EU Cyber Resilience Act

AFME Trilogue Position Paper

October 2023

Executive Summary

- AFME has called publicly for a sectoral exemption from the Cyber Resilience Act (CRA) on the basis of our view that "products with digital elements" within scope of the CRA will already be captured under the Digital Operational Resilience Act (DORA)[1]. A sectoral exemption would have brought financial services into line with other heavily regulated industries, who are likewise being exempted by virtue of key sectoral legislation.
- While short of our sought-after exemption, we welcome the Parliament explicitly referencing the incoming DORA/CRA overlap within their position. It is critical such provision is retained within the final compromise text and we set out below how the overlap would arise without further action. Similarly, we support the Parliament in calling for guidelines on how this horizontal Regulation relates to sectoral legislation, especially with regards to Remote Data Processing Solutions. We would look forward to building on our engagement to date with the Commission in the development of these Guidelines.
- Annex 1 of the CRA reflects the essential requirements and security risks for products with digital elements. The Appendix within this paper outlines how all requirements are extensively achieved, and exceeded, with DORA for financial services. The comprehensive gap analysis provided within this document is clear evidence that financial services should be exempted from the majority of requirements within the CRA.
- We also voice concern over the proposal by the Council and Parliament to in future mandate use of the EU's cybersecurity certification schemes: while there remains localisation requirements within these schemes, any mandatory imposition could detrimentally impact cybersecurity resilience. Furthermore, the policymaking process for implementing acts, as demonstrated within the cybersecurity certification schemes, is opaque and enforcing their usage could result in unintended consequences while the certification schemes have yet to be finalised.

AFME supports the Parliament in specifically addressing the incoming overlap with DORA, which will inevitably flow from its holistic approach to cyber risk across a firm's operating model. AFME further supports the Parliament in requiring the Commission to issue sectoral guidelines outlining the interplay between the CRA and other Union law, including DORA.

AFME fully recommends the inclusion of amended Recital 14(b) within the European Parliament text:

[1] DORA applies to financial entities' ICT systems and services. A financial entity's ICT systems and services constitute all of their digital products and remote data processing solutions and result in the scope of both DORA and the CRA being one-and-the-same.

> "*Regulation (EU) 2022/2554 establishes a number of requirements to ensure the security of network and information systems supporting the business processes of financial entities.* ***The Commission should monitor the implementation of this Regulation in the financial sector, to ensure compatability and to avoid overlaps for products with digital elements that may also be covered by Regulation (EU) 2022/2554***."

AFME fully recommends the inclusion of Recital 4a with the European Parliament text:

> "*The horizontal nature of this Regulation means that it will have an impact on very different segments of the Union's economy. It is therefore important that the specificities of each sector are taken into account and that the cybersecurity requirements laid down in this Regulation are proportional to the risks.* ***The Commission should therefore issue guidelines which explain in a clear and detailed manner how to apply this Regulation. Guidelines should cover inter alia a detailed explanation of the scope, in particular the notion of remote data processing*** *and the implications for free and open-source developers, the criteria used to determine how critical products with digital elements are classified and the interplay between this Regulation and other Union law*."

As we have previously argued, the incoming applicability of DORA will see robust controls on cyber risk, ICT risk management 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 and comprehensive testing requirements. DORA applies to a financial entities entire network and information systems and ICT services, all of which constitute their digital products and services. Addressing cybersecurity safeguards for products/services is most effectively addressed for financial services at the holistic level to more accurately reflect their business models and ICT infrastructure.

We highlight three examples where without further action the overlap between DORA and the CRA will occur, largely by virtue of the currently proposed definition of *Remote Data Processing Solutions* under Article 3(2).

A. Banks can provide merchant servicing (payment acquiring) services to a range of business customers including small and medium size businesses. These clients can be EU citizens or organisations, or from any other part of the world in which the firm operates. The bank would typically run a tool for the onboarding of those customers which allows them to access a webpage to get information on how to operate point of sale devices properly. The tool does not itself hold any data or provide any payment services or transactions. It is simply a feature to help merchants connect and operate the product correctly to ensure that payments operate smoothly. It is our understanding that such tools would currently fall within the scope of both regulations.

B. Banks now typically provide mobile banking apps for their customers as part of their digital offering. The app itself is not the actual product, but rather a channel of communication connecting the consumer to the bank's services and products. Critically, as a channel of communication, the bank retains operational control over the app, typically applying security

updates, patches and resets, and with ownership of the app's data. These apps fall within scope of DORA and yet have been specifically flagged within the Commission's reasons for and objectives of the CRA proposal.

