T Security

DORA Compliance

Strengthen operational resilience, manage ICT risks, and become DORA-ready.

What is DORA and why does it matter?

The Digital Operational Resilience Act (DORA) is the European Union's framework strengthening how financial institutions prevent, respond to, and recover from ICT disruptions.

As financial services now rely heavily on digital infrastructure and third-party providers, operational resilience has become critical for continuity, trust, and compliance.

Who is impacted by DORA?

DORA applies across a broad range of financial entities operating within the EU, including:

Banks and credit institutes | insurance and reinsurance providers | investment firms and trading platforms | payment institutions and fintech companies | ICT providers supporting financial services

The regulation also increases accountability across third-party vendors and technology providers connected to financial operations.

How is DORA compliance enforced?

DORA introduces stricter oversight and accountability across financial institutions and ICT providers.

Regulators can conduct audits, review ICT risk management frameworks, assess resilience testing processes, and evaluate how organizations respond to operational incidents.

Organizations are also expected to report major ICT incidents within defined timelines.

Penalties and Business Impact

Failure to comply with DORA can result in financial penalties, increased regulatory scrutiny, operational restrictions, and reputational damage.

Financial institutions may face fines of up to **2% of global annual turnover**, while critical ICT providers can face additional penalties and corrective actions for continued non-compliance.

What are financial institutions expected to do?

Financial institutions are expected to establish a structured operational resilience framework that includes:

- ICT risk management and governance
- Incident detection and reporting
- Operational resilience testing
- Third-party risk management
- Continuous monitoring and oversight

Organizations must ensure resilience across systems, operations, users, and external providers.

Common challenges across financial environments

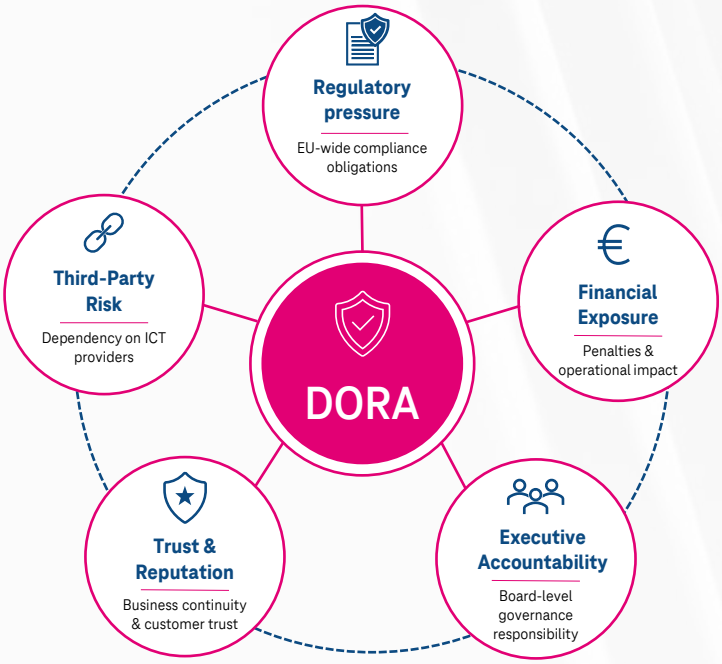
Many organizations continue to face challenges such as:

- Limited visibility across ICT systems and providers
- Increased dependency on third-party vendor
- Delayed incident response and coordination
- Inconsistent resilience testing and governance

Your roadmap to DORA compliance

1. **Establish top-down governance and strategy**
   - Define risk appetite
   - Assign Accountability
2. **Map dependencies and identify assets**
   - CMDB implementation
   - End-to-end mapping
3. **Implement robust risk & incident management**
   - Continuous Monitoring
   - Incident Classification
   - Regulatory Reporting
4. **Enforce threat-led testing & business continuity**
   - Annual testing
   - Threat-led penetration testing
   - Disaster recovery
5. **Manage third-party concentration risk**
   - Contractual accountability
   - Concentration risk
   - Exit strategies

Why DORA is a leadership priority?



How T Security supports your DORA readiness

DORA Readiness Assessment
Identify compliance gaps, ICT risks, and operational dependencies

Secure ICT Infrastructure and Cloud
Build resilient, compliant, and secure digital environments

Threat Detection and Incident Response
Improve visibility, monitoring and response across critical systems

Identity and Access Management
Strengthen user access controls, authentication, and governance

Compliance and Audit Support
Streamline compliance, oversight and evaluation readiness

Resilience Planning
Define structured protocols, incident reporting, and restoration plans synchronized to DORA deadlines.

Get in touch with our experts
cyber.security@t-systems.com

Published by
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Germany
security.telekom.de
t-systems.com