What are the MISRA C++:2023 guidelines?

The **MISRA C++:2023** guidelines define a safe subset of the C++17 language. This subset removes or minimizes opportunities for common errors, making the language suitable for use in **safety-critical, mission-critical, and high-reliability contexts**.

C++17 is a versatile and efficient language, frequently chosen for critical systems in both embedded and hosted applications. However, no programming language is foolproof. Functional safety standards, such as **ISO 26262** (Automotive) and IEC 62304 (Medical Devices), mandate restricting the language to a safe subset. MISRA provides this necessary, specific subset, which, when integrated into a robust development process, mitigates the language's inherent shortcomings.

History and background

The MISRA journey began in 1998 with **MISRA C**, primarily for safety-related systems in the automotive industry. This expanded globally to become the dominant standard for C in critical systems.

As C++ usage grew in critical applications, MISRA published **MISRA C++:2008**, targeting the C++03 version of the language. The guidelines have since expanded their influence beyond automotive into medical technology, transportation, and finance, in other words, anywhere code integrity is mission or safety-critical.

The latest standard, **MISRA C++:2023**, builds on this foundation by:

- Aligning with modern **C++17**.
- Integrating the best practices from the **AUTOSAR C++** guidelines.
- Improving the **decidability** of guidelines to better facilitate automated checking by static analysis tools.

How compliance is measured by MISRA

Every MISRA guideline is defined as either a directive or a rule.

- **Directives:** These require additional information, often found in design documents or requirements specifications, for a full compliance check. Tools can assist, but some interpretation is required.
- **Rules:** These are completely described, allowing static analysis tools to check compliance without external information.

Guidelines are further organized by MISRA compliance categories:

- **Mandatory:** Compliance is required, and no deviation is permitted.
- **Required:** Code must comply, or a justification for formal deviation plus a risk assessment/ mitigation plan must be produced.
- **Advisory:** These help improve code quality attributes, and any differences must be documented with a justification.

Guidelines are additionally classified by their decidability:

- **Decidable:** The rule can be definitively checked by a static analyzer.
- **Undecidable:** A tool may not be able to find all possible violations, as detection depends on factors like control flow or object values.

Achieve certifiable compliance with SonarQube

Compliance with standards like MISRA is an **unavoidable mandate** for functional safety. It cannot be added at the end of a project as an afterthought without severe repercussions and immense cost. By leveraging SonarQube'a MISRA C++:2023 Compliance capability from the start (included with Enterprise and Data Center editions), teams can leverage its high-fidelity automated analysis required to make compliance a continuous, manageable activity throughout the Software Development Lifecycle (SDLC).

For developers and platform engineering: Start left with instant feedback

SonarQube champions a **"start left" compliance strategy**, bringing real-time code quality and safety checks directly into your IDE with SonarQube for IDE when connected with SonarQube Server Enterprise or Data Center edition. This instantly checks your code against the full MISRA C++:2023 standard, even as you develop.

- **Instant correction:** Get immediate feedback, complete with clear guidance, on why an issue is harmful and how to fix it. This acts as a real-time coding coach, ensuring compliance errors never leave your local environment.
- **High-precision analysis**: SonarQube addresses the primary point of developer friction by providing drastically reduced false positive rates. Our advanced analysis reduces noise, so you can focus on **genuine safety or quality concerns**.

- **Safe C++17 enablement:** You can confidently adopt modern C++17 features (like structured bindings) because our analysis ensures you are using them safely and in full compliance with the 179 guidelines.

For development leaders: Strategic risk reduction at enterprise scale

The challenge of MISRA compliance in large organizations is managing it across vast codebases and distributed teams. SonarQube turns this organizational challenge into a predictable, automated process.

- **Enforce compliance universally:** SonarQube provides a flexible, scalable tool that integrates seamlessly into your CI/CD pipeline. It enforces compliance automatically on every branch and pull request, ensuring **your code changes meet the MISRA C++:2023 standard** before it is merged.
- **Reduce toil and cost:** The "start left" approach eliminates the costly rework and friction associated with finding and fixing safety and quality issues late in the cycle.
- **Confidence in all code:** SonarQube ensures adherence to the standard for all code, whether **developer-written or AI-generated**, establishing a single, verifiable standard across the organization.

For compliance and quality managers: Auditable assurance

SonarQube acts as the non-negotiable verification layer required for achieving and proving compliance.

- **Complete coverage:** SonarQube Server Enterprise and Data Center editions provide 100% coverage of all 179 guidelines within the MISRA C++:2023 standard, providing the certifiable assurance essential for regulatory compliance.
- **Automatic evidence creation:** By integrating automated checks into the SDLC, evidence of compliance is automatically created and maintained.
- **Mandated by major standards:** Safety standards like ISO 26262, DO-178C, and IEC 62304 explicitly cite MISRA compliance as a means to reach those standards. SonarQube's MISRA C++:2023 Compliance capability helps teams work towards those standards.

SonarQube's MISRA C++:2023 Compliance capability is available now in SonarQube Server Enterprise and Data Center editions. Start a free 14 day trial of SonarQube Server Enterprise edition or contact sales about SonarQube Server Data Center edition.