CyberDORA — My DORA obligations

FULL REGIME

Large financial entity

Bank, insurer, investment firm or other Article 2 entity exceeding the proportionality thresholds.

Your obligations

1. **ICT risk governance approved and overseen by the management body (Art. 5-6).**

   The board of directors or senior management must approve the digital resilience strategy, ensure its regular monitoring, and answer for it directly to the supervisor.

2. **Up-to-date register of information assets and ICT systems (Art. 8).**

   In practice: map all critical systems, applications and data flows, and identify the interdependencies between them.

3. **Detection, classification and notification of major incidents within regulatory deadlines (Art. 17-19).**

   An incident deemed major triggers an initial notification to the competent authority, followed by one or more intermediate reports and a final report.

4. **Annual digital resilience tests, with TLPT every 3 years if designated as significant (Art. 24-26).**

   The most important entities must also simulate real attacks through threat-led penetration testing (TLPT) on their production systems.

5. **Register of information covering all contracts with ICT providers (Art. 28).**

   This register, submitted to the authorities, lists each provider, the service provided, its criticality level and any subcontractors.

6. **Business continuity and disaster recovery plan (Art. 11-12).**

   It must set recovery time objectives (RTO) and maximum tolerable data loss (RPO), and be tested periodically.