EUROPEAN
COMMISSION

Brussels, 23.10.2024
C(2024) 7277 final

ANNEXES 1 to 4

# ANNEXES

**to the**

**COMMISSION IMPLEMENTING REGULATION (EU)**

**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**

# ANNEX I
## 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 | |

| Number of field | Data field | |
|---|---|---|
| 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 | |
| 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 | |

| Number of field | Data field | |
|---|---|---|
| 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 | |

| Number of field | Data field | |
|---|---|---|
| 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 | |
| 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 | |

| Number of field | Data field | |
|---|---|---|
| 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 | |

| Number of field | Data field | |
|---|---|---|
| 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 | |
| 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 | |

**ANNEX II**
**Data glossary and instructions for the reporting of major incidents**

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| **General information about the financial entity** | | | | | |
| 1.1. Type of submission | Indicate the type of incident notification or report being submitted to the competent authority. | Yes | Yes | Yes | Choice:<br>- initial notification<br>- intermediate report<br>- final report<br>- major incident reclassified as non-major |
| 1.2. Name of the entity submitting the report | Full legal name of the entity submitting the report. | Yes | Yes | Yes | Alphanumeric |
| 1.3. Identification code of the entity submitting the report | Identification code of the entity submitting the report.<br>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. | Yes | Yes | Yes | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | 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. . | | | | |
| 1.4. Type of the affected financial entity | 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.<br><br>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. | Yes | Yes | Yes | Choice (multiselect):<br>- credit institution;<br>- payment institution;<br>- exempted payment institution;<br>- account information service provider;<br>- electronic money institution;<br>- exempted electronic money institution;<br>- investment firm;<br>- crypto-asset service provider;<br>- issuer of asset-referenced tokens;<br>- central securities |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | | | | | depository;<br>- central counterparty;<br>- trading venue;<br>- trade repository;<br>- manager of alternative investment fund;<br>- management company;<br>- data reporting service provider;<br>- insurance and reinsurance undertaking;<br>- insurance intermediary, reinsurance intermediary and ancillary insurance intermediary;<br>- institution for occupational retirement provision;<br>- credit rating |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | | | | | agency;<br>- administrator of critical benchmarks;<br>- crowdfunding service provider;<br>- securitisation repository. |
| 1.5. Name of the financial entity affected | Full legal name of the financial entity affected by the major ICT-related incident and required to report the major incident to its competent authority under Article 19 of Regulation (EU) 2022/2554.<br><br>In case of aggregated reporting:<br>(a) list of all names of the financial entities affected by the major ICT-related incident, separated by a semicolon.<br>(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. | 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 |

| **Data field** | **Description** | **Mandatory for initial notification** | **Mandatory for intermediate report** | **Mandatory for final report** | **Field type** |
|---|---|---|---|---|---|
| 1.6. LEI code of the financial entity affected | Legal Entity Identifier (LEI) of the financial entity affected by the major ICT-related incident assigned in accordance with the International Organisation for Standardisation.<br><br>In case of aggregated reporting:<br><br>(a) a list of all LEI codes of the financial entities affected by the major ICT-related incident, separated by a semicolon.<br>(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.<br><br>The order of appearance of LEI codes and financial entities names shall be identical. | Yes, if the financial entity affected by the major ICT-related incident is different from the entity submitting the report and in case of aggregated reporting. | Yes, if the financial entity affected by the major ICT-related incident is different from the entity submitting the report and in case of aggregated reporting. | Yes, if the financial entity affected by the major ICT-related incident is different from the entity submitting the report and in case of aggregated reporting | Unique 20 alphanumeric character code, based on ISO 17442-1:2020 |
| 1.7. Primary contact person name | Name and surname of the primary contact person of the financial entity. | Yes | Yes | Yes | Alphanumeric |

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

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| 1.11. Second contact person email | Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication. | Yes | Yes | Yes | Alphanumeric |
| 1.12. Second contact person telephone | The telephone number of the second contact person, or of a team, that can be used by the competent authority for follow-up communication.<br>The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX) | 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. | Currency used for the incident reporting | Yes | Yes | Yes | Choice populated by using ISO 4217 |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| Reporting currency | | | | | 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.<br><br>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.<br>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) |
| 2.3. Date and time of classificatio | Date and time when the ICT-related incident was classified as major according to the classification criteria established in Regulation (EU) 2024/1772[1]. | Yes | Yes | Yes | ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss) |

[1] 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).

