Digital Fitness Check

Call for Evidence response - Operational Resilience & Cyber Security

March 2026

Executive Summary

In our Digital Omnibus Call for Evidence, AFME highlighted the need for a sectoral exemption from the Cyber Resilience Act, in light of the level of overlap with DORA. As a general overarching rule, it is vital that horizontal initiatives respect the primacy of sectoral legislation already in operation. Ahead of the trilogue negotiations, our position paper stressed how an exemption provides the most effective solution in terms of simplification, as opposed to the Commission's proposals on a reporting hub (single entry point). The imposition of new authorities, who have the power to amend legal obligations, and even withdraw financial sector applications from the market, on industry participants without interaction from sectoral policymakers, is a dangerous precedent which will inevitably invite unintended consequences.

In this response to the Digital Fitness Check, AFME is demonstrating how such overlap in regulation has direct repercussions in terms of EU compliance and supervision. In particular we are stressing that the overlapping nature of policy has cumulatively resulted in:

- Confusion for industry participants over terminologies having varied meaning and interpretation across inter-related files.
- Inconsistency in the application of carve outs, which requires significant manual reconfiguration from firms, despite the intention of policymakers to reduce regulatory burden.
- A corresponding overlap and duplication within supervisory exercises, with a reluctance in supervisory teams to bundle the various obligations.

This response is intended as evidence of the compliance burden sitting on financial entities, and which is being exacerbated by the failure to adopt bolder Simplification measures. It is intended as supplementary material which supports both our headline ask for a CRA sectoral exemption, and the requests for DORA simplification as outlined in our Call for Evidence. This burden also limits financial institutions' ability to focus resources and expertise on effective digital resilience, diverting attention from substantive controls and preventive activities. Simplification measures are therefore essential to enable operational efficiencies that strengthen the resilience objectives pursued by the legislator.

Confusion for industry participants over terminologies having varied meaning and interpretation across inter-related files.

We highlight how the inconsistent use of terminology, or more commonly slight adjustments of the same terminology, results in banks having to establish multiple approaches to dealing with the same underlying issue. This is currently a live issue with regards to the incoming EBA Guidelines on Sound Management of Third Party Risk, where an expanded interpretation of *Critical & Important Functions (CIFs)* risks forcing financial entities to establish two sets of CIFs – one under DORA and one under the incoming EBA Guidelines for non-ICT purposes.

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

This is particularly unfortunate given that industry supports the EU's underlying intention to break down the distinction in EU regulation between ICT and non-ICT risk in a way that was not previously embedded in the EU regime. While DORA has strengthened oversight of ICT risk, the resulting structural split between ICT and non-ICT risk is generating operational complexity for firms. While ICT services might introduce specific operational risk and resilience considerations and controls, what continues to be most effective are risk-based TPRM frameworks that are designed to adapt to evolving risks and allow firms to calibrate their controls to the characteristics and materiality of each arrangement – including ICT-specific considerations where relevant. Additionally, many services are operationally integrated, ICT-enabled or delivered through blended models; and a bifurcated framework therefore creates arbitrary categorisation challenges that add no value to risk management[1].

A prime existing example of terminologies having varied meaning and interpretation is on the definition of *incident* where we set out below how the parameters differ across several files which are all related to Operational Resilience. While policymakers may take the view that the difference in meaning is limited, the impact for firms is significant. Cumulatively, the below illustrates how an incident can result in firms having to set up and maintain 4 distinct systems or procedures for dealing with the same underlying instance. This is an illustration of the downstream complications which may arise from the dual application of DORA and the CRA, and which can be avoided by a sectoral exemption.

Case Study 1 - Incident definitions:

CRA	'incident having an impact on the security of the product with digital elements' means an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions;
NIS2	'incident' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

[1] This complexity is particularly concerning in the context of third-party registers. DORA already imposes a highly prescriptive and resource-intensive ICT third-party register. The incoming EBA TPRM Guidelines reflect a clear effort to promote consistency across the frameworks and incorporate register requirements that broadly align with DORA. However, as non-legislative guidelines, they do not create the same level of binding harmonisation and leave scope for multiple register templates, divergent data fields, and inconsistent supervisory expectations emerging across NCAs. This would undermine the objective of a harmonised and simplified EU TPRM framework and materially increase operational burden for firms – both in the context of register requirements and the broader design and operation of third-party oversight. From a simplification perspective, the ideal trajectory would be towards a genuinely harmonised EU TPRM framework that avoids structural fragmentation between ICT and non-ICT risk and supports a single, integrated approach to third-party risk management. The cumulative effect of layered regulatory initiatives risks undermining the harmonisation and simplification objectives of the EU

