Black Duck Audits

On-demand expertise to help you quickly identify license compliance, security, and quality risks in software

Overview
For over 15 years, the Black Duck® team has advised clients on risks in software. Black Duck Audits continue to be the industry’s most trusted open source due diligence solution for M&A and internal compliance, and it has set the standard for a comprehensive range of software due diligence services.

Black Duck Audits help your teams
• Mitigate potential legal exposure by uncovering unknown open source software and third-party code
• Detect open source license conflicts, security vulnerabilities, and other risks that may affect software asset values
• Identify, understand, and test software security vulnerabilities and expose potential security gaps in proprietary software
• Get an overall sense of the quality of the software and how well software development is managed

Black Duck Audits give you a complete picture of open source license obligations and application security and code quality risks, so you can make informed decisions with confidence.

Open Source and Third-Party Software Audits

Open Source and Third-Party Code Audit
These audits provide you with a complete open source Bill of Materials (BOM) for the target codebase, showing all open source components and associated license obligations and conflict analysis.

Open Source Risk Assessment
An open source risk assessment uses Black Duck enhanced vulnerability data to offer a detailed view of open source risks in the codebase, including known security vulnerabilities. This can serve as a high-level action plan to prioritize research and potential remediation actions. Additionally, this assessment can identify any encryption functions so you can disclose the proper information and ensure compliance with export regulations.

Web Services and API Risk Audit
A web services and API risk audit provides a list of the external web services used by an application, as well as insight into potential legal and data privacy risks. This allows you to quickly evaluate web services risks across three key categories: governance, data privacy, and quality.

“When we make an acquisition, we use a variety of Black Duck Audit services, which has allowed us to consolidate the third-party requirements into one vendor and one solution. That has made it a lot easier to understand the risks before we bring new technology into our portfolio.”

—PointClickCare
Application Security Audits

Penetration Test Audit
A penetration test audit assesses the security robustness of a software asset through an examination of the application in its full running state. It includes exploratory risk analysis to bypass security controls, and abuse business logic and user authorization to demonstrate how hackers might gain access and cause damage.

Static Application Security Test Audit
A static application security test audit combines automated tool-based scans with a source code review to systematically find critical software security vulnerabilities such as SQL injection, cross-site scripting, buffer overflows, and the rest of the OWASP Top 10.

Secure Design Review Audit
A secure design review audit evaluates the design of key security controls, including password storage, identity and access management, and use of cryptography against industry best practices to determine whether any are misconfigured, weak, misused, or missing. It also finds system defects related to security controls in the design of the application, but it does not include testing or analysis of the application or code.

Software Quality Audits

Code Quality Audit
A code quality audit combines static analysis tools and manual code review to analyze code quality. It includes comparisons to industry benchmarks to assess quality, reusability, extensibility, and maintainability in proprietary code.

Software Development Audit
A software development audit analyzes software development life cycle processes and practices. It includes interviews with key personnel to gain insight into the quality and maturity of these processes and it provides recommendations to improve code quality while reducing costs.

Design Quality Audit
A design quality audit combines the skills of experienced architects and powerful architectural analysis tools to assess overall architecture in terms of modularity and hierarchy, thus rounding out a complete picture of the health of the software. This audit includes an analysis of how the architecture affects maintainability and identifies potential risk areas that are candidates for code refactoring.

Trust the Experts
In the high-risk world of tech M&A, a target's software assets are a significant part of valuation. Speed and accuracy are critical to performing comprehensive software due diligence, so relying on expert advisors with experience and sophisticated tools is the right approach.

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.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software. Synopsys, Inc. 690 E Middlefield Road Mountain View, CA 94043 USA U.S. Sales: 800.873.8193 International Sales: +1 415.321.5237 Email: sig-info@synopsys.com

©2022 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners. March 2022