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| n of the incident as major | | | | | |
| 2.4. Description of the ICT-related incident | Description of the most relevant aspects of the major ICT-related incident.<br><br>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).<br><br>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. | Yes | Yes | Yes | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | | | | | |
| 2.5. Classification criteria that triggered the incident report | Classification criteria under Delegated Regulation (EU) 2024/1772 that have triggered determination of the ICT-related incident as major and subsequent notification and reporting.<br><br>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. | Yes | Yes | Yes | Choice (multiple):<br>- clients, financial counterparts and transactions affected;<br>- reputational impact;<br>- duration and service downtime;<br>- geographical spread;<br>- data losses;<br>- critical services affected;<br>- economic impact. |
| 2.6. Materiality thresholds for the classification criterion 'Geographic | EEA Member States impacted by the major ICT-related incident<br><br>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. | 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 |
|---|---|---|---|---|---|
| al spread' | | | | | |
| 2.7. Discovery of the major ICT-related incident | Indication of how the major ICT-related incident has been discovered. | Yes | Yes | Yes | Choice:<br>- IT Security;<br>- staff;<br>- internal audit;<br>- external audit;<br>- clients;<br>- financial counterparts;<br>- third-party provider;<br>- attacker;<br>- monitoring systems;<br>- authority / agency / law enforcement body;<br>- other. |
| 2.8. Indication whether the incident | Indication whether the major ICT-related incident originates from a third-party provider or another financial entity. | Yes, if the incident originates from a | Yes, if the incident originates from a | Yes, if the incident originates from a | Alphanumeric |

