# Position Paper

## EU Cyber Resilience Act – The crossover with DORA

May 2023

**Executive Summary**

This paper summarises AFME's views on the proposed EU Cyber Resilience Act (CRA), published 15 September 2022. This cross-sectoral initiative risks cutting across various sector specific frameworks, most notably the Digital Operational Resilience Act (DORA) in the field of financial services. The latter comprehensively targets cybersecurity risks and vulnerability testing of Information and Communication Technology (ICT) systems, which will duplicate materially with specific Articles proposed within the CRA. The application of the CRA as horizontal product regulation does not reflect the hybrid nature of products and services within financial services and risks creating both policy confusion, duplication of requirements and additional compliance burden with no expected additional value. The CRA should follow the rationale set out within the Network and Information Security (NIS2) Directive and recognise the primacy of financial services regulation over equivalent horizontal regulatory proposals. ***AFME strongly recommends exempting financial services from the Cyber Resilience Act, in line with other heavily regulated industries.***

**Cyber Risk is comprehensively monitored within financial services and addressed with robust, holistic cybersecurity requirements.**

Cybersecurity within financial services has in recent years been the subject of numerous regulatory and legislative initiatives by EU institutions. The consequence is that the policy landscape is now substantially further developed within financial services, with sector-specific frameworks interplaying with horizontal legislation, and regulation in several places being supported or underpinned by technical cybersecurity schemes overseen by the EU Agency for Cybersecurity (ENISA) on either a voluntary or mandatory basis[1]. This ensures that cyber risk is comprehensively tackled and supervised from various angles, with financial institutions investing heavily to put in place the various safeguards.

The incoming applicability of DORA will see further robust controls on cyber risk and corresponding cybersecurity protections across a financial institution's operating model, with any adverse impact on services provided to clients and consumers from cyber vulnerabilities monitored, mitigated against and subject to reporting provisions. Importantly, this milestone regulation takes a holistic approach, compelling financial institutions to factor within their broader digital operational resilience, the cybersecurity of their products and services. Addressing cybersecurity safeguards for products/services at this holistic level is the most effective way of ensuring comprehensive protection in our sector.

The complexity of the regulatory landscape mirrors the fast-evolving maturity of cybersecurity, but it can obscure EU policymakers' underlying objectives and create confusion over how the individual pieces

[1] We note non-exhaustively the NIS Directive; the Cybersecurity Act; the EBA ICT and security risk management guidelines; the Digital Operational Resilience Act; the EBA outsourcing guidelines, the G7 fundamental elements for third-party cyber risk management in the financial sector; the EU-TIBER framework for testing financial sector resilience to cyber-attacks; and the European Cybersecurity Certification Schemes.

fit together and which takes precedence. The overarching goal of the Commission within DORA to simplify and harmonise this growing plethora is strongly supported by industry. Similarly, the decision to recognise, within the NIS2 Directive, DORA as *lex specialis* is warmly welcomed as further integration with the existing state of play. Such streamlining brings real benefits in terms of driving down costs and encouraging competition.

Going forward, it is crucial that as the European Commission inevitably seeks to build on its cybersecurity strategy, it continues to recognise the collective body of law which is already in place. This should include the developments at the global level, where the Financial Stability Board (FSB) is striving to harmonise growing international divergence in cybersecurity[2]. Taking account of the wider perspective is the most effective way of securing policy objectives and ensuring that additional measures reap rewards.

**The natural consequence of this approach would be to exempt financial services from the CRA, as is the case with a number of other heavily regulated industries**. **Such an exclusion, by virtue of DORA, has already been proposed by both European Parliament committees reviewing the CRA (ITRE and IMCO). We fully support the relevant tabled amendments** (noted below).

Viewing the CRA as a complimentary addition to the financial services' cybersecurity landscape, by virtue of being product regulation, draws an artificial distinction with the existing body of regulation which does not reflect commercial realities. DORA, in comparison to the CRA, is more prescriptive and sets higher expectations and requirements for financial services.

