Contribution ID: 957606a8-5f9c-4a28-ae6a-bd26a708b4fb
Date: 04/03/2024 14:51:57

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

European Association of Public Banks

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

Mathilde Pradeau

* Email Address of Point of Contact

mathilde.pradeau@eapb.eu

* 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.

a), we propose that if the deadline for submitting an initial notification falls during the weekend or on a bank holiday, the reporting may be submitted the next working day, as it is the case for the intermediate and final reports in the draft RTS). Without this possibility, the financial entity (FE) must maintain 24/7 staffing with the ability to classify incidents, placing a significant burden. In some cases, more time may be required for classification than 24 hours after detecting the incident, especially if it is recognised after 24 hours that the incident is major. Even then, a report should be considered duly submitted if plausible reasons for the delay are provided.
b) adequate time must be allowed for the submission of an intermediate report, because the reporting data are extensive, involving various functions in the FE and possibly the incident-triggering ICT TPP. Therefore, the 72-hour period should commence from the initial notification, not from the classification of the incident as major, and it should refer to the next working day. One hour following regular starting time of the next working day is insufficient to obtain and fill in the information if weekends or public holidays fall within the 72-hour period.
c) in cases where the resolution of the major incident takes nearly or more than 1 month, sending the final report one day after the final resolution of the incident is too short. We propose that the final report be submitted within one month of the incident being resolved.
Article 6(3) overwrites the adjusted timelines in Article 6(2) for significant institutions (Article 6(4) EU 1024 /2013). According to Art 20 the ESAs should take into account the size, overall risk profile, scale and complexity of a FE. The classification of an institution is in our view not sufficient. The impact of an institution on financial stability is also defined by the preferred resolution strategy set by the SRB. Institutions which are subject to simplified obligations (in accordance with Article 11 of EU 806/2014) and for which the preferred resolution strategy in normal insolvency do not pose a threat to the financial system and financial stability. As such, significance should not be a criterion for overwriting the adjusted timelines in isolation and Article 6(2) should also apply to these institutions. We propose to explicitly exclude these institutions from Article 6(3) (e. g. ‘or that the FE is a significant credit institution unless simplified obligations apply’).

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 information required for the initial notification is too detailed. We recommend that it be based on the PSD2 reports. In particular, we suggest deleting the following fields in the initial report or moving them to the interim report:
Fields 2.7 - 2.15: only require in the interim report in order to achieve a high reporting speed in the initial report. Many of the details are also not yet available in the initial report. This applies in particular to fields 2.8-2.10, which relate to the effects on other FEs/ ICT TPPs, and fields 2.14/2.15, as an emergency plan can only be activated after the initial report.

In the interest of early and efficient reporting, we suggest that if the incident is triggered by an ICT TPP, the ICT TPPs should have the possibility to prepare the initial report on behalf of the affected FEs in a consolidated form with the general information about the incident.

Information on the field size limitation (alpha numeric) would be useful and helpful.

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.

It is not clear how operations being restored is defined, i.e. partial or full recovery. The impact on other financial entities (2.8, 2.9) is likely beyond the knowledge of the entity.
Too much individual information with too many detailed descriptions is required for proper and efficient reporting. We recommend focusing on concise, meaningful information about the cause and handling of the incident as well as information to minimize the risk of infection of other FE's or to inform entities about new attack scenarios or vulnerabilities, analog to the interim report in PSD2.
Field 3.1: The purpose of this field is not clear, 3.2 is the key field for identification. Please delete field 3.1. If field 3.1 is not deleted, the field should be required as part of the initial report.
Field 3.38: A financial entity should not be responsible for reporting the actions of a CSIRT in an incident report and it is unclear what the purpose of this data field is. Please delete field.
Field 3.41: Disclosure of vulnerability information poses a significant risk to cybersecurity, therefore the financial entity must be able to decide for itself whether and what detailed vulnerability information is reported.
If the incident is triggered and processed by an ICT TPP, the ICT TPP should be allowed to submit the consolidated interim report on behalf of the affected Fes and limit itself to the information known to it – duration, causes, technical effects and treatment, see answer to question 6.

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

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

Field 4.4: It is not clear what is meant by "information on the inability to meet legal requirements".
Please specify or give examples. Field 4.10: It is unclear which incidents reach the level that requires reporting to resolution authorities via an incident reporting mechanism. Incidents that have an impact on the capital and/or liquidity of critical financial entities are considered serious incidents with a significant economic impact. Regulators are likely to be involved and a DORA-based incident report would be an inappropriate mechanism for informing regulators. Proposal: Delete or mark as "not mandatory".
Field 4.13: Suggestion: "Yes, if applicable", as this threshold is only reached in a few cases.
Fields 4.15-4.24: A detailed breakdown of all costs and losses in the final report goes far beyond efficient reporting.
At the time of the final report, there are usually no concrete figures available (especially for indirect costs) and they have to be estimated based on empirical values. The annual report of the financial entities (see DORA Article 11(10)) already contains the "costs and losses of incidents" for reporting purposes. Additional information in the final report is disproportionate in terms of costs and benefits. This report should be limited to the estimated total costs if the "economic impact" criterion has been met or as an optional disclosure.

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.

As the reporting of cyber threats is voluntary, as few mandatory fields as possible should be defined here (only: information about the facility, description including causes and information on how to deal with it). An uncomplicated reporting rule that requires little effort encourages willingness to report. The specific instructions for field 14 in ANNEX IV suggest that there should be mandatory reporting of potential vulnerabilities and affected systems. This information can only be provided at an abstract level, but a list of specific vulnerabilities and affected systems represents a very high risk if this information becomes known. We request that the field description be clarified to state that it should be abstract information. We propose to change the field to "optional".

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

- ○ Yes
- ◉ No

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

Article 6 ITS 20b (outsourcing of the notification): It should be sufficient if FE informs the competent authority about the outsourcing once (and not for every incident) and then only in case of changes (change of ICT-DL, termination of outsourcing).
ICT-related incidents can result from an incident at an ICT service provider. In this case, only the ICT service provider can provide information about the cause of the incident and initiate the (technical) measures to rectify the incident. According to DORA, the FE can outsource the reports to the ICT TPP. According to Art. 19 (1) DORA, the reports should contain all information required by the competent authority to determine the significance of the serious ICT incident and to assess the potential cross-border impact. However, the notification procedure outlined in the draft RTS/ITS would place a heavy burden on ICT service providers and /or financial companies, as notification is only permitted on an individual basis. We propose to amend the procedure so that the reports are completed by the ICT TPP and submitted only once to the national authority, supplemented by a list of affected financial entities that have authorized the ICT TPP.
This procedure enables fast and effective reporting on the causes and handling of the incident "at first hand", but also ensures that the financial institution reports its specific information individually, but that identical information only needs to be reported once. At the same time, this procedure makes it easier for the financial supervisory authority to evaluate the incident quickly and provides a better overview. If the same incident is reported several times per institution, it is difficult or impossible for the financial supervisory authority to recognize that it is one and the same incident.
In addition, global institutions generally have global systems and global incident management. Solo reports from individual legal entities within a group cannot be used to draw conclusions about the specific impact of an incident within the group.

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

Contact

Contact Form