EFAMA
European Fund and Asset Management Association

CONSULTATION RESPONSE

Brussels, 11 September 2023

EFAMA RESPONSE TO THE CONSULTATION PAPER 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.

General remarks

EFAMA welcomes the launch by the ESAs of the first batch of public consultations on the level 2 legislation under DORA[1]. Due to their number and detailed scope they will be an important element of the new EU framework on digital operational resilience. They would also highly influence the amount of work that each financial entity would have to carry out while implementing new rules ahead of 17 January 2025.

While we also welcome that the authorities have envisaged a period of almost three months for market participants to submit their comments, we believe that the timing of the consultations will not work in favour of their outcome. The period of summer holidays is very challenging when it comes to gathering detailed feedback and analysis, in particular on topics as technical as these. Having four drafts simultaneously under consultation also impedes due consideration being given to all the details, in particular on drafts as elaborate as the ones concerning the risk management framework, or the register on contractual arrangements.

We are aware of the tight deadlines established in DORA for the submission of drafts by the ESAs to the European Commission. At the same time, we are of the opinion that it is in the common interest and power of those institutions to secure a timeframe which would favour best outcome of the process, including thought through views provided by all stakeholders. This should be taken more comprehensively into account when drafting provisions of the level 1 acts, as well as when scheduling future public consultations.

In reference to the 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

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

Regulation (EU) 2022/2554[2] (Draft RTS), we would like to draw the ESAs' attention to the following aspects:

- The Draft RTS lack a clear reference to the definition of major ICT-related incidents, which is included in DORA and should be acknowledged in this Draft RTS;

- The Draft RTS create a methodology which is very complex and will be burdensome, especially for smaller entities. It would require monitoring of all the proposed criteria and gathering of evidence which in many cases will not result in detecting an incident. This will have a financial impact on all entities as it will require significant resources and specialist technology, as well as the involvement of multiple business areas; and

- A higher number of incidents qualifying as "major" under the proposed methodology would not necessarily be beneficial for detecting those worth focusing on. If the number of incidents to be addressed by the entities is too high, it would be difficult to detect truly "major" incidents and subsequently involve all necessary resources.

- As a result, it could impede the achievement of DORA objectives.

Response to the ESAs' Questionnaire

Q1: Do you agree with the overall approach for classification of major incidents under DORA?

☐ Yes

☒ No

Q1b: Please provide your reasoning and alternative approach(es) you would suggest.

EFAMA is of the opinion that the overall approach is complex and will be burdensome, especially for smaller entities. It would require monitoring of all the proposed criteria and the gathering of evidence which in many cases will not result in detecting an incident. This will have a financial impact on all entities as it would require significant resources and specialist technology, as well as involvement from multiple business areas. In the occurrence of a major incident, the resources of the entity should be mainly focused on resolving the incident, rather than looking for the necessary information.

We are of the opinion that the principle of proportionality should be better incorporated to the Draft RTS, given also that art. 4(2) of DORA requires for the application of Chapter III ("ICT-related incident management, classification and reporting") to be proportionate to the size and overall risk profile, and of the nature, scale and complexity of services, activities and operations of financial entities. We would like to highlight that an approach based on what was previously designed for entities like banks, which provide critical IT infrastructure and are subject to the NIS2 Directive[3], will not be appropriate for asset managers and investment firms providing portfolio management and investment advice.

We would also like to draw attention to the fact that the Draft RTS misses a clear link to art. 3(10) of DORA, which provides a definition of a major ICT-related incident, with it being "*an ICT-related incident that has a*

[2] ESAs, Consultation paper 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.

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

high adverse impact on the network and information systems that support critical or important functions of the financial entity". Despite the mandate given to the ESAs in art. 18(3) of DORA to further specify criteria to classify ICT-related incidents, including major ICT-related incidents, it is obvious to us that they should still be aligned with the definition set in DORA. In particular, current wording of art. 6 and 8 of the Draft RTS lacks a clear link to the requirement that major incidents affect systems that support critical and important functions. Instead, the conditions proposed in art. 8(1) of the Draft RTS for a major ICT-related incident to occur include either thresholds of 2 primary criteria to be met, or thresholds of 3 or more criteria to be met, including at least one primary criterion. As they are irrespective of what is required by the definition of art. 3(10) of DORA, they should be amended.

