11 September 2023

FIA position on the ESAs first batch of DORA policy products

Public consultation on draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554

FIA appreciates the opportunity to comment on the European Supervisory Authorities' (ESAs) first batch of DORA policy products. We support the ESAs aim to specify the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats. However, we would like to highlight remaining industry concerns in our responses below.

Question 1. Do you agree with the overall approach for classification of major incidents under DORA? Yes/No. If No, why?

FIA does not fully agree with the approach followed. Below, we share remaining industry concerns:

- We are concerned that this approach loses the intended focus on critical and important functions by failing to align with the DORA definition of major ICT related incident. We suggest that that objective to protect specifically critical and important functions is clarified and emphasized or that the critical services criteria (currently a primary one) should be made a mandatory one for classification purposes Not doing so will result in significant overreporting.

- Additionally, the Consultation Paper (CP) acknowledges that "FEs are best positioned to identify their clients, and hence no further elaboration of this term is proposed in the CP." However, this sentiment is not reflected in all the criteria. The inclusion of fixed thresholds with fixed amounts does not reflect an approach based upon proportionality.

- Finally, 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.

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? Yes/No. If No, why?

FIA does not agree with the approach followed. Below, we share remaining industry concerns:

[Article 1. 3.] Financial entities do not always have access to the information that would allow for the assessment of the impact on their own business objectives or market efficiency of an incident impacting a third-party. 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 in order to avoid regulatory risk of not reporting an impactful incident. We recommend that

this criterion be removed and the focus remain on the impact of the incident on the financial entities clients, counterparts or transactions.

- *Suggested Text: ~~3. In relation to the relevance of clients and/or financial counterparts, the financial entity shall take into account the extent to which the impact on a client and/or a financial counterpart will affect the implementation of the business objectives of the financial entity, as well as the potential impact of the incident on market efficiency~~*

[Article 1. 5 and 2.] The term 'comparable reference period' does not have a clear meaning and would be difficult to apply consistently across different types of services and different financial entities. We agree that firms should estimate impact in the absence of precise figures, but we believe the methodology for doing this 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 in the RTS which only require financial entities to estimate, rather than to do so based on a comparable reference period.

- *Suggested Text: 5. Where the actual number of clients, financial counterparts or number or amount of trans-actions impacted cannot be determined, the financial entity shall use estimates ~~based on available data from comparable reference periods.~~*

2. Where the actual number of clients, financial counterparts or number or amount of transactions impacted cannot be determined, the financial entity shall estimate these based on available data ~~from comparable reference periods.~~

[Article 9. 1. A/B.] This is set at the PSD2 lower impact threshold but is considered a primary indicator in DORA (10% vs 25%). A lower limit may give rise to additional reporting particularly where it is triggered by 2 or more primary criteria having been met. We suggest maintaining 25%. FIA appreciates the ESAs highlighting that the number of clients is just one component of the criterion and will not by itself trigger the reporting of a major incident. However, FIA requests that the ESAs maintain consistency in materiality thresholds and set the appropriate boundaries to limit conditions met in order to lead to the identification of major incidents and prevent overreporting.

- *Suggested Text: a) the number of affected clients is higher than ~~10%~~ 25% of all clients using the affected ser-vice of the financial entity; or*
b) the number of affected financial counterparts is higher than ~~10%~~ 25% of all financial counterparts used by the financial entity related to the affected service; or

[Article 9. 1. C/E] We deem that the inclusion of fixed amounts within Article 9 (which are considered too low) results in metrics which do not relate to institutional clients, thereby undermining the proportionality principle. While in the context of payments incidents absolute numbers may have made sense, when applied to other lines of business, for instance retail banking, such numbers will likely result in a significant increase in the number of reportable incidents. For instance, a short outage of a retail banking application, even if in the middle of the night, would easily exceed the 50,000 threshold, even if it resulted in no impact. Given the expansion of incident reporting to cover so many other lines of financial services business, we recommend that relative figures be preferred or that the absolute numbers be doubled.

