WHITE PAPER

revenera

Managing Intellectual Property Risk During M&A

The Process

Executive Summary

While Merger and Acquisition (M&A) events create opportunities for both buyers and sellers, they also present challenges, particularly around Intellectual Property (IP) integrity. Open source software due diligence to protect a company's IP should now be a standard process in all M&A efforts.

Open Source Software's Impact on M&A

In today's software development environment, companies with access to third-party code and those leveraging the IP of commercial partners, outsourced engineering resources, and the open source community have substantial advantages—reduced costs, accelerated time-to-market, global software innovation, and differentiation of software products. The caveat, however, is these assets must be managed responsibly. This includes the requirement to comply with a complex set of licensing terms placed on any software by IP owners. Governance mechanisms must be in place to ensure compliance with license terms to mitigate financial and legal risks.

Data points to the fact that companies today have difficulty managing the third-party IP within their own codebases. Revenera data shows that only 37% of corporations have policies in place for open source management. This represents potential likelihood for issues to be present in code.

Given the difficulty to manage their own open source practices, doing so in M&A transactions presents even more challenges, especially given any technology acquisition will involve software in some form. Inbound code built by unfamiliar development teams is often a black box of third-party code and licenses. It falls to the M&A team managing the transaction to place a priority on software due diligence and to interject the right level of expertise to thoroughly perform a software code audit. Precise open source code audits are essential to ultimate M&A success.

Given that software development teams are increasingly utilizing open source in applications and products shipped to customers, there is no better way to gain quick, accurate insight into IP value than by software due diligence audits conducted by experienced IP software technology teams.

Only **37%**

of companies have policies in place for open source management.

	Assessment	Execution	Integration
Primary Driver	**GAP ANALYSIS:** Inorganic Planning → **EVALUATION:** Business Case → **DUE DILIGENCE:** Term Sheet → **DEFINITIVE AGREEMENT:** Close → **INTEGRATION PLAN** → **REMEDIATION PLAN:** Verification		
	Early validation of M & A objective, assessment of candidate's IP and any potential risks	Analysis of target IP pedigree and highlight of issues against due diligence criteria	Risk advisory for integration plan
Deliverable	**AUDIT PROFILE:** Key indications on degree of innovation and potential IP risks	**DUE DILIGENCE REPORT:** Inventory of all third-party software and licenses and assessment against acquirer's IP policy	**REMEDIATION ASSESSMENT:** Alternative third-party software libraries and licenses and verification of remediation efforts

Revenera Six-Step Audit Methodology

Audit Services Overview

M&A opportunities are an effective corporate strategy to acquire valuable IP assets for market consolidation. A premium is placed on accelerating deal-flow and undertaking precise but fast due diligence. M&A focused organizations must ascertain the true value of the Target (seller's) software IP quickly while also establishing the criteria for certifying the origins and ownership of IP. With up to 80 percent of a software company's valuation coming from its IP, companies that can discern the real worth of software IP will be more successful in fulfilling their M&A objectives.

To uncover this value, Revenera has developed a six-step best practices audit methodology for each phase of the M&A due diligence process. This methodology is invaluable to some of the world's largest corporations during M&A transactions, legal mediations, and compliance audits.

1 Asssemble Team ▶ **2** Identify Target App And Regs ▶ **3** Conduct Audit ▶ **4** Analyze Results ▶ **5** Report ▶ **6** Remediate

Step #1: Assemble the Team

Every open source software code audit requires buy-in, cooperation, and support from a cross-functional team. There are four primary roles that make up the team: an audit consultant, the acquiring company's counsel, a corporate development liaison, and a technical liaison from the Target company.

Audit Consultant

For software code audits, a professional software audit consultant serves as the central figure of every due diligence activity. The role supports the needs of the cross-functional team by listening to the audit requirements, conducting a scan of the code using a Software Composition Analysis scanning tool, analyzing the results of the scan, consulting with the development team to resolve questions surrounding suspect pieces of code, reporting the audit results during check-in meetings, and delivering a final code audit report. Most companies do not have an audit consultant on staff so this role is filled by a third-party audit services company.