To ensure compliance with the RTS, financial entities need to be able to determine what parts of their business operations are relevant in terms of "ICT related incident classification." The Draft RTS refers to "*the service*", "*critical services affected*", "*critical functions*", "*non-critical services*", and "*critical or important functions*" and the inconsistent and interchangeable use of these terms is expected to result in legal uncertainty for financial entities. To ensure clarity and certainty, we would propose a consistent use throughout the Draft RTS of the term "critical or important functions", as clearly defined in the Level 1 text.

It is also important to highlight the connection between this Draft RTS and the draft RTS and ITS that the ESAs shall develop under art. 20 of DORA. As they will establish contents of reports on major ICT-related incidents, time limits for the initial notification, notification for significant cyber threats as well as forms, templates and procedures thereof, there is a significant interlinkage between those two spheres. This will have a real impact on the ability of the entities to supply the data and reporting in time.

EFAMA favors the use of relative thresholds rather than absolute ones, which seem not appropriate as they don't reflect the scale of the entity and its business. In our opinion, thresholds should be relative where possible and reflect the proportionality principle, as otherwise they will not be aligned with DORA. Moreover, we are of the opinion that the calibration of the thresholds should be improved. If the number of incidents to be addressed by the entities is too high, it will be counterproductive to the task at hand. Following too many incident reports, it would become harder to detect truly "major" incidents and consequently channel all necessary resources toward them. It would also escalate the costs borne by financial entities.

Q2: 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

Q2b: Please provide your reasoning and suggested changes.

EFAMA agrees with the use of relative thresholds in art. 9 of the Draft RTS, however, they might not be properly calibrated for bigger entities. Thresholds set on a level which is too low will result in overreporting. Moreover, we strongly disagree with the additional absolute thresholds proposed under art. 9(1)(c) and (e) of the Draft RTS. We would like to highlight that a higher number of incidents qualifying as major under the proposed methodology would not necessarily be beneficial for detecting those truly major ones.

There is also the question of how to implement the condition specified under art. 9(1)(f) of the Draft RTS which relates to "*any identified impact on relevant clients of financial counterpart in accordance with Article 1(3)*". This condition, which refers to market efficiency, is very unclear and will be hard to interpret by financial entities, which will have a detrimental effect on the quick calculation of the criteria and identification of major incidents. Given also that there are already several thresholds that address the criterion of "clients,

financial counterparts and transactions affected", we see this one as excessive and would suggest its removal from the Draft RTS.

It should also be clarified that the thresholds should be applied to an entity level.

Q3: 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

Q3b. Please provide your reasoning and suggested changes.

Below please find our reasoning with regard to each of the criteria individually.

On the **"reputational impact" criterion**, we would like to highlight issues with both the way the threshold is calibrated, as well as the elements of the definition itself. As art. 10 of the Draft RTS speaks of "any impact" as meeting the criterion for a major incident, we are of the opinion that this could result in massive overreporting, despite the provisions of art. 8(1) of the Draft RTS. This is also combined with a very broad definition of reputational impact in art. 2 of the Draft RTS, which for example speaks of "media attention". As described by the ESAs during the public hearing on 13 July, this includes both traditional media and social media, however, it should not be understood as a single post or article. Given that art. 10 of the Draft RTS mentions "any impact", such conclusion is hard to be drawn from the provisions themselves. In fact, as we are speaking of a reputational impact, it should be also made clear that it should have a direct impact on the particular financial entity. When media attention is given to some issues arising in, for example banking sector, it should not be automatically understood as an impact on particular bank.

