Contribution ID: 3d2a6b87-48c4-4459-b3ab-c3f2d59e5c6e
Date: 08/09/2023 22:24:07

Public consultation on 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

Fields marked with * are mandatory.

Intorduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the first batch of Consultation Papers on the mandates stemming from the Digital Operational Resilience Act (DORA) with the aim to collect market participants' feedback on the proposed Technical Standard. This Consultation paper covers:

'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'
Market participants are invited to provide their feedback to the draft technical standards by responding to the questions presented in this consultation paper. The feedback received will be taken into account in the finalisation of the draft technical standards, which are due to be submitted to the European Commission by 17 January 2024.
Comments are most helpful if they:

- respond to the questions stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence (including relevant data, where applicable) to support the views expressed;
- reflect a cross-sectoral (banking, insurance, markets and securities) approach, to the extent possible; and describe any alternative approaches the ESAs could consider.

To submit your comments, please click on the blue "Submit" button in the last part of the present survey. Please note that comments submitted after 11 September 2023 or submitted via other means may not be processed.

Please clearly express in the consultation form if you wish your comments to be disclosed or to be treated

as confidential. A confidential response may be requested from the ESAs in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request.
Any decision we make not to disclose the response is reviewable by the ESAs' Boards of Appeal and the European Ombudsman.
The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the ESA websites.

General Information

* Name of the Reporting Stakeholder

Deutsche Börse Group

Legal Entity Identifier (LEI) if available

529900G3SW56SHYNPR95

* Type of Reporting Organisation

- ( ) ICT Third-Party Service Provider
- (•) Financial Entity
- ( ) Industry Association/Federation
- ( ) Consumer Protection Association
- ( ) Competent Authority
- ( ) Other

* Financial Sector

- [ ] Banking and payments
- [ ] Insurance
- [x] Markets and securities
- [ ] Other

* Jurisdiction of Establishment

Germany and Luxembourg

* Geographical Scope of Business

- (•) EU domestic
- ( ) Eu cross-border
- ( ) Third-country
- ( ) Worldwide (EU and third-country)

* Name of Point of Contact

Sujata Wirsching

* Email Address of Point of Contact

sujata.wirsching@deutsche-boerse.com

Questions

Question 1. Do you agree with the overall approach for classification of major incidents under DORA?

- ( ) Yes
- (•) No

* 1b. Please provide your reasoning and alternative approach(es) you would suggest.

For cyber incidents, there are two factors which should be considered as relevant in determining the materiality thresholds: Was the incident impactful? Was the incident caused by a threat actor who had a targeted and malicious intent?

Using the criteria above, only incidents that are both impactful and have targeted and malicious intent should be considered as reportable.

It is important to keep in mind that incidents that do not have a material impact can be important for intelligence sharing among financial entities to align protection activities. It could be helpful that financial entities are informed about such incidents – in an anonymised form - and this information is used as a source of threat intelligence.

A critical consideration emerges with regards to the suggested approach for classification of major incidents under DORA, particularly when applied to trading venues.

While we recognize the comprehensiveness of the suggested classification system, we hold reservations regarding its practical value. In particular, we believe that the proposed approach may not adequately account for the incident impact on services or the extent of client exposure to incident repercussions. This could lead to a high number of incidents being classified as major, irrespective of their actual magnitude and overall impact, which we do not agree with, nor consider reasonable.

In our current operational context, we conduct incident classification as well as reporting (i.e., to national regulators but also to regulators in countries where Eurex operates) in accordance with well-established standards and internal frameworks. Those procedures have proven to be effective and already encompass most of the parameters and criteria outlined in DORA and envisaged in this proposed RTS. For instance, the data losses, reputational and economic impact, duration and service downtime as well as clients impact criteria are included. The geographical spread criterion is not considered relevant within the trading venues context due to the international caliber and global presence of such entities.

We emphasize on the need to re-adjust the framework to better reflect and accommodate the environment of trading venues but also on the need to introduce more flexibility for financial entities to assess the criticality of incidents which could substantially enrich the efficacy, coherence and applicability of the classification framework. However, if the proposal put forward is kept, we strongly encourage the consideration of the adjustments, recommendations and overall suggestions we have provided to the following questions.