C. Banks offer mortgage calculators to aid retail customers in understanding how different mortgage products act in practice and how the products could relate to their financial goals. These often include jurisdiction-specific mortgage products, which are prevalent with government policy to encourage differing forms of home ownership. As calculators are accessible by any citizen, the calculator will come into-scope as a digital product that is accessible by an EU citizen, thus bringing into scope all international mortgage calculators across any jurisdiction worldwide. Mortgage calculators do not hold any sensitive information and do not constitute a cybersecurity risk.

AFME looks forward to working closely with officials on how to carve out functions such as the above from the CRA's scope, both during and after the trilogue negotiations. We would especially welcome the opportunity to engage with officials in the development of Guidelines as proposed by the Parliament within its amended Article 17a:

> *"The guidelines shall be published by ... [12 months after the date of entry into force of this Regulation] and shall be updated as necessary, in particular in light of potential amendments to the list of critical products set out in Annex III. They shall contain at least the following elements:* ***(a) a detailed explanation of the scope of this Regulation, with a particular focus on remote data processing solutions*** *and free and open-source software;"*

Additionally we caution against any mandating of the European cybersecurity certification schemes pursuant to Regulation (EU) 2019/881.

In principle, AFME supports the proposed presumption of conformity with regards to the European cybersecurity certification schemes. We fully agree with the institutions that manufacturers and distributors who have met the high technical standards of these ENISA-developed schemes should be spared the burden of additional assessments of conformity.

However, while there remains any localisation requirements within these schemes, even on a partial or limited basis, we strongly warn against any mandating of the schemes, for fear that these technical measures could provoke unintended consequences which are ultimately counterproductive for cybersecurity purposes. The Cybersecurity Act, which proposed certification schemes, stated that the schemes are voluntary and should seek to encourage harmonisation instead of enforcing harmonisation. Firms should be free to adopt cybersecurity products purely on the basis of technical expertise, rather than where a provider of such products is based. The policymaking process for the certification schemes, as is currently being demonstrated, has been opaque and could result in enforcing requirements that have unintended consequences for cybersecurity in the EU. We would recommend not enforcing the usage of these schemes before they are finalised and the impact of the schemes are fully understood.

We therefore strongly caution against the adoption of amended Article 27(a) within the Council text:

> *"in order to ensure a common adequate cybersecurity protection of these products with digital elements in the Union, it could be adequate and proportionate to subject these products, by means of a delegated act, to mandatory European cybersecurity certification where a relevant certification scheme covering those products is already in place and an impact assessment has been carried out by the Commission*."

Likewise, we caution against the proposed Article 6a(2)(b) within the Parliament text:

> *"The Expert Group shall advise the Commission with regard to the following… the implementation of European cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 and on the possibility to make them mandatory for highly critical products with digital elements;"*

AFME Contacts

Coen Ter Wal
Coen.terwal@afme.eu
+44 (0)20 3828 2727

Marcus Corry
marcus.corry@afme.eu
+44 (0)20 3828 2739

Stefano Mazzocchi
Stefano.mazzocchi@afme.eu
+32 2 8835546

Further information

AFME has particular concern over the requirements set out within Annex 1 & 2 of the CRA. We outline below the objectives for each respective product, to highlight the level of duplication:

Annex 1: Security requirements relating to the properties of products with digital elements

Objective 1: Products with digital elements shall be delivered with a secure by default configuration, including the possibility to reset the product to its original state.	
DORA overview	• DORA contains a distinct section on ICT operations security where a fundamental element to the section is ensuring the maintenance and recovery procedures of an entity's ICT services and systems. A continuous requirement for vulnerability scanning and testing, referred to in further distinct sections, alongside explicit statements on the ability to reset, restart and recover or have alternative availability of systems and services deliver on the stated objective.
Relevant references	• RTS Risk Management Framework, Article 8, ICT operating policies and procedures • RTS Risk Management Framework, Article 13, Network security management • RTS Risk Management Framework, Article 14, Securing information in transit • RTS Risk Management Framework, Article 16, ICT systems acquisition, development and maintenance