DORA	'ICT-related incident' means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity;
AI Act	'serious incident' means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following: (a) the death of a person, or serious harm to a person's health; (b) a serious and irreversible disruption of the management or operation of critical infrastructure; (c) the infringement of obligations under Union law intended to protect fundamental rights; (d) serious harm to property or the environment;

Inconsistency in the application of carve outs, which requires significant manual reconfiguration from firms, despite the intention of policymakers to reduce regulatory burden

We acknowledge there have been attempts by policymakers to reduce the burden on industry, by providing for targeted carve outs, or partial exemptions when introducing a file which overlaps with pre-existing regulation. A recent example has been in the field of incident reporting, where several files contain partial exemptions, on the basis of reports falling due under a parallel regime. Yet the inconsistent approach to framing these carve outs has resulted in a patchwork of obligations which firms must manually reconfigure and adjust, thereby hindering the intention of policymakers to simplify the regulatory landscape.

Case Study 2: Incident Reporting Exemptions:

- **NIS2 CRA Exemption:** "When a manufacturer notifies a severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 and the incident reporting under that Article contains relevant information as required under paragraph 4 of this Article, the reporting of the manufacturer under Article 14(3) of Regulation (EU) 2024/2847 shall constitute reporting of information under paragraph 4 of this Article."

- **AI Act NIS2 Exemption:** "Under the NIS2 Directive, essential and important entities have to notify the CSIRT or, where applicable, the competent authority of any significant incident… Insofar as these bodies are obliged to report incidents under NIS2, only the additional requirements of reporting violations of fundamental rights apply."

- **AI Act DORA Exemption:** "Therefore insofar AI systems falling under Annex III Point 5 (b) and (c) are considered financial entities in the meaning of Regulation 2025/302, only the additional requirements of reporting violations of fundamental rights apply."[2]

[2] In addition, there might be situations where incident reporting obligations overlap with Article 33 GDPR, when there is a "personal data breach", Article 23 NIS 2 Directive14 on reporting obligations for significant incidents affecting essential and important entities, the Cyber Resilience Act15 . The

- **NIS2 DORA Exemption:** "This Regulation constitutes lex specialis with regard to Directive (EU) 2022/2555… Given that the physical resilience of financial entities is addressed in a comprehensive manner by the ICT risk management and reporting obligations covered by this Regulation, the obligations laid down in Chapters III and IV of Directive (EU) 2022/2557 should not apply to financial entities falling within the scope of that Directive."

It is due to this haphazard patchwork of carve outs that AFME has prioritised the call for a wholesale CRA exemption. Yet should the Commission proceed with CRA application in financial services, we would at the very least request an identical carve out to that which is being proposed under the AI Act; namely that any report filed under DORA suffice for the purposes of the CRA Act. Information submitted via the DORA reports could be automatically transmitted to any other relevant authorities through the proposed reporting hub (single entry point), including for those designated under the Cyber Resilience Act. This would effectively ensure that a single submission is sufficient to fulfil all applicable reporting requirements.

Clarification is needed in any event, given that the European Commission consistently scopes entities within cybersecurity-related legislation according to the scope of NIS2. NIS2 is subject to a DORA *lex specialis* provision, which introduces significant uncertainty when the relevant legislation does not reference the interaction with DORA or the application to financial entities. Indeed, all NIS2 amendments by DG-CONNECT under the simplification agenda provide no indication of application to the financial sector.

A corresponding overlap and duplication within supervisory exercises, with a reluctance in supervisory teams to bundle the various obligations.

In recent years, there has been a plethora of regulatory initiatives across different bodies, agencies and departments within the operational resilience field. This is a welcome reflection of its increased importance within policymakers' priorities. Yet, despite assurances that any overlap in regulatory obligations would be addressed downstream holistically, our experience is that supervisors feel compelled to establish distinct supervisory mechanisms to demonstrate compliance with each regime.