- *Suggested Text: c) the number of affected clients is higher than 100,000 ~~50 000~~ clients; or*

[Article 9. 1. F] 'Any impact' can be interpreted to include non-critical operations and would lead to overreporting, especially if firms are expected to estimate because of the lack of access to appropriate information from their clients or counterparts. 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. Therefore, financial entities would be forced to guess and will likely err on the side of caution which will result in a significant increase in the amount of reporting. Moreover, Articles 9(1)(a) and 9(1)(b) set specific thresholds relating to clients and financial counterparts affected by the incident, whereas Article 9(1)(f) presents financial entities with a very broad threshold, possibly negating the thresholds set in 9(1)(a) and 9(1)(b).

- *Suggested Text: ~~f) any identified impact on relevant clients or financial counterpart in accordance with Article 1(3).~~*

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? Yes/No. If No, why?

FIA does not agree with the approach followed. Below, we share remaining industry concerns:

[Article 2. 1.] 'Attract media attention,' 'received complaints,' and 'lose clients' are too broad and will lead to overreporting. The lack of a tiered analysis approach to determining whether the reputational impact criterion will be met will result in the criterion being constantly triggered, rendering it ineffective.

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.

FIA recommends removing prong (a) from the criteria given the challenges with developing an appropriate materiality threshold. For prong (b), a single complaint could trigger the threshold for reputational impact. To remediate this, FIA suggests the ESAs consider implementing a percentage threshold to the complaints received by its clients or counterparts.

We also suggest applying 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 would 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.

- *Suggested Text: For the purposes of determining the reputational impact of the incident, taking into account the proportionality principle, financial entities shall take into account and 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:*

[Article 2. 1. C.] 'The financial entity will not be able to or is likely not to be able to meet regulatory requirements' needs to be further qualified. Most incidents could result in missed regulatory requirements given the extensive nature of financial regulation. A financial entity would be unlikely to incur regulatory sanctions unless the breaches were persistent or severe. PSD2 MIR qualifies this categorisation as

"regulatory requirements have not been complied with, resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available." We suggest similar language is included here.

- *Suggested Text: 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;~~ or*

[Article 3. 1] An incident should be measured from the point the financial entity becomes aware of the incident to when the financial entity restores normal or acceptable service levels, rather than after the final report and root cause analysis, which could take some time and do not impact the delivery of services.

- *Suggested Text: 1. Financial entities shall measure the duration of an incident from the moment the incident occurs ~~the incident occurs~~ until the moment acceptable levels of service are restored~~. when the incident is resolved~~. Where financial entities are unable to determine the moment when the incident has occurred, they shall measure the duration of the incident from the earlier between the moment it was detected and the moment when it has been recorded in network or system logs or other data sources. Where financial entities do not yet know the moment when the incident will be resolved, they shall apply estimates.*

[Article 11. B.] In Article 11, FIA believes the 24 hour timeline should be preferred. This would align to other EU Regulations such as NISD2, as well as be in line with international standards such as the reporting timelines required by EU financial regulators. Nonetheless, FIA highlights that for some financial institutions the duration of incident threshold of 24 hours is too short. This is particularly important if during the duration of the incident a root-cause analysis has to be performed, which typically takes longer than 24 hours. We propose that within the context of the definitions provided in Article 3 (Classification criterion 'Duration and service downtime'), only service downtime is used as a materiality threshold, since "resolving" the incident is more of an administrative task. Alternatively, the threshold should be set sufficiently long (7 days) to ensure that all incident management processes to "resolve" the incident are of a good quality (e.g. the root-cause analysis process).

