DORA - Draft RTS

Classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats

September 2023

Executive Summary

AFME welcomes the opportunity to respond to the draft Regulatory Technical Standard (RTS) on *Classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats* under DORA (Digital Operational Resilience Act)[1]. 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 three overarching points:

1. **The cumulative effect of expansive terminologies and low thresholds will result in significant overreporting**

   With the proposed materiality thresholds consistently set too low and numerous terms so vague or open to interpretation that financial entities will err on the side of caution and report, it is almost inevitable that there will be substantial overreporting of incidents as 'major', especially in relation to the article on recurring incidents. This will act as a significant barrier to the ESAs and other supervisors in identifying which incidents are truly capable of becoming a systemic threat. The thresholds should be raised, with quantitative absolute values avoided and the language tightened to reduce the room for interpretation.

2. **The ESAs have gone beyond the Level 1 Mandate in several instances**

   We note that this RTS, in contrast to other Level 2 instruments, has expanded beyond the scope of the Level 1 Mandate, for example in defining reputational risk as a standalone criteria or in setting out requirements for recurring incidents. While there may be reasons for doing so, we note this is an inconsistent approach, for example to the Critical Third Party consultation, where the overlapping criteria within the Level 1 text have been rigidly applied.

3. **Misaligned and rigidly applied regulatory frameworks risks delay and confusion for global firms on when and why to escalate**

   For multinational financial entities, the same threat can span various international borders, bringing numerous reporting requirements into play. Where these regulatory requirements are either too complex or prescriptive, financial entities will struggle to react with speed, especially given how the full set of facts will often not be known in the early stages. The CP itself acknowledges that "*FEs are best positioned to identify their clients, and hence no*

[1] https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTS_on_classification_of_ICT_incidents.pdf

further elaboration of this term is proposed in the CP." This logic should apply across all the criteria with greater flexibility from authorities in how a firm's global systems are relied upon, and less prescriptive in terms of process. Additionally, we appreciate that *lex specialis* will apply to NIS2 in relation to DORA, but encourage the ESAs to produce specific guidance on how the relationship will operate in practice, and to provide reassurance that incident reporting under NIS2 is fully exempted for financial entities.

Please see below our responses on questions 1 – 8. We remain available to discuss further any points raised.

Consultation Questions

Question 1 **Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.**

- We are concerned that the approach outlined fails to closely sync with the DORA definition of *major ICT related incident*, by losing the link with critical and important functions. We would want to see this link restored throughout the classification process and criteria. Given '*criticality of services affected'* is one of the criteria outlined, our proposed solution is:
    - Embed the critical/important functions link into each of the criteria AND
    - Make the critical services criteria, which is already a primary criteria, a mandatory one for classification purposes.

- Additionally, we find the proposed classification matrix too complex and prescriptive, bearing in mind that during an incident financial entities will be focused on incident response and mitigation, and often unable to assess the full set of facts in the early stages. The CP itself acknowledges that "*FEs are best positioned to identify their clients, and hence no further elaboration of this term is proposed in the CP*." This logic should apply across all the criteria, with the conclusion that materiality thresholds should be qualitative thresholds, based on a financial entity's judgment and where relevant their own standards. The inclusion of fixed thresholds with fixed amounts does not reflect an approach based upon proportionality; all the thresholds should be proportionate to the specific size of each financial entity, avoiding absolute measures. Classification should also not be occurring during the incident but afterwards during the post-mortem/post-incident review, once the incident has been mitigated and the full set of facts become available.

- We also flag that it will often be difficult to segregate the data under each of the criteria on an EU-only basis. For many international firms with a global presence it will not be feasible to distinguish the regional impact during an incident.

- Further, the thresholds are set at a mix of legal vehicle levels and group-wide levels. For groups with multiple legal vehicles, entity level calculation could substantially increase the complexity of calculating results, further distracting from incident management at the most critical time. If firms were able to choose whether to calculate a given threshold at an entity or at a group-wide level, this would allow for a less cumbersome assessment.

Question 2 **Do you agree with the specification and materiality thresholds of the criterion 'Clients, financial counterparts and transactions affected', as proposed in Articles 1 and 9 of the draft RTS? If not, please provide your reasoning and suggested changes**

- We propose the deletion of Art 1(3): Financial entities do not have access to the information that would allow them to assess the knock-on impact from an incident on a client or counterpart, including the implications for their business objectives and wider market efficiency. We believe that in practice this criteria would either become meaningless and would be ignored, or it would result in significant amounts of overreporting as firms would have to make significant assumptions. We recommend that this criteria be removed and the focus remain on assessing whether the incident has impacted on the financial entities' clients, counterparts or transactions.

