16 September 2026

DORA Incident Reporting – Operational Instructions

PURPOSE:

This document provides operational instructions intended to support competent authorities in their supervisory engagement with financial entities regarding the reporting of information on the major ICT-related incidents under Regulation (EU) 2022/2554 (DORA), to enhance data quality and promote greater consistency across jurisdictions.

The instructions are provided on 'best efforts' basis by the ESAs staff and therefore they do not represent any legal interpretation, nor do they represent official stance of the ESAs. These instructions have been agreed with the relevant competent authorities. They will be updated regularly, based on the experience of the ESAs and of the competent authorities with the DORA major ICT-related incident reporting.

DEFINITIONS:

- **DORA** – Regulation (EU) 2022/2554 on digital operational resilience for the financial sector
- **ITS 2025/302** (Commission Implementing Regulation (EU) 2025/302) – laying down implementing technical standards for the application of DORA with regard to the standard forms, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat (*the template fields in the following tables are the ones defined in this ITS*)
- **RTS 2025/301** (Commission Delegated Regulation (EU) 2025/301) – supplementing DORA with regard to regulatory technical standards. These standards define specifying the content and timelines limits for the initial notification of major ICT-related incidents, as well as the requirements and for intermediate and final reports on, major ICT-related such incidents. The RTS also covers, and the content of the voluntary notification for significant cyber threats
- **RTS 2024/1772** (Commission Delegated Regulation (EU) 2024/1772) – supplementing DORA regarding 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
- **DORA ICT-related incidents reporting process**: financial entities falling within the scope of DORA must, following the detection of an ICT-related incident classified as major, report information on the incident to their competent authority using the reporting channels, templates and format established at the national level. Upon receipt of such reports, competent authorities notify the ESAs by submitting the relevant information using ESAs pre-defined templates in English.

ID	Last update	Description	Template field(s)	Observations	Guidance
1	*16/09/2026*	Language of the DORA incident reporting templates and the information reported therein by competent authorities	General	ESAs receiving incident reports using a template with headers/elements and values translated into local languages	The entities in charge of reporting their incident notifications may consider that the competent authorities are expected to use the pre-defined templates in English for the purpose of notifying the ESAs (i.e. headers/elements and values provided in close ended questions are based on the terminology set out in the English language version of the ITS 2025/302). Free text fields may still be provided in the applicable national language.
2	*16/09/2026*	Monetary fields	General	Inconsistent reporting of monetary fields	For the fields that are identifying with as "Monetary" as field type, ITS 2025/302 requires that "*The data point shall be reported in units using a minimum precision equivalent to thousands of units*". To ensure common reporting practices, all fields designated as monetary in nature—namely Field 3.11, Field 4.13 and Field 4.14—are reported in **thousands of units**, further precision can be added after the comma for instance: - EUR 2 500 should be reported as 3 *(or 2,5)* - EUR 2 500 382 should be reported as 2 500 *(or 2500,382)*. In addition, all monetary amounts reported in these fields shall be expressed in the same currency as that specified in Field 1.15.
3	*16/09/2026*	Provision of information in the free-text (alphanumeric) fields	General	Inclusion of 'Not applicable', 'nothing', etc in the free-text fields.	Free-text (alphanumeric) fields, whether mandatory or conditionally mandatory should contain only information relevant to the purpose of the field. Where a field is not mandatory and not applicable, it is recommended to leave it blank. Where the ITS 2025/302 specifies or suggests the type of input to be provided in a free-text field, reporting entities are encouraged, where feasible, to follow the indicated wording and structure (e.g. as in Field 3.27) to promote consistency.
4	*16/09/2026*	Reporting of incident's final report	General	Missing final reports on notified incidents	RTS 2025/301 requires that the final report must be submitted "*no later than one month after either the submission of the intermediate report, or, where applicable, after the latest updated intermediate report*". Accordingly, after the submission of the initial notification and the first intermediate report, it is expected to receive at least one intermediate report per month updating the incident until the final report is produced and submitted.
5	*16/09/2026*	Reporting of correction reports	General	Wrong correction report	To ensure that the latest version contains always the most up-to-date and accurate information, when corrections are needed, it is expected that: - the correction is reported as a new version of the latest report submitted (i.e. if the last version was an intermediate report, submit a corrected version of the intermediate report).

ID	Last update	Description	Template field(s)	Observations	Guidance
					- the file that includes the correction should, in addition to the corrected information, contain all the information from the latest update on the major incident.
6	*16/09/2026*	Unique identification of an incident	1.3a, 1.3b, 2.1	Fields 1.3a/1.3b or 2.1 reported inconsistently throughout the life-cycle of an incident	- It is important that values reported in **Fields 1.3a**/**1.3b** and **Field 2.1** remain **UNCHANGED** from the submission of the initial notification through to the final report. These fields are used to uniquely identify incidents and amending any of these fields during the reporting life-cycle, might trigger wrong double counting of an incident.
7	*16/09/2026*	Inclusion of 'critical service affected' criterium in reporting of classification criteria.	2.5	Different practices in including or not 'critical service affected' as a criterium for triggering the major incident reporting.	Following Article (8)(1) of the RTS 2024/1772 an incident would be considered major where it has affected critical services, as referred to in Article 6, and where at least one of the additional conditions set out in that provision is met. Accordingly, the criterion relating to affected critical services must always be fulfilled, in addition to at least one other applicable criterion. Nevertheless, to ensure consistency in reporting, it is expected that all reports identify "critical services affected" explicitly among the criteria reported in field 2.5.
8	*16/09/2026*	Exclusion of Home Country as geographical spread	2.6	The home country of the affected financial entity has been included in the list of "geographical spread" countries.	As specified in the RTS 2024/1772 (Article 4), the "*geographical spread*" refers to the assessment of the major incident's impact across other Member States. Accordingly, it is expected that the country of the affected financial entity is not included in this field.

