European Association of CCP Clearing Houses

EACH Response – ESAs consultation on Draft RTS and ITS on major incident reporting under DORA

March 2024

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 18 Members from 14 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback to the consultation paper on Draft RTS and ITS on major incident reporting under DORA[1].

As an introductory comment, EACH would like to underline that the **timeline for the implementation of DORA** (which will apply from 17 January 2025) **appears to be extremely challenging**. EACH Members are calling for an **extension of such timeline** in order to ensure a smooth and **efficient implementation. We** would expect Authorities to provide comfort to the industry accordingly as well as some **prioritisation** of the aspects of DORA that should be implemented first.

Questions

Question 1 – Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

The reporting time limits for initial, intermediate and final reporting should be consistent with the time limits in NIS II[2]. NIS II, Article 23 (4) requires that significant incidents be reported without undue delay and in any event **within 24 hours of becoming aware of the significant incident**.

More specifically, EACH would like to put forward the following comments regarding **paragraph 1 of Art. 6** on time limits for the initial notification and intermediate report:

- Point (a) – We would like to **extend the 4-hour time limit** within which the **initial report** shall be submitted. Such timeframe would be too short in case there is an **extensive amount of data field** to be provided, and if the **root cause** of the major incident has to be identified. In addition, the deadlines for the various reports as per DORA are synchronized with NIS II, and if they are to be retained, the initial notification should in our opinion contain fewer fields.
- Point (b) – We agree with setting the timeframe within which the **intermediate report** shall be submitted **72 hours**, in line with NIS II.

[1] https://www.esma.europa.eu/sites/default/files/2023-12/JC_2023_70_-_CP_on_draft_RTS_and_ITS_on_major_incident_reporting_under_DORA.pdf
[2] https://eur-lex.europa.eu/eli/dir/2022/2555

We suggest **rewording Art. 6** as follows:

The time limits for the submission of the initial notification and the intermediate and final reports as referred to in Article 19(4)(a) to (c) of Regulation (EU)2022/2554 shall be as follows:

a) the initial report shall be submitted as early as possible ~~within 4 hours from the moment of classification of the incident as major~~, but no later than 24 hours from the time of detection of the incident.

*b) an intermediate report shall be submitted within 72 hours **from the detection of an incident** ~~classification of the incident as major~~, or when regular activities have been recovered and business is back to normal.*

*c) the final report shall be submitted no later than 1 month **from the submission of the initial report** ~~from the 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 resolved permanently.*

We also would like to point out that **point (f) of Art. 3** on the content of the initial notification, i.e. "Information about the source of the incident, *where available*" appears to be rather in contrast with the list of data fields provided in Annex I, as such data fields do not seem to foresee that information about the source of the incident shall be provided only *where available*. Additionally, we would like to kindly receive some **clarification** on whether the financial entity should nevertheless file the report **even though not all the necessary data may be available** within the established deadline.

Question 2 – 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.

We suggest that data **fields 2.8-2.10 as well as 2.15** be part of the data fields to be provided for the **intermediate report**, as it may be difficult to distinguish them within the timeframe of the initial report. **Data fields 2.8-2.10 concern potential impact on external parties**. In case of a major ICT related incident, the focus during the initial phase after discovery is and should be on the internal damage control and containment. It is not likely that the full impact on other entities and/or third-party providers is available at an early stage and premature information could be misleading. Therefore, it is prudent to **include this information in the intermediate report when a proper assessment has been made**.

We would like to underline that the **information to be provided by critical ICT TPPs under Article 3 is extensive**. Some information may not be shares with the ESAs by certain ICT TPPs due to themselves or their customers being subject to national laws with the purpose of protecting national security. Examples of information that is very sensitive and therefore may be not be shared include, for instance, the following:

- control measures to protect sensitive data;
- access controls;
- encryption practices

- incident response plans;
- information about the exact location of the data centres and ICT production centres, including a list of all relevant premises and facilities of the critical ICT third-party service provider;
- information about the overall response and recovery framework of the critical ICT third-party service provider, including business continuity plans and related arrangements and procedures;
- response and recovery plans and related arrangements and procedures;
- backup policies arrangements and procedures.

A mechanism on how to deal with such conflicts of laws/exemption needs to be established.

Question 3 – 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 aim of the intermediate report should be to provide **valuable information to other financial entities and third-party providers**, especially information on cyber incidents.

As mentioned in our answer to question 2, data **fields 2.8-2.10 and 2.15** should be **part of the intermediate report**.

We also suggest that:

- **Fields 3.6-3.12 should be moved to the final report**. Data fields 3.6-3.12 concern impact on clients, counterparties and transactions. In case of a major ICT related incident, the focus during the initial phase after discovery is and should be on internal damage control and containment. Due to the volume and complexity of trading and clearing, it may take more time to evaluate and report the impact. An early assessment might not be as detailed or complete as required and therefore not providing much value.
- **Field 3.40** includes details on user levels, which should be **removed from the list for privacy reasons.**
- As there **might not be a final list of impacted members, entities, transactions identified**, there should be best effort to provide this data with a possibility to adjust this information in the final report.

We are of the opinion that it would be sufficient for the reporting to provide the information whether *critical services were affected* or which *other two criteria* were met in order to classify the incident as major. All other details on the classification require individual documentation, but we consider that there is no need to include this in the reporting.

Question 4 – 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.

EACH would like to underline that the list of data fields to be provided for the final report appears **excessively detailed**. For instance, we believe that **fields 4.14-4.25 should be removed**. Data fields 4.14 - 4.25 contain too much detail on financial impact and should not be reported. Financial impact details should be reviewed and subtracted to more core/mandatory information (all categories compile to relatively large amount of details). **Reporting on gross costs and losses as in 4.14 is, in our opinion, more relevant**.

The guideline on the estimation of aggregated annual costs and losses caused by major ICT-related incident requires enough data in this respect. Details on aggregated gross and net costs and losses in an accounting year and additionally annual gross and net figures for each major ICT-related incident are included.

Question 5 – 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.

EACH Members would like to underline the following issues:

- The **definitions of significant cyber threat and cyber incident seem unclear**. From an EACH point of view, cyber threat would indicate a potential danger or malicious activity, while a cyber incident is an actual occurrence or event that compromises the security of information assets.
- The **information requested by the template fields seems to be excessive** and does not seem to allow an option for sharing a cyber threat anonymously, which is possible in CIISI-EU forum.
- It is **not clear where the reports would be stored** in terms of confidentiality.
- We consider that the **ESAs should make use of already known frameworks** (i.e. NIST SP 800-150 or CISA) for sharing and reporting cyber threats, which most of the companies already follow.
- **Annex III datapoint 18 "Actions taken to prevent materialization" would involve potentially disclosure of sensitive, infrastructure-related information** of the financial entity, which might prevent a financial entity from voluntarily reporting on such events. We suggest this data point is not requested as part of this notification template.

Question 6 – Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

The requirements for initial, intermediate and final reporting are too extensive and detailed. We would appreciate a simpler, more efficient approach that does reduce the burden of reporting.

Specifically, in case of ICT-related major incidents that are no cyber incidents, the collected data may be too specific, as the systems in use are also very different. Collecting and sharing information as much as possible only makes sense in the event of cyber-attacks. Financial

entities and ICT TPPs can still take countermeasures based on the shared information if necessary.

The requirements mentioned in Article 3 to 5 are more general. Reporting should not be misused to control whether financial entities have determined all the criteria for classifying an ICT-related major incident. This could be verified by the competent authority during an on-site audit.