DORA Checklist: Is Your Business Compliant with the DORA Regulation?

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) has been applicable since January 17, 2025. It introduced uniform and binding requirements for cybersecurity and ICT risk management for the entire EU financial sector, including crypto-asset service providers under MiCAR.

The goal of DORA is to ensure that the financial system remains resilient even in the event of a severe digital operational disruption. Although the regulation introduces the principle of proportionality, the requirements remain relatively strict even for smaller entities and demand a systematic approach.

This checklist is designed as a clear guide to help you review and assess whether your business complies with the key requirements of the DORA Regulation.

Special Considerations for Microenterprises

DORA recognizes the principle of proportionality, meaning the scope of obligations is adapted to the size, nature, and complexity of the entity. Microenterprises are eligible for significant simplifications.

> What qualifies as a microenterprise under DORA?
>
> In accordance with Article 3(60) of the DORA Regulation, a microenterprise is defined as an enterprise which:
>
> - employs fewer than 10 persons AND
> - has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million.

1. ICT Risk Management (ICT = Information and Communication Technology)

Governance and Organisation

☐ An internal governance and control framework for ICT risk is established.
☐ The management body possesses adequate knowledge to understand and assess ICT risks and their impact on the business.
☐ Roles and responsibilities for ICT risk management are clearly defined.

ICT Risk Management Framework

- ☐ The ICT risk management framework is part of the overall risk management system of the company.
- ☐ The framework is reviewed and updated regularly, at least annually.
- ☐ An independent control function is established to verify compliance with the framework.
- ☐ The framework includes a strategy for digital operational resilience (identification, protection, detection, response, and recovery).

💡 SIMPLIFICATION FOR MICROENTERPRISES:

DORA provides for a proportionate application of requirements for microenterprises. This means:

- Less stringent obligations regarding the extent of documentation (e.g., simpler business continuity policies).
- For microenterprises, there is no requirement for a separate internal audit function; the control function can be performed by other control functions.
- And other simplifications.

2. ICT-Related Incident Management and Reporting

- ☐ A process for monitoring, managing, and logging ICT-related incidents is in place.
- ☐ Criteria for classifying incidents (e.g., by criticality and impact) are defined.
- ☐ Major incidents are reported to the competent authorities within the prescribed deadlines.

3. Digital Operational Resilience Testing

- ☐ A comprehensive digital operational resilience testing programme is established.
- ☐ Resilience tests for systems and applications supporting critical or important functions are performed regularly (at least annually).
- ☐ A process for addressing identified vulnerabilities is in place.

💡 SIMPLIFICATION FOR MICROENTERPRISES:

Microenterprises are NOT required to conduct the most advanced form of testing – Threat-Led Penetration Testing (TLPT). Nevertheless, they must perform proportionate resilience tests, such as vulnerability assessments and scenario-based tests.

4. ICT Third-Party Risk Management

Strategy and Register

- ☐ A strategy for managing risks arising from arrangements with third-party ICT service providers has been adopted.

☐ A register of all contractual arrangements with third-party ICT service providers is maintained.
☐ The register distinguishes between providers supporting critical or important functions and others.

Contractual Provisions

☐ Contracts with ICT service providers include all minimum contractual provisions required by DORA (e.g., description of services, data locations, security standards, audit rights).
☐ Exit strategies are defined for terminating arrangements with providers that support critical functions.

5. Information-Sharing Arrangements

☐ Mechanisms are in place for sharing information and intelligence on cyber threats with other financial entities.

What's Next?

This checklist is the first step in verifying compliance with the DORA Regulation. Achieving full compliance requires the preparation of detailed internal documentation.

Save time and ensure compliance!
Our collection of professionally prepared templates and samples is specifically tailored to the needs of businesses. This includes versions specifically adapted for microenterprises, which already incorporate all relevant simplifications.

- Digital operational resilience strategy,
- Information security policy,
- Business continuity and crisis management plan,
- Policy on the use of ICT services,
- Business impact analysis,
- External ICT providers register,
- Register of ICT Assets,
- Risk management register.

Additional templates:

- Due diligence report for ICT providers Draft,
- ICT risk management report draft.