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 years.	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

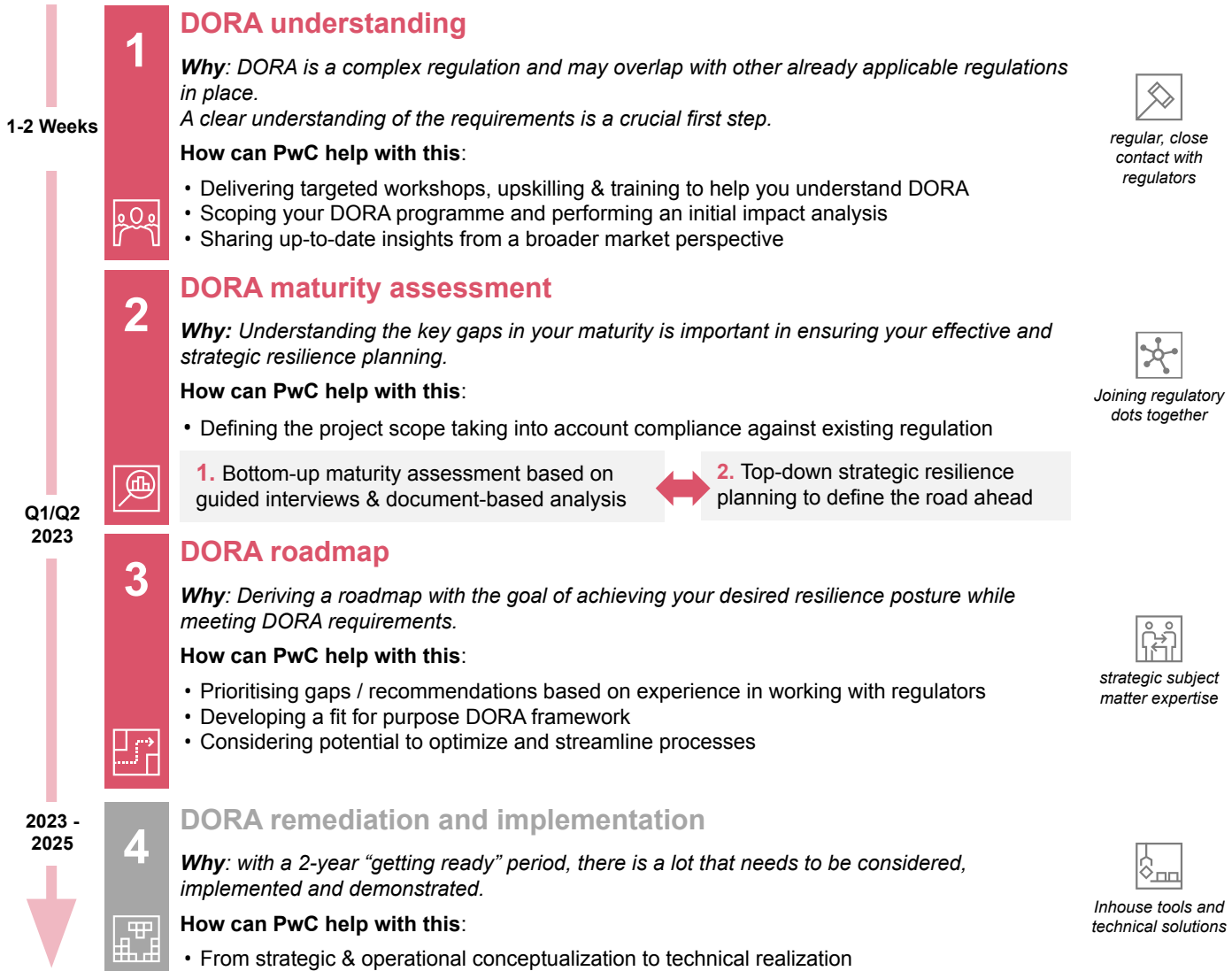| European Parliament and Council adopt DORA	DORA enters into force	Publications of RTS / ITS	**Expected enforcement of DORA**
Nov 2022	Jan 16th, 2023	Q1/Q2 2024	**Jan 17th, 2025**

We recommend these steps get DORA ready & operationally resilient

1-2 Weeks

1 DORA understanding

Why: DORA is a complex regulation and may overlap with other already applicable regulations in place.
A clear understanding of the requirements is a crucial first step.

How can PwC help with this:

- Delivering targeted workshops, upskilling & training to help you understand DORA
- Scoping your DORA programme and performing an initial impact analysis
- Sharing up-to-date insights from a broader market perspective

regular, close contact with regulators

2 DORA maturity assessment

Why: Understanding the key gaps in your maturity is important in ensuring your effective and strategic resilience planning.

How can PwC help with this:

- Defining the project scope taking into account compliance against existing regulation

1. Bottom-up maturity assessment based on guided interviews & document-based analysis ⟷ **2.** Top-down strategic resilience planning to define the road ahead

Joining regulatory dots together

Q1/Q2 2023

3 DORA roadmap

Why: Deriving a roadmap with the goal of achieving your desired resilience posture while meeting DORA requirements.

How can PwC help with this:

- Prioritising gaps / recommendations based on experience in working with regulators
- Developing a fit for purpose DORA framework
- Considering potential to optimize and streamline processes

strategic subject matter expertise

2023 - 2025

4 DORA remediation and implementation

Why: with a 2-year "getting ready" period, there is a lot that needs to be considered, implemented and demonstrated.

How can PwC help with this:

- From strategic & operational conceptualization to technical realization

Inhouse tools and technical solutions

Our view on DORA for CZ entities: Evolution rather than revolution

- DORA addresses many topics that have already been considered by **existing regulations in FS.**
- **Other topics** (e.g. 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

Petr Spirik	**Ondrej Linhart**	**Petr Simsa**
Partner	**Manager - DORA SME**	**Manager - DORA SME**
+420 774 191 101	+420 732 633 983	+420 735 701 568
petr.s.spirik@pwc.com	ondrej.linhart@pwc.com	petr.simsa@pwc.com

pwc.cz