



# DORA

## COMPLIANCE CHECKLIST

### Phase 1: Preparation and Planning

- Review the Digital Operational Resilience Act (DORA) to understand its scope and implications for your business.
- List all internal and external stakeholders involved in DORA compliance, including IT, compliance, risk management and third-party service providers.

### Phase 2: ICT Risk Management

- Document all ICT systems, assets and dependencies.
- Identify and categorise critical assets and functions.
- Perform thorough risk analyses of ICT systems.
- Establish and deploy robust cybersecurity protocols and measures.
- Maintain detailed records of all risk management activities and decisions.

### Phase 3: Incident Response and Reporting

- Create a comprehensive plan for responding to ICT-related incidents.
- Define procedures for internal and external incident reporting.
- Regularly test and update the incident response plan.

### Phase 4: Digital Operational Resilience Testing

- Plan and execute regular testing of ICT systems to identify vulnerabilities.
- For critical entities, ensure that advanced penetration testing is carried out.
- Record test results and remediation actions, and report to relevant authorities as required.

### Phase 5: Third-party Risk Management

- Evaluate all ICT third-party service providers for compliance with DORA standards.
- Ensure contracts with third parties align with DORA requirements.
- Regularly review third-party performance and compliance.

### Phase 6: Board of Directors' Involvement

- Ensure active board participation in developing and overseeing the Digital Operational Resilience Strategy.
- Establish a framework for ICT governance and risk management at the board level.

### Phase 7: ICT-related Incident Reporting

- Establish what constitutes a major incident and the thresholds for reporting.
- Create efficient processes for reporting major incidents to authorities.
- Continuously assess and refine the incident reporting mechanism.