DORA - Draft RTS (Second Batch)

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

March 2024

Executive Summary

AFME welcomes the opportunity to respond to the draft RTS and ITS on incident reporting under DORA. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors, and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

Our response to this consultation is from the perspective of our bank members, focusing on those issues which are most relevant to wholesale capital markets. We are responding to each of the specific questions set out in the consultation paper, but wanted to raise the following overarching points:

1. **Seeking too much information at the earlier stages will detract financial entities from focusing on incident management during the critical stages of an incident. Quantification of the impact, especially among third parties, should be relegated to the final report.**

   The proposed incident reporting requirements would see a lot of information submitted at the intermediate phase which would entail significant time and effort to collate, for example around the calculation of costs or economic impact. We strongly recommend that this type of information should only be required at the final stage in order to give financial entities maximum discretion during the critical stages of an incident to focus on threat mitigation and enacting remedial measures to prevent onward disruption or contagion. While the level of data fields correlate strongly with PSD2 incident reporting, payment incidents are unique and, as opposed to ICT or application incidents, map directly to specific criteria such as transaction amounts, clients affected or geographic location. Related to this, authorities should not be requiring financial entities to measure the economic impact of an incident outside their own group structures and operating models, for example within third party providers. Such data is dependent on other entities providing information to the financial entity and is therefore inevitably going to cause delay. We recommend that the financial entity should only report *'if'* a third-party provider has been impacted in the initial and intermediate reporting, while the final report should take account of the possibility of delay, where the information is not directly within the purview of financial entities themselves.

2. **The proposals create misaligned requirements on incident reporting for significant credit institutions in light of parallel ECB reporting obligations. The ESAs should work with the ECB on ensuring future alignment with DORA.**

We welcome the explicit *lex specialis* exemption from NIS2 reporting and the ESAs assurances that incident reporting under DORA will satisfy all PSD2 requirements. Significant credit institutions will however continue to be required to issue separate incident notifications to the ECB using the ECB's own reporting platforms and templates. The duplication may be justifiable for this subset of financial entities but reinforces the need for consistent and aligned reporting thresholds and timelines, to ensure that the entities in question can issue reports swiftly and efficiently, while focusing on actual incident management. This is not currently the case, for example over the timeframes for initial notifications. In addressing such misalignment, we encourage the ESAs to take account of the FSB work on incident reporting convergence, and to seek to harmonise where possible. We additionally note that the NIS2 Directive comes into application ahead of DORA, and so would seek confirmation that no reporting under NIS2 is expected ahead of January 2025 when DORA comes into application.

3. **Remove data fields which request confidential information to avoid breaching contractual sureties and legal principleS.**

The proposed templates request certain information which is not currently required under regulatory reporting, and which will often be subject to contractual restrictions. We highlight specific examples in Q4 of such instances, and as a rule would argue that such data requests do not sufficiently relate to the incident, or incident management, as to be relevant for the purposes at hand. We strongly encourage such confidential information not be requested in these reports, and the respective data fields be removed.

4. **Review the upcoming FSB work on international convergence in incident reporting, to facilitate alignment with future global standards.**

There is ongoing work at an international level on developing a consistent global framework for incident management, including the FSB's work on the FIRE framework. International consistency is particularly important for incident management, as many incidents may have international impacts, or international causes. Alignment between EU authorities and authorities in other jurisdictions will support global responses to incidents and coordination between authorities, as well as streamlining incident management processes for financial entities. As such, we would urge the ESAs to embed within the RTS specific provision for future reviews of the DORA incident reporting requirements, to facilitate alignment with international standards as these are developed.

Please see below our responses to questions 1 – 6. We remain available to discuss further any points raised.

Consultation Questions

Question 1 **Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.**

- We welcome the efforts of the ESAs to embed proportionality within the upcoming reporting templates, especially the recognition that some incidents will not be resolved within a default one month timeline for the final report. Allowing postponement of this report until the incident has been fully resolved will ensure that the final report has maximum value and is of most use to authorities. In line with this approach, we would further urge that the final report be due one month *after business has returned to normal* rather than from classification. This alignment with PSD2 would ensure authorities receive a final report which is as holistic as possible.

