Commission de Surveillance du Secteur Financier

Additional CSSF Operational Instructions on DORA Major ICT-Related Incident Reporting

ID	Last update	Description	Template field(s)	Observations	Guidance
1	*28/09/2026*	Description of the ICT-related incident	2.4	Descriptions provided in Field 2.4 are frequently too high-level or generic, risking a lack of necessary operational and technical detail	To ensure consistency and thoroughness in line with the ITS[1] requirements, it is expected that the field contains: 1. Overview elements: A high-level overview of possible causes, immediate impacts, systems affected, and the status of resolution of the incident. 2. Impacted third-party/entity details: Where known or reasonably expected, whether the incident impacts third-party providers or other financial entities 3. Evolution in subsequent reports: Updates reflecting ongoing understanding, any relevant information not captured elsewhere (such as the internal severity assessment: e.g. very low, low, medium, high, very high).
2	*28/09/2026*	Information required upon the reclassification of a major ICT-related incident as non-major	2.10	The necessary justification is omitted when an incident is reclassified from major to non-major	It is expected that the field contains a description of 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 whenever a reclassification occurs.

[1] *Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat*

Commission de Surveillance du Secteur Financier

ID	Last update	Description	Template field(s)	Observations	Guidance
3	*28/09/2026*	Guidance on selecting multiple incident types for classification	3.23	Only a single incident type is selected instead of selecting all applicable choices when multiple categories apply	It is expected that this multiple-choice field contains all applicable categories. Specifically, if the incident is payment-related, it is expected that "Payment-related" is selected in addition to any other applicable incident type (such as "System failure"). In a similar manner, it is expected that "External event" is also selected if the incident originates from a third-party or another financial entity, alongside other applicable categories.
4	*28/09/2026*	Information about affected infrastructure components supporting business processes	3.29	Descriptions provided in Field 3.29 are frequently too high-level or generic, or incomplete, risking a lack of necessary operational and technical detail	To ensure consistency and thoroughness in line with the ITS requirements, it is expected that the field specifies the infrastructure components impacted such as: a. Hardware aspects: servers, computers, data centres, switches, routers, hubs. Software aspects: operating systems, applications, databases, security tools, network components.
5	*28/09/2026*	Reporting temporary actions and measures taken or planned to recover from the incident	3.34	The field is occasionally submitted empty without indicating a reason	It is expected that the field contains a description of the actions taken or planned to recover from the incident. These actions may not necessarily be performed by the financial entity directly. In case no actions or measures have been taken, it is expected that the reason is documented in this field.

Commission de Surveillance
du Secteur Financier

ID	Last update	Description	Template field(s)	Observations	Guidance
6	*28/09/2026*	Consistency in reporting root causes and categories across related incident data fields	2.8, 3.23, 4.1, 4.2	Incoherent reporting between data fields 2.8, 3.23, 4.1, 4.2, particularly when incidents originate from third parties	It is expected that the choices proposed in Fields 4.1 and 4.2 are aligned with information provided in related fields including Field 2.8 regarding whether the incident originated from a third-party and Field 3.23 regarding the incident type.
7	*28/09/2026*	Reporting incident resolution measures and lessons learnt	4.6	The content provided in this field is generally very high-level and the field is occasionally left incomplete	It is expected that the field is not limited to high-level resolution and contains at least: 1. Resolution actions: Actions taken to permanently resolve the major ICT-related incident; indication of the potential involvement of a third-party provider and of the financial entity for each action; an indication of whether procedures have been adapted; and additional controls put in place or planned with a related implementation timeline. 2. Lessons learnt: Findings from the post-incident review and actions planned for remediation. These actions are expected to contain measures that will prevent the occurrence of similar incidents in the future or limit the impact should a similar incident occur. For actions not yet completed, an action plan including the Action Unique Identifier, Description of the Action, Responsible Owner, Current Status, and Deadline for Completion would enable a proper follow-up.