<table>
<tr><th>ID</th><th>Last update</th><th>Description</th><th>Template field(s)</th><th>Observations</th><th>Guidance</th></tr>
<tr><td>9</td><td>16/09/2026</td><td>Standardised reporting of information on TPP or other financial entity origin</td><td>2.8</td><td>Difficulty in reporting and processing and analysing Field 2.8</td><td>Field 2.8 indicates whether the incident originates from a third-party provider (TPP) or from another financial entity. The following information is required: the name of the relevant TPP or other financial entity, its identification code, and the type of identification code provided (e.g. LEI or EUID) in an open-text alphanumeric field.

To ensure consistency, it is recommended that, when it applies, Field 2.8 is reported in a standardised format where all elements included are separated by a semicolon (“;”) and reported in the specific order.

<table>
<tr><th>Sub-field</th><th>Sub-field type</th></tr>
<tr><td>1. Full legal name of the TPP/other financial entity</td><td>Alphanumeric</td></tr>
<tr><td>2. Identification code of the TPP/other financial entity, to be reported as either LEI or EUID</td><td>Alphanumeric</td></tr>
<tr><td>3. Identification of the type of code provided under (3)</td><td>Choice: LEI or EUID</td></tr>
<tr><td>4. Any additional information considered relevant</td><td>Alphanumeric</td></tr>
</table>
.
Examples:
- for a major incident that originates from a TPP or another financial entity:
PROVIDER REGISTERED LEGAL NAME;[LEI CODE];LEI; ”public statement issued by provider on xxx.”
- for a major incident that does not originate from a TPP or another financial entity: leave blank.</td></tr>
<tr><td>10</td><td>16/09/2026</td><td>Condition for reporting Field 3.17 “Information on whether the numbers for duration and service downtime are actual or estimates”.</td><td>3.17</td><td>Field 3.17 is defined in the ITS 2025/302 as Mandatory for intermediate and final reports “if ‘Duration and service downtime’ criterion met”</td><td>Field 3.17 indicates whether the values reported in Field 3.15 (Duration) and Field 3.16 (Service downtime) are actual or estimates. Since reporting of Field 3.15 is mandatory for both intermediate and final reports, it is expected that Field 3.17 is also completed for both intermediate and final reports and not only when the “duration and service downtime” is reported as a criterion in Field 2.5. This ensures correct interpretation of the reported duration.</td></tr>
<tr><td>11</td><td>16/09/2026</td><td>Typo concerning “Threats and techniques</td><td>3.25</td><td>Different wordings in the description vs the field type list</td><td>The ITS 2025/302 provides two contrary wordings for one of the predefined options in Field 3.25:
- Description:“(f) data exfiltration and manipulation, excluding identity theft;”
- Field Type list:“– Data exfiltration and manipulation, including identity theft”</td></tr>
</table>

ID	Last update	Description	Template field(s)	Observations	Guidance
		used by the threat actor"		for one of the predefined options in Field 3.25	It is expected that the wording provided in the **Description**, i.e. "*data exfiltration and manipulation, **excluding** identity theft*" is taken as reference when reporting Field 3.25. (n.b. there is a separate option for reporting "identity theft" technique).
12	*16/09/2026*	Information for resolution authorities	4.10	For some reports, Field 4.10 and Field 4.11 are filled when they do not apply (e.g. "none", "not applicable", etc)	It is expected that Field 4.10 is completed only when it has been determined that "*the incident poses a risk to critical functions of financial entities as defined in Article 2(1), point 35, of Directive 2014/59/EU*" (as defined in the ITS 2025/302). If the assessment concludes that the major incident did not pose such a risk, or if the information is not applicable to the affected financial entity, it is expected that this field is left empty, in line with the recommendation provided under Topic #3.
13	*16/09/2026*	Information for resolution authorities	4.11	Field 4.10 and Field 4.11 are filled when they do not apply (e.g. "none", "not applicable", etc)	It is expected that Field 4.11 is completed only when it has been determined that "*the incident has affected the resolvability of the entity or the group*". If the assessment concludes that the major incident has not affected resolvability, or if the information is not applicable to the affected financial entity, it is expected that this field is left empty, in line with the recommendation provided under Topic #3.
14	*16/09/2026*	Condition for mandatory reporting of Field 4.12 *"Materiality threshold for the classification criterion 'Economic impact'"*	4.12; 2.5	The ITS 2025/302 specifies that Field 4.12 is mandatory in final reports, while the data field name is "*Materiality threshold for the classification criterion 'Economical Impact'*"	ITS 2025/302 requires financial entities to report in Field 4.12 "*Detailed information about thresholds eventually reached by the major ICT-related incident in relation to the criterion 'Economic impact' referred to in Articles 7 and 14 of the Delegated Regulation (EU) 2024/1772"*. Therefore, it is expected that information in Field 4.12[1] is always reported in the final reports of incidents where "*Economic impact*" has been identified as a classification criterion in Field 2.5. At the same time, when information is available, entities can also report the "*Economic impact*" in Field 4.12, including for incidents which have been classified as major due to other criteria (reported in Field 2.5).

[1] When reporting the information on thresholds eventually reached by the major ICT-related incident in relation to the criterion 'Economic impact' (Field 4.12), financial entities can also consider the specific Q&A on staff costs calculation: 2025_7439 Staff costs (EBA).