> 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

Digital Operational Resilience Act (DORA)

Overview for financial entities and ICT third parties

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

- End-to-end service view and scenario based IT management
- Operational and technical cyber security capabilities
- Enterprise architecture resilience & BCM

Incident Reporting

- Reporting of ICT-related incidents
- Root-cause analysis following ICT incidents
- Identification and reporting of improvements

Resilience Testing

- Annual testing of all critical ICT systems
- Advanced threat-led penetration testing every 3 years
- Collaboration with third party service providers

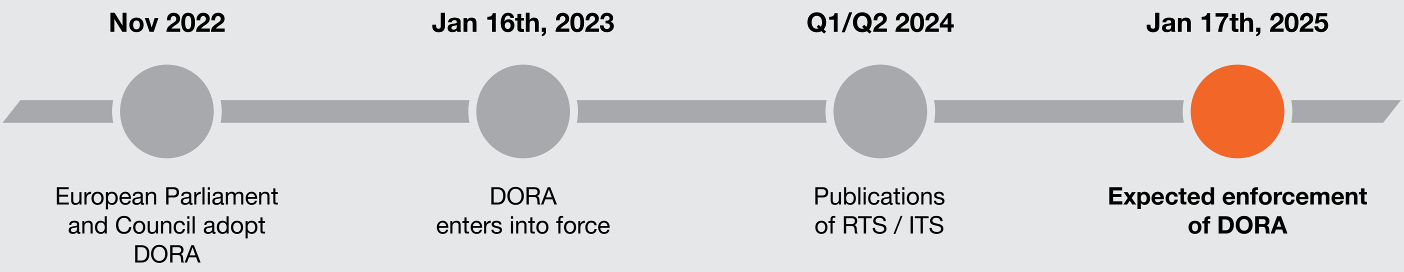
ICT Third Party Risk Mgmt

- Reporting complete outsourcing register and changes
- Ensuring complete monitoring of 3rd party services
- Assessing concentration risk & sub-outsourcing

Information Sharing

- Arrangements for exchange of threat intelligence
- Collaboration among trusted communities of financial entities
- Mechanisms to review and act on shared intelligence

Time schedule



Nov 2022
European Parliament and Council adopt DORA

Jan 16th, 2023
DORA enters into force

Q1/Q2 2024
Publications of RTS / ITS

Jan 17th, 2025
Expected enforcement of DORA

We recommend these steps get DORA ready & operationally resilient

1

DORA understanding

1–2 weeks

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

Q1/Q2 2023

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

3

DORA roadmap

Q1/Q2 2023

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

4

DORA remediation and implementation

2023 – 2025

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
Partner
+420 774 191 101
petr.s.spirik@pwc.com

Ondřej Linhart
Manager – DORA expert
+420 732 633 983
ondrej.linhart@pwc.com

Petr Simsa
Manager – DORA expert
+420 735 701 568
petr.simsa@pwc.com