Ostorlab

OSTORLAB'S

DORA Compliance Checklist

Ostorlab

DORA COMPLIANCE CHECKLIST

For Financial Institutions & Fintech Teams

What is DORA?

The Digital Operational Resilience Act (DORA) is a European regulation designed to strengthen the digital resilience of financial institutions. It ensures that banks, fintech companies, and other financial entities can withstand, respond to, and recover from ICT disruptions, including cyberattacks, system failures, and third-party risks.

DORA goes beyond traditional cybersecurity by focusing on prevention, detection, response, recovery, continuous testing, and evidence-based validation.

Overview

This checklist helps assess your organization's readiness across the core pillars of DORA.

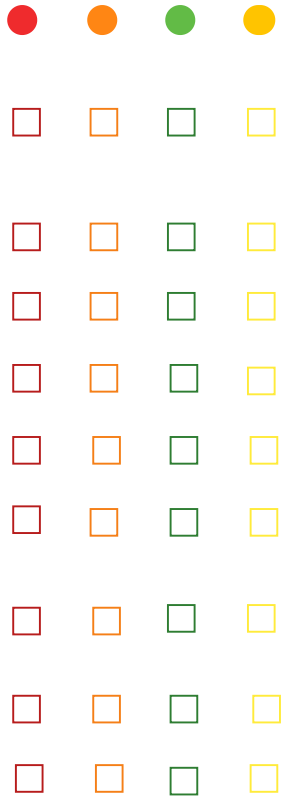
For each item, select the current status and attach supporting evidence where applicable.

Status Key: Not Started | In Progress | Implemented | Needs Review

1. ICT Risk Management

Objective: Ensure visibility, control, and protection of all digital assets.

- Maintain a complete inventory of ICT assets (applications, APIs, infrastructure)
- Classify assets based on criticality and business impact
- Define and document an ICT risk management framework
- Implement access control policies (RBAC, least privilege)
- Apply encryption for data at rest and in transit
- Enable centralized logging and monitoring
- Establish secure development practices (code review, dependency checks)
- Perform regular backups and test recovery procedures
- Define risk appetite and tolerance thresholds



Evidence:

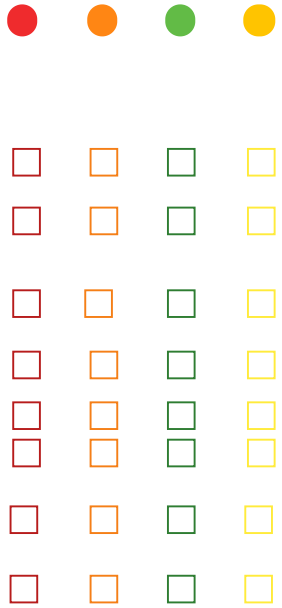
Asset inventory, security policies, architecture diagrams, logs

Add evidence...

2. Incident Management & Reporting

Objective: Detect, respond, and report incidents effectively.

- Define what constitutes an ICT incident
- Implement real-time detection mechanisms (alerts, monitoring tools)
- Maintain a documented Incident Response Plan (IRP)
- Assign roles and responsibilities for incident handling
- Classify incidents by severity levels
- Maintain incident logs and audit trails
- Conduct root cause analysis (RCA) after incidents
- Ensure compliance with regulatory reporting timelines



Evidence:

Incident logs, IRP documentation, post-mortem reports

Add evidence...

3. Digital Operational Resilience Testing

Objective: Validate security controls through continuous testing.

- Conduct regular vulnerability assessments
- Perform penetration testing (internal and external)
- Implement Threat-Led Penetration Testing (TLPT) for critical systems
- Test mobile applications, APIs, and backend systems
- Validate findings with technical evidence (not theoretical only)
- Track remediation progress and retest fixes
- Maintain documentation of all testing activities

Evidence:
Scan reports, pentest reports, remediation tracking

Add evidence...

4. Third-Party Risk Management

Objective: Manage risks introduced by external providers.

- Maintain a register of all ICT third-party providers
- Classify vendors based on risk and criticality
- Perform due diligence before onboarding vendors
- Include security and audit clauses in contracts
- Monitor vendor performance and security posture continuously
- Define contingency and exit strategies
- Assess concentration risk across providers

Evidence:
Vendor register, contracts, risk assessments

Add evidence...

5. Information Sharing

Objective: Strengthen resilience through collaboration and intelligence.

- Participate in threat intelligence sharing initiatives
- Share indicators of compromise (IOCs) where applicable
- Integrate external threat intelligence feeds
- Ensure compliance with confidentiality and data protection requirements

Evidence:
Threat intel subscriptions, sharing policies

Add evidence...

6. Governance & Oversight

Objective: Ensure accountability and strategic alignment.

- Establish board-level oversight of ICT risk
- Provide regular reporting to leadership
- Maintain updated policies and procedures
- Conduct employee security awareness training
- Perform internal audits and compliance reviews

Evidence:

Board reports, training records, audit results

Add evidence...

READINESS SUMMARY		
Pillar	**Status**	**Notes**
ICT Risk Management	Not Started	Add Notes...
Incident Management	Not Started	Add Notes...
Resilience Testing	Not Started	Add Notes...
Third-Party Risk	Not Started	Add Notes...
Information Sharing	Not Started	Add Notes...
Governance	Not Started	Add Notes...

Ostorlab

Your strategic partner in automated application security.

Ostorlab is a comprehensive security testing automation platform trusted by thousands of developers and security professionals across the globe. Our integrated platform combines AI-powered mobile and web application scanning, and External Attack Surface Management to provide a continuous, 360-degree view of your digital vulnerabilities.

We empower leading companies to secure their digital assets and achieve seamless regulatory compliance with global standards like GDPR, HIPAA, SOC2, OWASP MASVS, and more.

By integrating security directly into the DevOps pipeline, we turn complex vulnerability management into an automated, audit-ready process.

We're here to secure your vision. Contact our team at **contact@ostorlab.co**

TRUSTED BY

Google TikTok ROLEX Deloitte. BMW cisco bread savings PNC nubank

www.ostorlab.co

651 N Broad St, Middletown Delaware, DE 19709