Question 2. 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?

- ○ Yes
- ◉ No

* 2b. Please provide your reasoning and suggested changes.

We would like to put forward the following comments:

In Art. Art. 9(1)(a), 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 happen that an incident impacts 10% of clients, but 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 Art. 9(1)(e), 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 TR.
In Art. 9(1)(f), it appears arduous to assess any identified impact in accordance with Art. 1(3). We suggest leaving it to the discretion of individual firms to determine adequate thresholds for number of clients and transactions.

The specification and materiality thresholds of the 'Clients, financial counterparts and transactions affected' criterion, as outlined in Articles 1 and 9 of the draft RTS, introduce numerous concerns. While we agree with the general specification, a more precise definition is encouraged to enhance clarity. Moreover, we emphasize that this criterion should consider all clients, as opposed to only accounting for the EU customers, given the international client base and global presence of trading venues.

In regard of the materiality thresholds associated with this criterion, a recalibration appears necessary. Firstly, we do not agree with the stipulation “where any of the following conditions is met” (i.e., Article 9(1)). The stated conditions present considerable differences and must be revised, particularly their applicability to trading venues. We recommend focusing on either the “clients” or “affected transactions” which would allow for more flexibility when assessing the impact of an incident.

With regards to the proposed thresholds, several concerns emerge. Considering the trading environment, the relative condition of the number of affected clients being “higher than 10% of all clients” (i.e., Article 9(a)) appears myopic. A more suitable alternative could involve correlating this condition to the client market share per relevant products (e.g., products with a higher than x% portion of total volume), therefore taking into account the materiality and importance of the traded products and recalibrating this threshold based on substantial volume impact (e.g., above 10% of daily volume). Considering the client impact from a product and volume perspective when defining the incident criticality would allow to better account and reflect the operational characteristics of trading venues.

Similarly, the condition simulating that “the number of affected financial counterparts is higher than 10% of all financial counterparts” (i.e., Article 9(b)) is also to be revised. Given that trading venues frequently rely on a central clearing house, the number of affected financial counterparties would, in all cases, be 100%, resulting in over-reporting.

Lastly, focusing on the “number of affected transactions” (i.e., Article 9(d)(e)). While we agree with the relative threshold of “higher than 10%”, the absolute threshold “higher than EUR 15 000 000" is not in line with our view. Trading venues, especially for derivatives products, manage volumes that are substantially higher implying that this absolute threshold may not reflect the true impact of an incident. In addition, as already highlighted, we believe that the emphasis on EU transaction execution lacks practical feasibility and may require reconsideration given the international client base of trading venues.

In summary, from a trading venue perspective, we strongly emphasize on the need to re-evaluate the thresholds for the “clients, financial counterparts and transactions” criterion to ensure those are both meaningful and reflective of the operational reality of all financial entities.

Question 3. 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?

- ( ) Yes
- (•) No

* 3b. Please provide your reasoning and suggested changes.

