SYNOPSYS®

Sell-Side Guide for Technical Due Diligence

Understanding the Quality of IP in M&A

Know what questions to ask internally ahead of potential due diligence to ensure a clean exit at a compelling price

Overview

Intellectual property risk can account for more than 50% of a technology company's risk profile. For M&A transactions in which software assets compose much of the client company's value, you will face pointed questions about open source risks from the buy-side.

Even though open source is an essential element in application development today, most organizations lack visibility into their open source use, opening them up to legal and security issues. As a result, tech-focused private equity firms and serial strategic buyers routinely conduct open source code audits as part of standard due diligence.

The Black Duck audit services group has performed thousands of M&A-related software audits to identify open source code and associated licensing or security risks. We inevitably find undeclared open source, problematic or unknown open source licenses, and known open source security vulnerabilities. The sell-side can mitigate these risks by conducting an audit before or early in the deal cycle to assess the IP quality.

Address buyers' questions

Private equity firms and strategic acquirers want successful acquisitions. As a result, they need to know the company's entire risk profile. A client's overall management ability may come into question if the client has not effectively managed its open source software development. On the other hand, demonstrating visibility into and control of open source use will enhance the image of the company's software development process. This helps preserve desired valuation and terms, increase deal certainty, and accelerate the transaction timeline for the sell-side.

Get your (or your client's) ducks in a row

We recommend an audit prior to a buyer's technical due diligence. Additionally, we have developed a sell-side checklist of questions to help you assess your or your client's level of risk. Being proactive provides an opportunity for remediation ahead of buyer due diligence; more importantly, strong audit results pointing to high IP quality will attract more compelling bids.

✓	Questions to ask	Warning signs
☐	**1. BILL OF MATERIALS** Can you provide an accurate, real-time inventory of the open source components in use?	Hesitation or the inability to produce an accurate, current list indicates a serious lack of visibility into the open source in use and signals an organizational failure to understand the risks associated with open source use. An open source audit can quickly produce this required piece of technical due diligence ready to be populated into the data room.
☐	**2. USAGE POLICY** What are your policies for using open source and your processes for selecting, approving, and tracking it?	An absence of a written policy is a big red flag. It means the company is not giving guidance to its developers and is opening itself up to license and security risks. Without well-defined and used processes for selecting, approving and tracking open source, there is no way a company can have visibility into what is actually in its code. An open source audit can identify all components and can serve as the basis for a new or updated policy, signaling smart management to buyers.
☐	**3. LICENSE COMPLIANCE** How do you ensure legal compliance with open source license obligations?	Knowing what open source components are in use is fundamental, but a company also needs a legal understanding of licenses and obligations, especially with regard to its business model.. Some licenses may be permissible for internal use, but the company may be in violation if the licenses are used in a SaaS model or through a mobile app. A lack of management understanding or the absence of a legal obligation "check off" process translates to a lack of compliance and possible IP infringement. An open source audit can prioritize the highest-risk components and document all licenses for legal parties to review obligations in a single place.
☐	**4. SECURITY VULNERABILITIES** How do you identify and remediate known open source security vulnerabilities?	Unlike with commercial software, there is typically no company pushing open source security updates to your client's codebase. And with new vulnerabilities being discovered every day, it is practically impossible for developers to stay on top of the security of the components in their code. Without automation and accompanying processes for updating components with security fixes, an organization faces substantial security risk, especially when sensitive user, customer, or financial data is involved. An open source audit can identify and prioritize potentially debilitating security vulnerabilities to allow for targeted remediation before buyer due diligence, ensuring a high quality of IP.
☐	**5. OS MANAGEMENT** How do you train your developers on the importance of managing open source and your company's specific policies and processes?	When open source management is not top of mind, developers are likely to circumvent even well-defined policies and processes. With open source, it's easy to do. In the end, code scanning is the only way to be sure what is in the code, but well-trained developers are more likely to comply with company standards. An open source audit can be the first step in developing OS management processes that aren't invasive and allow for developers to use components of low risk.

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™

01/25/19.ds-bd-odmasales.