



Cyber Guru

Board Training DORA

BOARDROOM CYBER SKILLS TO MEET DORA OBLIGATIONS

The EU's Digital Operational Resilience Act (DORA), effective from January 2025, explicitly assigns responsibility for proactively managing cyber risks to boards and senior executives of financial institutions including banks, insurance companies, investment firms, and their critical providers.

Board Training DORA is an eLearning programme that directly addresses this obligation. It equips board members and executives with the strategic knowledge and practical skills required to effectively oversee and manage cybersecurity threats.

It specifically targets organisations covered by DORA, along with their supply chain partners, ensuring comprehensive readiness and compliance across the entire financial ecosystem. Participants gain actionable insights and expertise, enabling them to transform regulatory requirements into a proactive, strategic advantage.

From regulatory duty to board-level cyber leadership

This eLearning training programme turns DORA's regulatory requirements into strategic opportunities. Board members and business leaders acquire the knowledge and tools to strengthen their organisation's digital resilience, enabling proactive defence against cyber threats. By completing the training, participants will be able to:

- Understand the strategic cybersecurity landscape at national and international levels.
- Identify and assess key cyber risks specific to their organisation.
- Evaluate and approve effective mitigation strategies, policies, and action plans.
- Grasp the cyber-risk implications of emerging technologies, such as cloud computing and artificial intelligence.
- Interpret and apply the DORA regulatory requirements and related best practices.
- Fulfil the board-level training obligations mandated by the DORA Regulation.

A Structured Path to Dora-Aligned Cyber Resilience

To address this need, Cyber Guru has developed a structured training course organised into progressive learning levels. Each level comprises four training sections, focusing on key topics required to meet mandatory training obligations, including:

DORA Regulation

Obligations and requirements for affected companies.

Cyber Attacks

Recognising attack techniques and key defensive strategies.

Cloud & AI

Cybersecurity impact of emerging technologies.

Cyber Risk Management

Identifying, assessing, and mitigating cyber threats.

Supply Chain Security

Securing and protecting the wider business ecosystem.

Case Studies & Best Practices

Learning from concrete examples and proven methods for effective defence.

Board Training DORA Features



EFFECTIVE EXECUTIVE LEARNING

- Ongoing Training
- Engaging videos with lifelike avatars
- Complete & independent lessons
- Micro-learning that's easy on your calendar
- Executive recap
- Multilingual
- Regularly updated
- Accreditation of skills



DORA SPECIFIC CONTENT

- Regulatory framework
- Managing risk
- Operational resilience testing
- 3rd party risk management
- Incident reporting
- Info-sharing mechanisms
- Sanctions
- Industry specific case-studies



ZERO-IMPACT SUPERVISION

- Turnkey service
- SaaS platform with multi-device support
- Pre-established training plans
- Automated student caring
- Compliance-ready reportig
- Proof of participation/ completion