



Software composition analysis

Open source license compliance and vulnerability management

Why does it matter?

Today, developers are leveraging more than 50 percent of open source software (OSS) in their proprietary applications. This speeds up time to market, drives innovations, and revolutionizes the technology world.

In this new environment, security vulnerabilities, data breaches, and compliance lawsuits are real concerns. Organizations have to manage OSS assets proactively to manage security and license risk.

OSS license compliance

Open source components come with license obligations. OSS license compliance means that companies must observe all the copyright notices and satisfy all the license obligations for OSS they use in commercial products.

OSS vulnerabilities

The use of OSS comes with some type of exploitable vulnerability. With nearly 90 percent of software attacks aimed at the application layer, lack of careful oversight is a significant risk to every organization.

Risks

Depending upon how restrictive the license is, the use of OSS components in your development environment could lead to restrictions on the usage of your source code or even having to share your code externally.

Risks

Left untracked, OSS can leave your applications and data at risk to known vulnerabilities such as Heartbleed.

With the proliferation of OSS components in today's development environment, it is imperative that regular and timely audits are conducted of software developed, used, and distributed by the organization to detect vulnerability and compliance risks.

Powered by Flexera's FlexNet Code Insight, KPMG software composition analysis assists global organizations in discovering and understanding the use and impact of OSS components in their applications. We conduct OSS audits of an organization's most critical code. Our approach strategically aligns with our clients' business priorities, security, and compliance needs.

Coming out of the audit, organizations will get a detailed software bill of materials (BOM), with a deep understanding of the footprint of OSS, any known vulnerabilities that need to be patched, and risks around licensing that need to be addressed. These are essential for all organizations that build software. It is especially imperative for technology firms to include this as part of the technical due diligence process prior to making a software-related acquisition.



Market driver

Two broad use cases for KPMG software composition analysis are as follows:

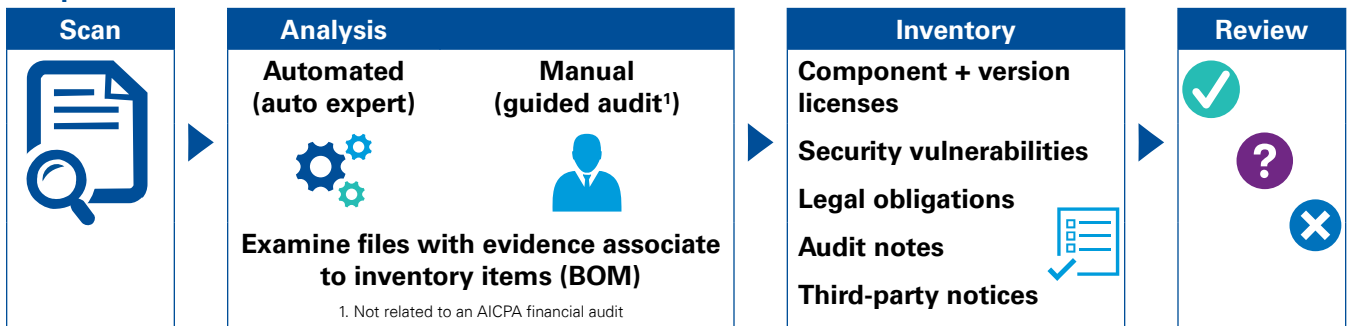
<p>M&A due diligence For tech acquirers, acquisition targets</p> <ul style="list-style-type: none"> — Understand the licensing restrictions and implications associated with the use of OSS components in the target’s externally distributed products — For example, using GPL licensed OSS in your commercial application may require you to release the source code externally 	<p>Baselines/investigations For software producers, consumers</p> <ul style="list-style-type: none"> — In addition to the licensing restrictions for internal and distributed products, understand the components included in the software build and the vulnerabilities associated with the of OSS components — For example, the use of an older version of Struts can expose the organization to potential hacks
--	---

Our services




KPMG software composition analysis is based on Flexera’s FlexNet Code Insight (formerly Palamida) platform.

<p>M&A due diligence Preacquisition due diligence (OSS license obligation), postacquisition deep dive (OSS license obligation/vulnerability detection assessment)</p>	<p>Baselines/investigations Software bill of material (BOM), OSS license obligations, vulnerabilities detection, and SDLC process reengineering to embed continuous OSS usage monitoring</p>
--	---

Our process



The KPMG difference

 <p>On-demand OSS license professionals for licensing assistance</p>	 <p>Global footprint and offshore capabilities</p>	 <p>Award winning Flexera partner of the year 2014–2017</p>
---	---	--

Contact us

Paul Baguley
Principal, KPMG LLP
T: 408-367-7608
E: paulbaguley@kpmg.com

Michael Adams
Managing Director, KPMG LLP
T: 614-249-2323
E: madams@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/us/flexera
kpmg.com/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 849150