- We support the use of estimates where the actual number of clients, counterparts or transactions cannot be determined, especially as it is common for the final number of clients/transactions affected to only become known at a later post-incident clean up stage. We object though to these estimates being based upon '*comparable reference periods'* which does not have a clear meaning and would be difficult to apply consistently across different types of services and different financial entities. The methodology for estimating should be left for the financial entity to determine based on the unique characteristics of the service impacted and the nature of the incident. This is in line with other references to estimates in this RTS. We also flag that the thresholds of 50,000 clients and 15,000,000 euros for transactions are too low for multinational corporates with institutional clients.

- The reference to 'any impact' in Article 9(1)(f) can be interpreted to include non-critical operations and would lead to over reporting, especially if firms are expected to estimate because of the lack of access to appropriate information. As stated above, firms do not have access that would allow for the assessment of impact on clients or financial counterparts or the subsequent impact that would have on objectives and market efficiency. We propose removing Article 9(1)(f).

Question 3 **Do you agree with the specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes.**

- ***Reputational Impact****:*
  - We highlight that many of the determinants are incredibly vague and expansive, for example '*attract media attention*,' '*received complaints*,' and '*lose clients'*. Such criteria will inevitably lead to overreporting. At a minimum we suggest adding language to limit the assessment of 'reputation impact' to the time of the incident to avoid overreporting caused by criteria being subsequently met in hindsight after the incident, and also making use of the more operational terminology applied by the ECB: "*the incident receives any national or international coverage in major newspapers or news agencies such as the Financial Times, Reuters, Bloomberg, or national equivalents of large audience*". Ideally however, this criteria should reflect the Level 1 mandate, and not sit as a standalone criteria, but as a point of consideration for

firms in assessing how many clients and counterparts have been impacted. The extension of the Level 1 mandate has been noted with surprise given the ESAs' stated intention not to deviate from a strict interpretation of the text in other areas of DORA.

- We also propose the explicit application of the DORA Article 4 proportionality principle. This will give financial entities the freedom to use discretion in assessing reputation impact. As currently drafted, one comment on social media or one complaint could constitute a breach of this criteria, making the criteria irrelevant in practice as this will likely be breached in every incident, regardless of its significance. It is also the case that for a large financial entity, it may not be possible to distinguish between client complaints resulting from an incident and those which originate through error on the client side. Granting firms flexibility will ensure a more tailored application, in line with DORA's objectives in this field.

- Taking account of the above points, Article 2(1) could be amended to "*For the purposes of determining the **substantial** reputational impact of the incident, **bearing in mind the proportionality principle,** financial entities shall take into account the level of visibility that the incident has gained in the market. In particular, financial entities shall, **within reason,** take into account whether one of the following are met **at the time of the incident***"

- With regards to Article 2(c), as currently drafted we believe this will create uncertainty within financial entities and likely lead to overreporting. We recommend that the ESAs adopt the approach in PSD2 (Payments Services Directive) which targets those regulatory omissions serious enough to merit the "*imposition of supervisory measures or sanctions*". We propose amending the wording to *"The financial entity will not be able to or is likely not to be able to **comply with regulatory requirements, resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available** ~~meet regulatory requirements;."~~*

- ***Duration and downtime:***
  - Regarding Article 3 several members have highlighted that measuring the duration of an incident 'from the time it was detected' is in practice the more realistic option, as opposed to "from the time it occurred", under Article 3(1). Additionally "the moment when the incident is resolved" should be clarified to mean "the moment at which the incident is contained or mitigated", as opposed to the conclusion of any retrospective investigation.

  - We are also concerned with the materiality thresholds, in particular the use of a 2 hour threshold in service downtime for services supporting critical functions. There are a plethora of services supporting critical functions where the failure would not have a material end impact. This is one example of how the criteria have lost the link with critical/important functions as set out in the Level 1 text. Not all services supporting critical or important functions will be themselves important. Moreover, the decision to apply a 2 hour timeframe is at odds with the standard 24 hours present in other parts of DORA and in other regulations, including NIS2 (Network & Information Security Directive). To restore the link with critical/important functions and ensure broader regulatory alignment, we strongly recommend at a minimum a

single timeframe threshold of 24 hours for duration and that Article 11(b) on service downtime be deleted. To further reduce the risk of overreporting and ensure this criteria focuses on longer running incidents, the ESAs should ideally also extend the threshold for duration of incidents beyond 24 hours.

