

## **OPEN SOURCE SOFTWARE DUE DILIGENCE IN AN M&A TRANSACTION**

### **A Buyer's Checklist & Guidelines**

Black Duck has performed thousands of M&A-related software audits to identify open source code and associated licensing or security risks.

Even though open source is an essential element in application development today, a majority of organizations lack visibility into the open source they're using and are too often blind to the license and security issues in their code. Black Duck's audits inevitably find undeclared open source, problematic or unknown open source licenses, and known open source security vulnerabilities.

During M&A due diligence it is essential for acquirers to identify problematic open source in the targets' code before the transaction terms and integration timelines are set. An open source code audit is the only way to know what is in the code and understand the risks. Savvy acquirers perform open source code audits whenever software assets are a significant part of the deal valuation.

Weak open source management practices indicate a higher likelihood of issues in the code. Black Duck has developed a checklist of questions to ask in assessing how well a target is managing open source, which likely makes up a significant portion of their code base.

✓	QUESTIONS TO ASK	WARNING SIGNS
<input type="checkbox"/>	<b>Can you provide an accurate, real-time inventory of the open source components in use?</b>	<p>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.</p> <p>A recent Black Duck analysis of M&amp;A code audits conducted on 200 commercial applications found that even companies that were able to produce a list, on average, only identified half of the open source components actually in use. A best practice is to have automated capabilities to identify and inventory the open source in use, detect known vulnerabilities and track remediation efforts.</p>
<input type="checkbox"/>	<b>What are the company policies for open source use and processes for selecting, approving, and tracking it?</b>	<p>An absence of a written policies is a big red flag. It means the company is not giving guidance to its developers and is opening itself up to open source risks.</p> <p>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.</p>
<input type="checkbox"/>	<b>How do you ensure compliance with open source license obligations, including those associated with code acquired from third parties?</b>	<p>Knowing what open source components are in use is fundamental, but companies also need a legal understanding of licenses and obligations. A lack of management understanding, or the absence of a legal obligation “check off” process translate to a lack of compliance.</p> <p>Companies are responsible for any third-party code they use and risk mounts if third-party providers are not held to open source policy standards.</p>
<input type="checkbox"/>	<b>What processes do you use to identify and remediate known open source security vulnerabilities and to monitor for new vulnerabilities?</b>	<p>From a security perspective, it’s vital for companies to have automated capabilities to continuously monitor for new vulnerabilities. Unlike with commercial software, there is typically no company pushing open source security updates. 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.</p>
<input type="checkbox"/>	<b>How do you train your developers on the importance of managing open source and your company’s specific policy and processes?</b>	<p>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.</p> <p>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.</p>

## ABOUT BLACK DUCK SOFTWARE

Organizations worldwide use Black Duck Software’s industry-leading products to automate the processes of securing and managing open source software, eliminating the pain related to security vulnerabilities, license compliance and operational risk. Black Duck is headquartered in Burlington, MA, and has offices in San Jose, CA, Vancouver, London, Belfast, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing. For more information, visit [www.blackducksoftware.com](http://www.blackducksoftware.com).

## CONTACT

To learn more, please contact: [sales@blackducksoftware.com](mailto:sales@blackducksoftware.com) or +1 781.891.5100  
Additional information is available at: [www.blackducksoftware.com](http://www.blackducksoftware.com)

