EIOPA - IRSG

ESMA
Securities and Markets Stakeholder Group

EBA EUROPEAN BANKING AUTHORITY
BANKING STAKEHOLDER GROUP

JC 2023 34

Deadline: **11 September 2023**

Joint European Supervisory Authority Consultation paper

Draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554

General observations

The stakeholder groups ("SGs" or "Stakeholders") recognise the importance of ensuring a high degree of ICT systems security and resilience. While all sectors of the financial services industry are potentially exposed to ICT security risks, the profile of such risks may vary considerably between different sub-sectors within the industry. In 2022, 119 incidents were reported by the Banking sector to ENISA under the NISD framework (Art. 15 & 16 NIS 1), an increase of 37% over the previous year. The Banking sector accounted for ca. 13% of all incidents reported to ENISA's CIRAS reporting platform for that period. Operators of financial market infrastructures (FMIs) reported another 8 incidents in the same period (+60%). In Banking, system failures were the most prevalent cause (66% of all incidents), followed by malicious activity (24%), and human error (9%). Of the much smaller sample of FMI incidents, however, as much as 63% were attributed to malicious activity, with only 37% caused by system failures.

It is important that the ESAs take the provisions in the NISD into account when criteria for incident reporting according to DORA are developed. DORA takes into consideration that double reporting stemming from potential overlaps between the reporting requirements according to NISD and reporting requirements according to DORA should be avoided. It is important that financial supervisory authorities make sure that this objective is maintained in the practical application of these regulatory frameworks at national level in each EU member state.

Detailed comments (Q1. – Q8.)

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.

The SGs agree with the proposed overall approach for major incident classification and note, in particular, that the distinction between primary and secondary criteria, which is not specifically made in the Level 1 text, is a useful and pragmatic approach, which makes allowance for the diversity of, and sectoral specifics within the financial sector, and allows for the principle of proportionality to be applied the implementation of DORA in a structured and consistent manner.

The SGs also support the ESAs' choice to rely, as much as possible, on binary criteria. Given the risk and potential cost of under-/over-reporting, and the need to streamline processes and shorten response times, criteria should be straightforward to apply and unambiguous.

The SGs note that certain definitions in Level 1 legislation that are relevant for determining the scope of reporting requirements could possibly be referenced explicitly in the RTS for clarity. It should be reiterated, in particular, that the definitions of *"ICT-related incidents"* and *"cyber threats"* in Art. 3(8) and Art. 3(12) DORA, respectively, do not reference any element of causation so that reporting obligations under Art. 18(1) and voluntary reports under Art. (18(2) DORA are not limited to incidents or threats that are attributable to malicious activity. Although malicious activity may attract more attention in the public and media stakeholders are mindful that the timely and specific reporting of accidental ICT incidents is equally critical.

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.

The SGs acknowledge the difficulty to specify absolute and/or relative thresholds given the diversity of, and sectoral specifics within the financial sector.

In the interest of legal certainty, the SGs suggest that the ESAs should consider reiterating in the RTS that any entity within the scope of DORA should also be considered, a priori, as a financial counterpart for the purposes of calculating the threshold values of *"financial counterparts affected"*.

The SGs observe that the proposed definition of *"relevance"* in Art. 1(3) of the RTS introduces a degree of ambiguity and discretionary latitude that is, arguably, not covered by the Level 1 text. It is not obvious that the term *"number and/or relevance"* in item a. of Art. 18(1) DORA specifies two different criteria that would need to be defined separately in the RTS. The *"relevance"* aspect could instead be considered adequately captured by the relative materiality threshold (10%), while the *"number"* aspect of the criterion is captured by the absolute materiality threshold (50,000). In the interest of making primary criteria as unambiguous as possible, and given that the secondary criteria provide for some discretionary latitude already, it would appear advisable to concentrate on empirical, numerical thresholds for the primary criteria. If financial entities were to apply largely discretionary weightings to quantify the *"relevance"* of clients or counterparts quantitative materiality thresholds, both absolute and relative, could be rendered effectively meaningless. An incident that affects 10% or more of the client base or financial counterparts should be considered relevant in any event, regardless of the specifics of the individual parties affected. Moreover, a degree of discretion for financial institutions, which would accommodate sectoral differences and proportionality

requirements, is already provided by the absence of an absolute threshold for *"financial counterparts affected"*. On this basis, Art. 1(3) of the RTS should be considered redundant.

The draft does not specify either if the concept "clients affected" refers to the clients registered in the specific channel/service affected by the incident (web application, mobile application,…) or to the clients that use the channel/service at the moment the incident occurs. Furthermore, it is necessary to stress that the threshold applies at entity level (rather than group level) which is consistent with the rest of DORA.

