BLACK DUCK®

ACHIEVING AND DEMONSTRATING SOFTWARE CODE COMPLIANCE

In today's rapidly evolving technology landscape, software is the backbone of many enterprises. From healthcare providers and financial services to aerospace and defense manufacturers, the reliability and security of software is paramount. The increasing complexity of applications, prevalence of open source software, and ever-evolving cybersecurity threats make it even more important to comply with coding standards and regulatory requirements to help ensure the reliability and security of your software.

Coverity® Static Analysis provides comprehensive software scans that help track and manage compliance with the standards that are most important to your business. This guide outlines the approach many leading organizations are taking to achieve code compliance with Coverity.

EASIER SAID THAN DONE: CHALLENGES TO ACHIEVING COMPLIANCE

Despite the importance of complying with industry and consumer requirements, many organizations face significant challenges adhering to necessary coding standards. These challenges include

- **Codebase complexity:** Large and complex codebases make it difficult to identify and fix all issues, especially those that span multiple files or libraries.
- **Diverse development environments:** Many organizations use a variety of development tools and environments, and that can complicate the implementation of consistent coding standards.
- **Resource constraints:** Developers are often under pressure to meet tight deadlines, which can lead to shortcuts in testing and code review.
- **Conflicting priorities:** Development teams are often forced to juggle multiple priorities, creating distractions that impact development velocity. This can force teams to choose between shipping on time and meeting all requirements.
- **Integration with existing workflows:** Integrating compliance tools into existing development and testing workflows can be challenging and may require significant changes to processes.

STEPS TO ENSURE SOFTWARE CODE COMPLIANCE

Align policies with your coding standards

The first step to ensuring code compliance is aligning your policies with your coding standards. This involves

- **Identifying relevant standards:** Determine which coding standards are most important for your business. Common standards include MISRA, CERT C/C++, and OWASP.
- **Defining your policies:** Create policies that map to these standards. For example, you might define a policy that all code must be free of CERT C/C++ security vulnerabilities.
- **Choosing tools that scale to your needs:** Many tools struggle to accurately identify defects and vulnerabilities in large-scale, complex software. Ensure that your testing tools are up to the task, so key issues are not missed.
- **Automating issue-mapping:** Integrate code scans into your development workflows, enabling defects and vulnerabilities to be mapped to the standards that matter most to your business without slowing development velocity.

Run policy-driven scans

Once your policies are defined, automating policy-driven scans can help ensure your code adheres to all requirements. Coverity provides several options for running policy-driven scans.

- **Scheduling scans:** Set up regular in-depth scans to identify all issues in your project, while automatically checking your code for compliance. Scans can be configured to run at specific intervals or as part of your continuous integration pipeline.
- **Triggering scans on pull requests:** Coverity can be integrated with popular source code management systems and automated to run on every pull request. Scans analyze any new or changed code to identify issues early, so they can be resolved before impacting releases.
- **Integrating with quality gates:** Scan results can be integrated into quality gates to ensure that no critical issues make it into production. Scans can be configured according to the project's risk profile and tuned to minimize false positives.

Track results and progress

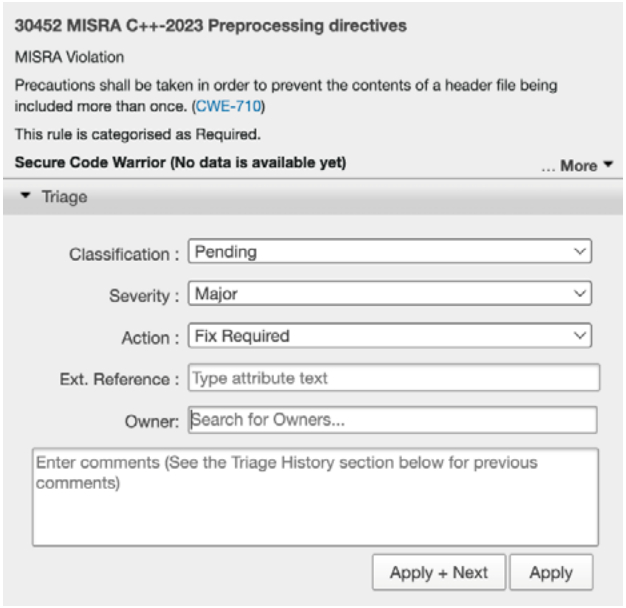
Coverity provides detailed reports that map vulnerabilities and defects to specific coding standards, and it can display and filter issues based on your preferred criteria. This makes it easy to identify critical issues and begin the process of prioritization. Coverity also provides configurable options to view vulnerabilities and defects related to specific standards.