What is more, point (c) in art. 2 of the Draft RTS includes circumstances where "*the financial entity will not be able to or is likely not to be able to meet regulatory requirements*", which is also a very broad concept. EFAMA would like to highlight that minor delays in regulatory reporting, or other small infractions, should not have any reputational impact. In our opinion, this should be limited to "significant regulatory requirements" or entirely removed.

In the case of the **"duration and service downtime" criterion,** we would like to highlight that the duration of the incident of no longer than 24 hours, and in case of a downtime no longer than 2 hours, mentioned in art. 11 of the Draft RTS, are too short. We believe that these provisions were based on the business models of banks that, unlike asset managers and investment firms, provide time-critical services. For some critical functions of the management companies, the recovery time objective (RTO) is defined for a longer period of downtime (e.g. 4 hours). The threshold defined at 2 hours would therefore lead to unnecessary overreporting. Therefore, in this case we would suggest a wider implementation of the principle of proportionality that would allow entities to adjust the duration of both incident and downtime to their business-impact analysis and RTOs.

Moreover, it is also not clear what a service that is "partially unavailable" means. Would it address circumstances where for example the service is fully unavailable to some clients, but others are not impacted, or some functions of the service are unavailable, but overall, the service is not considered as such? If a service is disrupted, it should not necessarily mean that there is a downtime when it can still meet its purposes.

EFAMA is also of the opinion that the 2 Member States threshold for the **"geographical spread" criterion** is too low and would highly increase the burden of this process for any entity with a multinational presence. This could mean that when there are two members of the staff impacted, but they are located in two different member states, the threshold would be met. It is also worth noting that art. 18(1)(c) of DORA, in regard to this criterion, mentions "*particularly if it affects more than two Member States*" which should be understood as at least three.

On the **"economic impact" criterion**, we would like to highlight that this particular one could be evaluated only after an incident occurs which would require financial entities to reevaluate their initial classification of incidents. We are also of the opinion that the threshold is too low and not consistent with the risk acceptance level of financial entities. Therefore, we would suggest it be set at the level of at least 1 million EUR or even 5 million EUR.

In this regard, we would also like to highlight the unclear connection between this threshold which is to be calculated taking into account direct and indirect gross costs and losses, and the estimation of aggregated annual costs and losses caused by major ICT-related incidents under art. 11(10) of DORA. It is not clear why in one case mere estimates would be sufficient, and in the case of this Draft RTS, specific costs have to be identified.

We would also like to question the inclusion in this criterion of "losses due to forgone revenues" under art. 7(1)(e) of the Draft RTS. There is a very wide range of factors that may, on a day-to-day basis, impact the revenue of a financial entity and it will be extremely challenging to assess to which extent revenue loss can be attributed to an ICT incident.

Q4: Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13?

☐ Yes

☒ No

Q4b: Please provide your reasoning and suggested changes.

As the term "significant impact" in art. 13 of the Draft RTS is not specific, we would assume that it is permitted for entities to make their own decision as to what is considered significant in their particular situation. For example, in case of confidentiality of data mentioned in art. 5(4) of the Draft RTS, if a single email is sent including confidential data to a single unauthorised recipient, the entity may make the decision that this is not significant.

We would also like to highlight the need for clarification on what is to be understood as "data loss", as there are different interpretations when looking from the intellectual property, privacy, or business point of view. Is it also important to specify if it is purely an actual loss of data, or if it include data that is temporarily unavailable, corrupted, and similar. Data loss is an area where many companies have built-in automation to identify and correct many data loss scenarios, therefore we question why the ESAs have taken an alternative approach to the identification and reporting of this. Clarification is required both on what the ESAs would like to achieve with this approach and the definition of loss.

Q5: Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14?

☐ Yes

☒ No

Q5b. Please provide your reasoning and suggested changes.

We would like to refer to our response to Question no. 1 and the clear link that the Draft RTS should have to the definition of major ICT-related incidents in art. 3(10) of DORA, in particular in the case of the criterion of "Critical services affected". We strongly oppose the introduction of a new definition in art. 6 of the Draft RTS as it should clearly link to the network and information systems that support critical or important functions of the financial entity. Those networks and information systems should be further assessed by financial entities at their own discretion, including the impact they have on business, their ICT structure and risk assessment.