Moreover, until this point, the two-hour recovery has been reserved for critical infrastructure operators. This would extend this requirement to a much larger number of financial institutions where 2-hour recovery may not be possible or where the lack of 2-hour recovery times have minimal impact to the financial institution or market stability. **We also note that, in extending this requirement to all financial entities, this RTS exceeds the DORA RTS on the risk management framework, which limits the 2 hour RTO to CCPs and CSDs.** By striking the first part of (b), requirements reserved for critical infrastructure operators is preserved while allowing proportionality to less critical financial institutions.
Another challenge with the 2hr timelines is that the word "supporting" is not clear and could encompass a great number of ICT services that are not material to a critical or important function and would not impact the delivery of that service. This threshold is therefore likely to capture a great number of incidents rather than only those of a more material nature.

- Suggested Text: ~~*or b) the service downtime is longer than 2 hours for ICT services supporting critical functions, without prejudice to stricter availability and recovery requirements set out in Regulation (EU) 2022/2554 and other EU legislation.*~~

[Article 4. A. C.] Financial entities do not have access to the external information at the time of an incident 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 in which it contracts services from the financial entity. The original financial entity would have no way to assess this, especially not at the time of the incident.

Financial entities also 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. Overreporting will occur if financial entities are expected to guess if a common third party is impacted in different territories. To avoid regulatory risks, financial entities will likely adopt a policy of reporting any incident at any third-party provider, regardless of the materiality of the incident or the likelihood it services financial entities in other EU member states. This will make the criteria meaningless in practice. Therefore, we believe it is better for financial entities to focus on assessing whether the incident has impacted their activities in other EU member states as conducted by their branches or other legal entities, within those member states.

In Article 7 (Classification criterion 'Economic impact'), the draft RTS lists criteria for determining economic impact. This is too detailed and complex and when the real incidents occur it will be operationally onerous and burdensome, if not impossible to calculate the economic impact for the purpose of determining reportability. We recommend that this criterion is not used for determination of whether the incident is major / reportable, but as a post-incident review activity.

- *Suggested Text: ~~a) The clients and financial counterparts affected; or [...]c) Financial market infrastructures or third-party providers that may be common with other financial entities~~*
  ~~c) Financial market infrastructures or third-party providers that may be common with other financial entities~~

[Article 12] According to RTS background paragraph 36, 'the ESAs have, therefore, arrived at the view to base the criterion on the FE's own assessment of the **material** impact in two or more jurisdiction(s) based on the affected clients and financial counterparts, branches or subsidiaries within a group, and financial market infrastructures or third party providers that may be shared with other FEs.' However, 'materiality' is not reflected in this language or article 12 and we recommend amending to include it.

- *Suggested Text: Any <u>material</u> impact of the incident in the territories of at least two Member States in accordance with Article 4 shall be considered as meeting the threshold of the criterion for major ICT-incidents under Article 8(3)(c).*

[Article 15. 1.] This limit is too low and will lead to overreporting. While Article 7 does state that Business as Usual (BAU) costs should not be included in this calculation, it is unclear if any technology costs related to fixing an incident to return it to its original state fall under this BAU category. An absolute cost closer to $250,000 would be more appropriate. Alignment with PSD2 would mean a threshold of 5m EUR.

- *Suggested Text: 1. The materiality threshold of the economic impact in accordance with Article 7 is met where the gross direct and indirect costs and losses incurred by the financial entity from the major incident have exceeded or are likely to exceed EUR 250,000 ~~EUR 100 000.~~*

- Moreover, on geographical spread:
    - In particular for globally operating financial entities, the determination might not be clear: non-EU clients could have accounts with EU-branches, EU clients could have accounts with non-EU-branches, or an application could be hosted in the EU but only serve branches and clients outside the EU.

Question 4. Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? Yes/No. If No, why?

FIA does not fully agree with the specification and threshold of criterion. Below, we share remaining industry concerns:

We believe it is important to maintain the linkage to critical and important functions/ critical processes.

It should 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". 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.

Question 5. Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? Yes/No. If No, why?

FIA does not fully agree with the specification and threshold of criterion. Below, we share remaining industry concerns:

[Article 14] We understand from this requirements that the ESAs intend escalation to mean formal escalation through governance or incident management processes, rather than informal internal exchange of information between staff and a senior manager. We suggest a minor edit below to make this clear.

