PCI DSS 4.0 compliance checklist

Strengthen your PCI DSS 4.0 compliance with SonarQube

PCI DSS 4.0 marks a critical evolution from annual compliance checklists to a culture of continuous, always-on security. The standard's expanded Requirement 6 now mandates that organizations "develop and maintain secure systems and software," explicitly requiring security controls to be embedded throughout the software development lifecycle (SDLC) rather than validated at the end. For development teams, this shifts security from a gatekeeper to a daily responsibility.

6 steps to streamline your compliance with PCI DSS 4.0:

1. **Achieve comprehensive vulnerability detection:** Detect a wide range of PCI DSS application security vulnerabilities, including injection attacks, cryptographic failures, and attacks on business logic, ensuring alignment with Requirement 6.2.4.
2. **Centralize enforcement across the organization:** Automate the enforcement of secure coding standards and best practices globally. This ensures developers write secure code early in the lifecycle and prevents new vulnerabilities from being introduced across the entire application portfolio.
3. **Enforce standards in the IDE:** Empower developers to use tools like SonarQube for IDE in connected mode. This "start-left" approach provides instant feedback on security weaknesses as code is written, preventing vulnerabilities from entering the repository and ensuring earlier, cheaper remediation compared to late-stage discovery.
4. **Conduct regular automated code reviews:** Implement extensive, automated code reviews that align with PCI DSS 4.0 standards (Requirement 6.2.3), streamlining the verification process and reducing the burden of manual checks.
5. **Stop non-compliant code with quality gates:** Use configurable quality gates within your Continuous Integration (CI) pipeline to ensure that only code meeting your defined security standards is promoted to production.
6. **Streamline compliance reporting:** Generate downloadable PDF reports for Qualified Security Assessors (QSAs) or Self-Assessment Questionnaires (SAQs). View coverage across the 12 high-level requirements to simplify audit preparation and evidence collection.

SonarQube serves as the essential verification layer for this new reality, integrating automated guardrails for code quality and security directly into the developer workflow. This enables organizations to satisfy strict PCI DSS 4.0 mandates for secure coding, vulnerability management, and continuous monitoring without compromising engineering velocity.

Learn more about SonarQube for compliance

Availability: Coverage of PCI DSS 4.0 application security vulnerabilities and security reports is supported in enterprise editions of SonarQube.