EFAMA
European Fund and Asset Management Association

CONSULTATION RESPONSE

Brussels, 4 March 2024

EFAMA response to the Consultation Paper on draft regulatory technical standards and implementing technical standards on content, timelines and templates on incident reporting.

General remarks

EFAMA, the voice of European investment management industry, has long recognised the importance of operational resilience in the financial market and supported the introduction of a framework that would foster cybersecurity across sectors. At the same time, since the beginning of these discussions, we have highlighted a need for an approach which would not pose challenges to firms' divergent organisational arrangements, nor impose barriers to growth and innovation by setting the bar too high, in particular for smaller entities or those that do not provide critical IT infrastructure. This approach emanates from the principle of proportionality being widely applied to the provisions of DORA[1] by virtue of its Art. 4.

In our response to this Draft RTS and Draft ITS[2], we would:

- Question the harmonised deadlines for submitting the reports on ICT incidents, irrespective of significant differences between entities subject to the NIS Directive and those outside of its scope,
- Call for a 48 hour deadline, calculated from the detection of the incident, to submit the initial report in case of asset management companies and some investment firms, as well as the deletion of the 4 hour deadline calculated from the classification of the incident,
- Call for the application of weekend/holiday rule also to the initial report, and
- Call for standarised specifications for the formats and interfaces to be established on an EU level.

[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) (DORA).

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

Response to the ESAs' Questionnaire

Q1: Do you agree with the proposed timelines for reporting of major incidents?

☐ Yes

☒ No

Q1b: Please provide your reasoning and suggested changes.

EFAMA disagrees with the timelines established in the Draft RTS, in particular those proposed for submitting the initial report. While we understand the supervisors' perspective, as presented during the joint public hearing on 23 January 2024, we are of the opinion that the harmonisation in line with the provisions of the NIS2 Directive[3] would be unjustified for financial entities that are not subject to the requirements of this directive. The scope of DORA goes far beyond the entities selected according to Annex I and II of NIS2 Directive and varies significantly in size and in the type of services provided. For example, asset managers as well as investment firms offering services of portfolio management or investment advice differ significantly from insurance companies or banks, which provide critical IT infrastructure. Investment funds are often distributed by intermediaries, namely banks or insurance companies, which act on behalf of a large number of underlying investors, with shares/units in the fund being registered in the name of the intermediary on behalf of the underlying investor. This provides means of safeguarding the assets managed on behalf of investors while protecting them from the insolvency of the asset manager. Investors do not have a direct relationship with the fund and the asset managers are not in possession of their data. As a result, a possibility of an incident affecting investors' access to their data or services is less possible in investment funds' services. Also, other types of incidents would usually be less time sensitive, given that investment decisions are not made instantly, particularly in case of portfolio management. This results in typically longer recovery times objectives (RTOs) for the funds' sector.

Moreover, the structure, size and business models of asset managers vary significantly, ranging from companies with a workforce of less than 50 employees to up to more than 1000. For such entities having to report on the incident within proposed deadlines will be a significant burden, when in fact they should be concentrating on resolving the problem.

These differences were recognised directly in Art. 20(a) of DORA, establishing the mandate for the ESAs to develop this Draft RTS. It is specifically said there that "*the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, the specificities of financial sectors (…)*". We do not see this recommendation being implemented in the Draft RTS.

Therefore, we would suggest that in case of asset manager as well as investment firms mentioned above the deadline for submitting the initial report should be not shorter than 48 hours from detection. This would be in line with international standards for this sector, where for example the US Securities and Exchange Commission proposed reporting deadline of 48 hours for significant cybersecurity incidents[4]. A longer deadline to submit the initial report, should also impact the deadline for the intermediate report.

We also question the need for the additional deadline for the initial report i.e. 4 hours from the classification of the incident. We do not see a potential benefit in this deadline, which is not included in the NIS2 Directive.

---

[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 (NIS2 Directive).

[4] Securities and Exchange Commission, Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, p. 41-42.

Reporting requirements, to be fulfilled while the financial entity is concentrating its efforts on resolving the incident, should be as simple as possible. Keeping track of multiple deadlines based on different starting points will overcomplicate the process. Therefore, we suggest for this additional deadline to be removed.

Moreover, EFAMA would like to highlight that the weekend/holiday rule established in Art. 6(2) of the Draft RTS should apply also to the initial report. For smaller financial entities, submitting this report will be particularly challenging if they would have to do it irrespective of the non-working days. This would require changes in the employment of staff to secure the ability to report even on days other than business days.

