iCompliance.eu

February 2026

CHECKLIST + EVIDENCE

DORA Implementation Pack

Practical guide + checklist for implementing DORA in Portugal

Next step

Use this checklist to accelerate compliance and prepare evidence for supervision.

Book a DORA Readiness Call

Talk to iCompliance

Quick checklist

1. Define the scope: entities, services and Critical or Important Functions (CIFs).

2. Run a gap assessment across the five pillars (governance, incidents, testing, third parties, threat intel).

3. Build a 90/180-day roadmap with quick wins and structural remediation.

4. Organise evidence: policies, registers, test reports and management decisions.

DORA in 5 pillars

Governance & ICT Risk

Framework, policies, responsibilities and controls.

Incidents & Reporting

Detection, classification, notifications and RCA.

Resilience Testing

Annual testing plan and remediation closure.

ICT Third Parties

Contracts, registers, monitoring and exit plans.

Threat Intelligence

Sharing and monitoring of threats (where applicable).

Tip: start with scope + incidents + critical contracts. These are the most common inspection pain points.

Scope and critical services

[ ] Map in-scope entities and business lines.
[ ] Identify services and CIFs (critical or important functions).
[ ] Inventory ICT assets, data, integrations and dependencies.
[ ] Define RTO/RPO per critical service and associated dependencies.

Governance and accountability

[ ] Approve the DORA programme at management body level (minutes and decisions).
[ ] Define governance model (committees, reporting, escalation).
[ ] Assign owners for ICT risk and for each critical service.
[ ] Define metrics/KRIs and periodic reporting to management.

Essential ICT risk controls

[ ] Access management (MFA, least privilege, periodic reviews).
[ ] Vulnerability & patch management (SLAs by severity).
[ ] Logging and monitoring (events, alerts, retention).
[ ] Change management (approvals and rollback).
[ ] Backups and restore testing (frequency, evidence, RTO/RPO).
[ ] Configuration management and hardening baselines.
[ ] BCP/DRP tested with business participation.
[ ] Data security (encryption, key management, classification, DLP where relevant).

ICT incidents and reporting

[ ] Define incident taxonomy and severity/classification criteria.
[ ] Ensure 24/7 response and decision capability (on-call).
[ ] Create scenario playbooks (ransomware, outage, data leak, third-party failure).
[ ] Prepare reporting templates (initial, intermediate, final) and responsibilities.
[ ] Run tabletop exercises focused on classification and reporting timelines.
[ ] Implement RCA and remediation plan with deadlines and owners.

Digital operational resilience testing

[ ] Annual testing plan (technical and process) approved and scheduled.
[ ] Backup/restore, failover and continuity tests (with evidence).
[ ] Pen tests/technical assessments with remediation closure.
[ ] Incident simulations and communication/escalation testing.

ICT third-party risk management

[ ] Inventory ICT providers and assess criticality per service/CIF.
[ ] Security and resilience due diligence (questionnaires, evidence, audits).
[ ] Contracts include key clauses (SLAs, incident notice, audit rights, subcontracting, location, exit).
[ ] Continuous monitoring of performance and risk (KPIs, reviews).
[ ] Exit plans for critical services (alternatives, migration, exit testing).

Evidence pack (for supervision/audit)

- Scope & CIF map + asset/dependency inventory.
- Policies & procedures (ICT risk, access, change, backups, continuity, incidents).
- Registers: incidents, tests, vulnerabilities, access, changes, third parties.
- Test reports and remediation tracking (deadlines, owners, closure evidence).
- Management body minutes and decisions (approval and oversight).

If you want, iCompliance.eu can run a DORA Readiness & Gap Assessment and deliver a 90/180-day roadmap.