Digital Omnibus

Operational Resilience & Cyber Security

January 2026

Executive Summary

- We welcome how increased recognition of the importance of Cyber Resilience has led to significant enhancing of Financial Services sectoral regulation. Insufficient streamlining of regulations across the EU threatens however to lead to regulatory duplication and unnecessary compliance burden.
- Due to the overlap with DORA, the Commission should have proposed a sectoral exemption for financial services from the Cyber Resilience Act. This is a missed opportunity for bold simplification. We urge the European Parliament and Council to challenge this decision not to exempt financial services, as has been done with industries such as aviation and automotives.
- The Commission has recognised the overlay in regulatory requirements through its proposal for an incident reporting hub (single entry point). The benefit would though be in the aggregation of reporting obligations with which market participants must comply. While the omnibus package requires ENISA to take account of the DORA templates, it is stressed that the underlying legal requirements re-main unchanged.

Context

We welcome how increased recognition of the importance of Cyber Resilience has led to significant enhancing of Financial Services sectoral regulation. Insufficient streamlining of regulations across the EU threatens however to lead to regulatory duplication and unnecessary compliance burden.

The growing recognition within EU policymaking of the importance of operational resilience, and in particular cyber security, is a welcome development which will benefit and support the growing digitisation of European markets. Within the field of financial services, the efforts of policymakers and regulators is best represented in the recent passage of DORA (the Digital Operational Resilience Act) which came into effect in January 2025, and which brought with it holistic upgrades in risk management, incident reporting and resilience testing.

The challenge in this widespread shift of attention across departments, regulators and national agencies is ensuring consistency and avoiding unnecessary overlap. As part of the Digital Omnibus, AFME is calling on the Commission to grasp this opportunity for a meaningful stocktake to remove any duplication of compliance burden while continuing to intervene in those parts of the market where there is currently a gap in regulation.

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

Our proposal for EU Simplification

Due to the overlap with DORA, the Commission should have proposed a sectoral exemption for financial services from the Cyber Resilience Act. This is a missed opportunity for bold simplification. We urge the European Parliament and Council to challenge this decision not to exempt financial services, as has been done with industries such as aviation and automotives.

Our priority has been removing the financial sector from the scope of the incoming Cyber Resilience Act (CRA), which has caused significant concern due to the level of overlap with DORA. Indeed, while in theory the two Regulations may appear to complement each other, as product regulation versus entity regulation, in practice they would capture the same systems, applications and operational tools. This reflects the highly digitised nature of the financial sector, with 'Digital channel' products, such as banking apps, online platforms and onboarding portals utilised by customers and clients to access financial services and products. These are in use across all parts of the business and embedded within a bank's IT infrastructure. As a result, these products and any cyber risk arising from them, are addressed under the holistic risk management of DORA.

Any application of the CRA within financial services would lead to duplicative enforcement authorities, additional incident reporting, and a set of needlessly duplicative risk assessments, without any net benefit in terms of cyber risk management. Given the scale of the operational costs associated with imposing this product regulation on financial services, such a scenario would only contradict the Commission's goal of regulatory simplification and competitiveness.

We strongly believe an exemption would be the most effective solution and is in line with the approach taken by the EU on the overlap between DORA and the NIS2 Directive. We wish to reassure this will not impede the EU's objective of enhancing European cyber security, which we fully support. DORA covers the entire lifecycle of a bank's systems/products, from development to decommissioning, and includes risk-based management, incident handling, vulnerability management, and customer communication strategies. While DORA is not itself product regulation, the outcome is nevertheless dual regulation.

Our calls for an exemption have been echoed across all parts of financial services and have been shaped in part by the industry's experience of DORA.

At a minimum, AFME encourages the removal of financial services from the incident reporting requirements under the Cyber Resilience Act. This would build on the recent Commission consultation on reporting under the AI Act, which proposes removing the requirements for incident reporting where there is overlap from DORA reporting. This approach could be extended to any overlap in reporting between the Cyber Resilience Act and DORA, offering a meaningful level of simplification for the sector.

Our concerns with the Commission proposals

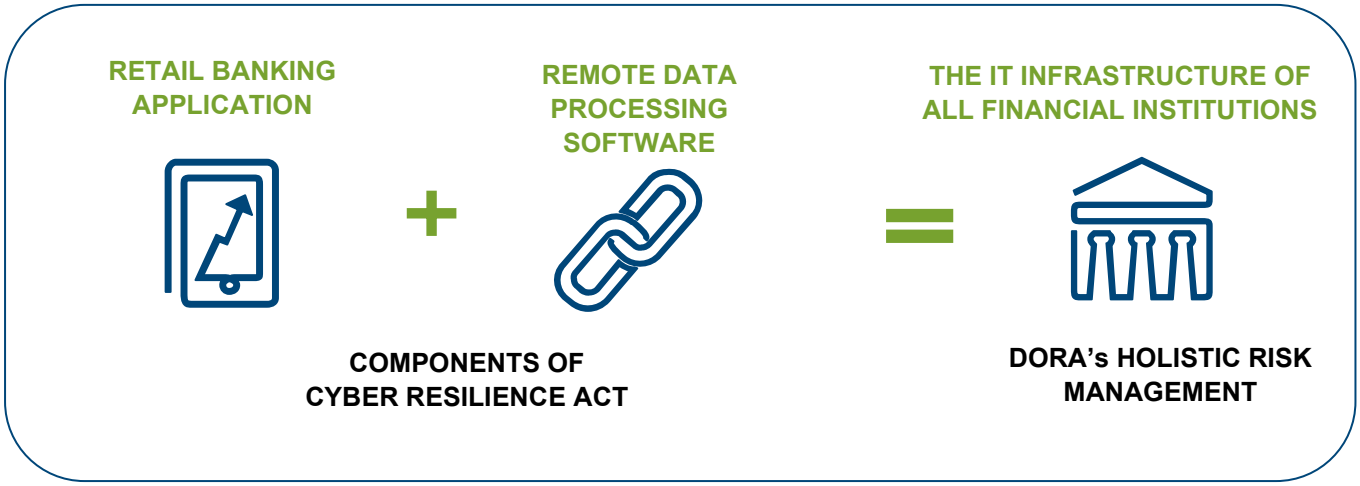
The Commission has recognised the overlay in regulatory requirements through its proposal for an incident reporting hub (single entry point). The benefit would though be in the aggregation of reporting obligations with which market participants must comply. While the omnibus package requires ENISA to take account of the DORA templates, it is stressed that the underlying legal requirements remain unchanged.