We would like to highlight that it is not clear what is meant by "services or activities which require authorization" in art 6 of the Draft RTS. We assume that it refers to the authorisation by the NCAs (i.e. the licenses granted to the entity), however, we would also like to highlight that not all services or activities of this kind should be automatically categorised as critical. In case of the asset management industry, there are some activities which are authorised by the NCAs, but are performed with no, or very little use of ICT infrastructure, and therefore should not be seen as critical for the purpose of DORA.

Q6: 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

Q6b: 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).

EFAMA would like to highlight that if an incident is not 'major', the entities are not collecting necessary data to analyze them retrospectively and check whether a recurring incident has occurred. This would mean additional work, as in order to check whether the thresholds have been met, the metrics for the criteria would have to be aggregated between separate events. This adds to the complexity of the analysis and reporting, which will be an overhead in particular for smaller entities.

We also do not see a clear mandate for the ESAs to specify this and include it in the Draft RTS. Recurring incidents are not mentioned in art. 18(1) of DORA creating the criteria to classify incidents, as well as not included in the art. 18(3) of DORA which provides the scope of this Draft RTS. Even though the definition of an ICT-related incident under art. 3(8) of DORA refers to a single event, or series of linked events, this does not give sufficient ground for the creation of this framework for recurring incidents. Therefore, we would argue that this part of the Draft RTS should be removed entirely.

We would also like to draw attention to the proper understanding of the phrase "*the same apparent root cause*". In our view, it should mean the same incident and the same service being affected. As this element of the criterion is not specific, we understand that it would be the entity who would have to decide.

Q7: Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17?

☐ Yes

☒ No

Q7b: Please provide your reasoning and suggested changes.

In our opinion, cyber threats (such as ransomware, for instance) are significant by design, and once the financial entity is connected to the Internet, it is inevitable that they would occur. Therefore, it seems very probable that, unless particularly targeted, no entity would report them. We are of the opinion that it would be more useful if the Draft RTS would focus more on specific threats which would give the financial entities a better understanding of what to report.

We would also like to highlight that this obligation would be especially problematic for smaller entities being members of a group with headquarters outside of the EU. Many entities would have cybersecurity managed at group level which would make it more difficult to determine specific vulnerabilities on an entity level.

Q8: 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

Q8a: Please provide additional comments (if any).

We understand the need to provide either the ESAs or the competent authorities (NCA) from another Member State with non-anonymised reports on incidents in order for a quick and successful prevention of their further spreading across the financial market. At the same time, we would like to highlight to the ESAs the dangers which could arise from such exchange and should be properly addressed in advance. It is undisputed that an entity would be facing reputational damage if such reports would be accessed by unauthorised parties, which highlights the importance of high ICT security standards that the NCAs and other authorities must impose. Lastly, due to national regulations on access to public records such information, as for example the name of the company submitting reports, or the amount of them, can be easily obtained by the press. This would also result in creating a reputational impact as mentioned under art. 2 of the Draft RTS. These issues should also be properly and in advance addressed by the authorities.

*****

ABOUT EFAMA

EFAMA is the voice of the European investment management industry, which manages EUR 28.5 trillion of assets on behalf of its clients in Europe and around the world. We advocate for a regulatory environment that supports our industry's crucial role in steering capital towards investments for a sustainable future and providing long-term value for investors.

Besides fostering a Capital Markets Union, consumer empowerment and sustainable finance in Europe, we also support open and well-functioning global capital markets and engage with international standard setters and relevant third-country authorities. EFAMA is a primary source of industry statistical data and issues regular publications, including Market Insights and the EFAMA Fact Book. More information is available at www.efama.org

Contact:

Zuzanna Bogusz
Regulatory Policy Advisor
zuzanna.bogusz@efama.org | +32 2 548 26 69