We are also of the opinion that in such case the submission of any of the reports should be expected anytime during the next working day. Expecting that the reports will be filed in within one hour is unrealistic and would affect the quality of data received by the competent authorities.

As regards the exceptions when paragraph 2 shall not apply, we are of the opinion that the impact on another financial entity should be subject to a materiality condition. Such impact can significantly differ from case to case, and it should be acknowledged in the provisions of Art. 6(3) of the Draft RTS that the financial entity is allowed to benefit from the rules of Art. 6(2) if it considers the impact on another entity as not material.

Q2: 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?

☐ Yes

☒ No

Q2b: Please provide your reasoning and suggested changes.

EFAMA would like to highlight issues with financial entities reporting their assessments of the impact of the incident on other financial entities or a TPP. Fields 2.9. and 2.10. of the initial report include description of the impact on other entities. This information would be very subjective, and in particular in case of initial reporting, financial entities would not have enough information to have definite opinion. This analysis would be an additional burden in high pressure circumstances and with very limited timeframes to submit the report. Moreover, in cases where the impact of the incident on other financial entities is caused by their reliance on the services of the same TPP, the reporting financial entity would unlikely be aware of that. It is crucial to assure that financial entities are not obliged to report circumstances that are to be known and managed by the TPP instead.

Therefore, fields 2.9. and 2.10. should be removed and, in case it is not possible, we would suggest limiting them to an indication whether an impact on other entities could be expected, without a further description of how exactly these could be affected. In this case, the current wording in fields 2.9. and 2.10. should be replaced with "*Indication of whether the incident affects or could affect other financial entities/third-party providers, where known or reasonably expected*". The DORA framework will provide the supervisory authorities with extensive information on providers and contractual arrangements, and these authorities will be best equipped to analyse how such impact could affect other financial entities and the whole system. This task must not be delegated to the financial entities.

We are also of the opinion that field 2.15, including the description of business continuity plan, is too prescriptive, especially for an initial report. It should be limited to particular information that the ESAs are looking for. Another solution could be providing financial entities with examples.

Q3: 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?

☒ Yes

☐ No

Q3a: Please provide additional comments (if any).

We do not have specific comments.

Q4: 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?

☒ Yes

☐ No

Q4a: Please provide additional comments (if any).

We do not have specific comments.

Q5: 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?

☒ Yes

☐ No

Q5a: Please provide additional comments (if any).

We do not have specific comments.

Q6: Do you agree with the proposed reporting requirements set out in the draft ITS?

☐ Yes

☒ No

Q7b: Please provide your reasoning and suggested changes.

EFAMA does not agree with the technologically neutral approach taken by the ESAs. This would leave the decision on the formats and interfaces for reporting to each competent authority individually and as a result lead to poor harmonisation across Member States. This would be challenging for companies that are active cross-border as they would have to implement multiple, different solutions. We are also of the opinion that having an EU standard would also be beneficial for smaller entities. Therefore, we call for standarised specifications for the formats and interfaces to be established on an EU level.

Additionally, we would like to highlight that the obligation in Art. 6(1) of the Draft ITS to inform competent authorities on the outsourcing of the reporting obligation "*prior to any notification or reporting*" is not sufficiently clear. Is the intention of the ESAs to receive such notification prior to submitting each individual report on each incident? We believe that such obligation would be excessive and a single notification of the outsourcing arrangements would be sufficient.

Q8: Do you have any further comment you would like to share?

EFAMA would like to highlight that due to their specificities incidents such as ransomware are particularly challenging to report on. The investigation of such incidents requires a longer period of time and forensic information is usually not available within the proposed reporting timelines. Therefore, we would suggest for these kinds of incidents to be treated separately with a longer deadline for submitting the final report.

It is also important to note that the incident reporting environment should be set up based on the principle of cooperation between financial entities and competent authorities, with a common goal to protect the resilience of the financial sector. The reporting of incidents takes place in high pressure circumstances, caused by the incident itself and the urgency for it being quickly resolved, as well as time available to submit the reports. It is, therefore, crucial that financial entities do not fear being penalised for mistakes in reporting or reclassifying major incidents as non-major if the conditions change, as well as the information included in the reports being used for other supervisory purposes than the operational resilience.

*****

ABOUT EFAMA

EFAMA is the voice of the European investment management industry, which manages about 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 | +32 456 16 58 67