Article 9 of the RTS establishes that the materiality threshold of this criterion is met if the incident has "any identified impact on relevant clients or financial counterparts". We consider that the article should refer to a significant impact in relevant clients (not to any impact). The proposed text is the following: "Any significant impact on relevant clients or financial counterparts".

Regarding the *"amount or number of transactions affected"*, it does not appear immediately obvious from the wording of Art. 18(1) DORA that the co-legislators intended to restrict the scope of reportable incidents to *"transactions that have a monetary value"*. In its current form, the proposed Art. 1(4) of the RTS would exclude transactions that do not contain a monetary amount but which may, nevertheless, involve the exposure or loss of other valuable data, such as confidential customer information. In Art. 18(1) DORA, the co-legislators provide a choice of indicators between the *"amount or number of transactions affected"* (arg. *"or"*), which is preceded by the qualifier *"as applicable"*. While the indicator *"amount of transactions"* implies that transactions must contain a monetary amount the same does not apply for *"number of transactions"*. Some stakeholders are of the view, therefore, that the qualifier *"containing a monetary amount"* should be applied in the calculation of the criterion only, whereas the criterion *"number of transactions"* should be calculated without that restriction and include transactions that do not contain a monetary amount. These stakeholders note that ICT incidents that affect a material number of transactions tend to be indicative of potential operational risks and should therefore be within scope unless there is clear evidence to the contrary.

Also, the duration of the impact must be taken into account (not just an additional factor but as an overarching one) for the relevance of the impact on clients. That is, events which affect many clients but have a very short duration (seconds, minutes), should not be reported regardless of the number of clients potentially affected, even when the incident could impact many clients, its short duration makes the real effect on them quite limited.

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.

The SGs agree with the classification of "reputational impact"as a secondary criterion and the proposed definition in Art. 2 of the RTS. In respect of the wording of item a. of Art. 2, the SGs observe that the notion that an incident has *"attracted media attention"* may be too vague and more precise wording may be preferable. Specifically, in order the cause reputational damage the incident would have been reported in the media or, at least, have prompted enquiries from the media. The SGs agree that no distinction should be made between different types of media. Social media, in particular, have proven very effective at propagating information and even triggering potential systemic events.

The wording in item b. of Art. 2 of the RTS (*"different clients or financial counterparts")* is exceedingly vague and does not provide sufficient guidance for determining the materiality threshold in accordance with Art. 10. The SGs assumes that the threshold should be set at such a level that complaints from only a few clients would not trigger the criterion. For reputational damage to

become a concern such complaints would have to be received, arguably, from a sizable number of clients and/or several financial counterparts.

In item d. of Art. 2 of the RTS the potential loss of clients or financial counterparts as a result of the incident is qualified with the clause *"with an impact on its business"*. The purpose of this qualifier seems unclear without further explanation since any loss of clients or counterparties should, a priori, have an impact on business. In the absence of further detail this wording could also be omitted.

Article 3(1) of the RTS requires a FE to measure the duration of an incident *"from the moment the incident occurs"*. This may in practice be difficult to specify depending on the circumstances. It may, therefore, be advised to replace the wording with *"from the moment the incident was detected".*

According to Art. 3(2) of the RTS, incident-related service downtime is deemed to end when *"regular activities/operations have been restored to the level of service that was provided prior to the incident."* In the absence of a precise reference point it could be difficult to determine to what level service would have to be restored. Moreover, it is unclear for the purposes of item b. of Art. 11 of the RTS whether it would be sufficient for the cause of the incident to be remediated temporarily, or whether it would have to be resolved permanently. Further clarification of this point may be useful.

Art. 11 of the RTS establishes that the materiality threshold is met if *"the service downtime is longer than 2 hours for ICT services supporting critical functions"*. However, some critical business processes or services are critical from a business continuity perspective only during specific time frames. For these services the impact of a service downtime will be more severe if the incident occurs during business hours than if it occurs during the night or the weekend. Some members of the SGs are of the view, therefore, that the 2-hour materiality threshold of this criterionshould apply for such services only if they occur during business hours. Furthermore, they believe that the timespan of 2 hours, from a business continuity perspective, seems short, even if the downtime occurs during business hours.

Article 15 (1) of the RTS set the materiality threshold of the economic impact at 100,000 EUR or above. This threshold appears low in light of regular expenditures for resolving major incidents, especially for large and complex FEs. For the same reason, the ESAs believe that the proposed threshold will likely less affect smaller Fes. This , however, may potentially lead to a higher number of reported incidents for the purposes of the RTS at the level of larger FEs.

In addition, it should be taken into account that it will be really difficult for financial entities to have the details of the economic impact when the incident is detected (which is the moment when the incident has to be notified to the competent authorities). Therefore, it will be difficult to determine whether the materiality threshold of this criterion is met. Determining the economic impact of the incident will be complex even during the incident management process.

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.

