IMMERSIVELABS

DATA SHEET

DORA Compliance

Discover how Immersive Labs helps organizations meet and sustain DORA compliance

The Digital Operations Resilience Act (DORA) was published in the Official Journal of the European Union on 27 December 2022. It comprises a Regulation and a Directive on digital operational resilience for the financial sector in the EU. The Regulation is now in force and will be fully applicable from January 2025.

DORA applies to all financial institutions in the EU, aiming to address digital operational risk consistently in a single legislative act. It introduces targeted rules on:

- Information and Communication Technology (ICT) risk management
- ICT-related incident management, classification, and reporting
- Digital operational resilience testing
- Managing ICT third-party risk, including oversight for critical ICT third-party service providers
- Information and Intelligence Sharing

KEY TRANCHES OF TECHNICAL STANDARDS DEVELOPMENT

The European Supervisory Agencies (ESAs) jointly lead the development of technical standards as required by the DORA Regulation. These standards were delivered in two tranches:

Tranche 1 (June 2023):

- Specifies elements of a financial entity's risk management framework
- Establishes criteria for incident classification and reporting
- Specifies outsourcing policies and standard templates for ICT service providers

Tranche 2 (December 2023):

- Defines reporting procedures for major ICT-related incidents and significant cyber threats
- Specifies subcontracting elements, testing criteria, and oversight conditions for critical ICT service providers

Trusted by the world's largest companies, governments, and defense organizations

HSBC Pfizer citi Humana nationalgrid

DORA Penalties

Entities found to violate the Digital Operations Resilience Act (DORA) may face significant financial penalties. Here's what you need to know:

- Non-Compliance Fines: Entities failing DORA requirements may face fines up to 2% of their annual turnover. Individuals max EUR 1,000,000. Fine severity depends on violation severity and cooperation.
- Incident Reporting: Failing to report incidents incurs fines.
- Third-Party Penalties: Critical ICT providers may face fines up to EUR 5,000,000. Individuals max EUR 500,000. ESAs enforce fines.

Understanding and adhering to DORA requirements is crucial to avoid these penalties and ensure compliance with financial regulations.

How Immersive Labs Contributes to DORA Compliance

The Immersive Labs' platform addresses several key DORA metrics:

Immersive Labs Helps Organizations Meet Multiple DORA Requirements

	Hands-On Lab	Application Security	Crisis Simulations	Cyber Threat Intelligence	Cyber Team Sim	The Platform and Reporting
Deployment Frequency	✓	✓				✓
Lead Time for Changes	✓	✓				✓
Time to Restore			✓		✓	✓
Change Failure Rate	✓	✓				✓
Information Sharing				✓		✓

Ready to Achieve DORA Compliance?

Immersive Labs offers a people-centric approach to cybersecurity, ensuring organizations can effectively respond to cyber threats and meet DORA compliance requirements.

[Click for an exclusive tour and learn more about our Cyber Workforce Resilience Platform!]

Certification & Compliance

Information Security Management ISO 27001 Certified

CYBER ESSENTIALS CERTIFIED PLUS

GDPR

Trusted by the world's largest organizations

Over **400** customers

>3.5M total labs completed

>100,000 unique users

>1,800 hands-on challenges

IMMERSIVELABS