EU Cyber Resilience Act

AFME Supplementary Briefing on the Depth and Breadth of Scope for the Financial Sector: Case Study of a Retail Banking Application

September 2025

Executive Summary

The Association for Financial Markets in Europe (AFME) supports DG-CNECT's intent to enhance cybersecurity across the EU market within the incoming Cyber Resilience Act (CRA). We recognise the incoming product-based framework will bring greater levels of protection and assurance, including in financial services. We remain however highly concerned by the level of overlap with sectoral rules in the field of financial services, namely DORA, which is likely to lead to misaligned supervisory expectations, unintended consequences and significant operational costs on firms with no corresponding benefit in terms of risk management. The CRA is the first product legislation to apply to financial services. Intangible services have historically been exempted from product-based regulation. As such, the CRA introduces new enforcement authorities, differing incident reporting bodies and terminology that does not adapt correctly to intangible services.

AFME, alongside all financial sector associations, continues to advocate that **the most effective solution would be to exempt from the CRA, by virtue of the delegated act under Article 2(5) and through the Guidance under Article 26(2)(c), all products which fall under DORA**, as called for in our Level 2 position paper and in the Joint Statement on Duplication in the Cyber Resilience Act, which maps the overlay between the CRA's Cyber Essentials Requirements and the DORA's Risk Management Framework. We are in parallel urging the Commission as part of the EU Simplification Agenda, to exempt financial services from the CRA, by virtue of a sectoral exemption under the digital omnibus package.

This paper is intended as further illustration of the level of overlap, as the basis for our continued calls for such an exemption. With the Commission currently looking at how to simplify aspects of its digital rulebook, including in cybersecurity, we look forward to these proposals and see CRA/DORA as a clear opportunity for removing duplication without lowering resilience.

AFME remains on hand to discuss in detail this position paper, or any of our advocacy on this important file. Please do not hesitate to contact the team via marcus.corry@afme.eu

The CRA applies to all 'products with digital elements' in the financial sector. The financial sector is highly digitised and involves significant customer and client interaction, resulting in a broad application of the CRA across the sector. 'Digital channel' products, where customers and clients access their financial services, are exhibited across all subsectors with the financial sector, and drive the breadth of the CRA's scope.

AFME has previously flagged examples of products with digital elements which are used by financial institutions through our trilogue position paper. This however does not fully illustrate the breadth of scope across all aspects of the sector. The financial sector encompasses a significant array of subsectors, all of which utilise products with digital elements as digital channels or business applications for customers and clients to access their financial services. Subsectors include banking, investment banking, asset management, payment services, FinTech, mortgage companies, credit unions, private banking and wealth management, insurance and foreign exchange services amongst others.

The below list is a non-exhaustive overview of products with digital elements that align to examples provided by the Commission concerning what is in scope of the CRA. All examples are in-scope of DORA and therefore demonstrate that the scope of the CRA and DORA intersect heavily and will result in a significant compliance burden for the financial sector.

Figure 1: Examples of products with digital elements in the financial sector.

