

## Position Paper

### DORA Incident Reporting: implementation lessons

July 2025

#### ***Executive Summary***

The Association for Financial Markets in Europe (AFME) has been supporting the credit institutions within membership to implement DORA's regulatory obligations since its application on the 17<sup>th</sup> January 2025. This has reinforced the operational challenge entailed and brought to light a number of consequences which we believe must have been unintended by policymakers. One of the top areas of concern is that of major incident reporting under Article 19 of DORA. While AFME and its members support greater transparency of incidents which have the potential to create knock-on, possibly systemic impact, there is early evidence of DORA reporting morphing into generic data analysis, rather than focusing on tangible, actionable information which can support incident management.

In particular we are keen to flag the following three themes which have emerged from member banks' first two quarters of reporting under DORA:

- 1. The reports are at risk of proving ineffective for the purposes of incident management by seeking information which bears no relevance to this goal, being neither actionable nor tangible.***
- 2. There are certain data fields and inputs which have not only proved burdensome but at times to be lacking in feasibility.***
- 3. Despite DORA's intention to focus on major incidents and harmonise the process of reporting, the current configurations are capturing minor instances which some NCAs have informed members should not be regarded as major but which are falling foul of the thresholds.***

We set out below in detail where we are seeing these issues arise within the current DORA framework, and would strongly encourage the ECB and ESAs to factor these insights in the upcoming end-of-year review on reporting obligations. AFME is confident that engagement with industry can assist authorities in using incident reporting to bolster operational resilience for the sector and remains on hand to discuss in detail this paper. Please do not hesitate to contact the team via [marcus.corry@afme.eu](mailto:marcus.corry@afme.eu)

- 1. The reports are at risk of proving ineffective for the purposes of incident management by seeking information which bears no relevance to this goal, being neither actionable nor tangible.***

In summary, we understand that authorities will want a thorough and comprehensive understanding of the facts relating to a major incident. Yet, we are concerned that requests for broader information, for example around longer term economic impact, are becoming entangled within the DORA incidents reports, rather than being reserved for other, more appropriate supervisory tools. We would strongly urge authorities in the DORA reports to only seek information which relates to incident management or which provides important insights into the scale of the incident under review. Data fields relating to BAU functions or longer term resolution would not fall within these categories, and risk turning DORA incident reports into generic data analysis. Further detail is provided in the table below:

<b><u>Issue</u></b>	<b><u>Reasoning</u></b>	<b><u>Recommendation</u></b>
Inclusion of BAU employee resourcing within reports as indirect costs	Global multi-national financial entities maintain 24/7 incident response teams as BAU and hence any replacement or relocation costs is not applicable. Identifying a cost for these functions on an incident basis is subjective and complex, while of no value to incident response.	Clarification is sought that only non-BAU costs should be included within an incident report (contrary to some NCA stipulations) e.g. regulatory penalty fines, client costs, P&L costs.
Economic Impact	The cost analysis, subject to 11 different criteria, is often not feasible across all IT infrastructure and business lines, as service costs are typically distributed across the entire institution and cannot be isolated to a single incident but are spread across contract non-compliance fees, communication costs, advisory costs etc In most cases, the immediate costs—such as those related to the incident response and staff time—are unlikely to exceed the €100,000 threshold, making this criterion difficult to apply in real time. Additionally, some NCAs have requested reports on incidents with economic impact where the other thresholds/criteria have not been met.	The economic impact article should be removed as part of the EU simplification agenda. It adds considerable complexity with no value in terms of incident management. Additionally we seek clear guidance on how operational (payment incidents) meeting only economic criteria should be reported or not. At a minimum we recommend that under 'Economic Impact' only payment related costs (interest fees), regulatory penalties/fines for late reporting, expropriated funds and financial assets liabilities should be retained.
Completing and submitting reports for information already captured / provided	For Intermediate or Final submissions, a lot of fields have already been answered on previous reports thereby causing delays in completing a submission with no value-add.	We would welcome an upgrade to the reporting portal so that it can save and pre-populate information from previous reports, with the bank able to edit any necessary updates. This could also be helpful to correct a submission with errors, without having to do a new full submission.
Assessment of risk to critical functions for resolution purposes within the meaning of Article 2 (1), point (35) of Directive 2014/59/EU: & Information relevant for resolution authorities	Given the impact to critical functions during a resolution incident relates to a rare occurrence where an institution is in a wind down event there appears little to no value to have this included in an incident report. Similarly with information for resolution authorities.	This information should be captured within the SRB process as opposed to incorporating this in DORA.

**2. *There are certain data fields and inputs which have not only proved burdensome but at times to be lacking in feasibility.***

While we accept that any new regime will have teething issues, it has already become evident that some of the data required under DORA's incident reporting obligations is proving a major challenge for firms. This has in part been for reasons that are outside of the control of financial entities and

which we anticipate will not be redressed as part of the bedding-in of the regime. A prime example is the requirement for weekend reporting when not all authorities have in place teams and systems which are accessible 24/7. The intermediate reporting timeline of 72 hours also fails to have any value where it includes weekends as additional information is not yet available and hence the same information as the initial incident report is typically submitted. In remedying these oversights, we would encourage the EU institutions to embed greater optionality within the reporting requirements in line with DORA's overarching proportionality principle. Further, as part of the EU's wider simplification agenda, we would encourage authorities to view incident reporting as an area of low-hanging fruit, where investments from authorities in their own systems would result in material savings for industry.