- Further, an incident can be ongoing without impact to clients – we would recommend amending the terms to consider the duration as it affects clients. In some circumstances an incident will be intentionally slowed down (e.g. to gather additional intelligence and evidence during a cyber-attack – this should not be discouraged).

- ***Geographic spread:***
  - We have serious concerns that some of the expectations on financial entities are not practically feasible. Financial entities do not have access at the time of an incident to the external information that would allow them to assess the impact on clients' and/or counterparts' operations in different territories. For instance, an incident in one EU member state could impact a client located there, but that client may then sell into another member state or have clients outside of the member state. The original financial entity would have no way to assess this, especially not at the time of the incident. Similarly, financial entities do not have access to external information to determine if a third-party provider that may be common is impacted by an incident in different territories.

  - The result is that the current wording of Article 4 will most likely see financial entities adopt a policy of reporting any incident at any third-party provider, regardless of the materiality of the incident or the likelihood of it servicing financial entities in other EU member states. This will make the criterial meaningless in practice.

  - We therefore believe it is better to focus on assessing whether the incident has impacted a financial entities' activities in other EU member states as conducted by their branches or other legal entities within those member states. We recommend that Art 4(a) and Art 4(c) should therefore be removed.

  - We additionally flag that the materiality threshold within Article 12 has lost the reference to "***material*** impact to ***its entities*** in two or more jurisdictions" as set out within recital 36. This should be reinserted.

  - Further, the DORA primary text sets out that: "*Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria: (c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects* ***more than two*** *Member States*". To reflect the proportionality principle, a proportion of the member states in which a firm operates should be established, rather than an absolute number, but at a minimum it should be more than two member states to align with the Level 1 text.

- ***Economic impact:***
  - We welcome the greater level of clarity, compared with PSD2, as to what should be taken into account as part of this criteria, in particular the exclusion of BaU costs. We would however propose the removal of advisory costs under Article 7(1)(h).

Nevertheless, AFME members have consistently flagged how the materiality threshold within Art 15(1), namely 100,000 euros, is incredibly low and will lead to significant overreporting. It certainly does not achieve the proportionality principle as suggested within paragraph 38 of the consultation paper. We have argued as a general principle in favour of relative, qualitative measures, which would see this binary figure removed. This is the most effective way of embedding the proportionality principle. If however an absolute value is needed then AFME at a minimum proposes a threshold of 10 million euros, reinforcing how low the current proposal would be in practice, and how surely the current threshold would lead to significant overreporting.

- It has been suggested this criteria is also relabelled "firm financial impact" for further clarity, and based on costs which are visible and known at the time of the incident.

Question 4 **Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes.**

- The term data loss should have been replaced with data breach, to be in line with GDPR. It should nevertheless be clarified across each of the four provisions within Article 5 that data loss entails as a further element "a real malicious use of the data" as opposed to simply an issue over the authenticity of the data. It is necessary to differentiate whether the data has been exploited or not, to avoid significant overreporting. For example, a customer base of 100,000 records whose access rights have been misplaced but whose data has not been exploited for malicious purposes should not trigger the criterion unnecessarily.

- The financial entity should also have the discretion to determine whether the data is critical, subject to its own classification systems, and if the level of impact is significant. Any 'significant impact' is too broad and will lead to overreporting. Recommend adding '*any significant impact* ***as determined by the financial entity*** *in accordance with Article 5*.'

Question 5 **Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes.**

- We agree with the ESAs in raising the existing PSD2 materiality threshold on *critical services affected* on the basis of internal escalation. The assumption is though that this escalation must be formal escalation through established governance or incident management processes, rather than informal exchange of information between staff. We propose inserting the words "formally" and "outside of any regular/routine reporting" within Article 14 to affirm this assumption and better align with ECB cyber incident reporting. (i.e. "*Any impact on critical services in accordance with Article 6, which has been* ***formally*** *escalated outside of any regular/routine reporting.").* There will continue to be significant variation across firms with this criteria, but failure to clarify could unintentionally result in reduced internal reporting which would ultimately backfire.

Question 6 **Do you agree with capturing recurring incidents with same apparent root cause, similar nature and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes.**

Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents).

