Open Source Software Audit Services

Keep your M&A transactions smooth, confidential, and actionable.

Confidentiality is a key concern during an open source audit for M&A transactions or technical due diligence. Because of this sensitivity, Snyk created Blind Audit, our unique methodology for performing audits and generating reports without exposing any proprietary source code.

Built on the market’s most comprehensive compliance and security knowledge base, Snyk’s audit services identify open source software and vulnerabilities in as few as 6 lines of code, quickly surfacing compliance issues in third-party code, open source dependencies, and transitive dependencies.

THE SNYK DIFFERENCE

Blind Audit

The highest level of security and confidentiality

- Audits of cryptographic hashes — source code is never accessed or transferred.
- Ridiculously easy to set up and administer, with fewer headaches for Legal.
- Performed entirely remotely.

Knowledge Base

Best-in-class knowledge base for compliance and security

- Scan whole components, files, and snippets to identify licenses, license obligations, and vulnerable lines of code.
- Accurate matches with optimal transparency — not just matches against a curated set of licenses or vulnerabilities.

Snippet Matching

Industry-leading precision in as few as 6 lines of code

- Snippet-level scanning removes the imprecise lists and false positives of component-level.
- AI-powered scan engine eliminates false positives and error-prone human interpretation of the results.
COMPREHENSIVE AUDITING MADE SIMPLE

01  Kickoff
Execute MNDA and Audit Agreement, define scope and deliverables, commit to timeline and scheduling, and discuss expectations.

02  Fingerprint Generation
Target company generates fingerprints/digital signatures (cryptographic hashes) of the source code. Source code is never exposed to Snyk or anyone else, and the fingerprints are impossible to reverse-engineer.

03  Audit
Snyk audits the target source code by comparing the fingerprints to the Snyk knowledge base to find and identify open source software licenses and vulnerabilities.

04  Results & Reports
The final meeting where Snyk presents the results of the audit and answer any questions that have arisen.

ACTIONABLE REPORTING

Executive Summary
High-level understanding of the open source licensing and security vulnerability status of the audited software.

SBoM
All detected security vulnerabilities and exposures (CVEs) and corresponding Common Platform Enumerations (CPEs) according to the National Vulnerability Database (NVD) and other sources.

SPDX® Report
An industry standard for communicating the components, licenses, and copyrights associated with software packages (XML file that can be imported into other tools).

Vulnerability Report
All detected third-party open source components, files, and code snippets. Interactive capabilities facilitate the filtering and reviewing of the audit findings, and the creation of follow-up actions.

Contact us to learn more
snyk.io/open-source-audit