EN EN

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| 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). | third-party provider or another financial entity | third-party provider or another financial entity | third-party provider or another financial entity | |
| 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.<br><br>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 if the major | Yes, if there is other information not covered in the template or if the major ICT-related incident has been | Yes, if there is other information not covered in the template or if the major | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | | ICT-related incident has been reclassified as non-major. | reclassified as non-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.<br><br>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) |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | | | | | |
| 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.<br><br>When assessing the number of clients affected, financial entities shall take into account Articles 1(1) and 9(1), point (b), of Delegated Regulation 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.<br><br>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 | 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.<br><br>Financial entities shall take into account Article 1(1) and Article 9(1), point (a), of Delegated Regulation 2024/1772 in their assessment.<br><br>A financial entity that cannot determine the actual percentage of clients impacted shall use estimates based on available data from comparable reference periods.<br><br>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. | No | Yes | Yes | Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| 3.6. Number of financial counterparts affected | Number of financial counterparts affected by the major ICT-related incident that have concluded a contract with the financial entity.<br><br>When assessing the number of financial counterparts affected, financial entities shall take into account Article 1(2) of Delegated Regulation 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.<br><br>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. | 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 | 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.<br><br>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 2024/1772 in their assessment.<br>A financial entity that cannot determine the actual percentage of financial counterparts impacted shall use estimates based on available data from comparable reference periods.<br><br>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. | 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 | 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 | Yes, if 'Relevance of clients and financial | Boolean (Yes or No) |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| counterparts | | | counterparts' threshold is met | counterparts' threshold is met | |
| 3.9. Number of affected transactions | Number of transactions affected by the major ICT-related incident.<br><br>When assessing the impact on transactions, financial entities shall take into account Article 1(4) of Delegated Regulation 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.<br><br>A financial entity that cannot determine the actual number of transactions impacted shall use estimates based on available data from comparable reference periods.<br><br>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. | No | Yes, if any transaction has been affected by the incident | Yes, if any transaction has been affected by the incident | Numerical integer |
| 3.10. Percentage of affected | 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. | No | Yes, if any transaction has been affected by | Yes, if any transaction has been affected | Expressed as percentage - any value up to 5 numeric characters including up |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| transactions | Financial entities shall take into account Article 1(4) and Article 9(1), point (d), of Delegated Regulation 2024/1772.<br>A financial entity that cannot determine the actual percentage of transactions impacted shall use estimates.<br>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. | | the incident | by the incident | to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up |
| 3.11. Value of affected transactions | Total value of the transactions affected by the major ICT-related incident shall be assessed in accordance with Article 1(4) and Article 9(1), point (e) of Delegated Regulation 2024/1772.<br>A financial entity that cannot determine the actual value of transactions impacted shall use estimates based on available data from comparable reference periods.<br>A financial entity shall report the monetary amount as a positive value.<br>In the case of aggregated reporting as referred to in Article 7 of | No | Yes, if any transactions have been affected by the incident | Yes, if any transaction has been affected by the incident | Monetary<br>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 2500). |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | this Regulation, the total value of the transactions affected across all financial entities. | | | | |
| 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):<br>- actual figures for clients affected;<br>- actual figures for financial counterparts affected;<br>- actual figures for transactions affected;<br>- estimates for clients affected;<br>- estimates for financial counterparts affected;<br>- estimates for transactions affected;<br>- no impact on clients;<br>- no impact on |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | | | | | financial counterparts;<br>- 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 2024/1772.<br><br>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):<br>- the major ICT-related incident has been reflected in the media;<br>- the major ICT-related incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships<br>- the financial entity will not be able to or is likely not to be able to meet |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | | | | | regulatory requirements as a result of the major ICT-related incident;<br>- 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.<br><br>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 | 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 |
|---|---|---|---|---|---|
| | negative comments by followers or users of social networks.<br><br>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.<br><br>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.<br><br>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. | | | | |
| 3.15. Duration of the incident | 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.<br><br>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 | No | Yes | Yes | DD:HH:MM |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | 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.<br><br>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. | | | | |
| 3.16. Service downtime | Service downtime measured from the moment the service is fully or partially unavailable to clients, financial counterparts or other internal or external users, 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.<br><br>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 | No | Yes, if the incident has caused a service downtime | Yes, if the incident has caused a service downtime | DD:HH:MM |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | incident was detected and the moment when it has been recorded.<br><br>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. | | | | |
| 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:<br><br>- Actual figures<br>- Estimates<br>- Actual figures and estimates<br>- No information available |
| 3.18. Types of impact in the Member States | Type of impact in the respective EEA Member States.<br><br>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: | No | Yes, if 'Geographical spread' threshold is met | Yes, if 'Geographical spread' threshold is met | Choice (multiple):<br><br>- clients<br>- financial counterparts<br>- branch of the financial entity<br>- financial entities within the group carrying out activities in the respective |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
| --- | --- | --- | --- | --- | --- |
| | (a) clients and financial counterparts affected in other Member States; or<br>(b) branches or other financial entities within the group carrying out activities in other Member States; or<br>(c) financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services. | | | | Member State<br>- financial market infrastructure<br>- third-party providers that may be common to other financial entities |
