afme/

Position Paper

DORA Incident Reporting

July 2026

This following paper sets out the AFME response to the release of the 2025 Report on major ICT-related incidents as the joint ESA report under Article 22 of DORA. It has been shared bilaterally with the EBA and ESMA.

AFME has reviewed the report's analysis and findings and is providing as our reaction, four main observations:

Firstly, there is a growing query as to the underlying purpose of incident reporting. At a fundamental level, the thematic report gives rise to the question; "Do the ESAs see the primary purpose of incident reporting as ensuring the right information is shared with authorities to enable educated, targeted interventions on incidents with potential systemic impact?"

This is not explicitly addressed in the ESAs' report but is fundamental to the design of incident reporting;

1. If the overarching priority for authorities is data analysis, there is an increased rationale for delaying or excluding the gathering of certain information, at least until later in the reporting process (i.e. the final report required one month after submission of the intermediate report) to provide for a fuller set of disclosures, for example on root cause analysis.

2. If the overarching priority is incident oversight for the purposes of targeted intervention, the analysis overlooks the need for and level of onward sharing between authorities on reports which could be relevant beyond the initial recipient. Equally, the analysis does not consider whether the continuous reporting of non-significant or client-impacting incidents actually supports incident oversight and management.

AFME strongly urges authorities to primarily focus on the second objective, in part due to the fact that annual high-level findings provide limited value to industry who will already have first-hand experience of the underlying incidents – for example, firms are well aware from their own internal processes that third party vulnerabilities are a major cause of incidents as set out within Figure 8. If authorities wanted to explore further such dependencies, this could in fact better be achieved outside the formal, structured templates of incident reporting, for example as part of the IT Risk Questionnaire follow-up, and AFME would be happy to assist.

Secondly, we are concerned that the burden to industry from incident reporting is not fully captured in the ESA analysis. While the ESAs identify that on average an FE submits 0.18 reports per month under DORA, breaking down further the aggregated totals by sub-sector would demonstrate how the reporting burden falls in particular on the wholesale banking sector. The 0.18 reports per entity fails to acknowledge that larger firms drive the reporting levels, as shown by the three incident types in the report that would be disproportionally felt by larger financial institutions. Further to this, the figure also fails to recognise the burden to firms from the triaging of all incidents to determine if they meet the necessary thresholds for a formal incident report. Typically, a bank's operating model requires involvement from multiple layers, including local entities, front-line teams conducting the initial assessment, and branches (including smaller locations). It also requires ongoing governance to support reporting, including maintaining and managing approval workflows, with 24/7 round-the-sun reporting teams. These costs to industry should be factored into authorities' reviews of incident reporting, including as part of the simplification agenda and in terms of the DORA 2.0 Review.

Association for Financial Markets in Europe
London Office: Level 10, 20 Churchill Place, London E14 5HJ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540
Frankfurt Office: c/o SPACES – Regus, First Floor Reception, Große Gallusstraße 16-18, 60312, Frankfurt am Main, Germany T:+ 49 (0)69 710 456 660
www.afme.eu

Company Registration No: 6996678 Registered Office: Level 10, 20 Churchill Place, London E14 5HJ
AFME is registered on the EU Transparency Register, registration number 65110063986-76

Additionally, the ESA analysis we flag fails to foresee how the reporting burden is likely to increase in coming months and years with the arrival of New Tech such as Frontier AI. This will likely result in hundreds of new potential vulnerabilities, especially on legacy systems.

Thirdly, AFME is keen to stress why cyber threat reporting should remain voluntary and not become mandated as part of the upcoming DORA review. While the analysis highlights a lower level of cyber reporting in 2025, this is only natural in the early period of DORA implementation, as firms focused on mandatory obligations. Such threat reporting will though naturally increase over time.

It is also important that authorities are conscious of the potential negative repercussions of mandating reporting on all cyber threats. Especially in the era of Frontier AI, it is likely that hundreds if not thousands of threats may require attention. Reporting each potential threat would therefore likely overwhelm authorities and leave them unable to effectively and efficiently circulate relevant intelligence to wider industry. Indeed, without clear and rehearsed plans for the onward distribution of cyber threat information in a safe and responsible way, competent authorities may find themselves in a position where they were in possession of threat intelligence before it impacted the financial sector more broadly but did not distribute it, opening authorities to political risk. ***Firms are best placed to identify through a risk-based approach which cyber threats may have wider effect and should be responsibly reported under the voluntary DORA mechanisms***. ***Cyber threat reporting should remain voluntary and not become mandated as part of the upcoming DORA review*****.** Forcing firms to formally report on all cyber threats would also detract hard-pressed resources from incident management.

Finally, we would suggest that the analysis supports AFME's view that the DORA thresholds and criteria require fine-tuning if they are to serve the purpose intended by policymakers. The current classification framework is only loosely aligned with actual impact and in large institutions, can be reached relatively quickly. This can particularly be seen on the following aspects:

1. We note that **service downtime** is identified as the main trigger/criteria for DORA reporting, and flag that with technological advantages, including Frontier AI, it is likely that this criterion will become even more common, both with regards to planned service times in order to pre-empt vulnerabilities and downtimes directly caused by an incident**.** Wholesale financial institutions also often struggle with the service downtime criteria, especially the 2-hour timeline for CIFs, for example over the weekend, yet effective IT segregation can safeguard against potential client impact. ***We would urge as part of next year's DORA 2.0 review that the Service Downtime criterion is de-listed under Article 18 of DORA as a classification criterion for incident reporting, and that this information is relegated to the intermediate and final stages of reporting.***

2. We agree with the ESAs' in finding that there is significant difficulty in assessing the **costs/losses of an incident**, reflected also in the 2025 ESAs' Q&A. AFME members have been forced to make subjective estimates and draw artificial distinctions where the business loss is effectively zero when excluding staff costs associated with incident management, in order to submit the requested information on Costs. It is our view that the *Economic impact* criteria is a poor determinant as to whether a major incident has occurred, especially given costs can only become clear over a longer time period. This information is more relevant as part of an ex post facto analysis of an incident, rather than as part of the initial classification or as major criteria under the regime. ***We would strongly urge as part of next year's DORA 2.0 review the Economic impact criterion is de-listed under Article 18 of DORA as a classification criterion for incident reporting, and that information on costs/losses is relegated solely to the final report stage, as part of concluding analysis, and with BAU costs for staff removed.***

3. We note that **geographical spread** is identified as the third most common criteria for triggering DORA classification and reporting. This reflects the experience of AFME members, who routinely found any incident would automatically trigger this criterion. The majority of our members have for example reported incidents under the geographical spread criteria that are related to cross border payment systems, but which have zero to no impact on clients in both countries. While part of this is to be expected given AFME's membership of globally significant institutions, ***we would nevertheless urge as part of next year's DORA 2.0 review that this criterion is tightened, and that the materiality threshold under Article 9 of the relevant delegated act is increased so that at least 3 member states must be impacted***

Contacts

Stefano Mazzocchi
Managing Director, Advocacy
stefano.mazzocchi@afme.eu

Marcus Corry
Director, Technology & Operations
marcus.corry@afme.eu