

Digital Operational Resilience Act (DORA)





Compliance made simple



As compliance e-learning specialists, we understand how complex and daunting compliance training can be. Your company faces compliance risks on many fronts, and you need to address these risks promptly to protect your company, your staff, and your reputation. Skillcast helps you respond to these needs efficiently and cost-effectively with our carefully curated set of off-the-shelf courses.

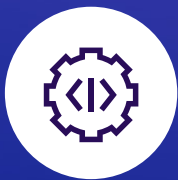


Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) mandates that financial entities and their third-party technology providers align with specific technical standards for robust operational security.



ICT risk management and governance: Financial entities must assess ICT risks and establish a comprehensive management framework.



Incident management, response, classification, and reporting: Entities must manage and report significant ICT incidents, classifying by impact, criticality, and duration.



Digital operational resilience testing: Entities must test ICT systems regularly, report results, and conduct annual vulnerability assessments; critical entities undergo penetration testing every three years.



Third-party risk management: Financial firms must manage ICT third-party risks, ensuring contracts meet security, accessibility, and performance standards.



ICT third-party providers' oversight framework: European Supervisory Authorities oversee critical ICT providers, enforcing security and terminating non-compliant contracts.



Information sharing arrangements: Financial institutions are encouraged to share cyber threat information within trusted communities, enhancing resilience and compliance.



Training Package

Our training package includes nearly 40 cybersecurity and risk management courses, including microlearning videos, to support staff in key compliance areas. Topics covered include reporting, resilience testing, third-party risk, and information sharing—ensuring compliance with the act enforced in January 2025 while strengthening cybersecurity.



In Depth

Longer courses with practice scenarios that last between 30 and 60 minutes.

- Business Continuity Management
- Digital Operational Resilience Act (DORA)
- Electronic Communications
- Information Security
- Operational Resilience
- Operational Risk
- Records Management

Refresher

These courses help reinforce your employees' knowledge and notify them of any updates they might not be aware of.

- Cybersecurity
- Information Security

Express

These deliver learning in bite-sized chunks, typically lasting between 10 and 15 minutes.

- Phishing



Microlearning



Compliance Bites are short, engaging, animated videos designed to make compliance training more efficient. These microlearning videos, which are included in the package, use compelling storylines to enhance employee knowledge retention in just a few minutes, without the time commitment of traditional e-learning.

- Advising customers on cybersecurity
- Bring your own device security
- Business email compromise
- CEO fraud
- Common cyber threats
- Creating strong passwords
- Deepfake awareness
- Device hygiene
- Guide to secure remote working
- Information classification
- Information security on the move
- Malware
- Multi-factor authentication
- Ransomware
- Reacting to password breaches
- Risks in the use of AI
- Secure web browsing
- Smishing
- Spear phishing
- Spot a phishing attempt
- Supply chain cybersecurity
- Tailgating and piggybacking
- Think before you click
- Transferring information securely
- Understanding information security
- Using Wi-Fi safely
- Video conferencing
- Vishing
- Zero trust cybersecurity model





Frequently Asked Questions

Are the courses SCORM-compliant?

Yes. This means they can be delivered via the Skillcast Portal or any other SCORM-compliant Learning Management System.

What other tools are needed beyond training?

A comprehensive compliance solution often needs more than just training. Alongside e-learning, tools like declarations, surveys and registers to track compliance tasks are usually essential. Skillcast provides full support to help you set up these additional tools.

How can I benchmark my team's cybersecurity awareness?

An anonymous cybersecurity awareness survey can assess your team's understanding of critical security practices. Skillcast offers ready-to-use surveys to benchmark awareness levels and identify areas needing extra focus.

support@skillcast.com

+44 20 7929 5000

