# The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation

**Category:** Infrastructure & IT Operations | **Vendor:** EIMF

**Duration:** 8.00 hours (1 days) **6.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

## Course Information

**Delivery Format:** Instructor Led - Online

## Course Overview

The course aims to provide a deep dive into the critical legislative package associated with the Digital Operational Resilience Act (DORA), which has recently come into force, and is designed to addresses a key risk factor in the EU digital space.

## About This Course

The course aims to provide a deep dive into the critical legislative package associated with the Digital Operational Resilience Act (DORA), which has recently come into force, and is designed to addresses a key risk factor in the EU digital space: cyberattacks and ICT disruptions in the EU financial sector. These risks have been a concern for Europe's bank and securities regulators for many years, notably the ECB, the EBA and ESMA. This long overdue piece of legislation now consolidates a patchwork of existing sectoral rules on ICT risk management, incident handling and resilience testing. Critically, and core to the thrust of DORA, is the explicit recognition on the reliance by financial services entities on third party ICT service providers. Oversight of 3rd party ICT service providers will fall to the ESA's (EBA, ESMA and EIOPA). ESMA is also currently drafting technical standards, following DORA's entry into force on 16 January 2023, with application scheduled for 17th January 2025. An overview of the complex nature of the EU legislative process and the key EU Institutions involved in the development of the DORA regulatory text will be examined during the course, covering:

The shift from operational risk mainly with the allocation of capital to managing all components of operational resilience.

The DORA rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.

Identifying the DORA explicitly referenced ICT risks via new sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.

## Who Should Attend

Who Should Attend

The course is addressed to:

Chief AML Officers

CFOs

Regulatory Compliance Officers

National Supervisors

Financial Services Trade Bodies

Chief Legal Officers

Internal ITC Specialist

Chief Data Officers

COOs

## Learning Outcomes

**Upon successful completion of this course, participants will be able to:**

The course offers the opportunity to:
Acquire a structure understanding of the current EU legislative landscape and priorities in relation to the DORA legislative package.
Become sufficiently conversant in the broad details of the key pieces of current EU FS legislation to engage in a discussion with their professional peers, regulators and apply the knowledge in reviewing the impact on their business models, compliance expectations and obligation More specifically, by the end of the course participants will:Understand the EU Institutional decision-making process from the EC proposal stage on both legislative packages to ratification by the EU Parliament and CouncilIdentify the various key provisions under the DORA legislative text that will have a direct impact on the firm's compliance framework and that of its outsourced ITC providersIdentify the new requirements and challenges under the DORA framework designed to strengthen cross-border monitoring of ITC systems and outsourced structuresBuild an awareness of the modified roles of Pan-EU supervisors in terms of monitoring, requests for information, reporting requirements, on-site inspections, with more assertive powers by the ESAsLearn how the scaled-up harmonisation and coordination of ESAs supervisory practices in the management of the firms ITC operations will affect your businessDevelop awareness of how the EU intends to monitor DORA requirements with third countries considered to be ®®high-risk' jurisdictions.Be capable of anticipating questions and queries via the new ESA's role in monitoring DORA application and compliance

## Detailed Course Outline

Background on DORA legislative packages scope exemptions, definitions, supervision, reporting/compliance

Outline of uniform requirements concerning the security of network and information systems supporting the business processes of financial entities:
A. requirements applicable to financial entities in relation to:
Information and communication technology (ICT) risk management
Reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities

Reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d)

Digital operational resilience testing

Information and intelligence sharing in relation to cyber threats and vulnerabilities

Measures for the sound management of ICT third-party risk

B. Requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities

DORA application framework vis-Ã -vis critical third parties which provide ICT-related services to financial entities in terms of digital operational resilience, requiring all firms ensuring that they can withstand, respond to and recover from all types of ICT-related disruptions and threats.

A review of the critical third-country ICT service provider rules vis-Ã -vis provision of services to financial entities in the EU (required to establish a subsidiary within the EU so that oversight can be assured)

A review of the DORA oversight framework, which provides for an additional joint oversight network to l strengthen the coordination between the European supervisory authorities (ESAs) on this cross-sectoral topic

# Additional Course Details

Nexus Humans The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward.

This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

# Frequently Asked Questions

### Q: What delivery options are available for The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

---

### Q: How many CPD hours does this course provide?

The 1-day The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation course provides up to 6.5 CPD hours of structured learning. CPD certificates can be provided upon request.

---

### Q: What is the duration of the The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation training?

The training takes place over 1 day(s), with each day lasting approximately 8.00 hours including breaks for lunch and refreshments.

---

### Q: Do you provide corporate training for The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation?

Yes, we provide corporate training, dedicated training, and closed classes for The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

---

### Q: What related terms do people search for?

Popular related searches include: D.O.R.A. DORA ESA Digital Operational Resilience Act

---

### Q: Why choose Nexus Human for The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

---

### Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your The Newly Enforced Digital Operational Resilience Act (D.O.R.A) Regulation training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.


## Nexus Human

**Professional Training & Development**

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)