- We flag however that the timeframes are not consistent with those set out for significant credit institutions as part of ECB supervision. The initial notification for ECB cyber incidents must be submitted within two hours of classification as significant, rather than the four hours proposed in the draft RTS. Additionally, the decision to alternate between NIS2 and PSD2 thresholds, relying on the former for the final phase timelines but the latter for the initial phase, has caused a degree of confusion. We propose aligning with the NIS2 wording in that submission is due: "*without undue delay […] and in any event within X following*" (as opposed to relying on the triggers set out within the consultation paper background). In summary, we recommend as timeframes the following, and will be seeking subsequent alignment by the ECB:

    - Initial: 4 hours from moment of classification
    - Intermediate: 72 hours from moment of classification
    - Final: One month *after business has returned to normal*.

- As worded Article 6(1) (a) of the draft RTS also sets out that the initial report shall be submitted "*no later than 24 hours from the time of detection of the incident*". In some instances, an incident may be classified as major more than 24 hours after its detection or may escalate to being a major incident over this timeframe. As such, the requirement to submit the initial report no later than 24 hours from the time of detection of the incident may cause financial entities to significantly over-report non-major incidents to avoid potential non-compliance in the event that these incidents might become classified as major at a later point. This could absorb substantial capacity amongst both the financial entities and authorities and detract from the incident management capabilities of both. In line with our point above, we propose that this provision be removed. If competent authorities have concerns that financial entities are unduly delaying their classification of incidents to defer reporting requirements, this could be dealt with through normal supervisory channels, without engendering a risk of over-reporting.

- We also request clarification concerning the use of secure channels as mandated by Article 4 of the ITS and the process for the reporting of incidents. Articles 21 and 22 of the DORA text includes references to the centralisation of reporting, however no information is provided as to the secure channels which must be utilised. The lack of information concerning the channel for reporting impacts the compliance programmes of financial entities and blocks the ability for entities to commit build cost for embedding incident reporting through their entities. Further, in relation to Article 4(3) of the draft ITS, financial entities would welcome clarification concerning the secure channel to be utilised to inform authorities that they have been unable to submit notifications or reports according to the DORA deadlines. Financial

entities would welcome clarification whether a report will include all fields, even if they are non-applicable, to be included within each reporting stage. This additionally impacts compliance programmes and internal product building.

- We request that greater consistency between incident reporting classification criteria and the instructions or descriptions within data fields is maintained. The incident classification criteria for economic costs and losses clearly state that these "*shall not include costs that are necessary to run the business as usual*." This is additionally repeated withing the guidelines on aggregated costs and losses. We believe this should be further embedded within the costs and losses data fields (4.13-4.25) and, most notably, in relation to staff costs. The recitals could, in addition, confirm that all incident fields on costs and losses are in line with the proposed incident classification RTS Article 7 and Article 18(3) DORA.

- We note the ESAs are applying proportionality to incident reporting by allowing microenterprises to not report incidents during the weekends or when national holidays are occurring within the relevant member state. AFME believes this should be expanded to all financial entities. Financial entities with numerous operations across member states face the same difficulty in obtaining all relevant information for intermediate reports within weekends and national holidays. Incident reporting response teams are available to significant institutions because of mature risk management practices, however, product teams that provide information concerning fields such as reputational impact, communication to clients or a description of CSIRT involvement are not available outside of normal business hours. Major incidents with a material impact will include supervisory attention for significant financial entities and it is unclear how reporting entities will use intermediate or final reports during weekends or national holidays.

- We support the fact all three reports can be submitted collectively if appropriate.

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? If not, please provide your reasoning and suggested changes.**

- In the instructions for data field 1.16 it states that "*Where there are multiple third party providers affected, the financial entity shall provide the names of all affected third party providers*". In practice it will not be possible for financial entities to list all affected third party providers. We would propose that this be amended to refer only to "*known third party providers*" and should be on a 'yes, if applicable' basis, enabling FEs to focus on those entities who have reported a knock-on impact.