- AFME has major concerns with the provisions for recurring incidents. With regards to the wording of Article 16:
    - The ability to determine that two or more incidents have the same *root cause* will be extremely challenging and burdensome for financial entities since this is unlikely to be known at the time of the incident. This is likely to result in financial entities erring on the side of caution and overreporting incidents as recurring to avoid any regulatory breach. Similarly, the suggestion that *similarity of nature* would suffice is far too broad a term and would likewise result in significant overreporting. Further, some root causes are likely to be very common, for example human error/fat finger.

    - The RTS should use this opportunity to rebolster the link with critical and important functions, as the definition of major incident set out within the DORA Level 1 text, by specifically requiring the impact of recurring incidents to be limited to the impact upon critical or important functions.

    - Additionally, the most practical solution would be to raise the threshold to compensate for the inevitable overreporting. We recommend *four* occurrences should be required for an incident to be defined as recurring under Article 16, with confirmation that no additional reporting for further instances is required.

    - At a minimum, we propose that Article 16(2) be amended to "*For the purposes of paragraph 1, recurring incidents shall occur at least ~~twice~~ **four** times, have the same apparent root cause and ~~shall be with similar nature and~~ impact critical or important functions.*"

- Moreover, we do not see how the proposed Article 16 is compatible with Article 3(8) and (9) of DORA. The former already defines an 'ICT-related incident' as a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity. It therefore appears that recurring incidents are already captured within the Level 1 text, and that this specific Level 2 provision goes beyond that mandate and creates new obligations. It therefore is a further example of the RTS failing to adhere in practice to the proportionality principle.

Question 7 **Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.**

- We support the alignment with the Level 1 text, and by extension the Cybersecurity Act 2019, in determining a *cyber threat*. We are concerned though by the highly speculative nature of Article 17(1) on what constitutes a *significant cyber threat*. Members do not view the current proposal as workable, particularly whether the threat could affect a critical or important function of another financial entity, client, counterpart or third party. Financial entities would not typically have this information available to them, and as a rule would not be in a position to determine whether the conditions set out within Article 8 could materialise in entities other than itself. Additionally, the RTS should recognise that mitigating controls will and should be factored into these decisions. We therefore recommend the following amendments:
    - *Article 17(1): For the purposes Article 18(2) of Regulation (EU) 2022/2554, a cyber threat shall be significant, where it fulfils all of the following conditions,* ***taking account of mitigating controls****:*

        a) the cyber threat could affect critical or important functions of the financial entity, ~~other financial entities, third party providers, clients or financial counterparts~~;

        b) the cyber threat has a high probability of materialisation at the financial entity ~~or other financial entities~~; and

        c) the cyber threat could fulfil the conditions set out in Article 8 if it materialises.

- Additionally, we highlight that Article 19(3) of DORA obligates financial entities, where applicable, to inform clients of 'significant cyber threats'. The extremely broad definition proposed in Article 17 of the RTS creates huge challenges when complying with this obligation:

    - Firstly, firms are duty bound to keep their intelligence confidential by virtue of MoU's and NDA's with intelligence providers. Whilst exclusion clauses exist to share information with regulators, they do not exist to share information with corporate third parties. Therefore, in attempting to comply with Article 19(3), firms would be in breach of contractual obligations to their intelligence providers and other entities.

    - Secondly, providing this information to clients would go against the spirit of the cyber intelligence sharing community which seeks to prevent oversharing in case it desensitises the industry and slows the collective response to an actual major incident:
        - It would put a firm in breach of TLP rules.
        - It could damage trust, with clients inundated with speculative threats that do not materialise, potentially impacting market stability.
        - Key outcomes of DORA, for example increasing information sharing and strengthening resilience, would not be achieved by this provision.

Question 8 **Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes.**

- In addition to the challenges set out in our comments to Articles 4 and 12, the industry strongly objects to the proposed changes to the approach given in the Level 1 DORA text. Sharing of unredacted, non-anonymised data on incidents without the explicit consent of the

financial entity could create material risks to the financial entity's security. We believe this approach is likely to result in far more risk to EU financial services than it mitigates, by increasing the circulation of highly sensitive information. In addition, the inclusion of not only financial authorities, but also national law enforcement agencies in the scope of sharing creates significant risk as the security practices of those organisations are often not equivalent to those of financial regulators. We believe that the proposed approach, if pursued, could be challenged at the highest level by some home authorities. For sake of clarity AFME stresses we do not support the sharing of non-anonymised data amongst authorities, and especially with non-financial authorities.

Contacts

AFME	Andrew Harvey	+44(0)20 3828 2694	andrew.harvey@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
AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@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/