AWARENESS TRAINING · DIGITAL OPERATIONAL RESILIENCE

DORA Awareness

Self-paced online training (video) · 10 modules · about 110 min of video · about 3 hours in total · English, with captions

Understand what the Digital Operational Resilience Act means for your financial entity and your own role, from ICT risk management and incident reporting to resilience testing and ICT third-party risk.

WHO IT IS FOR

Employees and managers at EU banks, insurers, investment firms, payment and e-money institutions, crypto-asset service providers and other financial entities, and staff of ICT service providers that support them.

WHAT YOU WILL LEARN

- Explain the purpose of DORA and which financial entities it covers
- Describe the ICT risk management framework and the management body's responsibilities
- Recognise ICT-related incidents and know how major incidents are reported
- Understand the purpose of digital operational resilience testing
- Describe how ICT third-party risk is managed, including the register of information
- Recognise your own part in digital operational resilience

MODULES (10)

1. Why DORA
2. A regulation for the financial sector
3. ICT risk management: the framework and board
4. Protection, prevention and detection
5. Response, recovery, learning, communication
6. Classifying ICT-related incidents
7. Reporting major incidents
8. Digital operational resilience testing
9. ICT third-party risk and the register
10. Oversight, penalties and your role

PRICE

US$19 per learner

Per learner, by team size

1–10 learners	**US$19**
11–50 learners	**US$15**
51–200 learners	**US$13**

Excluding taxes.

DURATION

About 3 hours in total (112 minutes of video)

MODULES

10

FORMAT

Self-paced online training (video)

LANGUAGE

English, with captions

ACCESS

12 months

CERTIFICATE

Sterling Academy Certificate of Completion

Scan for the course page, prices and enrolment