Contribution ID: 34e8dbd9-00e1-46ec-a91b-dc403bea08c8
Date: 01/03/2024 16:41:02

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

Deutsche Boerse 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 Esstablishment

Germany

* 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

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

- [x] 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

* 1b. Please provide your reasoning and suggested changes.

The proposed timeline for the submission of the initial notification, as provided in Article 6(1) points (a), is clear and reasonable from the trading venue perspective. However, we have concerns we would like to raise regarding the proposed timelines for the intermediate and final reports.
Firstly, with regards to the intermediate reports (i.e., Article 6(1) point (b)), while we agree with the first limit of “72 hours from the classification of the incident as major”, we would like to point out that the current proposal does not consider timelines for the submission of the intermediate report “after regular activities have been recovered and business is back to normal”, implying that such report updates must be submitted immediately after activities are recovered. Therefore, to enhance clarity and ensure consistency with the other timelines, we suggest that time limits should be explicitly provided for financial entities to submit these intermediate report updates. The considered time limits shall also be sufficiently broad to allow financial entities to ensure the good quality of the submitted information.
Considering all these aspects, we suggest the following changes to Article 6 (1) point (b):
“b) an intermediate report shall be submitted within 72 hours from the classification of the incident as major, or as early as possible within 4 hours after regular activities have been recovered and business is back to normal.”
Further, we do not agree with the following requirement as we see a risk for overreporting:
According to DORA Art. 19.4 (b) ‘as soon as the status of “the original incident has changed significantly” or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority‘.
The RTS does not provide further clarification as to what ‘significant’ change is and when do we have to send an intermediate report. Additionally, intermediate report requires a lot of information to be reported.
Lastly, regarding the final reports (i.e., Article 6(1) point (c)), we believe that one month timeline is very short and will pose significant challenges for financial entities, in particular when considering the amount of financial data fields that must be reported. We would suggest either allowing for more time or the provision of estimates for the financial information.

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.

The suggested data fields presented in the draft RTS and the Annex to the ITS for the initial notification of major incidents under DORA are acceptable, with the exception of the financial fields, which pose a greater challenge considering the short timelines.
We also would like to point out that the legal entity identifier (LEI) can provide numerous benefits for the unambiguous identification of financial entities and ICT third-party service providers. However, it is crucial to acknowledge that not all third-country ICT providers may possess or provide trading venues with an LEI, requiring a strong consideration of additional or alternative criteria, such as for instance Tax ID, to facilitate a comprehensive and effective identification mechanism
Article 3 (j): We suggest including after “j) Other information” the following clarification: “where sensible”.
Article 3 (j) would read as follows: A) Other information where sensible.

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

- [x] No

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

We mostly agree with the proposed content to be included in the intermediate report for major incidents. However, we would like to point out that the data field 3.13 (Value of affected transactions) in Annex II of the draft ITS (page 44) does not allow financial entities to estimate the value of affected transactions based on available data in case the actual value cannot be determined.
The instruction provided in this data field appears to be contradicting the requirements set in Article 1(5) and 9(2) of the RTS on the Classification of ICT-related Incidents (part of the first batch of DORA policy products), which stipulates: "Where the actual number of clients, financial counterparts or number or amount of transactions impacted cannot be determined, the financial entity shall estimate those numbers based on available data from comparable reference periods."
Further, the financial fields pose a greater challenge considering the short timelines.
Therefore, in order to align with the aforementioned requirement, we suggest adding “Where the actual value of transactions impacted cannot be determined, the financial entity shall use estimates” to the instruction section of the data field 3.13, which would then also align with the data field 3.11 (Number of affected transactions).
Following these amendments, the description of the data field 3.14 (Information whether the numbers are actual or estimates) shall be changed accordingly, i.e., "Information whether the values reported in the data fields 3.5. to 3.13 are actual or estimates”.

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
- [x] No

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

Similarly to the initial and intermediate reports, the financial data fields that must be included in the final report raise key concerns. In our view, it should be possible to provide estimates of the financial information. Please see responses provided to questions 1 to 3 above.

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

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

- [ ] Yes
- [ ] No

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

Contact

Contact Form