Contribution ID: b7363b08-8998-4eb5-9c84-1a8a77cb4e10
Date: 11/09/2023 17:44:57

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

Electronic Money Association

Legal Entity Identifier (LEI) if available

* Type of Reporting Organisation

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

* Financial Sector

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

* Jurisdiction of Establishment

Belgium

* Geographical Scope of Business

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

* Name of Point of Contact

Judith Crawford

* Email Address of Point of Contact

judith.crawford@e-ma.org

Questions

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

- (●) Yes
- ( ) No

1a. Please provide additional comments (if any).

We perceive a significant overlap between the ICT-related incident classification criteria detailed in the draft RTS and existing sectoral guidance (EBA Guidelines on major incident reporting under PSD2). We also note the changes introduced in the draft RTS through the introduction of (i) New incident classification criteria (Geographical spread, Data losses, Critical services affected) and of (ii) Revised Major Incident classification logic detailed in Art.8 of the draft RTS. We encourage the ESAs to streamline sectoral compliance and reporting requirements across these GLs and the draft RTS and to provide further clarity on the status of the EBA Guidelines after the publication of the final version of this draft RTS.

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 are concerned that the Materiality Threshold condition for this criterion listed in Art. 9(1) (c) of the draft RTS (the number of affected clients is higher than 50,000 clients) is set too low for medium/large financial service providers and may lead to large numbers of submitted ICT incident reports that are not necessarily indicative of a Major incident. We also want to highlight that this has been a historical industry concern with the predecessor of this condition that appears in the EBA Guidelines on major incident reporting under PSD2 (payment service users affected).

We propose that this condition is removed. The separate condition listed in Art.(1)(b) of the draft RTS (the number of affected financial counterparts is higher than 10% of all financial counterparts used by the financial entity related to the affected service) should be retained and can act as an appropriate major ICT incident condition trigger.

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

- [x] No

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

We are concerned that the Materiality Threshold conditions for the Duration and service downtime criterion listed in Art. 11 mix incident duration and service availability. An incident may last for an extended period of time without impacting the delivery of a service. We would propose that (a) This Criterion is escalated to a Primary criterion replacing the Critical Services affected criterion, (b) The materiality threshold condition referring to the duration of an incident is removed and (c) The materiality threshold condition referring to unavailability of ICT services supporting Critical business functions that extends beyond 2 hours is retained.

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

- [ ] Yes
- [ ] No

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

- [ ] Yes
- [x] No

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

As noted in our response to Question 3 above, we support the replacement of this new qualitative criterion by the quantitative Duration and service downtime criterion with revised materiality threshold conditions. The proposed Critical Services affected criterion can contribute to the generation of many "Major" ICT incident reports due to any issue escalation to the firm's senior management body even if the issue has not impacted the availability of any Critical/Important business function. This can impact the volume and quality of major incident reports received by the relevant competent authorities.

We perceive that a revised Duration and service downtime criterion that focuses on unavailability (or significant performance degradation) of ICT services that support the delivery of Critical functions would be more effective in identifying Major ICT-related incidents.

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

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

- [ ] Yes
- [ ] No

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

Contact

Contact Form