Joint Statement on Duplication in the Cyber Resilience Act

The Cyber Resilience Act ("CRA") reflects the increasing importance cybersecurity plays within a modern economy. Ensuring that all sectors are focused on mitigating vulnerabilities within the lifecycle of their digital products is the correct objective, however as stated within the CRA, there are sectors such as the financial sector who already have strong cyber resilience. The Digital Operational Resilience Act ("DORA") introduces a comprehensive cybersecurity and ICT risk management regime that introduces equivalent requirements for financial services to the CRA. The duplication between DORA and the CRA could result in a highly complex regulatory landscape for financial services and we therefore support the amendments by the European Parliament (Recitals 4(a) and 14(b)) that reference the compatibility of the CRA with other Union rules, notably DORA and financial services:

> 4a: *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.*
>
> 14b: *Regulation (EU) 2022/2554 of the European Parliament and of the Council 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 compatibility and to avoid overlaps for products with digital elements that may also be covered by Regulation.*

1. The scope of the Cyber Resilience Act

Financial services is a heavily regulated-sector with dedicated regulators, vertical rules applying solely to the sector and its own supervisory regime. The CRA is intended to be a horizontal product regulation and therefore utilises different terminology and definitions. This is most notable in the definitions used to set the scope for the CRA in comparison to existing cybersecurity and ICT risk management rules; definitions in DORA and many other cybersecurity rules apply to an institution's ICT infrastructure, whereas the CRA applies to products. However, for organisations such as financial entities that do not produce physical products and instead offer services often consumed through software via a web interface, it is not possible to distinguish between the product and the ICT systems in which that product exists.

DORA applies to a financial entity's network and information systems and their ICT services. These are the same systems in which their products with digital elements and all of the ancillary remote data processing exist. As a result, the scope of both the CRA and DORA are one-in-the-same. For instance, a financial entity's banking application for a retail product is a product with digital elements while at all times being governed by the rules which apply to all of the associated network and information systems and ICT services that enable its functionality. An investment bank's digital trading platform, equally, would represent a digital product, whilst also fundamentally being part of a bank's network and information systems and all of their ICT services.

The entire technological infrastructure of a financial entity is within scope of DORA and, therefore, as all products with digital elements are indistinguishable from a financial entity's infrastructure, both definitions within the CRA and DORA represent the same systems and products within a financial entity.

2. The objectives of the Cyber Resilience Act

As further illustrated within the Appendix of this paper, the objectives of the CRA and DORA align and at points the expectations of DORA exceed those of the CRA. The CRA introduces a cybersecurity framework throughout the lifecycle of a product with increased governance, transparency and reporting requirements. DORA, in comparison, further develops a comprehensive framework on cybersecurity and ICT risk management, with thorough governance, testing and incident reporting requirements, as well as increased supervision of financial entities. DORA builds on several prior EU and global financial regulations reflecting the higher maturity of financial services versus other sectors in the EU. Both Acts, therefore, serve to increase the cybersecurity and resilience of the EU economy, one through the lens digital products and the other via the ICT systems of financial entities. The result is the same.

3. European Parliament amendments to the Cyber Resilience Act

We support the European Parliament's amendments to the CRA in Recital 4a and 14(b). It is important to recognise other sectors that have similar requirements which result in the same objectives of the CRA. The below Appendix illustrates the overlap between the CRA and DORA and therefore why it is vital that the CRA recognises the equivalence of DORA and gives the Commission the freedom to set guidance on sector-specific application of its rules.

i. Appendix: Overlap between the Cyber Resilience Act and Digital Operational Resilience Act

The objectives of the CRA are illustrated most clearly within Annex 1. All of the objectives within the CRA are achieved, and even exceeded, within DORA. Further detail regarding the extent to which the financial sector is held to a higher standard will be further demonstrated in the coming months as the DORA Regulatory Technical Standards ("RTS") are finalised.

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