Objective 2: Products with digital elements shall protect the confidentiality of store transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms.	
DORA overview	• DORA has a stated overall objective to protect the confidentiality of data and is expressed through all relevant Chapters and Articles in the text. All incident management and response and testing of ICT systems aspects, equally, relate to a criteria concerning the loss of confidential data and all responses and learning objectives there relate to ensuring an entity is securing data in an effective matter. Encryption is enforced in a specific Article.
Relevant references	• DORA, Article 5, Governance and organisation • DORA, Article 9, Protection and prevention • DORA, Article 12, Backup policies and procedures, restoration and recovery procedures and methods • DORA, Article 18, Classification of ICT-related incidents and cyber threats

	• DORA, Article 26, Advanced testing of ICT tools, systems and processes based on TLPT • RTS Risk Management Framework, Article 3, ICT risk management • RTS Risk Management Framework, Article 4. ICT asset management policy • RTS Risk Management Framework, Article 6, Encryption and cryptographic controls • RTS Risk Management Framework, Article 8, ICT operating policies and procedures • RTS Risk Management Framework, Article 10, Vulnerability and patch management • RTS Risk Management Framework, Article 11, Data and system security • RTS Risk Management Framework, Article 13, Network security management • RTS Risk Management Framework, Article 14, Securing information in transit

Objective 3: Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions.	
DORA overview	• Protecting the integrity of data is within the stated objectives of DORA and is therefore referenced throughout all relevant Chapters and Articles. Monitoring, authorised access and the security of ICT systems, in relation to internal actors, is stated throughout all risk management sections and through logging requirements.
Relevant references	• DORA, Article 6, ICT risk management framework • DORA, Article 9, Protection and prevention • DORA, Article 12, Backup policies and procedures, restoration and recovery procedures and methods • RTS Risk Management Framework, Article 6, Encryption and cryptographic controls • RTS Risk Management Framework, Article 8, ICT operating policies and procedures • RTS Risk Management Framework, Article 12, Logging • RTS Risk Management Framework, Article 18, Physical and environmental security

Objective 4: Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data').

DORA overview	• DORA has a stated requirement that entities should securely delete data, on-premise or stored externally, that the entity no longer needs to collect or to store.
Relevant references	• RTS Risk Management Framework, Article 11, Data and system security

Objective 5: Products with digital elements shall protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks.	
DORA overview	• The availability of ICT systems and services, alongside resilience and cybersecurity, are foundational elements of DORA and are referred to throughout all Chapters and Articles.
Relevant references	• DORA, Article 5, Governance and organisation • DORA, Article 9, Protection and prevention • DORA, Article 14, Securing information in transit • RTS Risk Management Framework, Article 1, General elements of ICT security • RTS Risk Management Framework, Article 3, ICT risk management • RTS Risk Management Framework, Article 4, ICT asset management policy • RTS Risk Management Framework, Article 6, Encryption and cryptographic controls • RTS Risk Management Framework, Article 8, ICT operating policies and procedures • RTS Risk Management Framework, Article 13, Network security management • RTS Risk Management Framework, Article 25, Components of the ICT business continuity policy • RTS Risk Management Framework, Article 27, ICT response and recovery plans

Objective 6: Products with digital elements shall minimise their own negative impact on the availability of services provided by other devices or networks.	
DORA overview	• As DORA applies to all of a financial entity's ICT systems and services, there is an intrinsic embedment of minimising their negative impact on the availability of services provided by other devices or networks. Continuous requirements to monitor and to continual learn to enforce resilience ensure that any negative impacts are observed and resolved.
Relevant references	• DORA, Article 5, Governance and organisation • DORA, Article 9, Protection and prevention • RTS Risk Management Framework, Article 1, General elements of ICT security

	• RTS Risk Management Framework, Article 8, ICT operating policies and procedures

Objective 7: Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces.	
DORA overview	• DORA, as it applies to ICT systems and services, applies a requirement that all aspects of the regulation shall adapt according to the cyber-threat landscape and external environment. This ensures that reducing attack surfaces or external interfaces are all considered on the basis of their prevalence within the cyber-threat landscape.
Relevant references	• DORA, Article 13, Learning and evolving • RTS Risk Management Framework, Article 1, General elements of ICT security • RTS Risk Management Framework, Article 3, ICT risk management • RTS Risk Management Framework, Article 6, Encryption and cryptographic controls • RTS Risk Management Framework, Article 11, Data and system security

