Software Reviews

WP9 T2 provides a special service for GÉANT development teams to make their code more robust against all kinds of threats, to increase the quality of the code or to help them be compliant with the GÉANT Software IPR policy. Besides, the PLM process requires to pass a quality gate before the software can be put into production. A code assessment conducted by WP9 T2 or an IPR check are examples of such a quality gate. The prerequisite for an assessment is that the application or service is listed in the GÉANT Software Catalogue.

Introduction

We offer several types of review services for code assessment. They vary concerning the method of review, scope and granularity of the report.

Each type of the above-mentioned services is a combination of various review procedures. Differences between the procedures are briefly discussed below:

- **Automated code analysis** concerns maintainability and reliability as the core quality characteristics. SonarQube (SQ) scans the source code of the subject system, identifying flaws and vulnerabilities in the source code, based on internally computed software metrics, and by comparing the subject source code with known anti-patterns. Additionally, SQ defines so-called Quality Gates that verify if the subject code meets requirements to be transitioned to another step in the Product Lifecycle Management (PLM) and can provide recommendations for the decision-makers.
- **Manual expert review** also concerns maintainability and reliability and has similar objectives to the automated code analysis, but it is conducted by domain experts, using pre-defined checklists and/or in an exploratory manner. Experts review and re-validate the results reported by the automated code analysis, and independently review the parts of code that require particular attention, e.g., classes that are complex and play important roles in the system, or may expose known vulnerabilities. The expert code review requires significantly more effort than automated analysis, so it is performed according to the priorities defined by the requestor.

Additionally, we offer a WhiteSource software scan supporting software's IPR check.

Types of service we offer

SonarQube setup assistance

This is not a code review, but a special service offered to development teams. We assist you to set up your project in SonarQube so that your team can use the tool for continuous evaluation and improvement by itself. SonarQube should be used by all GÉANT software development teams to improve and assure software quality.

- We help you add your project to the SonarQube instance that we maintain
- We provide you with some introductory information on how to perform the review and interpret the results
- SonarQube continuously analyzes your code and provides the results of the analysis

This option requires the least effort for the requestor and provides instant, continuous access to the assessment results. It involves no proxy to execute the assessment.

Recommended for: Teams that expect regular, frequent feedback on the code quality.

SonarQube-based expert review

This review type is a combination of a tools-based SonarQube review and a manual expert analysis. It involves Subject-Matter Experts to cross-validate the results collected by the tool. This review type is most frequently asked for and therefore supposed to be the standard review type.

- We help you add your project to SonarQube
- Subject-Matter Experts review the SonarQube output and perform manual cross-validation of the results
- We provide detailed reporting on the results of the review
- We attest code quality as required by the PLM process

Recommended for: Teams that expect occasional and highly reliable reports concerning the code quality. Due to the considerable effort needed to perform the manual validation by experts, it is not recommended for frequent quality assessments.

Extended source code review

The extended review can be requested either as a one-off service or in addition to the *SonarQube-based expert review*. It focuses on a comprehensive, **ma nual assessment** of the code by selected Subject Matter Experts that best match with their expert skills your specific assessment requirements. Since the extended review often addresses special requirements, it does not necessarily aim for a code quality attestation as required by the PLM process.

- In case of critical services, software or parts of the software, an extended review can be requested.
- Our focus is on quality and/or security assessments and we partner with WP8 for other special review types like vulnerability assessments.
- We use additional assessment tools beyond those used in SonarQube. The analysis tools will be run and critical or major issues in their output are verified manually in the source code. Sometimes specific test cases/scenarios are executed with those tools.
- The used tool may support a peer review. In a peer review, several humans check the software mainly by viewing and reading parts of its source code, and this may happen at the end or during the development. A similar peer-review approach is used in the assessment of software aspects that are not directly bound to code quality.
- Check with us about potential reviews of documentation, architecture, UI, performance, alignment with functional requirements.

This is the most laborious, but also the highly customizable type of review, as it relies on a manual review that requires the involvement of (possibly) several subject-matter experts. It is not frequently expected in the usual practice of development teams and must be negotiated on a per-request basis.

Recommended for: Teams that expect a thorough, multi-directional insight into the project quality.

WhiteSource setup assistance

This is a technical supporting service for the PLM or IPR software compliance check. We assist you to set up your project in the WhiteSource tool, to get your team an insight into the 3rd party libraries imported into the software project. The tool delivers two-fold information about the 3rd party software: licence compliance and security information about the vulnerabilities and defects identified in the 3rd party components used in a project.

- We help you to add your project to the WhiteSource instance that is provided for GÉANT as SaaS by the commercial vendor
- We generate a set of reports identifying any non-conformance with defined IPR and security policies. These reports are delivered either directly to you or the appropriate Subject Matter Experts for further results analysis, depending on the origin of the request.
- We provide you with some introductory information on how to interpret the results (unless the request is accompanied by a request for a *WhiteSource licence scan*)
- This service can be required in combination with other software review services or as a stand-alone service
- WhiteSource can be incorporated into continuous integration platforms (such as Bamboo)

This option requires minimal effort from your side during the setup phase and provides instant, continuous access to the assessment results. However, once the WhiteSource scanning of libraries and licences and scanning is established, the teams should perform scans whenever a major refactoring of the software is made, or if there have been changes in software dependencies or input or output IPR and licences. Also, the teams should be able to interpret WhiteSource results and reports by themselves.

Recommended for: Teams that expect regular, frequent feedback for risks associated with the infringement of IPR and associated security vulnerabilities that may be inherent in third-party libraries; *WhiteSource setup assistance* is also performed as preparatory work for *WhiteSource scan analysis.*

WhiteSource scan analysis

This is a technical consulting service for the PLM or IPR software compliance check. We adjust the WhiteSource licence settings to be aligned with your intended or actual licensing policy, perform the scan of your software project and help you in interpreting the obtained results. Our experience shows that more than one scan is usually necessary until all possible parameters are adjusted the way that the result meets your needs.

We assist your team in getting insight into the 3rd party libraries imported into the software project and their licences, as well as the initial information about the vulnerabilities and defects associated with them. These are inputs for the refinement of the IPR policy and licence selection for the software as well as tweaking of the usage of libraries. Obtaining satisfactory results may require several iterations and WhiteSource scans.

The consultative nature of this service requires strong cooperation between our WhiteSource experts and your team. A clearly expressed expectation about the focus of the scan and resulting analysis is useful, as well as information about a trigger for the scan, such as a change in the IPR policy, in the software or in its dependencies. Any major refactoring of the software or change in software dependencies or input or output IPR and licences is likely to require a new request for a *WhiteSource scan analysis.*

Recommended for: Teams that want to verify their own licensing policy, licences of dependencies or effects of changes in the software.

Overview of request options

	Tool setup	Summary report	Detailed report	Quality gate confirmation for PLM
SonarQube setup assistance	SonarQube			
SonarQube-based expert review	SonarQube	x	x	y/n
Extended review	Custom	x	x	y/n
WhiteSource setup assistance	WhiteSource			x
WhiteSource scan analysis	WhiteSource	x	x	y/n

Contact us

Contact Task 2 team to request any of the before-mentioned services.