Digital Operational Resilience Act (DORA)

Summary

The Digital Operational Resilience Act (DORA) is an EU regulation effective January 17, 2025, designed to strengthen the operational resilience of financial entities against ICT-related disruptions and cyber threats. It harmonizes ICT risk management across the EU financial sector, ensuring organizations can withstand, respond to, and recover from digital incidents.

Key Requirements

- ICT Risk Management: Comprehensive frameworks with governance, risk assessments, and board-level oversight.
- Incident Management & Reporting: Detect, classify, and report ICT-related incidents to authorities within strict timelines.
- Digital Operational Resilience Testing: Regular vulnerability assessments, business continuity tests, and Threat-Led Penetration Testing (TLPT) for major entities.
- Third-Party Risk Management: Oversight of ICT service providers, contractual safeguards, and exit strategies.
- Information Sharing: Participation in cyber threat intelligence sharing arrangements.
- Governance & Accountability: Senior management responsible for ICT risk strategy and oversight.

Who Is Affected

- Banks and investment firms
- Insurance and reinsurance companies
- Payment institutions and e-money providers
- Crypto-asset service providers
- Asset managers and fund administrators

- Critical ICT third-party service providers (e.g., cloud providers)

Informational Resources

- EU Official DORA Page – EIOPA: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
- GRSee DORA Compliance Guide: https://grsee.com/resources/eu-assess/what-is-dora-compliance-purpose-requirements-and-checklist/
- Grant Thornton DORA Summary: https://www.grantthornton.ie/insights/factsheets/digital-operational-resilience-act-dora-regulation-summary/
- Hoxhunt DORA Compliance Checklist: https://hoxhunt.com/blog/dora-regulation
- Advisera Key Requirements: https://advisera.com/articles/dora-regulation-key-requirements/