Objective 8: Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	
DORA overview	• DORA introduces a harmonised incident reporting regime for all financial services in the EU, which will be subject to a further Regulatory Technical Standards. Embedded within incident reporting requirements is a requirement on entities to ensure they learn from incidents and therefore design, develop and produce digital systems and services that reduce any impact of an incident. All risk management Articles additionally require any system or monitoring of incidents to influence an entity's operations.
Relevant references	• DORA, Article 6, ICT risk management framework • DORA, Article 11, Response and recovery • DORA, Article 13, Learning and evolving • DORA, Article 17, ICT-related incident management process • DORA, Article 18, Classification of ICT-related incidents and cyber threats • RTS Risk Management Framework, Article 15, ICT project management

Objective 9: Products with digital elements shall provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions.	
DORA overview	• Financial services has prior regulatory guidelines on access management and the monitoring of internal activity, including the access to or modification of data is common practice. DORA further enforces these guidelines.
• **Relevant references**	• RTS Risk Management Framework, Article 21, Identity management • RTS Risk Management Framework, Article 22, Access control • RTS Risk Management Framework, Article 23, ICT-related incident management policy • RTS Risk Management Framework, Article 24, Anomalous activities detection and criteria for ICT-related incidents detection and response

• **Objective 10**: Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.	
• **DORA overview**	• DORA includes a risk management article outlining requirements regarding vulnerability and patch management. DORA further requires financial entities to test their ICT tools and systems and to scan and monitor all services and systems for vulnerabilities.
• **Relevant references**	• DORA, Article 8, Identification • DORA, Article 13, Learning and evolving • DORA, Article 25, Testing of ICT tools and systems • RTS Risk Management Framework, Article 10, Vulnerability and patch management • RTS Risk Management Framework, Article 23, ICT-related incident management policy

Annex 2: Vulnerability handling requirements

Objective 1: Identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product.	
DORA overview	• DORA's vulnerability management requirements including scanning and assessments of vulnerabilities, with weekly scanning requirements for critical or important functions. Entities will have to identify information resources to build and maintain awareness concerning any vulnerability.

Relevant references	• DORA, Article 8, Identification • RTS Risk Management Framework, Article 10, Vulnerability and patch management

Objective 2: In relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates.	
DORA overview	• DORA introduces vulnerability management procedures which includes the need to emergency procedure for patching and updating ICT assets alongside a requirement to test any procedures beforehand.
Relevant references	• DORA, Article 13, Learning and evolving • RTS Risk Management Framework, Article 10, Vulnerability and patch management

Objective 3: Apply effective and regular tests and reviews of the security of the product with digital elements.	
DORA overview	• DORA's vulnerability management requirements including continual scanning and assessments of ICT systems and services. Critical and important functions are required to be assessed on a weekly basis.
Relevant references	• DORA, Article 8, Identification • DORA, Article 24, General requirements for the performance of digital operational resilience testing • DORA, Article 25, Testing of ICT tools and systems • RTS Risk Management Framework, Article 10, Vulnerability and patch management

Objective 4: Once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities.	
DORA overview	• DORA's vulnerability management Article includes a requirement to responsibly disclosure vulnerabilities to clients, counterparts and the public when appropriate. As DORA applies to all ICT systems and services, there is not a requirement for public disclosure in all circumstances as is appropriate.
Relevant references	• DORA, Article 14, Communication • RTS Risk Management Framework, Article 10, Vulnerability and patch management

Objective 5: Put in place and enforce a policy on coordinated vulnerability disclosure.

DORA overview	• DORA's vulnerability management Article includes a requirement to responsibly disclosure vulnerabilities to clients, counterparts and the public when appropriate.
Relevant references	• RTS Risk Management Framework, Article 10, Vulnerability and patch management

Objective 6: Take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements.	
DORA overview	• DORA's vulnerability management requirements include a requirement for third parties entities to report vulnerabilities to the financial entity and to track and monitor usage of third parties.
Relevant references	• DORA, Article 1, Subject matter • DORA, Article 14, Communication • RTS Risk Management Framework, Article 10, Vulnerability and patch management

Objective 7: Provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner.	
DORA overview	DORA's vulnerability management requirements include requirement to ensure that exploitable vulnerabilities are fixed in a timely manner. This includes scanning and assessments on critical functions on a weekly basis and the testing of any software and hardware patches.
Relevant references	RTS Risk Management Framework, Article 10, Vulnerability and patch management

Objective 8: Ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	
DORA overview	• DORA's vulnerability management requirements include patch management procedures which and tested and deployed previously while also requiring emergency procedures.
Relevant references	• RTS Risk Management Framework, Article 10, Vulnerability and patch management