Brussels, 8 September 2023
FINAL - CDO

EACB comments on

ESAs' 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 DORA

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.

Overall, we find the ESA's approach for classifying major incidents under DORA appropriate. However, we have some reservations, particularly as our closest experience with incident reporting comes from PSD2, which seems in some cases to have inspired the ESAs when drafting this RTS for DORA. Nonetheless, we understand that the ESAs aimed to customise the classification criteria and thresholds to suit all financial entities under DORA.

The 'new' approach, with detailed specifications of certain criteria and the introduction of new materiality thresholds, appears to introduce a more complex evaluation process for financial entities when dealing with major incidents. For instance, the criterion 'Duration and service downtime' requires identifying the start time of service disruption through the extraction and analysis of logs. This necessitates collecting and processing more data compared to the current situation.

In light of these concerns, we recommend reviewing some of the criteria and thresholds, as we elaborate in our responses to questions 2, 3, and 4.

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.

'Number of financial counterparts affected' and lack of a clear definition of 'financial counterparts'

Regarding the 'number of financial counterparts affected' aspect of the criterion, we have some observations to share.

The ESAs propose setting a materiality threshold for this part of the criterion, which would trigger the reporting of a major incident, at 10% of all affected financial counterparts with a contractual arrangement related to the financial entity's service. However, we note that financial entities may sometimes have only one financial counterpart for a specific service, even though they might have multiple counterparts overall.

Let's consider the following two examples:

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

1) A fintech has an exclusive supply relationship with a bank for a service, making the entity the sole financial counterpart for that service. If an incident impacts this specific service, the threshold would be met.

2) An incident could occur on a service that involves a single financial counterpart, as an exclusive customer of that particular service offered by a bank.

We believe that one of the main challenges arises from the absence of a clear definition of 'financial counterpart'. DORA does not provide a definition, making it more of a level 1 rule issue than level 2. Without a definition or at least some specific criteria to identify relevant clients or financial counterparts, it becomes difficult to thoroughly assess the effectiveness of the proposed materiality thresholds for this criterion. As seen in the above examples, the materiality threshold would always be met, triggering the reporting of a major incident.
Moreover, in case of an incident affecting one of the entities within a banking Group, this would have repercussions on the group as a whole and consequently also on the entities of the group. We therefore recommend against treating banks within a group as individual counterparts. Instead, we propose considering a 'Group' as a cohesive entity to effectively address this scenario.

To accurately identify and assess the significance of clients and relevant counterparts, it is essential to evaluate them based on objective criteria. This would allow for the generation of comparable data at the European level.

Lastly, it would be beneficial to clearly distinguish between 'financial counterpart' and the term 'central counterpart' as defined in Art. 3, paragraph 40 of DORA.

Relative and absolute materiality thresholds

While we generally agree that a percentage is often more applicable than an absolute value, we have reservations about relying solely on the relative threshold for the specific criterion 'number of financial counterparts affected'. Depending solely on the relative threshold could lead to an unreliable criterion.

For instance, if a financial entity has 10 counterparts and the incident impacts only 1, the 10% threshold would be met. On the other hand, if a financial entity has 1000 counterparts and the incident impacts 90, the 10% threshold would not be met. As a result, in the first case, the criterion would be considered satisfied, while in the second case, it would not, despite the impact on a significantly larger number of counterparts, which should be deemed more severe. In such cases, the absolute number of affected financial counterparts may hold greater significance than the percentage.

To address this concern, we suggest the EBA revising the threshold for this criterion by also incorporating an absolute threshold. One approach could involve setting a specific number of financial counterparts affected by an incident, and once this threshold is reached, it would signal a level of severity that necessitates action or further consideration regarding the institution's digital operational resilience. This would provide a more balanced and reliable assessment of the criterion. However, it is important to note that the definition of 'counterpart' once again becomes significant, particularly in light of group structures with numerous entities, which should not be seen as individual counterparts.

'Number of clients affected'

The ESAs noted that they took into considerations various relative thresholds within a range of 5% to 25%. However, we suggest placing the threshold at 15% to avoid unnecessary regulatory and reporting burden.

Under PSD2, a threshold of 10% represented the lower impact level, while 25% indicated the higher impact level. We believe it is prudent and reasonable to propose a threshold slightly higher than the lower one under PSD2, as we seek to strike a balance between meaningful assessment and minimising unnecessary burden.

Based on the above, Art. 9.1 letter a) of the draft RTS should be amended as follows:

a) the number of affected clients is higher than ~~10%~~ **15%** *of all clients using the affected service of the financial entity*.

We also suggest specifying that the term 'affected clients' pertains exclusively to the institution's own clients. Consequently Art. 1 paragraph 1 of the draft RTS should be amended as follows:

The number of clients affected by the incident as referred to in Article 18(1), point (a) of Regulation (EU) 2022/2554, shall reflect the number of all **institution's own** *affected clients, which may be natural or legal persons, that make use of the service provided by the financial entity.*

Amount or number of transactions affected

In the consultation paper, it is stated that the ESAs interpret the term 'transactions' as having a monetary value based on the wording of DORA. However, we believe this interpretation is based on an assumption, as we cannot find any specific reference in DORA where the term 'transactions' necessarily implies a monetary element.

Based on the above, we suggest amending Art. 1 paragraph 4 as follows:

In relation to the amount and number of transactions affected by the incident, the financial entity shall take into account all affected transactions ***~~containing a monetary amount~~*** *that have at least one part of the transaction carried out in the EU*.