| 3.19. Description of how the incident has an impact in other Member States | 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:<br>(a) clients;<br>(b) financial counterparts;<br>(c) branches of the financial entity;<br>(d) other financial entities within the group carrying out activities in the respective Member State;<br>(e) financial market infrastructures;<br>(f) third-party providers that may be common to other financial entities as applicable in other member state(s). | No | Yes, if 'Geographical spread' threshold is met | Yes, if 'Geographical spread' threshold is met | Alphanumeric |
| 3.20. Materiality thresholds | Type of data losses that the major ICT-related incident entails in relation to availability, authenticity, integrity, and confidentiality of data. | No | Yes, if 'Data losses' | Yes, if 'Data losses' | Choice (multiple):<br>- availability<br>- authenticity |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| for the classification criterion ‘Data losses’ | Financial entities shall take into account Articles 5 and 13 of Delegated Regulation 2024/1772 in their assessment.<br><br>In case of aggregated reporting as referred to in Article 7 of this Regulation, the data losses affecting at least one financial entity. | | criterion is met | criterion is met | - integrity<br>- confidentiality |
| 3.21. Description of the data losses | 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 2024/1772.<br><br>Information about the impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements.<br><br>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.<br><br>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 | 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 |
|---|---|---|---|---|---|
| | secrecy, etc.).<br>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.<br>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. | | | | |
| 3.22. Classification criterion 'Critical services affected' | Information related to the criterion 'Critical services affected'.<br>Financial entities shall take into account Articles 6 of Delegated Regulation (EU) 2024/1772 in their assessment, including information about:<br>- the affected services or activities that require authorisation, registration or that are supervised by competent authorities; or<br>- the ICT services or network and information systems that support critical or important functions of the financial entity; | No | Yes | Yes | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | and<br>- the nature of the malicious and unauthorised access to the network and information systems of the financial entity.<br><br>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. | | | | |
| 3.23. Type of the incident | Classification of incidents by type. | No | Yes | Yes | Choice (multiple):<br>- Cybersecurity-related<br>- Process failure<br>- System failure<br>- External event<br>- Payment-related<br>- 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 |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| 3.25. Threats and techniques used by the threat actor | Indicate the threats and techniques used by the threat actor, including:<br>(a) social engineering, including phishing;<br>(b) (D)DoS;<br>(c) identity theft;<br>(d) data encryption for impact, including ransomware;<br>(e) resource hijacking;<br>(f) data exfiltration and manipulation, excluding identity theft;<br>(g) data destruction;<br>(h) defacement;<br>(i) supply-chain attack;<br>(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):<br>- Social engineering (including phishing)<br>- (D)DoS<br>- Identity theft<br>- Data encryption for impact, including ransomware<br>- Resource hijacking<br>- Data exfiltration and manipulation, including identity theft<br>- Data destruction<br>- Defacement<br>- Supply-chain attack<br>- Other (please specify) |
| 3.26. Other types of techniques | Other types of techniques<br><br>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 | Indication of the functional areas and business processes that are affected by the incident, including products and services.<br><br>The functional areas shall include but are not limited to:<br>(a) marketing and business development;<br>(b) customer service;<br>(c) product management;<br>(d) regulatory compliance;<br>(e) risk management;<br>(f) finance and accounting;<br>(g) HR and general services;<br>(h) information Technology;<br><br>The business processes shall include but are not limited to:<br>• account information;<br>• actuarial services;<br>• acquiring of payment transactions;<br>• authentication/authorization;<br>• authority<br>• client on-boarding;<br>• benefit administration;<br>• benefit payment management; | No | Yes | Yes | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | • buying and selling packaged insurances policies between insurances;<br>• card payments;<br>• cash management;<br>• cash placement or withdrawals;<br>• insurance claim management;<br>• claim process insurance;<br>• clearing;<br>• corporate loans conglomerates;<br>• collective insurances;<br>• credit transfers;<br>• custody and asset safekeeping;<br>• customer onboarding;<br>• data ingestion;<br>• data processing;<br>• direct debits;<br>• export insurances;<br>• finalizing trades/deals;<br>• financial instruments placing;<br>• fund accounting;<br>• FX money;<br>• investment advice;<br>• investment management;<br>• issuing of payment instruments; | | | | |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | • lending management;<br>• life insurance payments process;<br>• money remittance;<br>• net asset calculation;<br>• order;<br>• payment initiation;<br>• insurance underwriting;<br>• portfolio management;<br>• premium collection;<br>• reception/transmission/execution;<br>• reinsurance;<br>• settlement;<br>• transaction monitoring;<br><br>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. | | | | |
| 3.28. Affected infrastructure components supporting | 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:<br>- Yes<br>- No<br>- Information not available |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| business processes | | | | | |
| 3.29. Information about affected infrastructure components supporting business processes | Description on the impact of the major ICT-related incident on infrastructure components supporting business processes including hardware and software.<br><br>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:<br>(a) version information;<br>(b) internal infrastructure/partially outsourced/fully outsourced – third-party provider name;<br>(c) whether the infrastructure is used or shared across multiple business functions;<br>(d) relevant resilience/continuity/recovery/ substitutability arrangements in place. | No | Yes, if the incident has affected infrastructure components supporting business processes | Yes, if the incident has affected infrastructure components supporting business processes | Alphanumeric |
| 3.30. Impact on the financial | Information on whether the major ICT-related incident has impacted the financial interest of clients. | No | Yes | Yes | Choice:<br>- Yes<br>- No |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
| --- | --- | --- | --- | --- | --- |
| interest of clients | | | | | - Information not available |
| 3.31. Reporting to other authorities | Specification of which authorities were informed about the major ICT-related incident.<br><br>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):<br>- Police/Law Enforcement<br>- CSIRT<br>- Data Protection Authority<br>- National Cybersecurity Agency<br>- None<br>- Other (please specify) |
| 3.32. Specification of 'other' authorities | Specification of 'other' types of authorities informed about the major ICT-related incident.<br><br>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- | No | Yes, if 'other' type of authorities have been informed by the financial | Yes, if 'other' type of authorities have been informed by the | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | related incident. | | entity about the major ICT-related incident. | financial entity about the major ICT-related incident | |
| 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) |
| 3.34. Description of any temporary actions and measures | 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. | No | Yes, if temporary actions/measures have been taken or are | Yes, if temporary actions/measures have been taken or | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| taken or planned to be taken to recover from the incident | 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.<br><br>If no temporary actions/measures have been taken, please indicate the reason. | | planned to be taken (data field 3.33) | are planned to be taken (data field 3.33) | |
| 3.35. Indicators of compromise | 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.<br><br>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[2] 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. | No | Yes, if cybersecurity-related is selected as a type of incident in data field 3.23 | Yes, if cybersecurity-related is selected as a type of incident in data field 3.23 | Alphanumeric |