**Imposing a horizontal framework on top of DORA risks confusion and could bring about a compliance burden which hinders competition within financial services.**
In the event that the Commission proceeds with applying the CRA to the financial services sector, there is considerable concern this would conflict with the incoming application of DORA. At the overarching level, we flag firstly that to dissect a firm's products from its wider digital operational resilience would run counter to the holistic approach of DORA. Secondly, the creation of new, horizontal arrangements conflicts with the Commission's goal within DORA of harmonisation in this field. A clear example is the introduction under the CRA of further reporting and notification thresholds (Art 11), which DORA explicitly sought to harmonise for the financial sector. At a minimum, any market surveillance and enforcement powers should sit with financial supervisors for the entities they supervise.

More specifically, provisions within the CRA have the potential to overlap and misalign with numerous DORA provisions. There is particular concern over the requirements within Annex 1 of the CRA, where:

- Obligations on identifying and documenting vulnerabilities within products could overlap with the identification of risks and vulnerabilities under DORA (Art 8).
- Regular testing of products could be captured within the wider and far more comprehensive DORA resilience testing which will be undertaken by financial institutions (Art 25).
- Disclosure of vulnerabilities/reporting obligations under the CRA could cut across reporting provisions on cyber incidents under DORA (Art 19). Likewise, information sharing on

[2] FSB, Recommendations to Achieve Greater Convergence in Cyber Incident Reporting, Final Report, April 2023

vulnerabilities and identified risks are already captured by either the DORA provisions on communication (Art 14) or by the information sharing arrangements on cyber threats (Art 45). By way of example, if a financial services product suffered from a cyber vulnerability, this would already be subject under DORA to a number of potential disclosure requirements:

  - In the event that clients are even potentially affected from a cyber threat, firms shall inform them of any appropriate protection measures which should be considered.
  - Crisis communication plans would further ensure responsible disclosure of vulnerabilities to clients and counterparts as well as to the public where appropriate.
  - In the event it created a major ICT-related incident the firm would be subject to mandatory notification requirements with regards to the competent financial authorities.
  - In the event it amounted to a significant cyber threat, notification could be broadened to any relevant cross-sectoral authorities such as ENISA.

- The need for configuration settings, access controls and encryption strategies are addressed by the ICT security policies and information security policies due under DORA (Art 9).
- Data protections could be duplications of the DORA provisions on protection and prevention (Art 9).
- Finally, requirements on protecting the availability of essential functions would be addressed either by DORA's response and recovery provisions which apply to financial institutions themselves (Art 11) or through the oversight of Critical Third Parties (Art 33).

On the other hand, requirements under the CRA can appear inappropriate or ill-fitting with the financial services industry, for example the requirements on applying security updates, patches and resets do not reflect how the financial entity may typically retain operational control of the 'product' (e.g., banking app) throughout its lifecycle.

Additionally, should financial services institutions be compelled to perform the product conformity assessments under the CRA, alongside significant DORA requirements, we are of the view that the resulting compliance burden is likely to disproportionately impact smaller firms, impeding the Commission's wider support for greater competition in the sector. Initial analysis by an AFME member firm identified how over two hundred applications may be impacted, across virtually all their business lines, by virtue of being considered '*remote data processing solutions necessary for the product to function'* (Art 3.2).

**AFME strongly recommends that the Commission exempt financial services from the Cyber Resilience Act. DORA is a milestone regulation which ensures the same level of protection, if not greater, than that provided for within the CRA. As is the case with several other heavily regulated industries, our sectoral rules should have precedence.**

ANNEX: Suggested Amended Wording

Insert within CRA Article 2.2 a new subclause "*(d) Regulation (EU) 2022/2554*".

| Existing text | Proposed text |
|---|---|
| This Regulation does not apply to products with digital elements to which the following Union acts apply: (a) Regulation (EU) 2017/745; (b) Regulation (EU) 2017/746; (c) Regulation (EU) 2019/2144. | This Regulation does not apply to products with digital elements to which the following Union acts apply: (a) Regulation (EU) 2017/745; (b) Regulation (EU) 2017/746; (c) Regulation (EU) 2019/2144; ***(d) Regulation (EU) 2022/2554*** |

Note: In effect, this reflects **Amendment 210 tabled before the ITRE Committee** and **Amendment 115 before the IMCO Committee.**