

# Market Perspective and DORA Implementation

# #1

# DORA is part of the EU Digital Finance Package

The **DORA Regulation** is part of the broader "**EU Digital Finance Package**", aimed at enabling and further supporting the potential of digital finance in terms of innovation and competition, while mitigating the resulting risks for consumers, businesses and, in general, the financial stability of the Union.

Through these evolutionary regulatory acts, consumers and businesses will also be offered a **wider choice of financial services and modern payment solutions**, while ensuring their **protection and financial stability**.



## Markets in Crypto-Assets «MiCA» Regulation

The Regulation sets as its objective the definition of a harmonized system of rules on **crypto-assets**, and in particular **crypto-currencies (or virtual currencies)**, which makes it possible to seize their opportunities for the development of **innovative digital financial services and mitigate their risks for consumers**, businesses and the financial stability of the Union.



## Digital Operational Resilience Act «DORA» Regulation

The Regulation sets as its objective the definition of a **detailed and complete framework** of rules for the identification and management of **ICT and Cyber risks**, establishing obligations regarding testing of infrastructures and suppliers and the adoption and application of strategies, policies, procedures, tools and protocols on digital operational resilience.



## Digital Ledger Technology «DLT» Regulation

The Regulation, in combination with the MiCA, represents the **first concrete intervention** in the field of infrastructures to support the trading of crypto-assets, aimed at providing adequate levels of consumer and investor protection and legal certainty for the same crypto-assets, and **to enable innovative companies to use blockchain and Distributed Ledger Technology (DLT)**.



## Digital Operational Resilience Act «DORA» Directive

The **Directive** fits at a higher level in the context of the DORA and sets as its objective legal certainty in the **strengthening of digital operational resilience** through the **amendment** of certain **EU Directives relevant to the FS** sector such as UCITS IV, AIFMD, MiFID II, CRDIV, PSD2 and Solvency II.

# Why DORA?



*DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats*

## Reduction of differences between Member States

---

**Harmonization** of the organizational and procedural obligations regarding the identification of ICT risks for financial entities for the **creation of a level playing field among the Member States.**

## Governance of ICT and Cyber risks

---

**Enhancement of ICT and cyber risks as autonomous risks** in the operational and financial fields, with the consequent obligation for the financial entities to define an **organizational and procedural governance framework**, including financial aspects, integrated into the **broader framework of operational risks.**

## Uplevel the European standard on Cyber Security

---

The DORA Regulation is designed to **anticipate cyber security needs** given the acceleration of the **digitization** and **technological evolution** of **Financial Services**, even more marked following the COVID-19 pandemic.

## Supervisory Authorities

---

Centralization of the **role** of the **Supervisory Authorities** both for **control** and assessment of the digital operational resilience framework adopted by **financial entities; incident management** and the assessment of risks deriving from the **dependence of financial entities on ICT third party providers.**



\* Council of the EU

# Entities have to ensure compliance with DORA by January 2025



## Scope

- DORA applies to an estimated **22.000 entities** and forms part of a wider EU Digital Finance package as well as linking with European measures on cyber security & the European strategy for data.
- DORA's **scope of application** encompasses **traditional financial sector entities** such as **credit institutions**, **exchanges** and **clearing houses**, **alternative fund managers**, **insurance companies**, **payment institutions**, **electronic money institutions**, as well as **crypto-currency**, **crypto-asset** issuers and **token** issuers.