<b><u>Issue</u></b>	<b><u>Reasoning</u></b>	<b><u>Recommendation</u></b>
Weekend Reporting, & intermediate reporting on a Monday	Numerous NCAs do not have 24/7 resourcing to respond to initial reports submitted over a weekend, at times meaning the portal itself is not accessible. Additionally intermediate reports submitted on a Monday will contain little to no new information given market teams will not have been open for business.	i) Initial reports over a weekend should only be sought where an NCA is operational. ii) Amend the 72 hour deadline for intermediate reports to 3 business days.
Multiple Portals to report ICT Related incidents specific to DORA	Different FEs have different regulator portals, i.e. Bafin, CSSF, Spain etc. resulting in multiple different resources required in the end-to-end reporting chain. This can lead to inconsistency in process and an increase of resources. Duplicate NIS reporting at the national level, where only a small number of NCAs have opted to retain this reporting to CSIRTs, further exacerbates this issue.	We would welcome one portal to submit 1 report, i.e. Bafin MVP which then goes to the relevant bodies. This would ensure that only one consolidated report is required with information sharing between authorities for example the SCICF fully utilised to sight relevant authorities.
NCA dissemination of incident reporting	As DORA thresholds are set low, firms are reporting incidents that the NCA decides has not met the materiality threshold. This then means the information is not disseminated to the ECB – and on to other NCAs.	The NCAs should comply with the regulation as written and so do not take a determination themselves on materiality for the purposes of onward transfers.

Sub-business unit level impact splits	Breaking down the impact of incidents at the Strategic Business Unit (SBU) level for multiple units is challenging to do quickly. This level of granularity is not typically required for classifying a major incident under current internal standards, adding complexity to the DORA reporting process.	It should be recognised such break down will not always be possible and therefore this be an optional criteria.
Transferring collected data into the MVP Portal	For all submissions, data has to be either manually typed or Copy and Pasted into the MVP Portal, a considerable manual task which causes delay.	We would like to see greater ability to upload data, or a standard template provided to allow easy transfer rather doubling efforts on data that has already been captured, with data pre-population where relevant.
Root Cause Identification from Third Parties	This data field is outside the control of the financial entity and can create significant delay, as illustrated with the recent ECB T2 outage illustrated.	It should be clarified that this information is only to be provided where available/provided.

***3. Despite DORA's intention to focus on major incidents and harmonise the process of reporting, the current configurations are capturing minor instances which should not be regarded as major but which some NCAs have informed members are falling foul of the thresholds.***

While most credit institutions are familiar with incident reporting, DORA did represent a notable extension in scope, as illustrated by the inclusion of recurring incidents which collectively meet the thresholds on materiality. Early reporting indicates that the regime in practice is not operating as anticipated, with some of these novelties resulting in very minor incidents falling within scope of the reporting requirements. This will only add to the significant operational burden facing both firms and authorities, and we would strongly urge recalibrating those thresholds which have in practice proven to represent a very low bar. As outlined below this can in part be achieved through supervisory clarifications, but a more holistic and ambitious response is warranted, for example abolishing the recurring incidents criteria on the basis it is not meeting the original Level 1 goals of DORA.

<b><u>Issue</u></b>	<b><u>Reasoning</u></b>	<b><u>Recommendation</u></b>
Recurring incidents	Financial entities typically identify vulnerabilities and threats from monitoring, testing and governance, not cyber logging. This is reinforced by the overly broad criteria for cyber logging. For example, a change management root cause could relate to a specific control, business service, or employee error, despite being categorised as a recurring incident. Full analysis and reporting of every recurring incident, regardless of impact, does not link with the proportionality goal of DORA.	Given the level of complexity, cost and confusion which has been caused by this criterion, and the limited relevance to managing major, potentially systemic, incidents, we advocate the removal of recurring incidents from incident reporting. These trends can be gathered by other data analysis tools. Alternatively, limit mandatory follow up reports to incidents where there is a material impact under the Thresholds defined and develop clearer criteria on this threshold which align with the proportionality principle.
Service Downtime	The guidance on service downtime is complex and unclear. An incident may persist without any tangible impact on customers or business, yet technically touch upon the delivery of an SLA.	It should be clarified that only an incident which causes tangible impact is within scope of this criteria.
Rigid reporting timelines for cross-borders incidents	Complex incidents may require inputs from different branches and in some cases third parties.	Proposal of flexible early reporting deadlines for multi-region or evolving incidents. Limit the early reporting to known facts and investigations progress
Incidents occurring in multiple members states / Geographical Spread	This threshold has in practice proved a particularly low bar, due to Group structures, which has considerably increased the volume of DORA reports, but often with little correlation to incident severity. This is particularly problematic given that such incidents will typically require inputs from different branches and in some cases third parties in a different country.	It should be clarified that the geographic spread must be external to the Group's branches. Additionally, where third parties in another member state have provided partial information, only confirmed facts should be incorporated in the initial reports.
Incident Duration	We consider this criterion to be of questionable applicability. The end-to-end management of an event within large financial institutions often exceeds 24 hours in duration, especially when the reference point is the time of occurrence. Therefore, we do not consider this driver to be decisive for identifying the event as a major incident under the DORA framework.	We propose to delete this driver for the identification of an event as a major incident for DORA purposes.

Reputational Impact	The formulation of certain thresholds for this driver (e.g., the incident was reported by the media) leaves space for subjective assessments.	Additional details are desirable to ensure clearer interpretation when a reputational impact occurs. For instance, how to consider news on social media or news reported by online media with lower relevance.
---------------------	---	--

### AFME Contacts

Marcus Corry  
[marcus.corry@afme.eu](mailto:marcus.corry@afme.eu)  
+44 (0)20 3928 2679

Stefano Mazzocchi  
[stefano.mazzocchi@afme.eu](mailto:stefano.mazzocchi@afme.eu)  
+32(0) 2883 5546