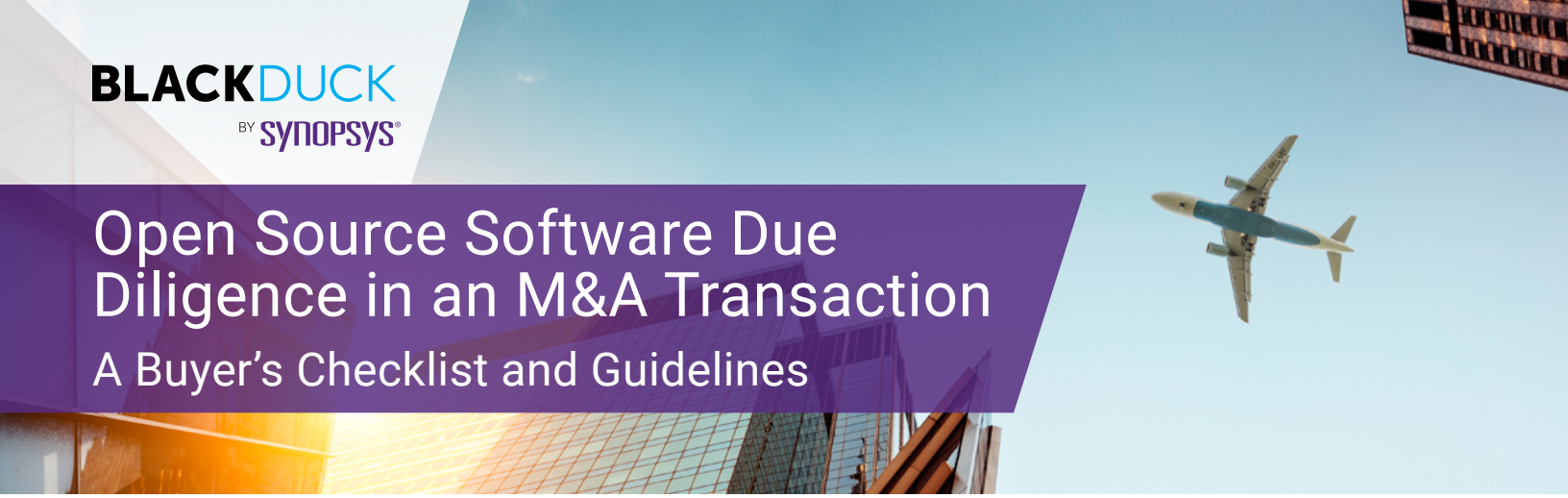
BLACKDUCK BY SYNOPSYS

Open Source Software Due Diligence in an M&A Transaction

A Buyer's Checklist and Guidelines



Ask the right questions to find out what's in the code you're acquiring and mitigate any potential open source risk

Overview

When you're evaluating a potential acquisition where software assets are a key part of the deal valuation, it's essential to assess what's in the code you're acquiring. Knowing what questions to ask during due diligence is key to mitigating any potential open source risk in M&A transactions. Black Duck by Synopsys 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.

95% of applications audited by On-Demand were found to contain open source

Due diligence and open source

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 codebase.

✓	Questions to ask	Warning signs
☐	**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. A recent Black Duck analysis of M&A code audits conducted on 200 commercial applications found that even companies that were able to produce a list identified only half (on average) 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.
☐	**What are the company policies for open source use and processes for selecting, approving, and tracking it?**	An absence of 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. Without using well-defined processes for selecting, approving, and tracking open source, there is no way a company can have visibility into what is actually in its code.
☐	**How do you ensure compliance with open source license obligations, including those associated with code acquired from third parties?**	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 a legal obligation "check off" process translates to a lack of compliance. 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.
☐	**What processes do you use to identify and remediate known open source security vulnerabilities and to monitor for new vulnerabilities?**	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.
☐	**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.

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™

©2018 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at http://www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners.
06/05/18.BDODMA-DS-UL.