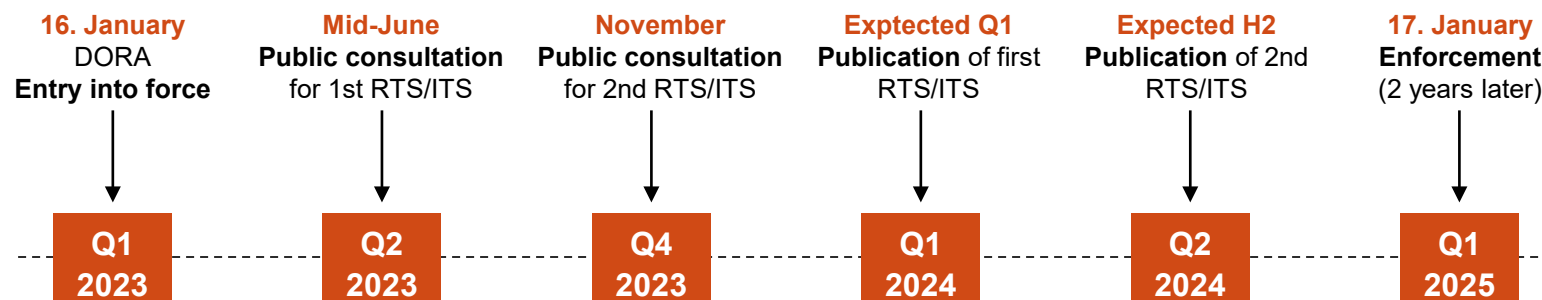


## DORA Pillars

- 2 End to End ICT & Cyber Risk Management
- 3 ICT / Cyber Incident Management & Reporting
- 4 Digital Resilience Testing Requirements
- 5 ICT Third Party Management & TPRM
- 6 EU Information Sharing
- 7 Competent Authorities



## Regulation Journey



## Detailed aspects will be defined through the regulatory technical standards (RTS):

- ICT risk management reporting;
- **Classification methodology, contents, timeframes** and **format** of the **reporting** of **ICT incidents** to the competent **Authorities**;
- Contents and modalities for the **implementation** and **updating** of the **register** containing information on all **contractual agreements** with third-party **ICT suppliers**;
- Conditions enabling the oversight of **critical ICT third parties**.

Until the RTS are published, financial entities must refer to the following regulations and guidelines as reference standard:

- **ESA** (European Supervisory Authority) **Guidelines: EBA; EIOPA; ESMA**;
- **TIBER EU**, with specific reference to **Pillar 4 - Digital Resilience Testing**.

# Specification through technical standards is expected throughout 2024



## DORA Regulation

**Regulation Adoption**  
2 years from entry into force\*

Regulatory Technical Standards (RTS)	Pillar 2 ICT & Cyber Risk	<ul style="list-style-type: none"> <li>ICT / Cyber Risk Management and reports</li> <li>Details of Security and ICT measures / processes</li> </ul>	1 year
	Pillar 3 ICT & Cyber Incident	Harmonization of criteria for incident and cyber threat classification at EU level	1 year
		<ul style="list-style-type: none"> <li>Timeframes for incident reporting</li> <li>Harmonization of templates for incident reporting and cyber threats notification at EU level</li> </ul>	18 months
	Pillar 4 Digital Resilience Testing	Establishment of centralized reporting of major ICT-related incidents (ESA Report)	24 months
		Test criteria, methodologies, requirements, in particular Threat Led Penetration Test	18 months
	Pillar 5 Third Party Risk Management & Agreements	<ul style="list-style-type: none"> <li>Third Party Risk Management Strategy</li> <li>Standard templates for the register of information</li> </ul>	1 year
		Sub-contract arrangements	18 months
EU Critical 3 <sup>rd</sup> Parties oversight		18 months	

\* DORA entered into force on January 16th, 2023.

# DORA has disruptive effects in the Financial Services Sector


## DORA: a priority for the FS Market

Main Impacts:

- **Improve** and **simplify** the activities of financial entities in the **management of ICT and Cyber risks**.
- Establish **assessment** mechanisms of ICT systems.
- **Increase** the **awareness** of Supervisory Authorities and financial entities on IT/cyber risks and ICT-related **incidents**
- Introduce **new powers for Financial Supervisory Authorities** to monitor the risks deriving from the dependence of financial entities on ICT third party providers.

Furthermore, DORA shares synergies and common objectives within a global regulatory environment which focuses increasingly on operational resilience and third party risk management, for instance the Bank of England's Supervisory Statement on Operational Resilience and Critical third parties, NIS 2 Directive, etc.

... the DORA Regulation is transversal to the regulatory frameworks applicable to the different segments of the Financial Services sector ...

