Sonar

Integrated code quality and security for financial services

Global financial services companies use SonarQube to deliver code they can trust

Financial institutions face a unique pressure: the need to innovate at speed while managing massive legacy codebases, strict regulatory compliance, and non-negotiable security requirements. AI coding can increase speed, but simultaneously puts availability, compliance, and security at risk. Sonar provides the code verification layer that allows developers to modernize and adopt AI safely without sacrificing stability.

Here's what SonarQube helps you do:

- **Centralize quality management:** SonarQube integrates with your DevOps ecosystem to standardize analysis and provide a unified view of code health, helping to harmonize diverse teams.
- **Streamline compliance:** Embed standards like PCI DSS and OWASP directly into the pipeline. Customizable quality gates enforce rules automatically, ensuring continuous, audit-ready compliance.
- **Manage technical debt:** From COBOL to Java, SonarQube analyzes 35+ languages to identify debt and complexity. This "actionable code intelligence" guides refactoring and ensures system stability.
- **Secure AI adoption:** SonarQube inspects AI-generated code for issues before merging, providing guardrails that protect without slowing developers down.
- **Simplify modernization:** Empower developers with real-time feedback via SonarQube for IDE. The start-left approach catches issues instantly, facilitating smoother migrations to modern frameworks.

> **"We have more than 20k developers using SonarQube Server in HSBC. It being a great SAST solution, it's now one of the mandatory quality gateways for our standard development process..."**
>
> Navneet Kumar Mittal, IT Service Owner, HSBC UK

> **"We have used SonarQube Server since very early on and its value in responding to audits and regulatory inquiries is immeasurable."**
>
> Gary Barter, Executive Director, JPMorgan Chase

Customer Story | M&T Bank

M&T Bank, a leading U.S.-based commercial bank, successfully utilized SonarQube to enhance code quality and security across their organization. They achieved ROI in less than six months, standardized their codebase, and ensured more secure, efficient code development without disrupting workflows.

Key SonarQube features for the financial services industry

Compliance and reporting
Generate detailed reports to demonstrate adherence to critical regulations (like PCI DSS, GLBA, NYDFS Cybersecurity Requirements, DORA, and NIS2). This capability is essential for streamlining compliance and proving your codebase meets rigorous industry standards.

AI Code Assurance
Ensure the secure and compliant use of AI-generated code. As financial institutions adopt AI, SonarQube validates that AI-generated code meets the same security and quality standards as developer-written code.

Advanced Security
Protect against supply chain attacks with software composition analysis (SCA) and automated software bill of materials (SBOM) generation. Given the high stakes of financial data, understanding and managing third-party dependencies is paramount for securing the software supply chain.

Quality gates
Enforce predefined quality and security standards within the pipeline. This feature ensures that only compliant, secure code is deployed, acting as an automated checkpoint that minimizes risks in the production environment without requiring manual intervention.

Customizable security rules
Create and enforce rules tailored to specific organizational security policies. This allows financial institutions to address unique industry threats and internal governance requirements that go beyond standard rule sets.

Vulnerability detection and taint analysis
Identify and prevent critical security vulnerabilities—such as SQL injection, XSS, and authentication flaws—using static application security testing (SAST). Taint analysis specifically tracks untrusted user input across the application to prevent data leaks, protecting sensitive financial information and preventing fraud.

Integration with CI/CD pipelines
Automate security and quality checks early in the development lifecycle. By integrating directly into DevOps platforms (like Azure DevOps, GitHub, or GitLab), teams can prevent vulnerabilities from reaching production and ensure compliance without slowing down the release of new products.

Sonar's approach: Actionable code intelligence

Analyze
Deep insight on architectural, quality, and security issues in all code, no matter the source

Code Quality
Deliver high-quality code, whether human, AI-assisted, or agentic.

Code Security
Prevent security risks early, both within your code and from 3rd parties.

→ **Review**
Define, apply, and attest to code standards and policies as a team

Code Orchestration
Automate governance and compliance while establishing standards across teams.

→ **Act**
Agentic or on-demand issue remediation

Code Remediation
Resolve issues before they become problems. Modernize old code with AI.

← **Vibe** with better context → then **Verify** every line of code, anywhere

Santander · Broadridge · Deutsche Bank · Prudential · US Bank · adyen

© 2008-2025, SonarSource S.A, Switzerland. All content is copyright protected. Sonar, SonarSource, SonarQube for IDE, SonarQube Server, and SonarQube Cloud are trademarks of SonarSource SA. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.