- As AFME highlighted during the earlier consultation on classification of major incidents, there are major difficulties for financial entities in gauging the impact of an incident outside their own financial entity or group structures, for example within third party providers. Such information can only be accurately assessed by those providers themselves and subsequently requested by the financial entity. There is no ability to compel or verify the information

provided, and it will almost certainly cause delays in reporting. It is therefore information which is, at the very least, not suitable for the initial notification phase, certainly in terms of providing detailed descriptions of how an incident could be affecting these other entities. We therefore recommend:

  - Data fields 2.9 and 2.10 be deleted.

  - Data field 2.8 be framed as a binary YES/NO option, with no including *no information available* as set out in the glossary instructions. At the initial stage the focus should be on identifying the parameters of an incident, rather than the level of impact.

- Similarly, in many cases it will be extremely difficult for financial entities to determine recurrence in the early stages of an incident. Doing so is a difficult and time-consuming task and may be impossible until much more information is available. We are of the view that diverting resources and attention from active incident management to attempting to determine common root causes would be contrary to the interests of both financial entities and the authorities. As such, we recommend that all references to recurrence should be deferred to the final report. Specifically, we propose:

  - Data fields 2.11 and 2.12 / RTS Article 3(h) be deleted.

- We also recommend that information on how business continuity plans (BCPs) have been executed is similarly deferred until the final report, with the intermediate report identifying simply whether BCPs have been invoked within the first 72 hours of an incident. We therefore recommend:

  - Data field 2.14 / RTS Article 3(i) and data field 2.15 be deleted.

- In order to bolster consistency across regulatory reporting, we additionally recommend that ECB terminology is applied where possible, for example data field 2.6 be reframed as incident classification. We also note that seeking contact details for a function, rather than specific person, may be more practical and fool-proof.

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? If not, please provide your reasoning and suggested changes.**

- With regards to the intermediate reporting, AFME stresses that authorities should not be looking to quantify the total impact of an incident until the final report, especially in light of the currently proposed 72-hour time limit. Such information will typically only be available at a later stage and will require substantial effort to accumulate. We recommend that for the intermediate report, authorities seek only a binary YES/NO determination as to which classification criteria have been impacted, and whether the associated materiality thresholds have been met. The full quantification of impact for each criterion should be deferred until the final report. We recommend:

- Data fields 3.6 – 3.13; 3.15 – 3.18; 3.20 and 3.22 be revised as binary YES/NO options.

- Data fields 3.14; 3.19; 3.21 and 3.23 would consequently be superfluous and we recommend these are deleted.

- By the same reasoning, the proposal to collate information on affected infrastructure components, indicators of compromise and exploited vulnerabilities should be deferred to the final report, and subsequently reported on an anonymised basis. Any onward sharing of non-anonymised information, for example between authorities, could pose a significant security risk. This information will require an analysis which is not feasible within the proposed 72-hour timeframe for intermediate reporting and could restrict a financial entity's ability to manage and mitigate live incidents. We recommend:

  - Data fields 3.30, 3.31/ RTS Article 4(f) be deleted.

  - Data field 3.40 / RTS Article 4(l) be deleted.

  - Data field 3.41 / RTS Article 4(k) be deleted.

- Regarding data field 3.33 on communications to clients / financial counterparts, the detail proposed to be included would be extremely onerous to be provided during a live incident management situation. As discussed previously, this could be detrimental to incident management efforts. The information should only be shared at the final report, with the principle of proportionality applied by allowing FEs to focus on those communications which are relevant to incidents where the FE has identified an actual impact on the financial interests of clients and counterparts. We recommend that:

  - Data field 3.33 be deleted.

- We are also concerned with the proposed data fields on remedial actions "*which have either been taken or are planned to be taken"*, and the subsequent request for information on CSIRT involvement. Collating and providing such information in advance of actual remediation presents a possible security risk and goes beyond existing practice. Despite the reliance on secure communication channels, authorities should not be seeking such information on a quasi-real-time basis. We recommend:

  - Data fields 3.36 – 3.39 / RTS Article 4(j) be deleted, with a full overview of remedial measures captured *ex post facto* in the final report.

