ANNEX II

Data glossary and instructions for the reporting of major incidents

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

JOINT COMMITTEE OF THE EUROPEAN
SUPERVISORY AUTHORITIES