Digital Operational Resilience Act

Everything you need to know about DORA

LRQA

OVERVIEW GUIDE

Contents

DORA regulation

What is DORA?

First drafted in September 2020 and ratified by the European Parliament in 2022, the Digital Operational Resilience Act (DORA) is a landmark European Union (EU) regulatory framework. It marks a shift in emphasis from solely ensuring organisations' financial stability to guaranteeing their ability to maintain resilient operations in the face of severe disruptions caused by cybersecurity and information communication technology (ICT) issues.

DORA seeks to keep the digital infrastructure of the financial sector robust and resilient in the face of evolving cyber threats. It aims to create a unified supervisory approach applicable to financial market participants - fostering the convergence and harmonisation of security and resilience practices across entities operating within the EU.

The regulation means that financial organisations will have to make sure they can prevent and mitigate cyber threats and withstand, respond to, and recover from all types of ICT-related disruptions.

Timeline to compliance

The DORA regulation applies from 17th January 2025. Full compliance must be achieved by this deadline.

How will DORA be regulated?

Specific authorities (known as competent authorities) in each member nation will be responsible along with the european banking authority (EBA).

Organisations must prepare for the increased regulatory engagement powers that DORA will give to both national and EU-level supervisors. Instead of merely viewing this as a compliance task, organisations may need to develop new operational resilience capabilities, that must be tested and proven to work, and fully commit to an ongoing mandate to enhance their cybersecurity maturity.

Competent authorities will take the following steps:

Supervisory powers

Regulatory authorities have the power to conduct on-site inspections, request information, and impose sanctions.

Enforcement actions

Penalties for non-compliance can include fines, public warnings, and the temporary or permanent restriction of activities.

Remediation plans

Organisations may be required to submit detailed remediation plans to address identified deficiencies within set timelines.

Cross-border coordination

DORA establishes a framework for cooperation between national authorities and the european supervisory authorities.

Does DORA apply to my organisation?

DORA encompasses over 22,000 financial entities and ICT service providers operating within the EU, along with the ICT infrastructure supporting them from outside the EU. The regulation establishes detailed and stringent requirements applicable to all participants in the financial market.

Financial entities covered by DORA include:

- Credit institutions
- Payment institutions
- Account information service providers
- Electronic money institutions
- Investment firms
- Crypto-asset service providers and issuers of asset-referenced tokens
- Central securities depositories
- Central counterparties
- Trading venues
- Trade repositories
- Managers of alternative investment funds
- Management companies
- Data reporting service providers
- Insurance and reinsurance undertakings
- Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- Institutions for occupational retirement provision
- Credit rating agencies
- Administrators of critical benchmarks
- Crowdfunding service providers
- Securitisation repositories

The DORA regulation means that financial services (FS) organisations must fully understand how their operational resilience, third-party risk management, cybersecurity and ICT practices impact their critical functions. This may mean that they need to develop new operational resilience capabilities that must be tested and proven to work before January 2025.

The DORA regulation also covers and brings in critical ICT third-party service providers that support the regulated entities - if they are deemed critical to the regulated entity, they fall in the scope of DORA regardless of where the third party is based/ operates from.

DORA massively raises the bar for ICT service providers, for those designated as ‘critical’ by the European supervisory authorities, it is bringing them under the direct scrutiny of regulators. They will need to perform a comprehensive assessment of their obligations under DORA.

The 5 pillars of DORA

DORA compliance is measured against five pillars:

1. Risk management

The requirement to identify, assess, mitigate, and be accountable for guaranteeing the ability to maintain resilient operations in the face of severe disruptions caused by cybersecurity and ICT issues.

2. Incident management, classification and reporting

The need to implement early-warning systems to detect and manage cyber incidents, and to report those incidents promptly. This level of vigilance requires a dedicated security operations centre (SOC).

3. Digital operational resilience testing

The requirement to maintain effective, risk-centric, and independent testing programmes. This could include the use of both a technology and human testing strategy of attack surface management and continuous assurance technology capabilities, combined with penetration testing, red team and purple team testing.

4. Third-party risk management

The need to include and manage ICT risks from third parties within overall ICT management frameworks.

5. Information sharing

Consenting to and participating in the exchange of valuable cybersecurity threat and intelligence information among critical entities.

What are the DORA compliance requirements?

