

# Digital Operational Resilience Act (DORA):

## Overview for financial entities and ICT third parties



“ 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.”  
- Council of the EU

### Why is DORA relevant for my organisation?

DORA will apply to more than 22,000 financial entities and ICT service providers. The regulation will introduce **new requirements to all financial market participants**.

We view DORA as a significant change for entities within ESMA or EIOPA supervision, but also for banks which have already had to comply with existing EBA guidelines on banking supervision.

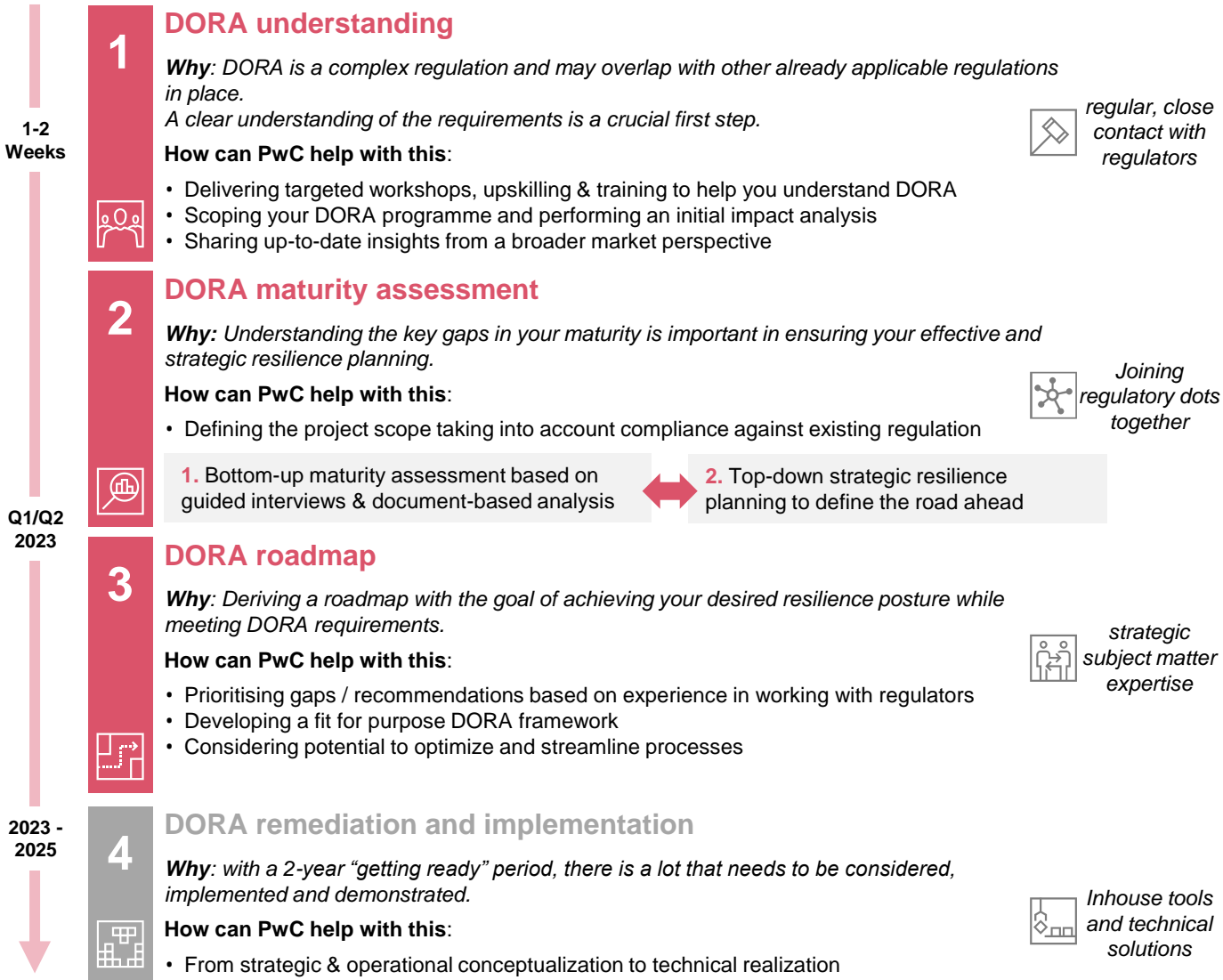
The regulation is **unique** in introducing a **Union-wide Oversight Framework on critical ICT third-party service providers**, as designated by the European Supervisory Authorities (ESAs).

### DORA will set the regulatory focus on five key topics

ICT Risk Management	Incident Reporting	Resilience Testing	ICT Third Party Risk Mgmt	Information Sharing
End-to-end service view and scenario based IT mgmt.	Reporting of ICT-related incidents	Annual testing of all critical ICT systems	Reporting complete outsourcing register and changes	Arrangements for exchange of threat intelligence
Operational and technical cyber security capabilities	Root-cause analysis following ICT incidents	Advanced threat-led penetration testing every 3 yrs.	Ensuring complete monitoring of 3rd party services	Collaboration among trusted communities of financial entities
Enterprise architecture resilience & BCM	Identification and reporting of improvements	Collaboration with third party service providers	Assessing concentration risk & sub-outsourcing	Mechanisms to review and act on shared intelligence

European Parliament and Council adopt DORA (Nov 2022) → DORA enters into force (Q1 2023) → Publications of RTS / ITS (Q1/Q2 2024) → Expected enforcement of DORA (Q1 2025)

# We recommend these steps get DORA ready & operationally resilient



## Our view on DORA for Hungarian entities: Evolution, not revolution

- DORA addresses many topics that have already been considered by **existing regulations in Hungary**
- **Other topics (ex. threat intelligence and TLPT)** are of new character and **require heightened attention**
- The ability to develop an **overarching visibility and understanding of all the key dependencies** between your entity and your critical ICT service providers is another challenge we see.

**Our recommendation** is that regardless of where you are in terms of the maturity of your digital and operational resilience, **DORA should be a trigger** to start or enhance your resilience journey.

Entities that are applying current regulatory requirements in line with current audit practices may be better positioned to implement the majority of DORA requirements. Yet, having supported numerous clients with their cybersecurity & resilience efforts, **we say: efficiency is key** – both, **for achieving your desired resilience posture, while ensuring compliance with DORA** requirements.

### Contact us

**Peter Durojaiye**

**Partner**

+36 70 685 0360

[peter.durojaiye@pwc.com](mailto:peter.durojaiye@pwc.com)

**Csaba Gyimesi**

**Director**

+ 36 30 211 2210

[csaba.gyimesi@pwc.com](mailto:csaba.gyimesi@pwc.com)

**Peter Matyas**

**Senior Manager**

+ 36 70 657 2353

[peter.matyas@pwc.com](mailto:peter.matyas@pwc.com)