Buyer's Legal Counsel

This role is filled by the acquiring company's legal counsel who is charged with assessing ongoing IP issues for corporate transactions as well as managing license compliance risks. As part of the team, legal counsel will help define the requirements for the audit, set IP policy, and advise on the remediation of issues uncovered during the software code audit.

Corporate Development Liaison

The corporate development liaison is responsible for the M&A event in its entirety. Regarding the open source software audit specifically, this person facilitates access to the candidate company during the audit process, advises on IP policy, and assists in business aspects related to audit priorities and overall deal evaluation.

Technical Liaison

Typically coming from the Target company, the technical liaison provides access to the seller's software development team in cooperation with the code audit process. Comprehensive IP analysis involves reviewing open source code scanning results, confirming any third-party code, and providing issue severity and remediation analysis. The expertise of the broader software development team is a key contributor to fulfilling the analysis and remediations steps.

Step #2: Identify Target's Applications and Audit Requirements

Before a software code audit begins, the IP audit team needs to identify the applications and products needed for the audit and provide answers to some basic questions:

- What are the names of the applications and products targeted for a code audit?
- What does the product do?
- How old are the products?
- Have other names ever been used for both the company and the products in question?
- What software languages is the code written it?
- Are there portions of the code that are Server or Client-based only?
- Are the portions of the code that are shared between client and server modules?
- How big is the source tree in megabytes?
  - How many files?
  - How many lines of code?
- What is the IP policy of the audit? For example, what products/licenses do we consider Severity I, II and III issues? What licenses are considered acceptable?
- What type of final deliverable is required at the end of the audit?

In addition to providing answers to the above pre-audit questions, the team needs to create a remediation plan for issues that may be uncovered during the audit. Beginning an audit without a remediation plan is ill-advised. Once the audit is complete, the idea is to continue to move the M&A activity along with expediency. A thoughtful and well-communicated remediation plan mitigates the risk of a stalled process following the conclusion of the audit.

Step #3: Conduct the Code Audit

Software audits are done to better understand the overall reliance on open source and third-party software. And, more importantly, to uncover compliance and security issues that could impact the M&A transaction.

With the basic questions answered, the audit consultant can begin the software code audit. In addition to professional expertise, audits typically utilize a valid Software Composition Analysis scanning tool to quickly and efficiently identify compliance, IP and security risks.

Timeframes for audit completion vary depending on the size of the codebase and required deliverables. Typical audits are accomplished within a two-week period but can range longer based on software code size and complexity.

Step #4: Analyze Results

The audit consultant will focus the majority of his/her time during this stage of the process. Analysis includes reviewing the results of the scan, confirming third-party usage, consulting with the technical liaison, offering advice on any technology risks, and suggesting open source and commercial software alternatives.

Step #5: Report

Once analysis is completed, the audit professional generates a standard or custom report as required by the IP team when they established the ground rules for how to proceed and what was expected.

Step #6: Remediate

After the audit and review of the reports, the IP team should immediately refer to the remediation plan and implement steps to resolve any issues discovered during the audit step. It may be necessary—depending on specific remediation requirements—to bring in systems integrators and outsourced software engineering firms to provide custom software development solutions.

Types of Standard Audit Reports

RISK PROFILE

Provides quantification of how much code is unique to the Target company, an inventory of the open source and commercial code, as well as licenses inside the codebase, and highlight of potential IP risk indicators.

FORENSIC

Details the IP pedigree and inventory of the detected third-party commercial and open source code and licenses, specifies supporting evidence of code similarities, and compares the third-party inventory against existing IP policy. These results provide teams with actionable remediation steps for a Target company to address before deal close, in addition to quantifiable information that may impact term sheets.