Financial entities must establish a comprehensive ICT risk management framework, which includes the following components:

- Setting up and maintaining resilient ICT systems and tools to minimise the impact of ICT risks.
- Identifying, classifying, and documenting critical or important functions and assets.
- Continuously monitoring all sources of ICT risks to establish protection and prevention measures.
- Establishing prompt detection of anomalous activities.
- Implementing dedicated and comprehensive business continuity policies and disaster recovery plans, including yearly testing of the plans, covering all supporting functions.
- Establishing mechanisms to learn and evolve from both external events and the entity's own ICT incidents.

Crucially, DORA compliance is not just a one-and-done service. The idea of resilience is a key factor within DORA, and resilience in the context of cybersecurity means that there is a need to stand up to repeated attacks.

DORA mandates that intrusion detection systems (IDS) should be tested at least yearly at a low level (using vulnerability scans, penetration testing, etc). Every three years, they should also be subjected to a large threat-led penetration test (i.e. a red team). Internal resources can be used for some of those deliveries, but the regulating body must sign off on the capability of an internal team, and there must also be no conflict of interest in terms of the scoping and delivery of the related tests. However, every threat-led penetration test must be supported by an external threat intelligence provider, and every third penetration test must be carried out externally.

The TIBER-EU framework for operational requirements

DORA details that advanced threat-led penetration testing must take place every three years in collaboration with third-party service providers, including mandatory purple teaming.. Therefore, DORA makes TIBER an acceptable testing framework for the three-year tests, which must be conducted by external parties.

It is not known whether there will be a central registry of companies that are trusted to deliver the testing that DORA requires. There is already a UK equivalent in the form of CBEST, maintained by the Bank of England and CREST, and that sets a minimum standard. LRQA is one of the handful of CBEST providers in the UK and, due to our experience, we suggest that the EU will eventually adopt something similar for TIBER. We have had universally positive feedback when delivering TIBER testing. A test for an EU national bank led to us being recommended as a tester for many other financial organisations.

How LRQA helps you achieve DORA compliance

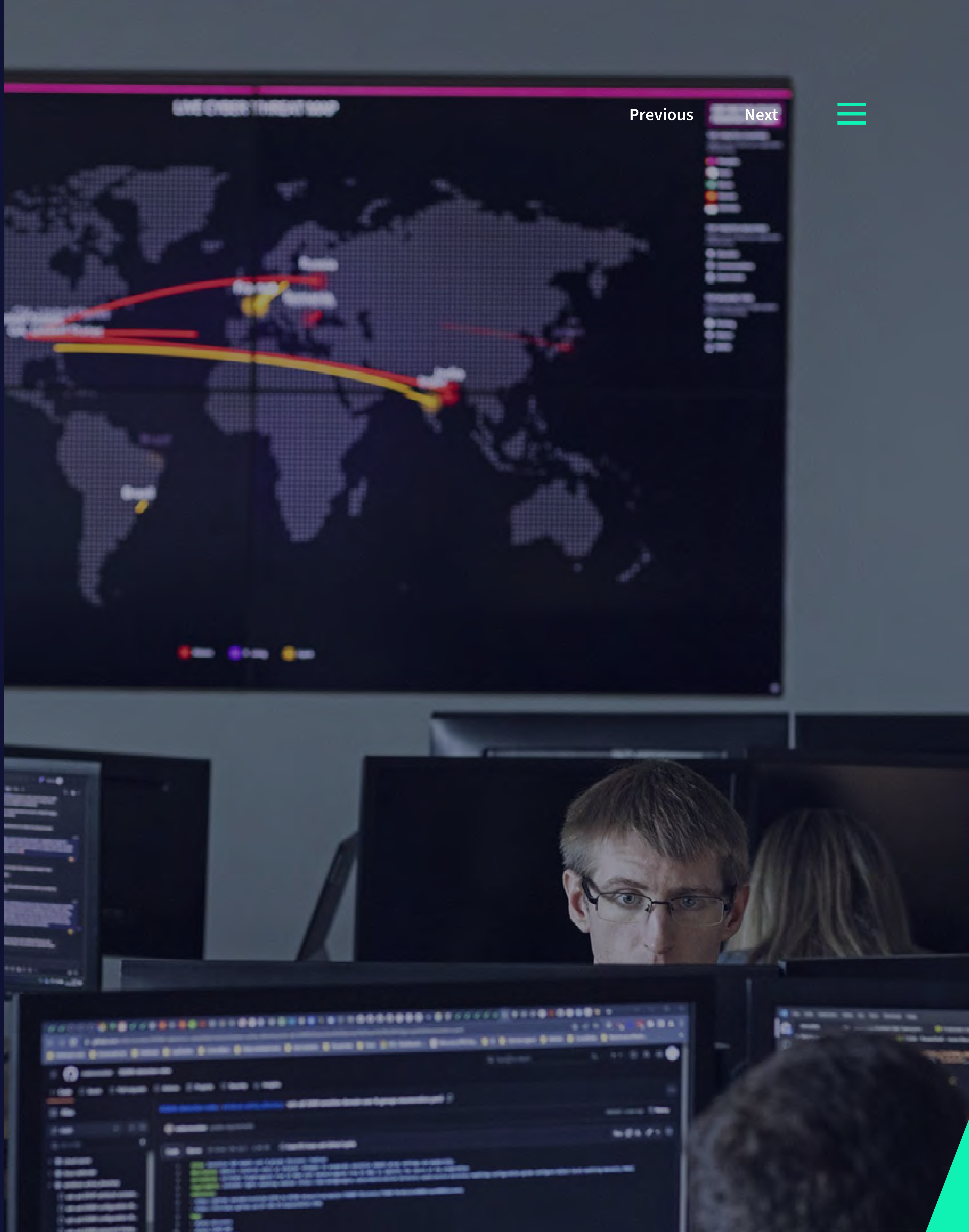
LRQA is uniquely placed as a full-service provider for achieving DORA compliance. We partner with you, providing comprehensive support and guidance throughout your journey.