Additionally, this article appears circular. The Level 1 text Article 17(e) states "ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body of at least major ICT-related incidents." Financial entities are expected to report at least major ICT-related incidents to senior management, yet one of the criteria to determine if it is a major incident is to determine if we would report to senior management.

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. 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 be counterproductive.

- *Suggested Text: Any impact on critical services in accordance with Article 6, which has been formally escalated outside of any regular/routine reporting by the financial entity to its senior management or management body shall be considered as meeting the threshold of the criterion for major incidents under Article 8(2)(c).*

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? Yes/No. If No, why?

FIA does not fully agree. Below, we share remaining industry concerns:

[Article 16. 2.] When triaging an issue, determining whether this criterion has been met in order to make a reportability decision is likely to be extremely challenging and burdensome since the root cause is unlikely to be known at the time.

Because of this, financial entities may be forced to assume that incidents are recurring to avoid missing the timeline requirements for reporting. Therefore, this criterion may lead to significant overreporting. We believe this can be addressed by raising the number of incidents that need to occur and narrowing the focus to incidents impacting critical or important functions. This will allow financial entities to be able to fully assess root cause before being compelled to report. Therefore, the RTS should 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.

We also suggest the removal of the term 'Similar nature and impact' as it is not precise and will likely lead to confusion and inconsistent application of this criteria by financial entities.

- *Suggested Text: 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 to critical or important functions.*

Question 7. Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? Yes/No. If No, why?

FIA does not agree with the approach followed. Below, we share remaining industry concerns:

FIA does not view the current proposal as workable, particularly whether a 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. FIA members support sharing information regarding significant cyber threats on a voluntary basis but we urge caution against requiring financial entities to address the elements in Article 17 due to the limited ability to obtain or have visibility into certain factors. We therefore recommend the following amendments:

[Article 17 1. A/B] We do not believe it is possible for a financial entity to assess impacts or effects on other financial entities, third-party providers, clients or counterparts. Almost any cyber threat could, in theory, affect the CIF of any financial entity, third-party provider, clients or financial counterparts, as this depends on the details of their control environment and unique risk profile. Systemically important financial entities employ sophisticated cyber defense mechanisms to prevent and detect cyber attacks that may not be stopped by financial institutions that have less sophisticated measures in place. Therefore, trying to determine the feasibility of the attack in the absence of controls or the potential for the attack to materialize in firms with lesser controls is challenging.

We believe it is better to limit cyber threat analysis to the financial entity itself and not expect any analysis of other entities. While many firms will monitor threats and may become aware of threats to another financial entity, this is done on an ad-hoc basis, mostly based on threat intelligence. Mandating this would like detract for the focus on threats targeted at the financial entity itself and ultimately be a distraction for all but the best resourced entities.

- *Suggested Text: 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:*
  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.

[Article 17. 2. C] There needs to be attribution to determine the capabilities and intent of threat actors. The ability to attribute a cyber attack to a particular cyber threat actor or group may require significant time and the assistance of external threat intelligence (e.g., government agencies). A financial entity on its own may not be able to attribute. We suggest that attribution should be an objective of information sharing and should, therefore, be stripped from the classification criterion for a single entity.

- *Suggested Text: c) <u>If known at the time of the threat,</u> the capabilities and intent of threat actors, and*

Additionally, we highlight that Article 19(3) of DORA recommends 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. 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? Yes/No. If No, why?

FIA does not agree with the approach followed. Below, we share remaining industry concerns:

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 political and security alignment of these organisations could itself be questionable. We believe that the proposed approach, if pursued, could be challenged at the highest level by some home authorities.

When sharing with other authorities, details of the reports should be redacted to remove strictly-confidential data of the affected financial institution. This is especially relevant for cyber incidents, as it may contain data which could present a blue-print how a financial institution can be compromised. This type of data should not be distributed broadly and only on a need-to-know basis.