SYNOPSYS®

Black Duck Code Quality Audit

Get a qualitative and quantitative assessment of your code across 5 key categories, and identify code problems that can lead to quality issues

Overview

Assessing code quality requires answers to several key questions: Are there bugs? How well does it work? Is it well-written? Are the comments and documentation sufficient for maintenance? How is the formatting? The answers to these questions determine the quality of both the code and the processes behind building it.

The Black Duck Code Quality Audit (CQA) focuses on identifying problems in the code and code construction techniques that can lead to quality issues. These issues generally drive concerns regarding the cost of remediating defects in the code and additional costs necessary to maintain the codebase.

Key features

Code audit requests are typically urgent. The Black Duck audit services group offers speed of service, deep software development expertise, and industry-leading tools when assessing the quality of a codebase and the processes behind it. The result is a comprehensive, relevant, and actionable report. We use industry standard categorization for analyzing the quality of the processes used to create the code and to prepare an overall qualitative assessment of the codebase. The service also determines quantitative aspects by assessing the code on the following metrics:

- Is it built using industry best practices?
- Is it structured in a reasonable and formal way to enable efficient ongoing development?
- Does it avoid complexity (due to poor code construction techniques) that leads to inefficient maintenance?
- Is it well-documented?

The Black Duck audit team uses a combination of tools to make this assessment, including source code analysis, interviews, comparative benchmarks, and inspection techniques, as shown in the diagram below

How it works

The CQA project consists of parallel tasks, including interviews and qualitative analysis, software development process (SDP) and documentation assessment, static code analysis, and reporting.

Preparation. First we send a detailed survey to the code owner. Then we have a kickoff meeting to understand the goals of the CQA process, the requirements of the code owner, and the contents of the deliverables requested in the survey.

Software development life cycle (SDLC) process analysis. We complete an analysis of the internal technical documentation and processes that compose the SDLC. Experienced code architects conduct interviews (typically over the phone) to clarify survey results, dig into areas of concern, and answer any questions. The goal is to provide insight into the quality and maturity of the processes used to construct the code.

Static code analysis. Using analysis tools, we process and analyze source code for apparent code quality and key issues of complexity and design.

Report generation. Architects review and analyze quantitative results and compare the vetted metrics to industry norms. Similarly, they put process analysis in the context of the industry.

Final report

The analysis identifies key quality criteria, including reliability, efficiency, and maintainability. The contents of the final CQA report provide an integrated picture:

- Qualitative analysis
  - Software development process analysis
  - Other product development and quality processes (including build and release)
  - Technical documentation and comments
  - Engineering organizational structure
- Quantitative analysis
  - Metrics from static code analysis

Integrated end-to-end solution

When you combine the CQA with an Open Source and Third-Party Audit, you benefit from a comprehensive integrated solution for your technical auditing needs. Whether you need an internal audit or support for M&A due diligence, we can give you a complete picture of the integrity of your code assets.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

12/06/18.ds-bd-odcodeaudit.