Not only can our expert cybersecurity advisory team carry out the initial gap analysis, but we also provide all the necessary services to make sure you achieve compliance against each of the five pillars of DORA. You will not have to subcontract anything.

When you partner with LRQA, you gain access to a team of highly skilled and experienced cyber threat intelligence (CTI) analysts, governance risk and compliance consultants, and cyber incident response experts. Our experts have unparalleled expertise in the industry and utilise a comprehensive suite of proprietary and commercial tools, harnessing millions of data points. This combination empowers us to provide you with advanced insights and actionable intelligence, enabling proactive identification, mitigation of cyber threats, and measures to meet compliance objectives.

We begin with an initial gap analysis, assessing your current readiness and then follow up with tailored measures to meet requirements, and customised remediation plans to suit your organisation.

Like many of our competitors, we have threat intelligence and red team capabilities. However, unlike them, we also have everything else you need and more under one roof. If required, we can operate our in-house teams independently of each other. This makes us very agile. You can simply pick up the phone with any of our in-house teams and get the support you need, eliminating time spent waiting and if we find something on an engagement, we work with you to resolve it.



How LRQA helps you achieve DORA compliance

The LRQA team covers every part of the testing process for DORA. We are your full-service provider for achieving DORA compliance.

We provide hands-on, practical, clear guidance every step of the way.

- We have cybersecurity experts with rich experience working with the financial sector (including ex-financial regulators).
- We go far beyond what our competitors offer (i.e. just an audit) and allow your organisation to understand what is happening in our testing process.

The myLRQA Client Portal is a key part of this, as it allows you to manage the cybersecurity services you have with us, and gives you a view of a full lifecycle of interactions. In the case of DORA, it tracks your cyber maturity assessments, attack surface management, red teaming, and more.

Our comprehensive services include:

Advisory and compliance consulting

- We provide consultancy-led expert guidance on aligning cybersecurity practices with DORA requirements.
- We work with you to create, develop, and implement policies and procedures for DORA compliance.

Managed detection and response (MDR)

- We partner with you to achieve 24/7 monitoring and response services using leading industry technology capabilities to swiftly identify and mitigate cyber threats while leveraging advanced threat intelligence to enhance detection capabilities.

Resilience testing

- We provide penetration testing to identify vulnerabilities in financial systems and applications. You receive detailed reports with actionable recommendations for remediation.
- We go beyond point-in-time testing with attack surface management and continuous assurance capabilities.
- We conduct advanced threat-led penetration testing utilising award-winning red and purple team capabilities under regulatory frameworks such as TIBER, CBEST and iCAST.

Incident response

- We deliver an expert service as an assured NCSC level 2 cyber incident response provider. We offer cyber incident response services designed to aid your organisation’s preparedness in the event of a serious cyber incident.

Steps to DORA compliance

A **gap analysis** to identify

1) what areas are already in line with the articles in the legislation, and...

2) what areas need improvement.

Set priority strategies to **bridge the identified gaps.**

Conduct remediation and implementation activities to verify and assure **DORA compliance.**

Start your journey to DORA compliance today

Contact **cybersolutions@LRQA.com** to discuss your organisation's needs.

About LRQA:

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

Get in touch

Visit **www.lrqa.com** for more information or email **cybersolutions@lrqa.com**

1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.