[2] 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).

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
| --- | --- | --- | --- | --- | --- |
| | The IoC provided by the financial entity shall include the following categories of data:<br>(a) IP addresses;<br>(b) URL addresses;<br>(c) domains;<br>(d) file hashes;<br>(e) malware data (malware name, file names and their locations, specific registry keys associated with malware activity);<br>(f) network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic);<br>(g) e-mail message data (sender, recipient, subject, header, content);<br>(h) DNS requests and registry configurations;<br>(i) user account activities (logins, privileged user account activity, privilege escalation);<br>(j) database traffic (read/write), requests to the same file.<br><br>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 | | | | |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | websites observed hosting malware or exploit kits. | | | | |
| **Content of the final report** | | | | | |
| 4.1. High-level classification of root causes of the incident | High-level classification of root cause of the major ICT-related incident under the incident types, including the following high-level categories:<br><br>(a) malicious actions;<br>(b) process failure;<br>(c) system failure/malfunction;<br>(d) human error;<br>(e) external event. | No | No | Yes | Choice (multiple):<br>- malicious actions;<br>- process failure;<br>- system failure / malfunction;<br>- human error;<br>- external event. |
| 4.2. Detailed classification of root causes of the incident | 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:<br><br>1. **Malicious actions** (if selected, choose one or more the following): | No | No | Yes | Choice (multiple):<br>- malicious actions: deliberate internal actions;<br>- malicious actions: deliberate physical damage/manipulati |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | (a) deliberate internal actions;<br>(b) deliberate physical damage/manipulation/theft;<br>(c) fraudulent actions.<br><br>2. **Process failure** (if selected, choose one or more the following):<br>(a) insufficient monitoring or failure of monitoring and control;<br>(b) insufficient/unclear roles and responsibilities;<br>(c) ICT risk management process failure;<br>(d) insufficient or failure of ICT operations and ICT security operations;<br>(e) insufficient or failure of ICT project management;<br>(f) inadequate internal policies, procedures and documentation;<br>(g) inadequate ICT systems acquisition, development, or maintenance;<br>(h) other (please specify).<br><br>3. **System failure/malfunction** (if selected, choose one or more the following):<br>(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;<br>(b) hardware maintenance: major ICT-related incidents resulting | | | | on/theft;<br>- malicious actions: fraudulent actions;<br>- process failure: insufficient monitoring or failure of monitoring and control;<br>- process failure: insufficient/unclear roles and responsibilities;<br>- process failure: ICT risk management process failure;<br>- process failure: insufficient or failure of ICT operations and ICT security operations;<br>- process failure: insufficient or |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | from inadequate or insufficient maintenance of hardware components, other than "Hardware obsolescence/ageing" ;<br>(c) hardware obsolescence/ageing: this root cause type involves major ICT-related incidents resulting from outdated or aging hardware components;<br>(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;<br>(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;<br>(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 | | | | failure of ICT project management;<br>- process failure: inadequacy of internal policies, procedures and documentation;<br>- Process failure: inadequate ICT systems acquisition, development, and maintenance;<br>- process failure: other (please specify);<br>- system failure: hardware capacity and performance;<br>- system failure: hardware maintenance;<br>- system failure: |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | affecting connectivity or communication;<br>(g) physical damage: major ICT-related incidents caused by physical damage to ICT infrastructure which lead to system failures;<br>(h) other (please specify).<br><br>**4. Human error** (if selected, choose one or more the following):<br>(a) omission (unintentional);<br>(b) mistake;<br>(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;<br>(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;<br>(e) miscommunication;<br>(f) other (please specify). | | | | hardware obsolescence/ageing;<br>- system failure: software compatibility/configuration;<br>- system failure: software performance;<br>- system failure: network configuration;<br>- system failure: physical damage;<br>- system failure: other (please specify);<br>- human error: omission; –<br>- human error: mistake;<br>- human error: skills & knowledge; |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | **5. External event** (if selected, choose one or more the following)<br>(a) natural disasters/force majeure;<br>(b) third-party failures;<br>(c) other (please specify).<br><br>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. | | | | - human error: inadequate human resources;<br>- human error miscommunication;<br>- human error: other (please specify);<br>- external event: natural disasters/force majeure;<br>- external event: third-party failures;<br>- external event: other (please specify). |