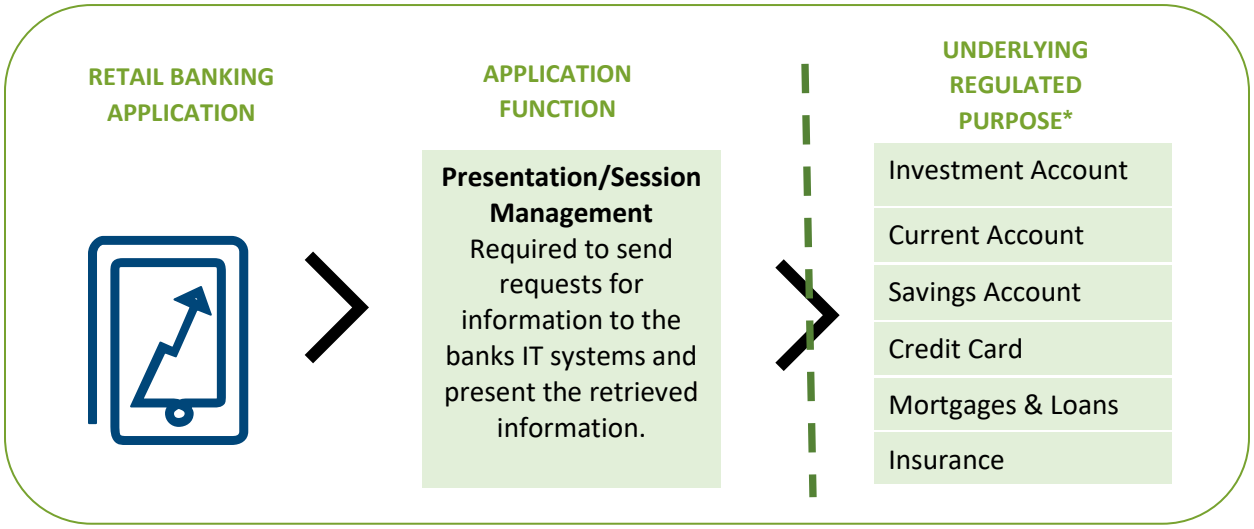
Products with Digital Elements	Financial Sector Examples
Mobile Applications	Retail banking applications
	Investment/trading platforms
	Money/payment transfer applications
	Investment research applications
	Digital asset applications
	Lending/credit applications
	Business banking financial management applications
	Large corporate/ institutional client financial management applications
Smartcards	Retail banking credit and debit cards
	Business banking cards
Hardware devices	Point of Sale terminals
	Automated Teller Machines
	Banking kiosks

The CRA introduces further duplication with DORA due the depth of application of the CRA's requirements to the IT infrastructure of in-scope businesses. The CRA applies to products with digital elements and all of the data processing that is required to allow the product to function. The depth

of data processing required to allow financial sector applications to function is extensive and *de facto* results in the CRA applying to an extensive proportion of back-end IT infrastructure. This AFME paper will use the example of a retail banking application to demonstrate the depth of the CRA's scope and provide further clarification regarding the duplication with DORA.

A majority of the products with digital elements included in Figure 1 are a small aspect of the scope overlap with DORA. This flows from the fact that the "product" practically serves as a digital channel for accessing the underlying financial services, whether this be a current account or financial loan. A retail banking application, for instance, acts as a digital channel whereby a customer can access their banking account, cards, mortgages, loans or private investments.

Figure 2: Retail banking application as a digital channel for financial services.



*Non-exhaustive list.

These financial products are supported by a range of IT systems responsible for data processing, storage and integration alongside other functionalities. As a vertically integrated application for all retail banking services, the IT systems include all relevant IT infrastructure that are required to provide all relevant financial services (e.g. current accounts, transactions, fraud detection, onboarding, data synchronisation). Figure 3 provides further detail to show the range of IT systems that provide data processing and are required for a retail banking application to function.

Figure 3: IT systems used for data processing in a retail banking application.

IT SYSTEMS[1]	REQUIREMENT OF IT SYSTEM FOR APPLICATION TO FUNCTION (non-exhaustive list)
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 eligibility for differing financial services.
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 (note customers hold multiple financial services that interrelate).
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.

Without a financial sector exemption or explicit clarification within the Level 2 technical standards, financial institutions will conclude they are compelled to treat as in-scope the IT systems accessed through the application that provide data processing and are critical for the product to function. This is reinforced by the fact the scope of the CRA extends to remote data processing solutions which are defined as any data processing that is necessary for the product with digital elements to function.

[1] 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.

Figure 3 provides evidence, through the example of a retail banking application, that the CRA's scope will extend through a significant proportion of the IT infrastructure of financial institutions and materially overlap with DORA's scope. The depth of the scope in the case study will be shown across all products with digital elements included in Figure 1, bringing a high number of IT systems across private banking, insurance, banking, payment services and asset management where business to client interaction is high. By bringing into scope all IT systems responsible for data processing, the CRA in effect captures and directly regulates a high number of IT systems creating the substantial and direct overlap with DORA.

The extent of the overlap outlined is causing significant concern amongst the financial services industry, and is the basis of our continued calls for an exemption of all products covered by DORA, by virtue of Article 2(5) and through the Guidance under Article 26(2)(c).

Figure 4

SCHEMATIC OVERVIEW OF CRA DORA SCOPE DUPLICATION

DORA & UNINTENDED 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.

AFME Contacts

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

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