The SGs agree with the proposed definition of "data losses" in Art. 5 and the materiality thresholds in Art. 13. It is particularly important, in the given context, to concentrate on the perspective of the financial entity and the potential impact of data losses its core business activities. Data that may be considered merely *"temporarily unavailable"* from the perspective of the ICT system operator may effectively become *"inaccessible or unusable"* for the financial entity, especially when it relies on such data for critical, time-sensitive transactions.

The concept “authenticity” should be clarified in Article 5 of the RTS, since international security standards usually refer only to confidentiality, integrity and availability.

The SGs observe, in addition, that the definition of data losses *"in relation to confidentiality"* according to Art. 5(4) of the RTS does not make specific reference to potential losses of customers' personal data. Personal data of individual customers enjoy particular protection under Regulation 2016/679 (GDPR) – ICT systems that handle such data should, therefore, meet the highest standards of security and operational resilience, and receive particular supervisory attention. Moreover, lost or compromised customer data have the potential to cause significant consequential damage, e.g. through fraud and as a vector for cyberattacks. The notion of confidentiality in Art. 5(4) should be expanded to include, as a sub-criterion, whether the incident has resulted in the unauthorised disclosure of individual customers' personal data that fall under the protection of the GDPR.

Overall, the interplay between the GDPR (Articles 33 and 34) and "data losses" as per DORA needs to be clarified.

Additionally, consideration 42 of the RTS “Background” Section establishes that “any loss of critical data” will determine that the materiality threshold of this criterion is met. Even though Article 13 of the RTS refers to data losses with “significant impact”, this article of the “Background” section should be clarified, to ensure that not every data loss will determine that the threshold of this criterion is met.

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.

For the purposes of determining criticality, the SGs note that the terminology in item e. of Art. 18(1) DORA departs slightly from the terms used elsewhere in DORA, especially the term *"critical or important function"*, which is defined in item 22 of Art. 3 DORA. The SGs agree with the proposed approach of reinstating this reference in Art. 6 of the RTS. While rec. 70 DORA states explicitly that any functions deemed to be critical according to item 35 of Art. 2(1) BRRD should be included as such under DORA, further clarification would be welcome, especially, on the definition of "important functions". The BRRD requires requires credit institutions to specify *"critical functions"* (item 35 of Art. 2(1) BRRD) and *"core business lines"* (item 36 of Art. 2(1) BRRD) for the purposes of recovery and resolution planning. This assessment is subsequently reviewed, and monitored continuously, by supervisory and resolution authorities. A similar approach is taken in other jurisdictions, e.g. in the UK for the identification and supervision of *"important business services"* (PRA Policy Statement PS6/21 of March 2021 on operational resilience). To operationalise the term, financial entities within the scope of DORA could be to provide an assessment of their *"critical or important functions"*, e.g. when documenting their ICT risk management framework in accordance with Art. 6(5) DORA. Credit institutions would be able to draw on the relevant documentation prepared in compliance with the BRRD requirements and relevant EBA and SRB guidance.

Article 6 of the RTS also includes in this criterion “incidents that affect services or activities that require authorisation”. The concept “services that require authorization” should be clarified.

"Authorisation" should not constitute a criterion to define criticality. Business Impact Analysis would be considered more appropriate, rather.

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).

Capturing recurring incidents having the same root cause and with similar nature and impact may in practice be difficult to identify. *"Similarity of nature"* is a broad concept and may lead to significant over- or even underreporting of major incidents. Article 16(2) of the RTS may be amended to: *"For the purposes of paragraph 1, recurring incidents shall occur at least twice, have the same apparent root cause ~~and shall be with similar nature~~ and impact."*

"Recurring incident" does not feature in the DORA Level 1 text and it would therefore be helpful to get clarification as to what is meant by "recurring".

The inclusion of this criterion in the RTS will determine that two non-significant incidents that affect critical services but do not affect a large number of clients and do not have a relevant economic impact as isolated incidents would have to be classified as major incidents when considered in an aggregated manner. This will result in a considerable increase in the number of incidents that have to be reported to the competent authorities by the financial entities. We consider that this criterion should not be included in the RTS unless reporting is required when the aggregated impact of individual events is significant.

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.

The SGs agree with the general approach for classification of significant cyber threats. For the voluntary reporting framework under Art. 18(2) DORA to be successful, close cooperation among financial entities and between financial entities and third-party ICT service providers will be essential.

The SGs note, however, that it could be challenging for entities to assess the likelihood that a cyber threat could also affect another financial institution, third-party provider, client or financial counterpart. In addition, the detection of cyber threats could also expose vulnerabilities in the ICT systems of an entity. In the interest of encouraging all market participants to share information on cyber threats in a timely and pro-active manner, reporting should therefore focus on the specifics of the detected threat, its probability of materialisation, and potential for contagion. Sensitive information, especially related to the systems of the reporting entity, and the circumstances of the detection, should be kept to the necessary minimum.

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.