| 4.3. Additional classification of root causes of the incident | 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.<br><br>The field is mandatory for the final report if specific categories | No | No | Yes | Choice (multiple):<br>- monitoring of policy adherence;<br>- monitoring of third-party service providers;<br>- monitoring and |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | that require further granularity are reported in data field 4.2.<br><br>**2(a) Insufficient or failure of monitoring and control:**<br>(a) monitoring of policy adherence;<br>(b) monitoring of third-party service providers;<br>(c) monitoring and verification of remediation of vulnerabilities;<br>(d) identity and access management;<br>(e) encryption and cryptography;<br>(f) logging.<br><br>**2(c) ICT risk management process failure:**<br>(a) failure in specifying accurate risk tolerance levels;<br>(b) insufficient vulnerability and threat assessments;<br>(c) inadequate risk treatment measures;<br>(d) poor management of residual ICT risks.<br><br>**2(d) Insufficient or failure of ICT operations and ICT security operations:**<br>(a) vulnerability and patch management;<br>(b) change management;<br>(c) capacity and performance management;<br>(d) ICT asset management and information classification;<br>(e) backup and restore;<br>(f) error handling. | | | | verification of remediation of vulnerabilities;<br>- identity and access management;<br>- encryption and cryptography;<br>- logging;<br>- failure in specifying accurate risk tolerance levels;<br>- insufficient vulnerability and threat assessments;<br>- inadequate risk treatment measures;<br>- poor management of residual ICT risks;<br>- vulnerability and patch management;<br>- change management;<br>- capacity and performance |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | **2(g) Inadequate ICT Systems acquisition, development, and maintenance:**<br>(a) inadequate ICT Systems acquisition, development, and maintenance;<br>(b) insufficient software testing or failure of software testing. | | | | management;<br>- ICT asset management and information classification;<br>- backup and restore;<br>- error handling;<br>- inadequate ICT systems acquisition, development, and maintenance;<br>- insufficient or failure of software testing |
| 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 | Description of the sequence of events that led to the major ICT-related incident and description of how the major ICT-related | No | No | Yes | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| about the root causes of the incident | 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.<br><br>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. | | | | |
| 4.6.<br><br>Incident resolution | Additional information regarding the actions/measures taken/planned to permanently resolve the major ICT-related incident and to prevent that incident from happening again.<br><br>Lessons learnt from the major ICT-related incident.<br><br>The description shall contain the following points:<br><br>1. **Resolution actions description**<br><br>(a) actions taken to permanently resolve the major ICT-related incident (excluding any temporary actions); | No | No | Yes | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| | (b) for each action taken, indicate the potential involvement of a third-party provider and of the financial entity;<br>(c) indicate whether procedures have been adapted following the major ICT-related incident;<br>(d) indicate any additional controls that were put in place or that are planned with related implementation timeline.<br><br>Potential issues identified regarding the robustness of the IT systems impacted /or in terms of the procedures or controls in place, if applicable.<br><br>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.<br><br>**2. Lessons learnt**<br><br>Financial entities shall describe findings from the post-incident review. | | | | |
| 4.7. Date and time when the | Date and time when the incident root cause was addressed. | No | No | Yes | ISO 8601 standard UTC (YYYY-MM-DD |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| incident root cause was addressed | | | | | Thh: mm:ss) |
| 4.8. Date and time when the incident was resolved | Date and time when the incident was resolved. | No | No | Yes | ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss) |
| 4.9. Information if the permanent resolution date of the incidents differs from the initially planned implementation date | Descriptions of the reason 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 whether the major ICT-related incident poses a risk | No | No | Yes, if the | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| Assessment of risk to critical functions for resolution purposes | 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[3].<br><br>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[4] and mapped to the specific entity in Template Z07.02. | | | incident poses a risk to critical functions of financial entities under Article 2(1), point 35, of Directive 2014/59/EU | |
| 4.11. Information relevant for resolution | Description of whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group. | No | No | Yes, if the incident has affected | Alphanumeric |