REMEDIATION ASSESSMENT

Provides risk advisory for key redevelopment areas such as open source and commercial alternatives for any third-party products that come into question as a result of the audit. Additionally, this report presents the team with a final Bill of Materials (BOM) of all third-party code and licenses found in the code and offers a baseline for managing ongoing IP integrity.

M&A Due Diligence Case Studies

The emphasis during a due diligence activity is on findings that could impact a go/no-go decision, in addition to IP valuation. Every M&A transaction may differ or offer up variances, but the need for an effective process to understand the depth of use and reliance on open source software is a constant. Here are two real-life examples of M&A events.

Entertainment Company (Acquirer)

A multi-billion dollar entertainment company completed the acquisition of a European-based consumer software company with the objective to commercially license and sell the company's product. The acquiring company believed the acquisition gave them a new OEM revenue stream from PDA manufacturers that wanted to give consumers a way to download music to their devices.

PROCESS OVERVIEW

The Target company provided an inventory of software components upfront. However, the Acquirer wanted an independent party to review the codebase quickly and discreetly. During the due diligence phase of the acquisition, the acquiring company engaged with Revenera and the company's Open Source Software Audit Services team to perform a software audit.

The Acquirer provided Revenera with their IP policy, and the Target company provided their codebase in addition to the answers to questions about the specific product's distribution model. Revenera performed an IP audit, matching it against a large database of popular open source projects as well as the Acquirer's IP policy. The audit uncovered several red flags and high priority issues, including components licensed under the General Public License (GPL), an open source license that was incompatible with the Acquirer's business model.

RESULTS

The acquiring company discovered that, despite the Target's best intentions to manage third-party software components, several open source projects were not included in the "third-party" code folder in the source code system and they were also missing from the original inventory list provide by the Target. The audit enabled the Acquirer to avert potential distribution issues by requiring the Target to replace all GPL code before acquisition close.

Technology Company (Acquirer)

A multi-billion dollar tech company was acquiring a VoIP software company because they felt the technology acquired would strengthen their position in the telecommunications market. The intention was to integrate the Target company's software into their existing product line.

PROCESS OVERVIEW

Post-acquisition, the technical team at the acquiring company noticed that a portion of the Target's product software appeared to contain open source software associated with GPL. The Acquirer engaged with the Revenera Audit Services team to perform an audit on the product to determine the extent of the reliance on open source software. By scanning the codebase, the audit team discovered that a key area of the code was licensed under GPL, representing almost half of the application's overall code. As we presented at the beginning of this paper, the majority of companies do not have a complete picture of their open source software use. In this case, the open source audit showed that there was a significant disparity from the Target's initial disclosure compared to the reality of what was in the code.

RESULTS

Performing an audit prior to finalizing the acquisition would have uncovered the disclosure disparity. Moreover, an IP audit could have quantified the value of the business and subsequent risk factors for the Acquirer. Because of the substantial amount of GPL code eventually uncovered, the acquiring company would face restrictions and liability issues in commercializing the product.

Additionally, the audit services team pinpointed the risk factors associated with the proposed remediation plan, estimating it would take up to 12 development man-years to rearchitect the product for commercial use. Had these legal risks been known during the M&A due diligence effort, the acquiring company could have cancelled the deal or renegotiated the purchase price. With that said, the Acquirer most certainly saved themselves potential legal problems by initiating an audit that uncovered open source software license issues prior to shipping product to customers.

Conclusion

Open source due diligence is one of many focuses during M&A transactions. Given that open source software use is more widespread today than ever before—across all industries—license compliance, IP and security risks are a very real possibility. It's important for acquiring companies to perform effective due diligence early in the M&A process in order to uncover issues as soon as possible, allowing both parties to manage any potential scenario.

Open source audit services help identify open source code and third-party components while alerting acquiring companies to potential legal risks which could impact a go/no-go decision.

NEXT STEPS

Learn more about how Open Source Software Audit Services meets your M&A needs.

LEARN MORE >