ESMA
Securities and Markets Stakeholder Group

EIOPA - IRSG

eba European Banking Authority
BANKING STAKEHOLDER GROUP

JC 2024 19

10 02 2024

Joint European Supervisory Authority Consultation paper on Draft Regulatory Technical Standards and Draft Implementing 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

Background

The Digital Operational Resilience Act (DORA) mandated the European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) to jointly develop policy instruments, including technical standards, to ensure a consistent and harmonized legal framework in the areas of ICT risk management, major ICT-related incident reporting and ICT third-party risk management for all EU financial entities.

The second batch, that is open for consultation until 4 March 2024, comprises the following:

- RTS and ITS on content, timelines and templates on incident reporting
- GL on aggregated costs and losses from major incidents
- RTS on subcontracting of critical or important functions
- RTS on oversight harmonisation
- GL on oversight cooperation between ESAs and competent authorities
- RTS on threat-led penetration testing (TLPT).

General comments

The Stakeholder Groups (SGs) welcome the opportunity to comment on the *"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 cyberthreat".

In our response, the SGs will concentrate on those elements that we feel competent enough to provide meaningful input on.

The SGs welcome and support the ESAs' general approach of aligning the requirements of this RTS and ITS, to the greatest extent possible, with existing sectoral legal instruments, such as the revised EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2), and the various related Guidelines issued by ENISA under Directive (EU) 2022/2555 (NIS2). The SGs agree that cross-sectoral harmonisation is essential given that ICT incidents and cyber-threats are not inherently sector-specific and should therefore be addresses in a consistent manner that concentrates on the nature and significance of the incident or threat rather than the place where it originates or is first detected. Within the financial sector, a degree continuity of reporting requirements with existing, proven incident reporting frameworks is, of course, highly desirable to reduce implementation costs and capitalise on existing investments in infrastructure, systems. skills and experience.

Questions for consultation

Q1. Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

The SGs largely agree with the ESAs proposal to introduce harmonised timelines for all financial entities across all sectors (policy option 1a).

While the SGs acknowledge that some of the sectors covered by DORA operate in very different ways – including, in particular, the architecture and use of ICT systems and the frequency and 'cycle time' of transactions – they appreciate that ICT-related risks are capable of propagating rapidly and across sectors. It is of critical importance, therefore, for financial institutions – as much as for other providers of essential services that are subject to similar obligations, e.g. under Directives (EU) 2022/2555 (NIS2) and 2022/2557 (CER2) – to adhere to consistent, harmonised timelines. Moreover, some entities subject to incident reporting under DORA may be in scope of more than one regulator; different timelines could create uncertainty and needlessly complicate the implementation process for these entities.

From a sectoral perspective, however, some members of the SGs observe that the proposed timelines may not be feasible to implement for the insurance sector, in particular. They note that these deadlines are stricter than any comparable legislation that applies to the sector – e.g. 72 hours under GDPR or 24 hours for an 'early warning' under NIS 2. They suggest that a more appropriate timeline would be for an initial notification to be submitted, at the latest, within 24 hours after classification, or on the next working day if the due date a major incident is detected on a weekend or bank holiday. They propose that the intermediate report could be submitted within ten working days of the initial notification, and the final report within 30 working days from the permanent resolution of the incident.

The SGs emphasise that proportionality must be maintained in order not to overload smaller entities which may have limited capacities and may therefore be less capable of detecting, analysing and reporting on ICT incidents than their larger peers. The SGs therefore welcome the provisions in Article

6(2) and 6(3) RTS, which exempt financial entities from the obligation to file intermediate and final reports for major incidents over the weekend or bank holidays if they are not classified as 'significant' or the incident does not have a systemic or a cross-border impact. The SGs are satisfied, moreover, that a significant degree of proportionality is already reflected in the criteria for classifying an incident as 'major' and refer to their comments to the ESAs' earlier consultation on this matter.

The SGs note that the ability of financial entities which rely on third-party providers (TPPs) to operate some or all of their ICT services to report on major incidents in a timely manner critically depends on the alertness and responsiveness of these TPPs. An incident that occurs within the sphere of the TPP and affects the operations of a financial entity may not immediately be detected by the financial entity. Instead, the financial entity may be reliant upon the TPP to issue an alert. The responsibility for timely reporting, however, still lies with the financial entity unless incident reporting itself has been outsourced (Article 6 ITS). It is important, in any event, that the relevant service-level agreements are consistent with financial entities' obligations under DORA. It may be helpful, in this context, for the incident reporting framework to provide additional transparency on the effectiveness of these arrangements so that regulation and supervision can be designed and calibrated more effectively.

The SGs agree with the principle of aligning the reporting framework under DORA as much as possible with that of NIS2, subject to adjustments for financial-sector DORA specificities (policy option 2b).

Given the interconnectedness of the financial sector, and the potential systemic risk arising from a major incident, the introduction of a shorter notification period (24 hours from detection) and of an additional criterion (4 hours after the incident has been classified as 'major') appears appropriate and prudent. The SGs notes, however, that the rationale for extending the deadline for submission of the final report from 20 days (under NIS2) to one month is not well explained in the draft RTS. The SGs appreciate that a balance needs to be struck between the objectives of incentivising entities to report, resolve, and analyse major incidents rapidly, on the one hand, and the need to allow for a thorough forensic analysis and ex-post assessment, on the other. The draft RTS appears to prioritise the latter – if so, the argument should be spelt out more clearly.

Q2. Do you agree with the data fields proposed in the draft RTS and the Annex (I and II) to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree with the ESAs approach to differentiate between essential, mandatory data fields and additional, optional data fields that provide valuable information for supervisory, regulatory or statistical purposes (policy option 3b).

