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?

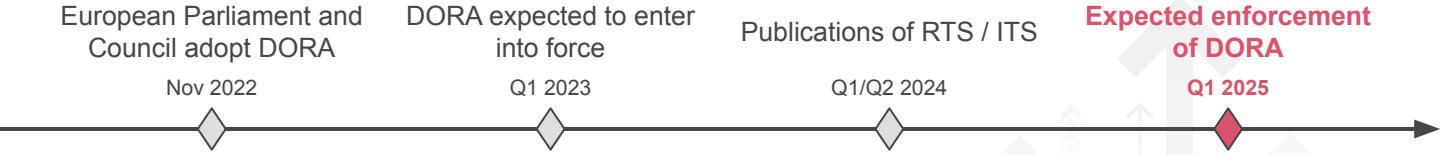
DORA will apply to more than 22,000 financial entities and ICT service providers. The regulation will introduce **new requirements to all financial market participants.**

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



pwc

pwc.cee

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.

regular, close contact with regulators

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

2 DORA maturity assessment

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

Joining regulatory dots together

How can PwC help with this:

- Defining the project scope taking into account compliance against existing

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

Q1/Q2 2023

3 DORA roadmap

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

strategic subject matter expertise

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

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.*

Inhouse tools and technical solutions

How can PwC help with this:

- From strategic & operational conceptualization to technical realization

Our view on DORA for Slovenian entities: Evolution – no revolution?

- DORA addresses many topics that have already been considered by **existing regulations in Slovenia**
- **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

Thomas Magill
Partner
+386 51 687 073
thomas.m.magill@pwc.com

Senad Dzananovic
Senior Manager
+ 387 62 008 855
senad.dzananovic@pwc.com

Tomas Besinsky
Manager
+386 51 613 139
tomas.besinsky@pwc.com