Guidance on the interplay between DORA and the Cyber Resilience Act

AFME briefing for DG-FISMA

July 2026

Overview

Under Article 26 of the Cyber Resilience Act (CRA), the Commission shall produce guidance on the interplay between the CRA and Union harmonisation legislation, which we understand would encompass DORA. This aspect was not incorporated within the Implementation Guidance produced by DG-CONNECT at the beginning of 2026 and is now expected within a standalone instrument.

This briefing sets out the rationale for further Guidance by highlighting four ways in which the CRA will overlap with DORA, as the primary set of sectoral rules within the financial sector. It is our overarching position that the Commission should exempt duplicate CRA requirements, or at a minimum ensure that evidence of DORA compliance is sufficient for demonstrating CRA requirements have been fulfilled.

In this submission we are highlighting four overlapping aspects of risk management policy:

1. Vulnerability Management
2. Risk Assessments
3. Technical documentation
4. Incident Reporting

This briefing has been developed as an alternative to a list of CRA products covered by DORA, as legal advice remains unclear as to the intended scope without further clarity on Remote Data Processing Solutions (RDPS). We would strongly recommend that any guidance complement the draft Implementation Guidance by explicitly confirming that mobile banking apps, intended for use on the Union market, are the only example of a CRA product within the financial services sector.

Issues for redress

1. Vulnerability Management

Firstly, there is considerable overlap between the two files in the field of vulnerability management, where the comprehensive DORA obligations would adequately fulfil the security objectives of the CRA. Therefore, where a financial entity has implemented the vulnerability management and patch management requirements of Article 10 of the RMF Delegated Act, this evidence of DORA compliance should suffice for the purposes of the CRA in relation to any products falling under the DORA policy.

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

CRA	DORA
Part II of Annex I to the CRA requires the identification and documentation of vulnerabilities and components contained in the product, the address and remediation of vulnerabilities without delay including through security updates, the application of effective and regular security testing and the disclosure of information about fixed vulnerabilities.	Article 10 of the RMF RTS requires financial entities to develop, document, and implement comprehensive vulnerability management procedures including the identification and updating of relevant and trustworthy information resources to build and maintain awareness about vulnerabilities, the performance of automated vulnerability scanning and assessments on ICT assets with a frequency commensurate to their classification, the verification that ICT third-party service providers handle vulnerabilities and report critical vulnerabilities in a timely manner, the tracking of third-party libraries including open-source libraries, the establishment of procedures for the responsible disclosure of vulnerabilities to clients, counterparties, and the public, the prioritisation of the deployment of patches and other mitigation measures, the monitoring and verification of remediation, and the recording of detected vulnerabilities and monitoring of their resolution. Articles 10(3) and (4) of the RMF RTS further require patch management procedures covering the automated identification of available patches, emergency patching procedures, and deployment deadlines with escalation procedures.

2. Risk Assessments

Similarly, the ICT risk assessment carried out by financial entities under Article 3 of the RMF Delegated Act would cut across the cybersecurity risk assessment obligation imposed by Article 13(2) of the CRA, with CRA products captured under the holistic DORA assessment. We would again urge any guidance to stipulate that an ICT risk assessment under DORA suffices for all CRA products within its scope. This would still safeguard against cyber risk as intended by DG-CONNECT without requiring a duplicate assessment to be conducted by banks.

CRA	DORA
Article 13(2) requires manufacturers to undertake a cybersecurity risk assessment covering the planning, design, development, production, delivery, and	Article 3 of the DORA Risk Management Framework (RMF) RTS requires financial entities to develop, document, and implement ICT risk management policies

maintenance phases of the product with digital elements, with a view to minimising cybersecurity risks, preventing incidents, and minimising their impact. That assessment is to be documented and updated as appropriate and, according to Article 13(4) requires the assessment to be included in technical documentation.	and procedures containing a methodology to conduct ICT risk assessments, the identification of vulnerabilities and threats affecting supported business functions and ICT assets, quantitative or qualitative indicators to measure impact and likelihood, procedures to identify and implement ICT risk treatment measures, and provisions for the monitoring of residual ICT risks.

3. Technical documentation

Thirdly, we note that a financial entity will already have set out the information requested, albeit within a different format and at a holistic architecture level, within the technical documentation requirements under Article 31 of the CRA via a number of DORA policies and reports, namely:

- the ICT risk management framework review report required by Article 27 of the RMF Delegated Act;
- the ICT systems acquisition, development, and maintenance documentation required by Article 16 of the RMF Delegated Act;
- the vulnerability management records required by Article 10 of the RMF Delegated Act.

Rather than requiring firms to submit the same information in a different format, it should be established within any guidance on the interplay between sectoral and horizontal frameworks, that documentation developed under sectoral rules can be directly relied upon as evidence of CRA compliance.

CRA	**DORA**
Article 31 of the CRA requires manufacturers to draw up technical documentation containing all relevant data or details of the means used to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Annex I.	Article 27 of the RMF RTS requires financial entities to submit a report on the review of their ICT risk management framework in a searchable electronic format, containing an executive level summary of the current and near-term ICT risk profile, threat landscape, the assessed effectiveness of controls, and the security posture of the financial entity, together with a description of major changes and improvements to the ICT risk management framework, a summary of findings and detailed analysis of weaknesses,

	deficiencies, and gaps, and a description of measures to address those weaknesses. Article 16 of the RMF RTS requires financial entities to maintain documentation of security practices and methodologies for ICT system acquisition, development, and maintenance, including results of source code reviews, security testing, and the controls implemented to protect the integrity of source code.

4. Incident Reporting.

Finally, we highlight again in the table below how the CRA vulnerability reporting obligations create overlap with the DORA major incident reports. In the event that DORA and CRA reporting are not merged under the ongoing Digital Omnibus proposals, we stress that a financial entity should only be required to report under DORA to financial competent authorities, with that report satisfying CRA requirements, and with CAs responsible for necessary onward disclosure to CSIRTs and ENISA. The duplication on formal reporting is also reflected in terms of the communications with impacted users/clients/counterparties.

CRA	**DORA**
Article 14(1) and (3) of the CRA requires manufacturers to notify simultaneously to the CSIRT designated as coordinator and to ENISA any actively exploited vulnerability contained in their product and any severe incident having an impact on the security of their product.	Articles 17 to 23 of Regulation (EU) 2022/2554 impose on financial entities a parallel tiered reporting obligation in respect of major ICT-related incidents and significant cyber threats, directed to their competent authority. Articles 22 and 23 of the RMF RTS require financial entities to develop, document, and implement a comprehensive ICT-related incident management policy covering the detection and monitoring of cyber threats, the detection of anomalous activities, vulnerability management, evidence retention, and the analysis of significant or recurring incidents, together with mechanisms to promptly detect anomalous activities and criteria for triggering incident response processes.
Article 14(8) requires manufacturers to inform impacted users of the product, and where appropriate all users of the vulnerability or incident.	Article 14(1) of DORA additionally requires firms to responsibly disclose major ICT-related incident or vulnerabilities to clients and counterparts as to the public, as appropriate.

AFME Contacts

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

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