- **Dashboards:** Stakeholders can view key insights into software health, developer productivity, and trend analysis to gauge progress toward achieving compliance.
- **Issue filters:** Users can apply filters to specify the scope of issues and related data to display. Issues can be filtered and sorted based on a wide range of criteria, including standards, CWEs, impact, severity, and more.
- **Custom views:** Search criteria can be saved to create a custom view that focuses on issues that meet specific criteria or are related to any unique coding standards your organization follows. Reports can then be generated that are tailored to your organization's needs.

Prioritize critical issues

Effective triage and prioritization are crucial for managing compliance and ensuring that critical issues are addressed first. Coverity provides several features to help teams quickly prioritize issues for remediation.

- **Issue severity levels:** Severity levels are assigned based on an issue's potential impact, so the most important issues are identified and resolved immediately.
- **Autoassignment:** Issues can be assigned to specific developers based on their expertise or availability, or they can be automatically assigned to the person most likely to have created the issue.
- **Trend reports:** Issue trend reports are updated with each code scan, giving development and security managers insight into risks, progress toward achieving compliance, and productivity across teams.



RESOLVING ISSUES QUICKLY

Once issues have been prioritized, it's important for developers to resolve them quickly to accelerate time to compliance, without impacting release timelines or introducing new issues.

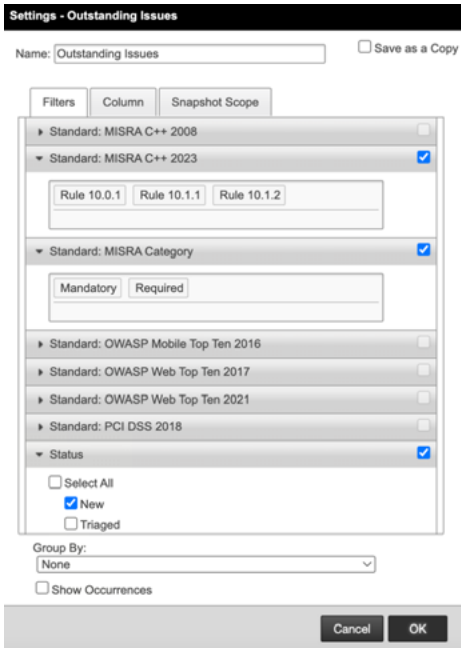
Code Sight™ IDE Plug-in enables developers to view all project issues directly within their development environment, and they can sort them by priority or filter based on various criteria (e.g., owner, severity, CWE, etc.). The plug-in leverages Coverity's analysis engine to scan code as developers write it, ensuring that issues are resolved properly and without introducing additional defects. Detailed descriptions and actionable remediation advice are included with each issue, so it can be resolved quickly without requiring the developer to switch tools.

DEMONSTRATING COMPLIANCE WITH BUILT-IN REPORTS

Coverity's built-in reports provide proof that your code adheres to specific coding standards or regulatory requirements. These reports are based on user-defined criteria to show a project's current level of compliance for any supported standard. Reports can be customized to highlight key details or include specific issues, such as those that are classified as high-severity, are mandatory or required for a specific standard, or have yet to be triaged.

Once a report has been generated, it can easily be shared with key stakeholders, such as auditors, compliance officers, and management, to demonstrate your level of compliance.

Ensuring that your software code adheres to the necessary standards is essential for maintaining security, reliability, and visibility into your software. Coverity provides the comprehensive code scans and issue management capabilities needed to align your policies with coding standards, implement policy-driven analysis, prioritize issues effectively, and prove compliance to stakeholders. By integrating testing into your development workflows, you can ensure that your software code meets the highest standards of compliance, helping you achieve your business goals and adhere to regulatory requirements.



ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.