Contribution ID: f8a48a9e-9c9b-4fdd-8fb1-83c32f5b36c9
Date: 04/03/2024 22:03:27

Public consultation on Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat

Fields marked with * are mandatory.

Intorduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the second 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 Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat.

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 July 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 4 March 2024 or submitted via other means may not be processed.

Please clearly express in the consultation form if you wish your comments to be published 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 Esstablishment

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

* Please provide your explicit consent for the publication of your response.

- ☑ Yes, publish my response
- ☐ No, please treat my response as confidential

Questions

Question 1. Do you agree with with the proposed timelines for reporting of major incidents?

- ◉ Yes
- ○ No

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

Acknowledging the significant differences in major incident classification logic and criteria introduced by the final ESA report on draft RTS on classification of major incidents and significant cyberthreats, we support the proposed timelines for submission of the Initial notification and of the Intermediate and Final reports detailed in Art. 6 of the draft RTS. We encourage the ESAs to provide guidance to the relevant national competent authorities on the consistent application of the risk-based extensions to the deadline for submission of the Intermediate & Final reports detailed in Art. 6(3) of the draft RTS.

Question 2. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA?

- ○ Yes
- ◉ No

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

We believe that the requirement to include detail on the activated elements of the business continuity plan of a financial entity (FE) in the initial notification for a major incident will add further complexity to this task without offering significant benefits. Our perception is that the focus of the initial notification must be on capturing the characteristics/impact/origin of the major incident. We would propose that this field is removed from the Template of the Initial notification; we note that information on business continuity activities undertaken by the FE to address a Major incident is provided in the Intermediate report template.

Question 3. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA?

- ○ Yes
- ◉ No

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

Our members continue to struggle with the definition of “authenticity” as a Data Loss criterion that was provided in Art. 5(2) of the RTS on classification of major incidents and significant cyberthreats compared to integrity. Specifically, it is not clear that a data loss of authenticity can be recorded on its own without the corresponding loss of integrity of data that is provided or managed by the source of that data. We encourage the ESAs to provide further clarity on the use of this Data Loss criterion.

We are concerned about the inclusion of the mandatory data field Indicators of compromise (Field 3.40) in the Intermediate report. FEs are expected to provide extensive, and sensitive information on Live incidents in this field that is likely to be rapidly evolving. The effort that FEs would need to expend to collect/collate such data is significant. It is also not clear whether any change in the Indicators of compromise must trigger the submission of another Intermediate Report; such an approach will result in over-reporting of ongoing incidents. The value-add of sharing such dynamic data as part of submitted Reports appears limited. Finally, we perceive that the current instructions on how to populate this field (in Annex II of the ITS) will result in submissions of varying quality and of low consistency. In this context, we propose that the description of this data field is revised to focus on high-level malware data (source, means of propagation) and a description of the incident’s impact on identified ICT resources.

Question 4. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA?

- ◉ Yes
- ○ No

4a. Please provide additional comments (if any).

Overall, we agree with the scope of the fields included in the Final report for Major incidents under DORA.

We wish to point out that the calculation of the costs associated with the Incident (in fields 4.15-4.24 of the report) may be ongoing at the deadline for submission of the Final report. Therefore, we propose that the Template is amended to allow FEs to indicate that some of the identified costs may be Estimates.

Question 5. Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA?

- ○ Yes
- ◉ No

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

We are concerned about the inclusion of the mandatory data field Indicators of compromise (Field 20) in Annex IV of the draft ITS for the Optional significant cyberthreat notification (Data glossary and instructions for notification of significant cyber threats).

FEs will likely receive information on significant cyberthreats through their access to threat intelligence platforms/services. The scope & accuracy of information on cyberthreats' indicators of compromise that is provided by such services is variable and often cannot be verified by the FEs, themselves. The information is also subject to rapid change. In this context, we propose that the description of this data field is revised to focus on high-level cyberthreat data (source, means of propagation, targeted resources, impact) and a description of recorded symptoms.

Question 6. Do you agree with the proposed reporting requirements set out in the draft ITS?

- (●) Yes
- ( ) No

7a. Please provide additional comments (if any).

We support the reporting approach in the draft RTS/ITS whereby a single template is used for all incident reports/notifications and where the mandatory/optional fields are clearly identified.

We note our concerns on the scope of malware/cyberthreat data recorded in the relevant Reports under Questions 3 and 5, above. We would encourage the ESAs to review the scope of Mandatory data fields in Intermediate Incident reports that trigger the mandatory submission of new Intermediate reports for the same incident. In this context, we would also welcome further guidance from the ESAs to the industry on these triggers. We believe that the focus of the Intermediate reports should be the delivery of consistent, quality updates on the characteristics, scope and actions undertaken to address an ongoing Major incident. The continued re-submission of Intermediate reports that offer no new insights adds to the incident handling workloads of FEs with limited benefits for the regulator and for the entire ecosystem.

8. Do you have any further comment you would like to share?

Contact

Contact Form