

DORA Compliance Readiness Checklist

Use this checklist to assess your organization's DORA readiness:

ICT Risk Management

- Establish documented ICT risk management framework approved by management body
- Identify and document all ICT assets, systems, and dependencies
- Implement access controls, encryption, and network security measures
- Deploy detection capabilities for anomalous activities
- Develop and test business continuity and disaster recovery plans

Incident Response & Reporting

- Establish incident classification criteria aligned with DORA requirements
- Implement incident response procedures with defined roles and escalation paths
- Configure reporting mechanisms to meet regulatory timeframes
- Maintain incident register with root cause analysis and lessons learned

Operational Resilience Testing

- Schedule regular vulnerability assessments and penetration testing
- Conduct scenario-based testing of business continuity plans
- Engage qualified providers for threat-led penetration testing (if required)
- Document testing results and remediation actions

Third-Party Risk Management

- Maintain register of all ICT third-party service arrangements
- Conduct due diligence on ICT providers before and during engagement
- Ensure contracts include required DORA provisions
- Develop exit strategies for critical ICT services
- Monitor concentration risk across providers