	Banking & Payments Markets	Investment Services	Asset Management	Insurance
 <b>EU Regulation</b>	CRD/CRR	MiFIR	UCITS IV	Solvency II
	PSD2	EMIR	AIFMD	IDD
	EMD2	MiFID2		IORP II
	EBA Guidelines	ESMA Guidelines		EIOPA Guidelines
	GDPR			
	SFDR			
	NIS2 Directive			
	TIBER-EU Framework			



# PwC view: DORA Pillars and main impacts



## End-to-End ICT and Cyber Risk Management (Chapter II)

<b>Governance, Strategy and Internal Structure</b>	<ul style="list-style-type: none"><li>• Establishment, adoption and approval of the <b>Digital Operational Resilience Strategy</b>, detailing how DORA is implemented and including key performance indicators and key risk metrics;</li><li>• <b>Central role of the management body</b> in adopting, managing and monitoring the internal ICT risk management framework;</li><li>• Empowerment of responsibilities for internal <b>ICT functions</b>;</li><li>• <b>Monitoring</b> of the correct application of the internal ICT risk management policies and process;</li><li>• <b>Continuous reporting</b> by ICT functions on incidents and corrective solutions implemented;</li><li>• Customized Digital Operational Resilience <b>training to all staff</b>, senior management and ICT third-party service providers.</li></ul>
<b>2nd Line of defense</b>	<ul style="list-style-type: none"><li>• ICT/Cyber risk assessment and management policies, frameworks and processes <b>integrated in the overall operational risk management framework</b>;</li><li>• <b>Definition of impact tolerances</b>, scenario analysis and RAF integration (management body approval);</li><li>• <b>Business-centred view</b> on ICT and Cyber Risk</li><li>• <b>Annual review</b> / update or in case of incidents.</li></ul>
<b>1st Line of defense</b>	<ul style="list-style-type: none"><li>• Definition of Business Services (<b>critical or important functions</b>), process mapping and CMDB;</li><li>• <b>Threat analysis</b> and <b>scenario management</b>;</li><li>• <b>Security Strategy</b>, processes and technologies, including protection of customers' data confidentiality, integrity and availability</li><li>• Technical and organizational measures for ICT/Cyber <b>protection and prevention</b>;</li><li>• Design and implementation of <b>resilient infrastructures and architectures</b>;</li><li>• <b>Predictive monitoring</b> and early detection of anomalies;</li><li>• <b>Continuous improvement</b>, root cause and incident post-mortem analysis;</li><li>• Business <b>continuity, backup and disaster recovery strategies</b> based on plausible scenarios and with business-service based view.</li></ul>

# PwC view: DORA Pillars and main impacts



## ICT and Cyber Incident Reporting (Chapter III)

- Definition and implementation of processes and procedures to monitor, manage and record ICT/Cyber incidents.
- Classification of incidents on the basis of relevance thresholds defined by the Authorities.
- Reporting of major ICT/Cyber incidents, including operational and security payment-related ones, to the Competent Authorities on the basis of severity, including losses.
- Notification of Cyber threats to Competent Authorities
- Transparency to the market.
- Internal/external communication strategies and processes, including end customer.



## Digital Operational Resilience Testing (Chapter IV)

Definition of an all-encompassing program of digital operational resilience test that also includes cyber security aspects and Threat-Led Penetration Test, on the basis of TIBER-EU framework.



## Third Party Risk Management (Chapter V)

- Adoption, within the ICT/Cyber Risk Framework, of a strategy for monitoring and managing risks arising from third party ICT/Cyber service providers.
- Inclusion of standard clauses in contracts with third party ICT/Cyber service providers.
- Maintaining and updating a register with information on all agreements with ICT/Cyber suppliers.
- Monitoring the implementation status of ICT/Cyber measures by ICT/Cyber service providers.
- Integration into management processes by providing for specific supplier obligations, including: Configuration & Asset Management; Incident Management; Digital Resilience Test Program.



## Info Sharing (Chapter VI)

Program (on a voluntary basis) to share anonymized information related to cyber threats within the community of financial entities subject to DORA in order to:

- Improve the digital operational resilience of the European FS market
- Increase awareness of cyber threats
- Contain the spread of cyber threats
- Strengthen the defense capabilities of financial entities



# Thank you.

[pwc.de](https://www.pwc.de)

© 2023 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.

All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, which is a member firm of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.