Digital Operational Resilience Act (DORA):

Overview for financial entities and ICT third parties

OPRA 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	⊕= ⊒ .ll 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
DORA entered into force 16.01.2023	2nd Public consultation on RTS/ITS Dec. 2023 - Mar. 2024		2nd Batch of RTS/ITS finalization 17.07.2024	

Jun. - Sep. 2023
1st Public consultation on
RTS/ITS

17.01.2024 1st Batch of RTS/ITS finalization 17.01.2025 Enforcement of DORA



We recommend these steps get DORA ready & operationally resilient

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:



Regular, close contact with regulators

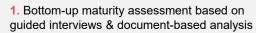


- Delivering targeted workshops, upskilling & training to help you understand DORA
- · Scoping your DORA programme and performing an initial impact analysis
- Sharing up-to-date insights from a broader market perspective

DORA maturity assessment and roadmap

Why: Understanding the key gaps in your maturity and deriving a roadmap is important to achieve your desired resilience posture while meeting DORA requirements.

How can PwC help with this:





Top-down strategic resilience planning to define the road ahead



Strategic subject matter expertise



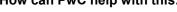
- Prioritizing gaps / recommendations based on experience with regulators
- Identification of the critical path in order to create a realistic roadmap
- Developing a fit for purpose DORA framework

DORA remediation and implementation

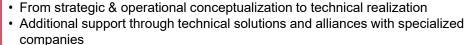
Why: With a less than one year "getting ready" period, there is a lot that needs to be considered, implemented and demonstrated.

How can PwC help with this:





Inhouse tools and technical solutions





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

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

Philipp Schulz

Director DORA Lead +49 151 46164136 philipp.schulz@pwc.com

independent legal entity.

Fiona Marschollek

Manager DORA SME +49 151 50630688 fiona.marschollek@pwc.com

Rüdiger Giebichenstein

Partner DORA Insurance +49 175 7954901 ruediger.giebichenstein@pwc.com