The proposal for a single entry point recognises that firms are submitting the same information in different formats and to multiple authorities, not only with regards to the CRA and DORA, but also NIS2, CER, GDPR and eIDAS (with further duplication under the AI Act). While we support the "report once, share many" principle behind the hub proposal, experiences to date indicate that an exemption would be significantly more effective. There is limited, if any, value to firms from a hub which serves simply as a reservoir for multiple, divergent submissions. From the perspective of a bank, this means that distinct, siloed reporting processes and assessments must be retained, with the hub submission likely to serve only as an additional overlay requirement, which does not fulfil the overarching goal of simplification.

Additionally, we are concerned that while there are provisions around the security of the future platform, these do not appear sufficient. Given the sensitive nature of incident data, the central platform itself must be highly secure, resilient, and compliant with relevant cybersecurity standards. Otherwise, it will put the whole industry, including critical infrastructure operators, at risk. As GDPR reports will also be submitted, there is the added dimension of (sensitive) personal data being at risk.

Further information

AFME has produced a series of illustrations demonstrating how the overlap between DORA and the CRA arises in practice, using a retail banking app as the case study. This highlights that when you bring into scope both a banking application and the remote data processing software which supports it, this results in an extensive proportion of back-end IT infrastructure being captured in practice, despite all of this being covered by the holistic risk management of DORA. Please see below a summary, with a full schematic breakdown in the annex.



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

We have also highlighted the importance of a sectoral CRA exemption as part of our publication ***Digital Finance, Simplified***, which was released in advance of the Commission proposals and can be found here. This builds on our earlier briefing of the DORA versus CRA overlap which can be found here.

AFME Contacts

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

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

SCHEMATIC OVERVIEW OF CRA DORA SCOPE DUPLICATION

DORA & UNITENDED CRA SCOPE

INTENDED CRA SCOPE

RETAIL BANKING APPLICATION* + **REMOTE DATA PROCESSING**

- Remote data processing is defined as any software that is necessary for the product with digital elements to function.
- Retail banking applications serve as a channel through which a consumer can receive a range of financial services. Those financial services in turn rely on a large range of applications and supporting infrastructure within the bank to function.
- The definition therefore brings into scope of the CRA all IT systems in the FI that are required for the retail banking application to perform those services for the customer.
- The CRA therefore directly regulates all IT systems of the financial entity creating direct overlap with DORA, an existing cyber regulation that applies to all IT systems in a financial institution.

= **THE IT INFRASTRUCTURE OF ALL FINANCIAL INSTITUTIONS**

UNDERLYING REGULATED PURPOSE**	IT SYSTEMS***	REQUIREMENT OF IT SYSTEM FOR APPLICATION TO FUNCTION
Financial Product	Identity Verification	Required to validate a customer's identity when opening the application.
	Loan Management	Required to manage mortgage applications and accounts.
	Credit Scoring	Required to evaluate customer credit worthiness to determine mortgage eligibility.
	Database Management	Required to store all customer application information including account details, transaction history and personal information.
	Notification	Required to alert customers of account activities and updates.
	Fraud Detection	Required to monitor transactions for fraudulent activity.
	Data Synchronization	Required to ensure consistent data across all IT systems.
Current Account	Account Management	Required to manage customer accounts and update application preferences, such as transaction limits. Accounts with separate IT systems include current, savings, shared, joint, investments, rewards, and relevant cards.
	Transaction Processing	Required to execute and record financial transactions.
	Direct Debit	Required to schedule and execute regular payments.
	Internal Transfer	Required to manage transfers within the same financial institution. Other IT systems include external transfer, out-going, in-going, SEPA settlement.
	Customer Servicing	Required to provide customer support and can include support agent and in-app messaging systems.

*A retail banking application is used as an example of a product with digital elements. Financial institutions have applications that cover investment banking, private banking, asset management and insurance. All IT systems that support these apps, which include all IT systems in the financial institution, are in-scope of the CRA.

** Non-exhaustive examples of services provided through retail banking applications. Other examples include debit cards, wholesale banking applications, asset management apps, investments and insurance.

*** Non-exhaustive examples of IT systems required to ensure services can functions. Certain IT systems (e.g. fraud detection) underpin multiple services and proliferate across all IT infrastructure.

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