DORA

Digital Operational Resilience Act

Compliance deadline:
January 2025

What is DORA?

DORA is a sector-specific directive for financial institutions, targeting their approach to operational risk. It introduces rules for managing all aspects of operational resilience, particularly emphasizing protection, detection, containment, recovery, and repair capabilities against ICT-related incidents.

Here's why it matters

DORA fosters a cyber-resilient ecosystem, safeguarding critical functions and customer trust. While NIS2 is a directive that allows countries to develop rules based on their specific national needs, DORA is a regulation, leaving no room for discretion at the Member State level.

Who it impacts?

Financial entities and ICT service providers within the European Union (EU)., including:

- Traditional financial institutions
- Emerging financial entities
- Critical third-party service providers

What it means for your business

You'll need to develop digital operational resilience.

Actions required:

- Establish a sound, comprehensive and a well-documented information and communication technologies (ICT) risk management framework.
- Implement an ICT incident management process to detect, manage, classify, and notify incidents.
- Manage and monitor risks related to ICT third-party service providers.
- Establish a sound and comprehensive digital operational resilience testing program.