- Similarly, regarding indicators of compromise, it is critical that these communications remain as secure as possible. Channels already exist for the secure sharing of indicators of compromise, and it is our view that these should continue to be used in favour of new, untested communication means which are likely to be less secure and which could pose substantial risks to financial entities. As such, we recommend:

  - Data field 3.40 be deleted.

- Additionally, we call for a replication of proposed data fields 4.11 and 4.12 / RTS Article 5(f) on the possible reclassification of a major incident as non-major, to allow this remediation at the earlier stage if already known.

- We also flag that data field 3.24 refers to materiality thresholds for the criteria "*critical services affected*" despite these being removed in the final report, published 17th January 2024.

- Finally, the ESAs' webinar confirmed that the incident reference code will be maintained throughout all reporting stages, as opposed to PSD2 where multiple references codes are provided. Multiple codes add complexity and block automated incident response mechanisms being developed within financial entities and AFME welcomes this development.

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? If not, please provide your reasoning and suggested changes.**

- AFME believes that the incident reporting regime for recurring incidents is highly burdensome for financial entities to implement. The incident classification RTS Article 15(1)(b) infers that the root causes in data field 4.1 will be used to determine if there has been a recurrence. The root causes listed, however, remain high-level and a small proportion of root causes, such as change management and software compatibility, will likely disproportionality trigger reporting on the basis of recurrence. An incident may have a change management root cause that is significantly different to another incident with differing incident management controls, processes or error. As the stated purpose behind reporting recurring incidents is to indicate "*significant deficiencies and weaknesses in the financial entity's incident and risk management procedures*," we believe there should be greater recognition of the FE's ability to determine if a root cause has repeated. Recurring reporting, due to high-level root cause criteria, would result in material overreporting due to a concentration of incidents relating to specific causes and improper reporting due to a lack of direct link in incident management procedures between incidents. We therefore propose that a financial entity can determine when a root cause is recurring within the data field 4.3 and the data field 4.1 is maintained for normal incident reporting-only. We recommend:

    - Data field 4.1 Root causes of the incident; Instructions: "The following categories shall be considered <u>unless being reported as a reoccurring incident:</u>"

    - Data Field 4.3 Information about the root causes of the incident; Description: "Description of the sequence of the events that led to the incident <u>and description of root cause similarity when being reported as a recurring incident</u>."

    - Data Field 4.3 Information about the root causes of the incident; Instructions: "Description of the sequence of events that led to the incident including a concise description of all underlying reasons and primary factors that contributed to the occurrence of the incidents. <u>Include description of how the incident has a similar apparent root cause if the incident is classified as a recurring incident. The data field is mandatory if the incident is classified as a recurring incident</u>."

- AFME recognises that the types of costs to be captured within the final report must sync with the final RTS on classification of major incidents, thereby limiting the level of discretion at this stage. Nevertheless, we caution the ESAs against requiring financial entities to disclose confidential information concerning clients, entities, and contracts. Data fields 4.4, 4.5 and 4.18 all require entities to provide regulators and supervisors with confidential information. It is also unclear how each respective data field correlates to the assessment of an incident, its impact, or the response of the financial entity to resolve the incident.

    - Data field 4.4 / RTS Article 5(b): A financial entity will not be comfortable hypothesising their potential legal exposure within regulatory reporting. There are material consequences to providing details regarding how a financial entity may have failed to comply with the law, especially if shared with their financial regulators and supervisors. Financial entities, when responding to ICT incidents, will focus on root cause identification, incident containment, remediation, and management of communications with and continuing to support our clients. An exercise of identifying all relevant regulations and speculating their potential for non-compliance across all relevant articles does not meaningfully contribute to common risk management practices or the resolution of the incident and the entity's services. This data field / clause should be removed.

