DORA
COMPLIANCE CHECKLIST

OneCollab

This checklist outlines the key steps your organisation can take to achieve compliance with the Digital Operational Resilience Act (DORA).

1

Understand DORA Requirements

Familiarise yourself with the DORA regulation to understand its specific requirements for your organisation's size and sector.

2

Conduct a Risk Assessment

Assess your entire organisation and its extended supply chain to identify potential vulnerabilities to cyber threats.

3

Collaborative Approach

Form a cross-functional team to analyse risk assessments and build a comprehensive compliance strategy.

4

Employee Training Programmes

Implement cyber security awareness training programmes for all employees at various levels of the organisation.

5

Build a Operational Resilience Strategy

Including a detailed business continuity plan for cyber threats,data breaches, and operational disruptions.

6

Third-Party Risk Management

Implement robust risk management measures to ensure third-party services comply with DORA requirements.

7

Regular Testing and Assessments

Conduct regular penetration testing (pen testing) at least every three years as mandated by DORA.

8

Automated Threat Detection

Allocate sufficient resources to ensure effective detection, response, and prompt action on any security alerts.

9

Continuous Improvement

Regularly update your operational resilience strategy based on insights gained from pen tests and previous incidents.

10

Prepare for the Worst

Ensure a clear plan is in place for responding to and recovering from worst-case scenarios.

11

Data Security

Secure data storage, transmission, and access controls to prevent unauthorised access and data breaches.

12

Evidence of Compliance

Maintain records of your compliance efforts, including test results, risk assessments, and incident reports.

www.onecollab.co.uk
info@onecollab.co.uk