DORA 10-Point Self Assessment

a PRIVALEX checklist

THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA) is in full force and it's designed to ensure that banks, insurers, investment firms, and their ICT providers can withstand and recover from digital disruptions.

For financial institutions, **compliance isn't optional. But where should you start?**

This 10-point self-assessment* helps you quickly benchmark your readiness against DORA's core requirements.

BENEFITS OF BEING COMPLIANT WITH DORA

GREATER RESILIENCE AND OPERATIONAL CONTINUITY

Implementing DORA allows you to anticipate, withstand, and quickly recover from cyber attacks, technological failures, and disruptions, protecting business stability

COMPETITIVE ADVANTAGE IN THE FINANCIAL SECTOR

Demonstrating DORA compliance strengthens your reputation with clients, regulators, and investors, positioning your company as a trusted technology and financial partner

MARKET ACCESS AND REGULATORY COMPLIANCE

Complying with DORA ensures regulatory alignment across the EU, avoiding penalties and securing access to contracts and operations within the European financial system

SCORING YOUR READINESS

8–10 Yes: Strong readiness.
You're on the right track, but you'll need to review specific details to fully meet the requirements.

4–7 Yes: Moderate risk.
The gaps may expose you to fines, delays or incidents. Prioritise resolving them.

0–3 Yes: High risk.
Immediate action is needed to prepare for compliance and reduce exposure.

**For each question check the box what applies to you*

1 Governance & Accountability

Is ICT and cyber risk management overseen by the board and senior management, with clear accountability?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

2 ICT Risk Management Framework

Do you have a documented framework for identifying, assessing, and mitigating ICT risks across the organization?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

3 Incident Response & Reporting

Can you detect, classify, and report major ICT incidents to regulators within the prescribed timelines?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

4 Business Continuity & Recovery

Do you maintain tested business continuity and disaster recovery plans that cover ICT disruptions?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

5 Digital Operational Resilience Testing

Do you perform regular penetration testing and advanced resilience testing (e.g., threat-led tests for critical functions)?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

6 Third-Party Risk Management

Do you assess and monitor the resilience of critical ICT service providers (e.g., cloud, SaaS, outsourcing)?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

7 Contractual Safeguards

Do your contracts with ICT providers include mandatory clauses required by DORA (access rights, data handling, termination, reporting obligations)?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

8 Information Sharing

Are you engaged in sectoral information sharing arrangements to exchange cyber threat intelligence and best practices?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

9 Audit & Oversight

Are your ICT risk and resilience practices fully documented, auditable, and subject to independent review?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

10 Compliance Roadmap

Do you have a designated DORA compliance owner, a gap analysis, and a roadmap to meet the requirements?

☐ *Yes, in place* ☐ *Partial / needs work* ☐ *Not in place*

WHAT'S NEXT?

We're seeing financial firms struggling to understand DORA, especially around third-party risk and testing requirements. A structured self-assessment like this is the fastest way to identify gaps.

At PrivaLex Partners, we help firms translate DORA into actionable roadmaps aligned with ISO 27001, NIS2, and sector best practices.

GET IN TOUCH IF YOU'RE INTERESTED IN ACHIEVING *DORA* COMPLIANCE WITH

PRIVALEX