    - Data field 4.5 / Article 5(c): Contractual arrangements and SLAs are confidential, and a financial entity would not provide details concerning confidential client information within regulatory reporting. As a financial entity will have to list client and financial counterparts within reports (3.6 - 3.10) and the costs of non-compliance (4.18), there is a risk that descriptions of contractual arrangements or SLAs could be linked to specific clients of the financial entity. This could place legal risk on the financial entity if costs were able to be linked directly to a client. As the data field does not relate to the incident and could reflect confidential information, we recommend this data field / clause are removed. Any specific concerns by authorities should be disclosed separately on request.

    - Data field 4.18: As mentioned above, contractual obligations constitute confidential information. There is a risk both that costs could be directly linked to specific clients included within the incident report and that this could potentially affect a financial entity's self-defence rights against certain clients/counterparties. Such contractual costs do not inform the risk assessment of the specific incident and are not linked to how the incident was resolved, the root cause or the impact of the incident, rather, they depend on the service offered and the specific contractual arrangement with the individual client. We recommend that the data field is removed.

- Additionally, we highlight:

    - Data field 4.1: In some circumstances the root cause may be impossible to discover (e.g. incidents related to actions by highly sophisticated state actors). In such cases financial entities may not be able to state the root cause with certainty. Caveats to this effect should be included in the definition of the data field.

    - Data field 4.8: The date and time an incident is resolved, and root cause addressed can be different. We recommend this is split into two separate data fields. Further

clarification on what amounts to permanently resolved has also been requested, noting this is again distinct from addressing the root cause.

- Data field 4.10: Information relevant for resolution authorities will be extremely rare. This should only be completed on a "yes, if applicable" basis, rather than mandatory.

- Data field 4.20: it is evident that the scope of forgone revenues remains open to interpretation and is flagged that this concept is not included in CRR3.

- Data field 4.24: Similarly, the "amount of financial recoveries" will be complex and will be difficult to report at any particular given time. This field should be optional.

- Finally, while banks will provide information to the best of its abilities, we stress that the final report should be timebound, in that it sets out or estimates the most accurate information/data available at the time in question, and there is no expectation on financial entities to update the final report if further information/detail becomes available at a later stage. Key updates can instead be incorporated or captured within the upcoming annual reporting processes, outside the incident reporting timeframe.

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? If not, please provide your reasoning and suggested changes.**

- We agree with proposed data fields in Annex III.

- This section would though benefit from clearer definitions of what would be considered a significant cyber threat suitable for notification and when it should be reported. As it stands, this is ambiguous. Additionally, the requested fields for cyber threat notification should be flexible to allow organizations to report any type of cyber threat which meets the significance criteria, along with known details of their likely attack path or third-party providers.

- Authorities should also be mindful of not seeking information on potential vulnerabilities which may be confidential: for example requiring confidential information as part of the description of a cyber threat and related risks.

- Finally, the method for significant threat notification is not clear, including whether this will be the same method as proposed for major incident reporting.

Question 6 **Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.**

- Firstly, we highlight there is a degree of concern over the proposed use of XBRL, given its complexity and unsuitability for operation in degraded mode. We recommend the permissibility of other formats, including CSV and JSON, to ensure that reporting is not unintentionally hindered, and do not see how this would create any compromise in terms of security or integrity of the data. It is also unclear whether individual reports will need to be

filed in each member state for incidents that impact multiple entities of a broader organisation. A single report should be required for each incident, and the impact to outside entities and member states will be addressed within that report.

- Secondly, the use of estimates in lieu of actual figures will at times be necessary, as acknowledged by the ESAs. We suggest though Article 1(3) of the draft ITS be amended to make clear estimates should be used only where data is not available, rather than "accurate data".

- Finally, we again flag that the decision to require solo reporting at the entity level, while consistent with the published final RTS on classification of major incidents, will result in substantial overreporting from financial groups. Similar duplication/overreporting will occur with regards to intragroup providers. Future reviews of DORA should refine the volume of information sought by authorities, removing such duplications, in order to enable more efficient incident response handling.

Contacts

AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@afme.eu
AFME	Stefano Mazzocchi	+32(0) 2883 5546	stefano.mazzocchi@afme.eu
AFME	Coen Ter Wal	+44(0)020 3828 2727	coen.terwal@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/