[3] 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).

[4] 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).

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| authorities | Entities as referred to in Article1(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.<br><br>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.<br><br>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. | | | the resolvability of the entity or the group. | |
| 4.12. Materiality threshold for the classification criterion | 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 2024/1772. | No | No | Yes | Alphanumeric |

| Data field | Description | Mandatory for initial notification | Mandatory for intermediate report | Mandatory for final report | Field type |
|---|---|---|---|---|---|
| 'Economic impact' | | | | | |
| 4.13. Amount of gross direct and indirect costs and losses | Total amount of gross direct and indirect costs and losses incurred by the financial entity stemming from the major ICT-related incident, including:<br>(a) the amount of expropriated funds or financial assets for which the financial entity is liable;<br>(b) the amount of replacement or relocation costs of software, hardware or infrastructure;<br>(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;<br>(d) the amount of fees due to non-compliance with contractual obligations;<br>(e) the amount of customer redress and compensation costs;<br>(f) the amount of losses due to forgone revenues;<br>(g) the amount of costs associated with internal and external communication;<br>(h) the amount of advisory costs, including costs associated with legal counselling, forensic and remediation services;<br>(i) the amount other costs and losses, including:<br>(i) direct charges, including impairments and settlement charges, to the profit and loss account and write-downs due 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 |
|---|---|---|---|---|---|
| | (ii) provisions or reserves accounted for in the profit and loss account against probable losses related to the major ICT-related incident;<br>(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;<br>(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;<br>(v) timing losses, where they span more than one financial accounting year and give rise to legal risk.<br><br>Financial entities shall take into account in their assessment Article 7(1) and (2) of Delegated Regulation 2024/1772. Financial entities shall not include in this figure financial recoveries of any type.<br><br>Financial entities shall report the monetary amount as a positive | | | | |

| **Data field** | **Description** | **Mandatory for initial notification** | **Mandatory for intermediate report** | **Mandatory for final report** | **Field type** |
|---|---|---|---|---|---|
| | value.<br><br>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.<br><br>Financial entities shall report the data point in units using a minimum precision equivalent to thousands of units. | | | | |
| 4.14. Amount of financial recoveries | Total amount of financial recoveries.<br>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.<br>Financial entities shall report the monetary amount as a positive value.<br><br>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. | No | No | Yes | Monetary<br><br>Financial entities shall report the data point in units using a minimum precision equivalent to thousands of units |
| 4.15. Information | Information on whether more than one non-major ICT-related incident have been recurring and are together considered to be a | No | No | Yes, if the major | Alphanumeric |

| **Data field** | **Description** | **Mandatory for initial notification** | **Mandatory for intermediate report** | **Mandatory for final report** | **Field type** |
|---|---|---|---|---|---|
| on whether the non-major incidents have been recurring | major incident within the meaning of Article 8(2) of Delegated Regulation 2024/1772.<br><br>Financial entities shall indicate whether the non-major ICT-related incidents have been recurring and are together considered as one major ICT-related incident.<br><br>Financial entities shall also indicate the number of occurrences of these non-major ICT-related incidents. | | | incident comprises more than one non-major recurring incidents. | |
| 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) |

