Brussels, 1 March 2024

FINAL

EACB comments on

ESAs' Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents

and

Draft Implementing Technical Standards On the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat

Q1: Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

We appreciate the effort made by the ESAs in recognising the dual need, both from Competent Authorities (CAs) to promptly receive information for potential actions and from financial entities (FEs) to allocate their internal resources adequately and have sufficient time to report major ICT-related incidents. However, we believe that some adjustments to the reporting timelines are necessary.

In particular, we suggest the following changes for Art. 6, paragraph 1, letters a), b), and c) of the draft Regulatory Technical Standard (RTS):

For letter a), **we propose that if the deadline for submitting an initial notification falls on a weekend day or a bank holiday, the reporting may be submitted the next working day**, as it is the case for the intermediate and final reports in the draft RTS (see Art. 6.2). Without this possibility, the FE must maintain round-the-clock staffing with the ability to classify incidents, placing a significant burden. For example, if the major incident is triggered, detected, and handled by an ICT Third Party Provider (TPP), the FE may only receive information during the next working day's normal hours, provided there is no crisis situation. In some cases, more time may be required for classification than 24 hours after detecting the incident, especially if it is recognised after 24 hours that the incident is major. Even then, a report should be considered duly submitted if plausible reasons for the delay are provided, which can be submitted in data field 2.16.
It goes without saying that for the sake of coherence the wording '*the initial report*' in letter a) should be replaced with '***initial notification***'.

For letter b) in combination with Art. 6.2, adequate time must be allowed for the submission of an intermediate report, particularly because the reporting data are extensive, involving various functions in the financial institution (FI) and possibly the incident-triggering ICT service provider (see also our answer to

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

question 3). Therefore, **the 72-hour period should commence from the initial notification, not from the classification of the incident as major, and it should refer to the next working day.** With regard to this last comment, one hour following regular starting time of the next working day is insufficient to obtain and fill in the information if weekends or public holidays fall within the 72-hour period.

For letter c), in cases where the resolution of the major incident takes nearly or more than 1 month, the time for sending the final report one day after the final resolution of the incident is much too short. Adequate time is required for coordinating information within the bank and, if applicable, with the incident-triggering ICT service provider. **We propose, analogous to NIS2, that the final report be submitted within one month of the incident being dealt with**.

Consequently Art. 6.1 c) should be as follows:

*The final report shall be submitted **within** ~~no later than~~ 1 month **of the financial entity handling the incident**. ~~from classification of the incident as major, unless the incident has not been resolved. In that latter case, the final report shall be submitted the day after the incident has been re- solved permanently.~~*

Q2: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The 16 content data fields required for an initial notification are quite extensive. We recommend aligning the granularity of the initial notification with the existing PSD2 reporting framework.

The level of detail required in the description is overly intricate for the initial notification. For example, concerning the information for fields 2.7-2.15, it may not be readily available at that stage. Including them in the initial notification could potentially negatively impact the reporting speed.

Additionally, the details related to an emergency plan (fields 2.14/2.15) might only be activated after the initial notification, and collecting such detailed information could sometimes cause delays or be unavailable. If known facts are available, they could be reported in the free-text field.

Overall, **we propose reserving the request for this information (fields 2.7-2.15) solely in the intermediate report**.

In the interest of an early and efficient reporting, we propose, if the major incident is triggered by an ICT TPP, the ICT TPP should be allowed to prepare the initial notification aggregated on behalf of the FEs concerned (see our answer to question 6).

Q3: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The current requirements for the intermediate report demand too many individual details with overly detailed descriptions, hindering the efficiency of reporting.

In our opinion, streamlining the selection fields and providing a more robust summarisation of information would enhance efficiency in reporting incidents. **We suggest focusing on concise, meaningful details regarding the cause and handling of the incident, as well as information to mitigate the risk of infection for other FIs and to inform institutions about new attack scenarios or vulnerabilities**.

