BLACKDUCK®

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 mergers and acquisitions (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.

Assess Process Risks

Software development audits offer a complete analysis of the processes and practices that comprise the software development life cycle. Experts conduct in-depth interviews with key personnel to gain insight into the quality and maturity of the organization and its development practices, including coding standards, processes, and tools. From this, they provide an assessment of the current state as well as recommendations for improving the process while reducing development and maintenance costs.

Assess Code Risks

Open Source and Third Party

Open source and third-party software audits draw upon world-class tools that use a range of software composition analysis techniques, the Black Duck KnowledgeBase™ and expert open source auditors to provide a complete and accurate Software Bill of Materials. The codebase is analyzed for open source and third-party components, associated license obligations, and license conflicts.

> *"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

Additionally, open source risk analyses utilize a range of sources including proprietary Black Duck Security Advisories to identify known security vulnerabilities and operational risks, and provide guidance on remediation. The audit reports also identify encryption functions in use in applications so you can ensure compliance with internal, external, and governmental encryption requirements.

A **web services and API risk audit** generates a list of the external web services used by an application, providing insight into potential legal and data privacy risks.

Security

Static application security testing audits combine automated, tool-based scans with expert 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. They provide an inside-out view of the security of the code.

Penetration test audits are essentially ethical hacking to assess the security robustness of a software asset. They provide an examination of the applications from the outside-in, in their full running state. These tests include exploratory risk analysis in which auditors try to bypass security controls (such as WAFs and input validation) and attempt to abuse business logic and user authorization to demonstrate how hackers could gain access and cause damage.

Secure design review audits find system defects related to security controls in the design of an application. These audits include interviews with the engineers responsible for application security to evaluate the design of key security controls. Password storage, identity and access management, and use of cryptography, among others, are compared against industry best practices to determine whether any are misconfigured, weak, misused, or missing. No testing or analysis of the application or code is performed.

Quality

Design quality audits combine insights from experienced software architects with powerful architectural analysis tools to assess the overall architecture in terms of modularity and hierarchy, and provide a complete, top-down picture of the health of the software. The audit report includes an analysis of how the architecture impacts software maintainability and identifies potential risk areas that are candidates for code refactoring.

Code quality audits combine static analysis tools with manual code review to give insights into how well code is written. They include comparisons to industry benchmarks of quality, reusability, extensibility, and maintainability of proprietary code.

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.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.