DORA Compliance Checklist

By addressing these key areas, your organisation can take steps to ensure compliance with DORA and promote operational resilience.

☑ **Understand the scope**
Determine if your organisation falls within the Digital Operational Resilience Act (DORA) jurisdiction and identify the specific requirements applicable to your business.

☑ **Conduct a risk assessment**
Evaluate the potential risks and vulnerabilities in your information and communications technology (ICT) systems, considering both internal and external threats.

☑ **Develop an incident response plan**
Create a detailed plan outlining how your organisation will detect, respond to, and recover from security incidents and operational disruptions.

☑ **Implement robust ICT risk management practices**
Establish policies, procedures, and controls to identify, assess, and mitigate risks related to your ICT systems, including cybersecurity threats and operational vulnerabilities.

☑ **Enhance information security measures**
Strengthen your organisation's information security framework, including access controls, encryption, secure coding practices, and data protection mechanisms.

☑ **Establish resilience testing procedures**
Develop standardised resilience testing methods to assess the effectiveness of your ICT systems under various scenarios and ensure their ability to withstand disruptions.

☑ **Foster intelligence sharing**
Collaborate with other organisations, industry groups, and relevant authorities to share threat intelligence, best practices, and insights for improving operational resilience.

☑ **Manage third-party risk**

Evaluate your third-party suppliers' resilience and security measures and ensure their compliance with DORA requirements to minimise potential vulnerabilities in your supply chain.

☑ **Implement an Information Security Management System (ISMS)**

Establish an ISMS aligned with international standards like ISO 27001 to ensure a structured approach to information security and operational resilience.

☑ **Train employees and raise awareness**

Provide comprehensive training programs to educate employees on cybersecurity best practices, incident reporting procedures, and their roles in maintaining operational resilience.

☑ **Maintain documentation and records**

Keep detailed records of risk assessments, incident response plans, resilience testing results, and compliance measures to demonstrate adherence to DORA requirements.

☑ **Continuously monitor and assess**

Implement ongoing monitoring processes to detect and respond to emerging risks, vulnerabilities, and changes in the operational landscape promptly.

☑ **Engage with regulators and authorities**

Stay informed about regulatory updates and engage in open dialogue with relevant authorities to understand their expectations and ensure compliance.

☑ **Conduct internal audits and assessments**

Regularly review your organisation's operational resilience measures through internal audits and assessments to identify areas for improvement and address any compliance gaps.

☑ **Stay updated on industry best practices**

Continuously monitor advancements in cybersecurity and operational resilience practices to adapt your strategies and align with evolving standards.

Simplify Your Journey to DORA Compliance Today

Get started →