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.

'Reputational impact'

The 'Reputational impact' criterion requires the financial entity to consider the level of visibility that the incident has gained in the market.

The draft RTS outlines certain conditions, including 'the financial entity has received complaints from different clients or financial counterparts' and 'the financial entity has lost or is likely to lose clients or financial counterparts'. We believe it is important to distinguish the criticality of customer complaints from the termination of business relationships. While some customer complaints may be common in relation to incidents, it is when these issues are not resolved to the customer's satisfaction that reputational risks may arise or when there is a large quantity of complaints that cannot be adequately addressed.

Based on the above consideration, we suggest amending Art. 2 letter b) as follows:

[…] In particular, financial entities shall take into account whether one of the following are met:
a) […]

b) The financial entity has received **a large number of** *complaints from different clients or financial counterparts* **that could not be resolved in a reasonable time***; or*

'Duration and service downtime'

We acknowledge the ESAs' recognition of potential cases where the financial entity may not have precise information on when the incident has occurred or the service downtime has started. The consultation paper proposes that in such situations, the financial entity shall refer to network and system logs to measure the overall duration of the incident.

However, it is essential to consider the following aspects:

1. Logs can be extensive files, sometimes stored on offline systems, which may require significant time for recovery.
2. Extracting and analysing logs involve processing a large volume of information, making it a laborious and time-consuming activity.
3. In some instances, logs may be recorded and stored on the same system where the incident occurred, rendering them not readable.

Due to these challenges, the approach suggested in the draft RTS (Art. 3.1) may prove ineffective. As an alternative, we propose that financial entities could estimate not only the moment the incident ended but also the time when it occurred.

Based on the above point, we suggest amending Art. 3.1 as follows:
'
'[…] Where financial entities do not yet know the moment when the incident ***has occurred or*** *will be resolved, they shall apply estimates.'*

Additionally, there are scenarios in which identifying the precise starting point of the incident is challenging. For example, in cases of a progressive incident caused by a specific bug, it may not be clear whether the financial entities should measure the duration from the moment performance started to degrade or from the moment when the full services block occurred.

In relation to Art. 11 letter a concerning the materiality threshold, we have some concerns about the suggested 24-hour threshold. We would prefer greater flexibility in terms of the time limit.

'Economic impact'

We wonder whether the effort required to implement or adhere to the criterion is justified by the benefits it brings.

In the consultation paper the ESAs stated that the criterion was rarely used under the Guidelines on major incident reporting under PSD2. We believe the same may apply to DORA.

The 'economic impact' criterion requires significant effort in terms of time, information, and dedicated human resources for calculation.

- The extensive data collection, storage, and processing involved make it costly and time-consuming, posing challenges for quick reporting. The various costs listed in Art. 7 may not be known at the time

of incident classification, may be challenging to estimate due to a lack of data, or may be subject to imprecise estimations. For instance, concerning the following letters in Art. 7.1:

a) The expropriation of funds and assets does not occur immediately within a narrow time frame (e.g., during investigation times), so information about such costs is not readily available at the time of the incident.
b) Due to replacement times for software, hardware or infrastructure, these costs may not be immediately known.
c) The involvement of confidential elements, such as the costs of the staff who solved the incident may (and should) not be known by the person in charge of the incident classification.
d) Those responsible for incident management may not be fully aware of all contractual clauses for all services (e.g., due to industrial secrecy).
e) Compensation costs may not be defined at the contractual level. In such cases, the cost would depend on the number of customers requesting compensation (not known in advance), and could be determined by a court judge, unless the Data Protection Authority intervenes to define it.
f) Revenue losses are potentially estimable, but the assessment is complex and cannot be done immediately.
g) Estimating costs related to communications involves organisational complexity, as the incident manager needs to liaise with responsible parties to obtain estimates.
h) Costs are highly variable, depending on the type of event and the number of affected users, rendering them not immediately ascertainable (e.g., costs associated with legal cases or law firm remuneration).

- Moreover, some costs may only emerge long after reporting, such as customer complaints and prolonged lawsuits for damages.

- Lastly, we have reservations about the absolute threshold, which is currently set at EUR 100,000, as we consider it to be too low. In comparison, the threshold established under the Guidelines on major incident reporting under PSD2 for the 'Economic impact' criterion is EUR 5,000,000 or 0.1% of Tier-1 capital.

Based on all the above considerations, **we suggest discarding the economic impact criterion from the classification criteria**. If this recommendation is not taken into account, we advise retaining the thresholds set under PSD2, while also deleting letter c) in paragraph 1 of Art. 7:

~~c) staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff;~~

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.

Art. 13 states that any significant impact on the availability, authenticity, integrity, or confidentiality of critical data, resulting in an adverse effect on the financial entity's business objectives or compliance with regulatory requirements, shall be considered as meeting the thresholds of the criterion for major incidents.

We have the following two observations:

1) The term 'critical data' lacks clarity, as there is no reference to it in DORA or the consultation paper. DORA refers to critical functions and critical operations, and there is no explicit definition of 'critical data' in GDPR or PSD2. Further information is needed to understand the ESAs' intent regarding 'critical data'.

2) The meaning of 'adverse impact on meeting regulatory requirements' is vague and not well-defined. We suggest removing this condition from Art. 13 of the draft RTS.

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.

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).

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.

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.

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)
- Marco Mancino, Deputy head of Department, Banking Regulation (marco.mancino@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser for Digital Policies (chiara.delloro@eacb.coop)