## ANNEX III
## Templates for notification of significant cyber threats

| Number of field | Data field | |
|---|---|---|
| 1 | Name of the entity submitting the notification | |
| 2 | Identification code of the entity submitting the notification | |
| 3 | Type of the financial entity submitting the notification | |
| 4 | Name of the financial entity | |
| 5 | LEI code of the financial entity | |
| 6 | Primary contact person name | |
| 7 | Primary contact person email | |
| 8 | Primary contact person telephone | |
| 9 | Second contact person name | |
| 10 | Second contact person email | |
| 11 | Second contact person telephone | |
| 12 | Date and time of detection of the cyber threat | |

| Number of field | Data field | |
|---|---|---|
| 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 | |

## ANNEX IV
## Data glossary and instructions for notification of significant cyber threats

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| 1. Name of the entity submitting the notification | Full legal name of the entity submitting the notification. | Yes | Alphanumeric |
| 2. Identification code of the entity submitting the notification | Identification code of the entity submitting the notification.<br>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.<br>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. | 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. | Choice (multiselect):<br>- credit institution;<br>- payment institution;<br>- exempted payment institution;<br>- account information service provider; |

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| | | | - electronic money institution;<br>- exempted electronic money institution;<br>- investment firm;<br>- crypto-asset service provider;<br>- issuer of asset-referenced tokens;<br>- central securities depository;<br>- central counterparty;<br>- trading venue;<br>- trade repository;<br>- manager of alternative investment fund;<br>- management company;<br>- data reporting service provider;<br>- insurance and reinsurance undertaking;<br>- insurance intermediary, |

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| | | | reinsurance intermediary and ancillary insurance intermediary;<br>- institution for occupational retirement provision;<br>- credit rating agency;<br>- administrator of critical benchmarks;<br>- crowdfunding service provider;<br>- 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 and surname of the primary contact person of the financial entity. | Yes | Alphanumeric |

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| name | | | |
| 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 | The telephone number of the primary contact person that can be used by the competent authority for follow-up communication.<br>The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX) | Yes | Alphanumeric |
| 9. Second contact person name | Name and surname of the second contact person of the financial entity or an entity submitting the notification on behalf of the financial entity, where available. | Yes, if name and surname of the second contact person of the financial entity or an entity submitting the notification for the financial entity is available. | Alphanumeric |
| 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 |

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| 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.<br><br>The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX). | 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.<br>Financial entities shall provide:<br>(a) a high-level overview of the most relevant aspects of the significant cyber threat;<br>(b) the related risks arising from it, including potential vulnerabilities of the systems of the financial entity that can be exploited;<br>(c) information about the probability of materialisation of the significant cyber threat; and<br>(d) information about the source of information about the cyber threat. | Yes | Alphanumeric |
| 14. Information | Information about the potential impact of the cyber threat on the financial entity, its clients or financial counterparts if the cyber threat | Yes | Alphanumeric |

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| about potential impact | has materialised | | |
| 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):<br>- clients, financial counterparts and transactions affected;<br>- reputational impact;<br>- duration and service downtime;<br>- geographical spread;<br>- data losses;<br>- critical services affected;<br>- economic impact. |
| 16. Status of the cyber threat | Information about the status of the cyber threat for the financial entity and whether there have been any changes in the threat activity.<br><br>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. | Yes | Choice:<br>- active<br>- inactive |
| 17. Actions taken to prevent | High-level information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if | Yes | Alphanumeric |

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| materialisation | applicable. | | |
| 18. Notification to other stakeholders | Information about notification of the cyber threat to other financial entities or authorities. | Yes, if other financial entities or authorities have been informed about the cyber threat). | Alphanumeric |
| 19. Indicators of compromise | Information related to the significant threat that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.<br><br>The IoC provided by the financial entity may include, but is not to be limited to, the following categories of data:<br>(a) IP addresses;<br>(b) URL addresses;<br>(c) domains;<br>(d) file hashes;<br>(e) malware data (malware name, file names and their locations, specific registry keys associated with malware activity);<br>(f) network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic);<br>(g) e-mail message data (sender, recipient, subject, header, content);<br>(h) DNS requests and registry configurations;<br>(i) user account activities (logins, privileged user account activity, privilege escalation); | Yes, if information about indicators of compromise connected with the cyber threat are available.) | Alphanumeric |

| Data field | Description | Mandatory field | Field type |
|---|---|---|---|
| | (j) database traffic (read/write), requests to the same file.<br>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. | | |
| 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 |