Digital Operational Resilience Act (DORA) for Financial Institutions Training Course

16 – 20 August 2027
Zoom

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Digital Operational Resilience Act (DORA) for Financial Institutions Training Course

Ref: 103600318_65475 **Date:** 16 – 20 August 2027 **Location:** Zoom **Fees:** 3000 Euro

Course Overview:

Digital Operational Resilience Act DORA for Financial Institutions Training Course is a comprehensive program designed to help professionals in the financial sector achieve compliance with the Digital Operational Resilience Act DORA while enhancing digital resilience, ICT risk management, and cybersecurity compliance. With DORA becoming a key regulatory framework, organizations must adapt to stringent financial risk management requirements, develop strong operational resilience, and conduct in-depth risk assessments to mitigate ICT threats.

This course provides an interactive learning experience with real-world compliance training strategies, case studies, and best practices for ICT risk assessment. Participants will learn how to align their institutions with DORA regulatory requirements training, implement cybersecurity frameworks for financial institutions, and manage third-party ICT risks effectively. By the end of this course, attendees will be well-prepared to pass the DORA certification course online and take proactive steps to reduce ICT security vulnerabilities.

Target Audience:

- Financial institution executives and decision-makers
- Compliance officers and regulatory managers
- IT and cybersecurity professionals
- Risk management professionals
- Consultants specializing in financial sector compliance

Targeted Organizational Departments:

- Compliance and regulatory affairs
- IT security and risk management
- Cybersecurity and operational resilience teams
- Internal audit and governance units
- Third-party vendor management teams

Targeted Industries:

- Banking and financial services
- Fintech and digital payments
- Insurance and investment firms
- Regulatory bodies and government agencies
- Consulting firms specializing in cybersecurity compliance

AGILE LEADERS
Training Center

Course Offerings:

By the end of this course, participants will be able to:

- Understand DORA compliance requirements and their impact on financial institutions
- Develop digital operational resilience strategies to protect financial assets
- Implement ICT risk management best practices to mitigate cyber threats
- Strengthen cybersecurity compliance through effective regulatory frameworks
- Conduct comprehensive risk assessments and audit third-party ICT service providers
- Enhance incident response capabilities and improve crisis management procedures
- Prepare for and pass the DORA certification course online

Training Methodology:

This course adopts an engaging and interactive approach, combining instructor-led sessions, real-world case studies, and hands-on workshops. Participants will engage in:

- Scenario-based exercises to assess cybersecurity frameworks for financial institutions
- Discussions focused on DORA implementation strategies
- Practical risk assessments to analyze ICT security vulnerabilities
- Role-playing activities to simulate third-party oversight under DORA
- Quizzes and assessments to track progress and ensure knowledge retention

Course Toolbox:

Participants will receive a variety of resources, including:

- Digital workbooks and compliance checklists
- Case study analysis reports
- DORA policy framework templates
- Risk assessment tools and methodologies
- Access to online learning materials and regulatory updates

AGILE LEADERS
Training Center

Course Agenda:

Day 1: Introduction to DORA & Digital Operational Resilience

- **Topic 1:** Overview of the Digital Operational Resilience Act DORA
- **Topic 2:** Key objectives and scope of DORA compliance for financial institutions
- **Topic 3:** Fundamental concepts of ICT risk management and digital resilience
- **Topic 4:** Governance and organizational requirements for DORA implementation
- **Topic 5:** Planning and preparing for a successful DORA compliance strategy
- **Topic 6:** Understanding financial risk management in a digital environment
- **Reflection & Review:** Key takeaways and discussion on initial implementation steps

Day 2: ICT Risk & Incident Management Under DORA

- **Topic 1:** Identifying ICT-related risks in financial institutions
- **Topic 2:** Developing a risk-based approach to ICT risk management
- **Topic 3:** ICT incident management framework and reporting obligations
- **Topic 4:** Cybersecurity compliance and best practices for financial institutions
- **Topic 5:** Regulatory compliance expectations for ICT security and resilience
- **Topic 6:** Financial risk assessment techniques for regulatory alignment
- **Reflection & Review:** Practical scenarios and lessons learned from ICT risk incidents

Day 3: Third-Party ICT Risk Management & Oversight Framework

- **Topic 1:** Digital operational resilience testing for third-party ICT providers
- **Topic 2:** Managing third-party ICT risks in the financial sector
- **Topic 3:** The Oversight Framework and the role of the Lead Overseer
- **Topic 4:** Information and intelligence sharing for cybersecurity resilience
- **Topic 5:** Legal and contractual obligations under DORA for third-party vendors
- **Topic 6:** Risk monitoring and reporting frameworks for ICT supply chain security
- **Reflection & Review:** Challenges and strategies in managing third-party risks

AGILE LEADERS
Training Center

Day 4: Continuous Improvement & Regulatory Compliance

- **Topic 1:** Training and awareness programs for digital resilience in financial institutions
- **Topic 2:** Competent authorities and regulatory enforcement of DORA compliance
- **Topic 3:** Monitoring, measurement, and evaluation of operational resilience
- **Topic 4:** Internal audit techniques for ensuring ICT security and compliance
- **Topic 5:** Best practices for ongoing improvement in cybersecurity frameworks
- **Topic 6:** Digital resilience strategies for financial executives and risk managers
- **Reflection & Review:** Case studies and review of internal compliance strategies

Day 5: Strengthening Digital Resilience & Future Compliance Strategies

- **Topic 1:** Advanced approaches to financial sector cybersecurity risk management
- **Topic 2:** Integrating DORA compliance into enterprise-wide resilience strategies
- **Topic 3:** Emerging trends and challenges in ICT governance for financial institutions
- **Topic 4:** Developing an action plan for long-term digital resilience compliance
- **Topic 5:** Reducing ICT security vulnerabilities and strengthening risk management
- **Topic 6:** Preparing for future regulatory updates and evolving cybersecurity threats
- **Reflection & Review:** Final course insights, discussion, and key takeaways

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

There are no mandatory prerequisites, but a basic understanding of financial regulations, ICT security, or risk management is beneficial.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session lasts approximately 4-5 hours, with breaks and interactive activities. The total course duration spans one week, approximately 20-25 hours of instruction.

What is the role of third-party oversight in DORA compliance?

Third-party oversight is crucial under DORA as financial institutions must ensure that ICT service providers comply with operational resilience requirements. This course provides strategies to assess and manage third-party risks effectively.

How This Course is Different from Other DORA Compliance Courses:

This course stands out by offering an interactive, real-world approach to DORA compliance training for financial institutions. Unlike standard courses that focus solely on theory, we integrate:

- Live case studies tailored to the financial risk management sector
- Cybersecurity framework simulations to help participants apply knowledge in real-time
- Regulatory compliance workshops covering DORA implementation strategies
- Comprehensive exam preparation for achieving DORA certification

This program is designed not just to educate but to empower financial professionals to enhance cybersecurity resilience, reduce ICT security vulnerabilities, and develop actionable compliance strategies.