CRA compliance checklist

Streamline your codebase compliance with CRA using SonarQube

The Cyber Resilience Act (CRA) mandates that organizations deliver secure-by-design software, holding manufacturers legally responsible for vulnerabilities in their products. As the velocity of AI-assisted development increases, manual peer review becomes a physical bottleneck. Organizations must scale their verification to match the speed of AI creation, as the CRA makes no distinction between code written by a human and code suggested by an AI.

8 steps to streamline CRA compliance:

1. **Minimize vulnerabilities through SAST:** Leverage Static Application Security Testing (SAST) to identify exploitable coding weaknesses early in development, satisfying the Article 13 mandate to minimize vulnerabilities before products are placed on the market.
2. **Safeguard system access:** Scan the entire codebase to detect and block hard-coded API keys, passwords, and sensitive tokens, fulfilling the Annex I requirement to ensure protection against unauthorized access.
3. **Manage third-party risk:** Use Software Composition Analysis (SCA) to identify vulnerable dependencies and monitor component risk continuously, supporting CRA obligations for transparency and lifecycle risk management.
4. **Verify the absence of known exploits:** Utilize databases like NVD, EPSS, KEV, and OSV to verify that components are free from known risks, directly addressing the Annex I mandate to ship products without known exploitable vulnerabilities.
5. **Master supply chain transparency:** Automatically generate machine-readable Software Bills of Materials (SBOMs) to ensure a traceable inventory management process, helping teams maintain control over the software lifecycle and meet explicit CRA mandates.
6. **Generate audit trails and proof:** Maintain secure, immutable audit logs that capture lifecycle changes, configuration updates, and security events, simplifying the creation of documentation required for CRA risk assessments.
7. **Enforce standards at the point of creation:** Empower developers with instant feedback in the IDE and use configurable quality gates in your CI/CD pipeline to ensure no non-compliant code proceeds to production.
8. **Assess risk with strategic governance:** Leverage portfolio management and customizable project dashboards to gain a high-level view of codebase health, transforming invisible code debt into visible data for leadership and risk officers.

SonarQube provides the essential infrastructure to meet these rigorous standards. By acting as an automated verification solution, it ensures that all code—regardless of its origin—is production-ready, secure, and maintainable, seamlessly integrating compliance directly into the developer workflow.

Learn more about SonarQube for compliance

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