall also indicate whether the major ICT-related incident affects the solvency or liquidity of the financial entity and the potential quantification of the impact.</p> <p>Those entities shall also provide information on the impact on operational continuity, impact on resolvability of the entity, any additional impact on the costs and losses from the major ICT-related 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 entity.</p>	No	No	Yes, if the incident has affected the resolvability of the entity or the group	Alphanumeric

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
4.12. Materiality threshold for the classification criterion 'Economic impact'	Detailed information about thresholds eventually reached by the major ICT-related incident in relation to the criterion 'Economic impact' referred to in Articles 7 and 14 of the Delegated Regulation (EU) 2024/1772.	No	No	Yes	Alphanumeric
4.13. Amount of gross direct and indirect costs and losses	<p>Total amount of gross direct and indirect costs and losses incurred by the financial entity stemming from the major ICT-related incident, including:</p> <ul style="list-style-type: none"> (a) the amount of expropriated funds or financial assets for which the financial entity is liable; (b) the amount of replacement or relocation costs of software, hardware or infrastructure; (c) the 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; (d) the amount of fees due to non-compliance with contractual obligations; (e) the amount of customer redress and compensation costs; (f) the amount of losses due to forgone revenues; (g) the amount of costs associated with internal and external communication; (h) the amount of advisory costs, including costs associated with legal counselling, forensic and remediation services; (i) the amount other costs and losses, including: <ul style="list-style-type: none"> (i) direct charges, including impairments and settlement charges, to the profit and loss account and write-downs due to the major ICT-related incident; (ii) provisions or reserves accounted for in the profit and loss account against probable losses related to the major ICT-related incident; 	No	No	Yes	Monetary

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>(iii) 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;</p> <p>(iv) material uncollected revenues, related to contractual obligations with third parties, including the decision to compensate a client following the major ICT-related incident, rather than by a reimbursement or direct payment, through a revenue adjustment waiving or reducing contractual fees for a specific future period of time;</p> <p>(v) timing losses, where they span more than one financial accounting year and give rise to legal risk.</p> <p>Financial entities shall take into account in their assessment Article 7(1) and (2) of Delegated Regulation (EU) 2024/1772. Financial entities shall not include in this figure financial recoveries of any type.</p> <p>Financial entities shall report the monetary amount as a positive value.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall take into account the total amount of costs and losses across all financial entities. Financial entities shall report the data point in units using a minimum precision equivalent to thousands of units.</p>				
4.14. Amount of financial recoveries	<p>Total amount of financial recoveries. Financial recoveries shall relate to the original loss caused by the incident, independently from the time when the financial recoveries in the form of funds or inflows of economic benefits are received.</p>	No	No	Yes	<p>Monetary</p> <p>Financial entities shall report the data point in units using a minimum precision equivalent to thousands of units</p>

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>Financial entities shall report the monetary amount as a positive value.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall take into account the total amount of financial recoveries across all financial entities.</p>				
4.15. Information on whether the non-major incidents have been recurring	<p>Information on whether more than one non-major ICT-related incident have been recurring and are together considered to be a major incident within the meaning of Article 8(2) of Delegated Regulation (EU) 2024/1772.</p> <p>Financial entities shall indicate whether the non-major ICT-related incidents have been recurring and are together considered as one major ICT-related incident.</p> <p>Financial entities shall also indicate the number of occurrences of these non-major ICT-related incidents.</p>	No	No	Yes, if the major incident comprises more than one non-major recurring incidents.	Alphanumeric
4.16. Date and time of occurrence of recurring incidents	Where financial entities report recurring ICT-related incidents, date and time at which the first ICT-related incident has occurred.	No	No	Yes, for recurring incidents	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)

- (¹) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, <http://data.europa.eu/eli/dir/2022/2555/oj>).
- (²) Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190, <http://data.europa.eu/eli/dir/2014/59/oj>).
- (³) Commission Implementing Regulation (EU) 2018/1624 of 23 October 2018 laying down implementing technical standards with regard to procedures and standard forms and templates for the provision of information for the purposes of resolution plans for credit institutions and investment firms pursuant to Directive 2014/59/EU of the European Parliament and of the Council, and repealing Commission Implementing Regulation (EU) 2016/1066 (OJ L 277, 7.11.2018, p. 1, http://data.europa.eu/eli/reg_impl/2018/1624/oj).