The threshold for reputational impact defined in Art. 2 is very low and we encourage a proportionality/risk-based approach. Regarding ‘Duration and service downtime’, Art. 3(1) states that FEs shall measure the duration of an incident from the moment the incident occurs until the incident is resolved, but there is no definition or explanation when an incident shall be considered as “resolved”. 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 RTS. On ‘Geographical spread’, 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 Art. 18(1c) 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 MSs. The threshold of minimum two MSs is particularly low and for any FE with scale it is challenging to find an incident that would not affect at least two MS (it is indeed more a function of the size of the service rather than of the materiality of the incident). Art. 11(b) 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, it should not reach the threshold. While the overall consideration of “Reputational impact”, as in Art. 2 and 10, within the framework of incident assessment aligns with our view, we question the proposed provision related to an incident's market perception and media attention. From a trading venue perspective, tracking and assessing every instance of media coverage, especially on a global scale, is a complex undertaking exceeding practical feasibility.
We would like to highlight that the media attention could potentially arise at later stages (e.g., once the incident report has been completed) and therefore, should not be used as a condition to determine the reputational impact. We recommend considering alternative, more distinctive parameters or thresholds that would enhance precision and clarity. On “Duration/downtime”, we agree with the overall specification, assuming that the restoration of regular activities and operations stated in paragraph 2 refers to the pre-trading level of service. However, if our assumption is not correct, a more precise distinction and clarification is then recommended in order to allow for a better understanding. When considering the materiality threshold for this criterion, we recommend for the duration of the incident to be assessed in alignment with the system availability for non-critical functions (i.e. Art. 11(a)). Discerning incident impact in contexts where non-critical functions remain available appears as essential to ensure that incidents occurring, e.g. on Friday evening and resolved by early Monday, do not disproportionately contribute to materiality considerations. For the purpose of evaluating the “Geographical spread” with regard to the areas affected by an incident, the criterion requiring financial entities to assess the impact of the incident in the territories of “at least two MSs” introduces a level of stringency. This threshold will create challenges for trading venues (TVs) as, given the international client base of such entities, this criterion will most certainly be met for each and every incident, irrespective of its impact, magnitude or significance. Consequently, in order to ensure a comprehensive and effective representation we encourage either excluding TVs from the scope of these criteria or, alternatively, incorporating an additional provision that explicitly provides an exemption for TVs in such scenarios. On the “Economic impact” of a major incident, the requirement for FEs to account for “losses due to forgone revenues”, in Art. 7(1)(f), poses a considerable challenge due to the high difficultly to accurately estimate those losses, in the context of TVs. In addition, we emphasize that the proposed “EUR 100 000” threshold when considering the costs and/or losses incurred from a major incident (i.e., Article 15(1)) does not align with the interest nor reflect the characteristics of TVs, as it is considerably low and will certainly always contribute to materiality considerations.
In summary, similarly to the “clients, financial counterparts” criterion, we encourage a re-evaluation of the specification/ thresholds of the proposed criteria ‘Reputational impact’, ‘Duration’, ‘Geographical spread’ as well as ‘Economic impact’ in order to ensure the applicability to TVs.

Question 4. Do you agree with the specification and threshold of the criterion ‘Data losses’, as proposed in Article 5 and 13?

- Yes

- (●) No

* 4b. Please provide your reasoning and suggested changes.

Art. 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).

Question 5. Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14?

- ( ) Yes
- (●) No

* 5b. Please provide your reasoning and suggested changes.

The definition in Art. 6 should not, in our opinion, add to 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. If such services are not critical, they should not be included in the criterion.

When determining the criticality of the services affected, the provision for financial entities to assess "whether the incident has affected services or activities that require authorization" (i.e., Article 6) is perceived as extensively broad and must be narrowed down to allow for a better understanding and clarity. In addition, we recommend that financial entities shall also assess the incident materiality and criticality level according to their already established internal procedures (as explained in Q1 above).

Question 6. 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?

- ( ) Yes
- (●) No

* 6b. 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 are supportive of increasing the number of recurring incidents to higher than two, but it will be extremely challenging and burdensome for some FEs to determine that two or more incidents have the same root cause since this is unlikely to be known at the time of the incident. This is likely to result in financial entities staying on the side of caution and overreporting incidents as recurring to avoid any regulatory breach. Similarly, the suggestion that similarity of nature would suffice is far too broad a term and would likewise result in significant overreporting.

Moreover, we do not see how the proposed Article 6 is compatible with Article 3(8) and (9) of DORA. The former already defines an 'ICT-related incident' as a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity.

It therefore appears that recurring incidents are already captured within the Level 1 text hence we suggest removing this criterion.

Question 7. Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17?

- ○ Yes
- ◉ No

* 7b. Please provide your reasoning and suggested changes.

We would appreciate the 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 this 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 is not transparent for trading venues and would involve a high degree of speculation. We, therefore, strongly believe that this aspect cannot be taken into consideration when defining the significance of a cyber threat.

Question 8. 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?

- ○ Yes
- ◉ No

* 8b. Please provide your reasoning and suggested changes.

The criteria for identification of incidents are in line with our view, particularly in regard of security incidents. However, in the context of trading venues, we have reservations and do not consider reasonable the proposed combination of criteria in order to determine and assess a "major incident". The primary threat to an exchange 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.).

Contact

Contact Form