It's crucial to consider that at the time of the intermediate report, the incident may still be in the processing stage, and therefore, much of the information may not be known yet. The abundance of information and the extensive descriptions required might pose challenges for the supervisory authority in analysis, and there's a risk that relevant reports for other FIs may be difficult to filter out.

If the incident is triggered and handled by an ICT TPP, the ICT TPP should be allowed to submit the intermediate report on behalf of the involved FEs and limit itself to the information within its knowledge, such as duration, causes, technical effects, and treatment (i.e., data fields 3.3 - 3.5, 3.17-3.23, 3.26-3.31, 3.36-3.41). The other data fields should either not be mandatory or be moved to the final report (see also our answer to question 6).

Q4: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

We have some concerns with regard to data fields 4.15-4.24. Providing a detailed breakdown of all costs and losses in the final report exceeds the scope of an efficient reporting system. Frequently, costs and losses are estimated at the time of the final report, and providing detailed breakdowns may give a false sense of accuracy. **The report should be limited to the total costs if the criterion 'Economic impact' has been met. If applicable, a multiple-choice field could be included to indicate the types of costs incurred. Alternatively, instead of reporting the detailed breakdown in the final incident report, it could be included in the annual report on costs and losses, if necessary**.

Regarding data field 4.10 (i.e., 'Information relevant for resolution authorities'), we propose marking it as 'not mandatory' since exemptions are provided by Directive 2014/59/EU establishing a framework for the recovery and resolution of credit institutions and investment firms (BRRD). Moreover, incidents of this magnitude (affecting the resolvability of the entity or the group) are exceptional. **We recommend incorporating this topic into data field 4.25 (i.e., 'Details related to economic impact') under the 'Instructions' column, if relevant**.

Q5: Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.

Given that the reporting of cyberthreats is voluntary, **mandatory data fields should be limited to a minimum, focusing on essential information such as details about the institution, a description including causes, and information on how to deal with the threat**. An uncomplicated reporting rule that demands minimal effort can enhance the willingness to report.

Q6: Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

ICT-related incidents may result from an incident triggered by an ICT service provider. In such cases, only the ICT service provider possesses the necessary information to determine the cause of the incident and can implement technical measures to address it.

While we acknowledge that under DORA, the FE is obligated to submit the report, this reporting can still be delegated. The reports should include all the relevant information for the CA to determine the significance of the serious ICT-related incident and assess the potential cross-border impact (DORA Art. 19 (1)). However**, the reporting process outlined in the draft RTS/ITS places a significant burden on ICT service providers and/or FEs, as reporting is allowed on a solo basis only. To address this issue, we propose modifying the procedure so that the initial notification and intermediate reports can be completed by the ICT TPP and submitted once to the national authority, accompanied by a list of affected FEs that have authorised the ICT TPP. The final report may be supplemented on a solo basis with specific information from each FE**.

This procedure facilitates swift and effective reporting of incident causes and handling 'at first hand'. It also aligns with DORA by requiring FEs to report specific information individually, although identical information only needs to be reported once. Simultaneously, this streamlined process aids financial supervisory authorities in quickly analysing and obtaining a comprehensive overview. Reporting the same incident multiple times per entity can cause the financial supervisory authority to overlook the fact that it is one and the same incident, or make it challenging to recognise.

For instance, let's consider an ICT TPP with a hundred clients delegating reporting to it. In the initial report, the ICT TPP would otherwise need to send 100 individual reports within 24 hours. Apart from general information about the institution, the details are identical. Given that each report takes an estimated 5 minutes, the service provider would spend over 8 hours on the report without providing the supervisory authority with any additional information. Alternatively, if each FE reports individually, these entities would need to be informed by the ICT TPP, establishing a 24/7 service to transmit information from the ICT service provider within the 24-hour period from the discovery of an initial notification. Smaller institutions may encounter significant organisational challenges in meeting this requirement.

Contact:

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Digitalisation and Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser for Digital Policies (chiara.delloro@eacb.coop)