The SGs agree, in principle, with the proposed format and data fields of the initial report, subject to the following observation:

- As mentioned previously (Q1.), additional information on the circumstances of the detection of a major incident could be useful for supervisory authorities to evaluate the effectiveness of outsourcing arrangements, and the attendant sharing of monitoring and incident reporting responsibilities. With respect to fields 1.16 and 1.17 it may be of considerable relevance for the assessment of the incident by supervisory authorities to include information on whether the

incident was detected by the affected TPP or by the financial entity. An additional, optional data field could be added for that purpose.

- Some members of the SGs observe, however, that certain data points, in particular items (d), (e), (g) and (h) from Article 3, might be included more appropriately in the intermediate or final notification as this information may be too burdensome to collect at the time of the initial notification, or might not yet be available.

Q3. Do you agree with the data fields proposed in the draft RTS and the Annex (I and II) to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree, in principle, with the proposed format and data fields of the intermediate report, subject to the following observations:

- For the purposes of completing fields 3.8 to 3.10, financial entities are required to make an assessment of the number/percentage of financial counterparties affected by the incident and the impact of the incident on these counterparties. The SGs agree with the intended purpose of this information, i.e. to alert supervisors to potential spillover effects and any risk of cross-border contagion. Financial entities may find it difficult, however, to provide accurate, factual information on these points at the time when the intermediate report is due, i.e. most likely before a comprehensive forensic analysis could have been completed. The draft RTS should therefore be amended to clarify that the reporting entity would only be expected to provide a preliminary assessment on this stage, based on available information and reasonable assumptions. This preliminary assessment should then be updated and completed in the final report.

- Some members of the SGs expressed concerns that the timeline of 72 hours may not allow sufficient time for companies to provide material updates. They suggest that reporting should be reduced so as to not pose an excessive burden while the incident is ongoing. In particular, they suggest that information already covered by the initial notification (items (d) and (e) of Article 4) should be limited, and non-essential information that will require more time to be collected (items (b), (k) and (l) of Article 4) should be moved to the final report.

- Some financial entities also expressed concerns about the breadth of the requested information on affected infrastructure components (field 3.31). They argue that the list of components is too detailed, bearing in mind that many components may be affected in a major incident. The SGs are of the view that the relevance of this information depends materially on the nature of the incident. Reporting at the proposed level of granularity appears justified if this information appears relevant to assess, in particular, the potential cause, scope, or systemic risk, i.e. the speed and scale of propagation, of the incident. A detailed list should be provided in the final report, in any event.

- For the purposes of correctly determining the time for submission of the intermediate report (item. b. of Article 6(1) RTS), it would be helpful to define in more detail when *"regular activities"* are deemed to "*have been recovered and business is back to normal"*. In particular, it appears unclear if all services have to be restored to or whether a partial resumption of services would be considered sufficient. Similarly, it is not entirely clear if services should be considered as having been restored as long as 'temporary actions' (field 3.37) are still in place.

Q4. Do you agree with the data fields proposed in the draft RTS and the Annex (I and II) to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree, in principle, with the proposed format and data fields of the final report, subject to the following observations:

- As for the intermediate report, the conditions for submission of the final report (*"the incident has been resolved permanently";* item. c. of Article 6(1) RTS) should be defined more precisely. The SGs are mindful that the problem management process may be complex and time-consuming, and may not be completed within one month even though normal operations may have been fully restored by then. Arguably, the final report should be submitted at the earliest possible time, but not until the root cause of the incident has been identified and analysed, and a permanent fix has been applied.

- In the present draft ITS, financial entities are required to provide a description of data losses associated with the incident (field 3.23). According to the current wording, "the financial entity may also indicate the type of data involved in the incident." The SGs are of the view that this wording suggests a degree of optionality that does not correspond to either the classification of the item in this ITS (as 'mandatory' for both the intermediate and final report) or the separate, but related legal obligation to report a 'personal data breach' to the competent authority under Article 33(1) of Regulation (EU) 2016/679 (GDPR) within 72 hours of its detection. In the interest of legal consistency, transparency, and procedural efficiency, the SGs would suggest to add clear instructions in this field that any loss of personal data in the context of the incident would be have to be notified, assessed and, if appropriate, notified to the competent authorities.

- Some members of the SGs are of the view that the current deadline for the final report –one month after the incident or one day after closing – may not be feasible, especially in the insurance sector, as financial entities will be focused on resolving the incident and not have sufficient time to gather the necessary data.

Q5. Do you agree with the data fields proposed in the RTS and the Annex (III and IV) to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.

The SGs agree with the ESAs approach of creating a simple, low-barrier template to encourage financial entities to report cyber threats, which is voluntary. In the interest of making this data usable, e.g. for sectoral/cross-sectoral threat analysis and statistical purposes, a broad categorisation, in addition to the threat description (field 14), may be useful. These broad categories could be based, for instance, on the list used by ENISA in its periodic Threat Landscape (ETL) report. This categorisation may require inserting an additional, mandatory data field.

Q6. – Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

The SGs agree in principle with the ESAs proposed approach. They note, however that if an incident affects several financial entities within a consolidated group, it should be possible for them to file one consolidated report, by the parent company, provided that all affected entities are supervised by the same competent authority. Some members of the SGs suggest that it should be possible for financial

entities to submit the reports in any of the official EU languages, including English, as the need to translate them for the regulator prior to submission may cause delays.

This advice will be published on the websites of the European Supervisory Authorities.

Adopted on 10 March 2024

[signed]	[signed]	[signed]	[signed]
Rim Ayadi Chair Banking Stakeholder Group	Michaela Koller Chair Insurance and Reinsurance Stakeholder Group	Veerle Colaert Chair Securities and Markets Stakeholder Group	Christian Stiefmueller Rapporteur