*DORA compliance checklist*

# Strengthen your codebase compliance with DORA using SonarQube

The Digital Operational Resilience Act (DORA) mandates a unified framework for managing ICT risk, requiring financial entities to build resilience into their systems from the ground up. This regulation emphasizes proactive risk management, supply chain security, and continuous testing to withstand operational disruptions.

## 8 steps to streamline DORA compliance:

1. **Proactively identify vulnerabilities:** Leverage powerful Static Application Security Testing (SAST) with taint analysis to detect complex flaws like SQL injection and XSS before applications are deployed, addressing core ICT risk management requirements.
2. **Manage third-party risk:** Perform Software Composition Analysis (SCA) to identify known vulnerabilities (CVEs) in dependencies and generate detailed Software Bills of Materials (SBOMs) to maintain a comprehensive register of ICT services.
3. **Secure infrastructure from the start:** Scan Infrastructure as Code (IaC) configurations to ensure underlying cloud environments are secure, supporting comprehensive risk management.
4. **Prevent data leaks:** Detect and block hard-coded secrets and credentials in the IDE before they are committed, ensuring the confidentiality required by DORA.
5. **Enforce security standards:** Use automated standard enforcement mechanisms, such as quality gates, to fail builds that miss security or reliability thresholds. This ensures only secure, high-quality code reaches production.
6. **Streamline audit and compliance reporting:** Automatically generate detailed reports that map to major industry standards (OWASP, CWE, PCI DSS) to provide the necessary evidence for regulatory audits and compliance verification.
7. **Secure AI-generated code:** Apply rigorous quality and security checks to AI-generated code with automated standard enforcement, ensuring all code meets organizational standards regardless of its source.
8. **Build operational resilience:** Enforce code quality standards alongside security to build reliable, maintainable software that is less prone to unexpected failures and easier to recover during disruptions.

SonarQube serves as the automated code verification layer, integrating rigorous security and quality checks directly into the developer workflow to meet these requirements efficiently. It helps to ensure that all code—regardless of its origin—is production-ready, secure, and maintainable.

Learn more about SonarQube for compliance

Availability: DORA-relevant security reports and requirements are supported in enterprise editions of SonarQube. Software Composition Analysis (SCA) and SBOM generation require SonarQube Advanced Security.