European Association of CCP Clearing Houses

EACH Response to the ESAs' consultation paper on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats

September 2023

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 19 members from 15 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 Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554[1].

Questions

Q1. Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.

EACH Members are **concerned about the proportionality of the criteria proposed by the ESAs** regarding the classification of major incidents. We are in particular of the opinion that this approach will result in a potentially considerable amount of non-significant incidents which may be reported, leading to extensive over-reporting. This may also lead to the risk of firms being disincentivised from raising incidents.

We therefore **encourage the ESAs to share publicly the results of the incident reporting assessment** mentioned in paragraph 11[2] to ensure a proportionate approach in the final standards.

Q2. Do you agree with the specification and materiality thresholds of the criterion 'Clients, financial counterparts and transactions affected', as proposed in Articles 1 and 9 of the draft RTS? If not, please provide your reasoning and suggested changes.

Regarding this criterion, EACH would like to put forward the following comments:

- In **Article 9(1a)**, the **10% threshold of affected clients appears very low**, as any incident on a widely used service would affect more than 10% of clients. The percentage of clients could be misleading and could trigger a major incident where there is none. For example, it may occur that an incident impacts 10% of clients, but

[1] https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTS_on_classification_of_ICT_incidents.pdf

[2] *Consequently, CAs and ESAs will be carrying out additional testing based on data from real incident reports and will further assess if the proposed classification approach and materiality thresholds cover the respective sector-specific requirements.*

those 10% count for a small volume, whereas one large client could account for over 50% of a volume for a particular product or service;

- In **Article 9(1e)**, the **€15m threshold of affected transactions** is, in our view, **extremely low for many types of entities and transactions**. An incident is triggered if, for instance, one repo could not be traded or one swap could not be reported to a trade repository (TR);
- In **Article 9(1f)**, it appears **arduous to assess any identified impact** in accordance with Article 1(3). We suggest leaving it to the discretion of individual firms to determine adequate thresholds for number of clients and transactions.

Q3. Do you agree with the specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes.

Concerning the criteria mentioned in this question, we would like underline the following:

- We consider that the **threshold for reputational impact** defined in **Article 2 is very low**, and encourage a proportionality as well as risk-based approach. Additionally, reputational impact is a criterion which can only be properly assessed from a longer time-perspective. The reputational impact may not manifest itself (fully) while an incident is managed or within the timeframes of incident reporting;
- Regarding **'Duration and service downtime', Article 3(1)** states that financial entities shall measure the duration of an incident from the moment the incident occurs until the moment the incident is resolved, but there is no definition or explanation when an incident shall be considered as resolved. Also, we suggest that a **business continuity measure or workaround could be applied** and shall fulfil the criteria for resolving an incident, but this is not clearly defined in the proposed RTS;
- The **duration of incident threshold of 24 hours appears too short**. This is particularly important if during the duration of the incident a root-cause analysis has to be performed. This typically takes longer than 24 hours. We propose that within the context of the definitions provided in **Article 3 (Classification criterion 'Duration and service downtime')**, **only service downtime is used as a materiality threshold**, because "resolving" the incident is more of an administrative task. Alternatively, the threshold should be set sufficiently long (7 days) to ensure that all incident management processes to "resolve" the incident are of a good quality (particularly important is here the root-cause analysis process). In developing guidance, **already existing NIS[3] incident reporting thresholds and upcoming NIS 2[4] requirements should be taken into account** to ensure convergence.
- In **Article 7 (Classification criterion 'Economic impact')**, the proposed RTS list criteria for determining economic impact. This appears **too detailed and complex** and when the real incidents occur it would be **operationally onerous and burdensome,**

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1694437015969

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1694434979722

if not impossible to calculate the economic impact for the purpose of determining reportability. We therefore respectfully recommend that this criterion is not used for determination whether the incident is major / reportable, but as a post-incident review activity.

- Concerning the **criterion 'Geographical spread' defined in Article 4**, we wonder why the requirements of assessing the impact of the incident in the territories *of at least two Member States* has been introduced, considering that the Level 1 text in Article 18(1c)[5] specifies that the impact of ICT-related incidents shall be assessed when the geographical spread with regard to the areas affected by the **ICT-related incident affects *more than two Member States.*** The threshold of minimum two Member States is particularly low and for any financial entity with scale it is challenging to find an incident that would not affect *at least* two Member States (it is indeed more a function of the size of the service rather than of the materiality of the incident).
- **Article 11(b) (criterion 'Duration and service downtime')** concerns ICT services supporting critical functions, not the actual critical function itself, and we consider that it should only be incorporated if it affects the critical function. If the critical function can continue to operate, we believe it should not reach the threshold.

Q4. Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes.

Article 5(1) refers to a situation in which an incident has rendered the data on demand by the financial entity, its clients or its counterparts inaccessible or unusable. This is likely to affect any incident. We suggest that this criterion **should be linked to duration and not be self-standing** (e.g. inaccessibility of data for one second – or less – would qualify in this context), as it depends on how crucial the data is (market data vs non-financial data, or time sensitive vs non-time sensitive data). It should be clear that only *"data losses"* as defined in Article 5 of the proposed RTS with significant impact will count in as a primary criterion for qualifying an incident as major – thus triggering a reporting obligation, provided that additional criteria are also fulfilled.

Q5. Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes.

The definition in **Article 6** should **not, in our opinion, add in the requirements for financial entities** to assess whether the incident has affected services or activities *that require authorisation*, as this does not represent a function of criticality and therefore unduly expands the Level 1 text. We consider that, if such services are not critical, they should not be included in the criterion.

[5] *2. Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria: […] c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;*

Q6. Do you agree with capturing recurring incidents with same apparent root cause, similar nature and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes. Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents).

We **respectfully disagree with Article 16(1)** and could not identify any mandate to define specific additional requirements and standards for recurring incidents.

Article 17 (2) of DORA states that financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, *to ensure that root causes are identified, documented and addressed* ***in order to prevent the occurrence of such incidents***. The conclusion is therefore the following: if a financial entity is compliant with DORA Article 17(2) there should be ***no*** **or** ***close to zero*** **"recurring incidents"**. As a consequence, **we suggest removing Article 16**.

Q7. Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.

We would appreciate seeing **alignment with DORA and the relevant cybersecurity rules** in defining a cyber threat.

With respect to the approach for classification of significant cyber threats, proposed in **Article 17** and further explained in section 3.2.2. of the proposed RTS, we recommend the **deletion of impact on *"other financial entities"***, as the cyber threat spread and impact on critical or important functions of other financial entities are not transparent for trading venues and would involve a high degree of speculation. Additionally, the probability of materialisation of a cyber threat in Article 17 of the draft RTS is a particularly difficult assessment to make. We therefore firmly believe **that these aspects should not be taken into consideration when defining the significance of a cyber threat**.

Q8. Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes.

We consider the **criteria for identification of incidents to be in line with our view**, particularly in regard of security incidents. However, in the context of CCPs, we have **reservations on the proposed combination of criteria in order to determine and assess a "major incident"**. The primary threat revolves around system unavailability.

Considering the international customer base of such entities, the geographical reach and affected critical services, each and every incident, including minor ones, would be subject to reporting requirements. To allow for more flexibility but also ensure effectiveness, we **encourage a more adaptable approach that would primarily focus on significant, critical incidents** (e.g., duration/down-time as of today, etc.).

In addition, we believe that when sharing with other authorities, details of the reports should be redacted to remove strictly-confidential data of the affected financial institution. This is especially relevant for cyber incidents, as it may contain data which could present a blue-print how a financial institution can be compromised. This type of data should not be distributed broadly and only on a need-to-know basis.