TEMPLATES FOR NOTIFICATION OF SIGNIFICANT CYBER THREATS

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

DATA GLOSSARY AND INSTRUCTIONS FOR NOTIFICATION OF SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory field	Field type
1. Name of the entity submitting the notification	Full legal name of the entity submitting the notification.	Yes	Alphanumeric
2. Identification code of the entity submitting the notification	<p>Identification code of the entity submitting the notification.</p> <p>Where financial entities submit the notification/report, the identification code shall be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.</p> <p>Where a third-party provider submits a report for a financial entity, it may use an identification code as specified in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554.</p>	Yes	Alphanumeric
3. Type of financial entity submitting the report	Type of the entity referred to in Article 2(1), points (a) to (t) of Regulation (EU) 2022/2554 submitting the report.	Yes, if the report is not provided by the affected financial entity directly.	<p>Choice (multiselect):</p> <ul style="list-style-type: none"> — credit institution; — payment institution; — exempted payment institution; — account information service provider; — electronic money institution; — exempted electronic money institution; — investment firm; — crypto-asset service provider; — issuer of asset-referenced tokens; — central securities depository; — central counterparty; — trading venue; — trade repository; — manager of alternative investment fund; — management company; — data reporting service provider;

Data field	Description	Mandatory field	Field type
			<ul style="list-style-type: none"> — insurance and reinsurance undertaking; — insurance intermediary, reinsurance intermediary and ancillary insurance intermediary; — institution for occupational retirement provision; — credit rating agency; — administrator of critical benchmarks; — crowdfunding service provider; — securitisation repository.
4. Name of the financial entity	Full legal name of the financial entity notifying the significant cyber threat.	Yes, if the financial entity is different from the entity submitting the notification	Alphanumeric
5. LEI code of the financial entity	Legal Entity Identifier (LEI) of the financial entity notifying the significant cyber threat, assigned in accordance with the International Organisation for Standardisation.	Yes, if the financial entity notifying the significant cyber threat is different from the entity submitting the report	Unique alphanumeric 20 character code, based on ISO 17442-1:2020
6. Primary contact person name	Name and surname of the primary contact person of the financial entity.	Yes	Alphanumeric
7. Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication.	Yes	Alphanumeric
8. Primary contact person telephone	<p>The telephone number of the primary contact person that can be used by the competent authority for follow-up communication.</p> <p>The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)</p>	Yes	Alphanumeric
9. Second contact person name	Name and surname of the second contact person of the financial entity or an entity submitting the notification on behalf of the financial entity, where available.	Yes, if name and surname of the second contact person of the financial entity or an entity submitting the notification for the financial entity is available	Alphanumeric

Data field	Description	Mandatory field	Field type
10. Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication, where available.	Yes, if email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication is available	Alphanumeric
11. Second contact person telephone	The telephone number of the second contact person that can be used by the competent authority for follow-up communication, where available. The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXXX).	Yes, if the telephone number of the second contact person that can be used by the competent authority for follow-up communication is available	Alphanumeric
12. Date and time of detection of the cyber threat	Date and time at which the financial entity has become aware of the significant cyber threat.	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
13. Description of the significant cyber threat	Description of the most relevant aspects of the significant cyber threat. Financial entities shall provide: (a) a high-level overview of the most relevant aspects of the significant cyber threat; (b) the related risks arising from it, including potential vulnerabilities of the systems of the financial entity that can be exploited; (c) information about the probability of materialisation of the significant cyber threat; and (d) information about the source of information about the cyber threat.	Yes	Alphanumeric
14. Information about potential impact	Information about the potential impact of the cyber threat on the financial entity, its clients or financial counterparts if the cyber threat has materialised	Yes	Alphanumeric
15. Potential incident classification criteria	The classification criteria that could have triggered a major incident report if the cyber threat had materialised.	Yes	Choice (multiple): — clients, financial counterparts and transactions affected; — reputational impact; — duration and service downtime; — geographical spread; — data losses; — critical services affected; — economic impact.

Data field	Description	Mandatory field	Field type
16. Status of the cyber threat	<p>Information about the status of the cyber threat for the financial entity and whether there have been any changes in the threat activity.</p> <p>Where the cyber threat has stopped communicating with the financial entity's information systems, the status can be marked as inactive. If the financial entity has information that the threat remains active against other parties or the financial system as a whole, the status shall be marked as active.</p>	Yes	Choice: — active; — inactive.
17. Actions taken to prevent materialisation	High-level information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if applicable.	Yes	Alphanumeric
18. Notification to other stakeholders	Information about notification of the cyber threat to other financial entities or authorities.	Yes, if other financial entities or authorities have been informed about the cyber threat)	Alphanumeric
19. Indicators of compromise	<p>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.</p> <p>The IoC provided by the financial entity may include, but is not to be limited to, the following categories of data:</p> <ul style="list-style-type: none"> (a) IP addresses; (b) URL addresses; (c) domains; (d) file hashes; (e) malware data (malware name, file names and their locations, specific registry keys associated with malware activity); (f) network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); (g) email message data (sender, recipient, subject, header, content); (h) DNS requests and registry configurations; (i) user account activities (logins, privileged user account activity, privilege escalation); (j) database traffic (read/write), requests to the same file. <p>This type of information may include data relating to 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), and URLs relating to phishing sites or websites observed hosting malware or exploit kits.</p>	Yes, if information about indicators of compromise connected with the cyber threat are available)	Alphanumeric
20. Other relevant information	Any other relevant information about the significant cyber threat	Yes, if applicable and if there is other information available, not covered in the template	Alphanumeric