A recent example is how policymakers stressed there was no obligation to establish distinct DORA policies, where the firm had already addressed the risk within existing operational structures. Yet, the recently updated SREP Guidelines suggests that stand-alone DORA policies are in fact required and should be part of an authority's approach. We fear this issue will next arise with regards to the ECB Cloud Outsourcing Guidelines, where firms are already reporting that the intended optionality of outlined practices has not been adopted by supervisors who instead are demanding compliance with each and every aspect. As part of the Simplification process, the Commission should put into motion a review of duplicating supervisory activities, to ensure that the intended reduction in burden is actually felt in practice.

Commission will at a later point specify the interplay between incident reporting under sectorial legislation, horizontal legislations and the AI Act.

The below case study provides further evidence of this issue, by highlighting the overlap between the DORA RMF (Risk Management Framework) Reviews and the ECB's ITRQ (IT Risk Questionnaire). The ECB requires supervised firms to submit the ITRQ under the SREP. The ITRQ is an extensive RFI, covering over 300 separate ICT Guideline-related RFIs covering the entire IT infrastructure of the financial institution. The DORA RMF Review is a 40-50 page overview of a financial institution's approach to digital and ICT risk management. The activities and objectives are duplicative and do not reflect a proportionate or consistent application of the SREP for ECB-supervised institutions, especially given they may be supplemented with an On-Site Inspection, a DORA Threat-Led Penetration Test and additional supervisory engagements.

As part of the simplification agenda, or follow up to the omnibus, AFME calls on EU authorities to be bold and ambitious and remove such overlap and duplication within supervision. This should include scrapping the RMF Review reports, in favour of leveraging the ITRQ submissions.

Case Study 3 – Duplication in the Supervision of ICT risk

DORA RMF Report clause	**RMF Requirement**	**Corresponding ECB IT Risk Questionnaire references**	**Nature of overlap / evidence already required under ECB**
1	Searchable electronic report and reporting format	ECB 5.1–5.4	ECB requires a designed ICT reporting process, secured channels, and regular cadence, which underpin DORA's format requirement.
2(a)	Introductory context, critical functions, dependence on in-house and contracted ICT	ECB 2.5–2.10; 6.1–6.5; 19.1–19.4; 18.1–18.4	ECB mandates inventories of functions, assets, and third-party dependencies; DORA asks to narrate the same data.
2(b)	Date of approval by management body	ECB 2.2; 7.1	ECB requires management body approval and periodic review; DORA requires reporting of those approvals.

2(c)	Reason for the review (e.g., supervisory instructions, incidents)	ECB 4.1; 3.6–3.7; 16.3–16.6	ECB requires post-incident reviews and documentation; DORA asks to cite these triggers.
2(d)	Start and end dates of the review period	ECB 4.4; 22.1–22.9	ECB requires documented follow-up and change schedules; DORA requests the same periodization for the review.
2(e)	Function responsible for the review	ECB 3.5; 2.2	ECB assigns responsibility to control functions and sets governance; DORA requests identifying the responsible function.
2(f)	Major changes and improvements since previous review	ECB 22.1–22.9; 4.1; 3.6–3.7	ECB requires change management and periodic reviews; DORA requests a synthesis of those changes.
2(g)	Findings and severity of weaknesses, deficiencies, gaps	ECB 3.11(i)–(iv); 3.12; 3.9	ECB requires residual risk identification, inventory, acceptance, and review, plus threat monitoring; DORA requires a consolidated analysis.

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

2(h)(i)–(vi)	Remediation measures, timelines, tools, accountable function, resource impact, notifications, residual-risk acceptance	ECB 3.10(a)–(c); 3.11(i)–(iv); 2.2(g); 2.2(i); 11.2(b)	ECB requires risk treatment, monitoring effectiveness, budgeting for resilience, reporting lines, and residual-risk governance; DORA requests the same elements in report form.
2(i)	Planned further developments of the framework	ECB 1.1–1.8; 3.13	ECB mandates forward-looking ICT strategy and alignment with business and risk strategies; DORA requests planned developments.
2(j)	Conclusions of the review	ECB 3.7; 4.2	ECB requires senior ICT reporting to the management body and internal audit cycles; DORA seeks the synthesized conclusions.
2(k)	Past reviews and implementation status	ECB 4.1–4.5	ECB mandates an audit universe, regular ICT audits, and formal follow-up; DORA asks to report the same implementation status.
2(l)	Sources used: internal audit, compliance, digital operational resilience testing (incl. TLPT), external	ECB 4.2; 29.1–29.4; 1.8(g); 11.2(e)	ECB requires these activities and evidence; DORA requires listing them as sources.

AFME Contacts

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

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