DORA is here - are you ready?

BY INTIGRITI · JANUARY 17, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **What the Digital Operational Resilience Act (DORA) is and why it matters** for financial institutions and ICT service providers operating in the EU, including its goal to strengthen digital and cyber resilience across the sector.
- **What the core DORA compliance requirements are,** from ICT risk management and incident reporting to continuous resilience testing and third party ICT risk oversight, so you can assess readiness and gaps.
- **How to prepare and act now to meet DORA's expectations**, including leveraging appropriate security testing, documentation, and evidence based workflows to not only comply but improve operational resilience.

Today, January 17, 2025, marks a pivotal moment for the EU financial sector as the Digital Operational Resilience Act (DORA) officially comes into effect. Designed to combat the growing threat of cyberattacks, DORA sets a new standard for cybersecurity resilience across financial institutions and their critical ICT service providers.

With cyberattacks costing the financial sector over €12 billion in the past two decades, DORA is a much-needed step toward ensuring a high common level of digital operational resilience. But the question is: Is your organization ready to comply?

What is DORA?

DORA is an EU regulation aimed at strengthening the digital operational resilience of financial entities. It establishes a unified framework to ensure that financial institutions can withstand, respond to, and recover from cyber threats.

The regulation applies to nearly all financial entities within the EU, including banks, insurance companies, investment firms, and their critical ICT service providers.

Key DORA Requirements

To comply with DORA, financial institutions must meet several critical requirements:

- **Enhanced ICT risk management framework**: Financial institutions must implement robust frameworks to identify, manage, and mitigate ICT risks.
- **Streamlined incident reporting**: Organizations must report significant ICT-related incidents in a timely and structured manner.

- **Third-party ICT service provider risk management:** Financial institutions must ensure that their critical ICT service providers meet stringent security standards.
- **Continuous operational resilience through testing:** Regular and thorough testing of ICT systems is required to ensure resilience against evolving cyber threats.

How Intigriti can help

At Intigriti, we understand the challenges of navigating new regulations like DORA. Our platform and services are designed to help both financial institutions and ICT service providers meet DORA's requirements while strengthening their overall cybersecurity posture.

For Financial Institutions

- **Continuous security testing**: meet DORA's Article 24(6) requirements with ongoing, real-world testing of your systems.
- **Access to elite security researchers**: Leverage the expertise of our global community of ethical hackers to uncover vulnerabilities before attackers do.
- **Real-time vulnerability reporting:** Receive actionable insights and manage vulnerabilities in real time.
- **Comprehensive documentation**: Ensure you have the necessary evidence to demonstrate compliance to regulators.
- **Annual testing obligations:** Adopt a structured approach to meet DORA's annual testing requirements.
- **Third-party assessments:** Expand your testing scope to include critical third-party ICT service providers.

For ICT Service Providers

- **Demonstrate robust security:** Showcase your commitment to security testing to meet financial clients' procurement requirements.
- **Compliance documentation:** Provide financial clients with the necessary documentation to support their DORA compliance.
- **Strengthen competitive position:** Stand out in the financial sector by demonstrating your commitment to operational resilience.

Why Act Now?

DORA is not just a compliance requirement—it's an opportunity to strengthen your organization's cybersecurity posture and gain a competitive edge in the financial sector. By adopting a proactive approach to DORA compliance, you can:

- Protect your organization from costly cyberattacks.

- Build trust with clients and stakeholders.
- Ensure seamless operations in an increasingly digital world.

Get DORA-compliant with Intigriti

As the financial sector enters this new era of operational resilience, Intigriti is here to support your compliance journey. Whether you're a financial institution or an ICT service provider, our platform offers the tools, expertise, and flexibility you need to meet DORA's requirements and stay ahead of cyber threats.

Don't wait—ensure your organization is DORA-compliant today.

Contact us to learn more about how Intigriti can help you navigate DORA and strengthen your cybersecurity resilience.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com