German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Public consultation on draft RTS on the content of thenotification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat (JC 2023-70)

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Frank Trojahn
Telephone: +49 30 20225-5513
E-mail: frank.trojahn@dsgv.de

Berlin, 2024-02-27

General drafting principles

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

Comments Public consultation on draft RTS on the content of thenotification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat (JC 2023-70)

Question 1. Do you agree with with the proposed timelines for reporting of major incidents?
No
1b. Please provide your reasoning and suggested changes. Art. 6 (1): The deadlines set (4h/24h for the initial report, 72h for the interim report) mean an unnecessary reduction in processing time compared to PSD2.

At the very least, however, weekends and public holidays should be excluded. Otherwise, an inappropriate increase in resources would be necessary for an on-call service without the added value being clear. Furthermore, it is unclear whether the message recipient will process the messages 24/7.

Proposal: The first report should be made within the next working day at the latest (instead of within 24 hours).

Sufficient time must be allowed for the interim report because the notification data is very extensive and various departments in the FE and possibly at the ICT service provider must be involved in collecting the data. The 72-hour period should therefore begin with the first notification, not with the classification.

In the event that the resolution takes almost or more than a month, the deadline for submitting the final report one day after the final resolution of the incident is far too short. Sufficient time is needed to coordinate the information within the bank and, if necessary, with the initiating ICT service provider. We suggest that the final report be submitted within one month of the submission of the last interim report.

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?
No
2b. Please provide your reasoning and suggested changes. The information required for the initial report is too detailed. We recommend orientation to 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 (see answer to question 6).

Information on 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?
No
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 FIs or to inform institutions about new attack scenarios or vulnerabilities, anlaog 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 institution 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 institution must be able to decide for itself whether and what detailed vulnerability information is reported.

If the incient is triggered and processed by an ICT TPP, the ICT TPP should be allowed to submit the interim report in a consolidated form on behalf of the affected FEs and limit itself to the information known to it - duration, causes and technical effects as well as 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?
No
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 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 generally no concrete figures available (especially for indirect costs) and they have to be estimated based on empirical values. The annual report of the financial institutions (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 criterion ''economic impact'' 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?
No
As the reporting of cyber threats is voluntary, as few mandatory fields as possible should be defined here (only: information on 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.

Comments Public consultation on draft RTS on the content of thenotification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat (JC 2023-70)

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?
No
Art. 6 ITS 20b: It should be sufficient if FE informs the competent authority about the outsourcing once (and not for every incident) and then only in the event of changes (change of ICT-TPP, termination of outsourcing).

If ICT-related incidents result from an incident at an ICT service provider, only the latter 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 reporting procedure outlined in the draft RTS/ITS would place a heavy burden on ICT service providers and/or financial undertakings, as reporting is only permitted on an individual basis.

Proposal: The reports can be completed by the ICT TPP and submitted only once to the national authority, supplemented by a list of the financial companies concerned that have authorized the ICT TPP. This will ensure fast and effective first-hand reporting on the causes and handling of the incident. It 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. Individual reports from individual FEs 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?
No comments.