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.

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.

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
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:

M&A due diligence
For tech acquirers, acquisition targets

- 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

Baselines/investigations
For software producers, consumers

- 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

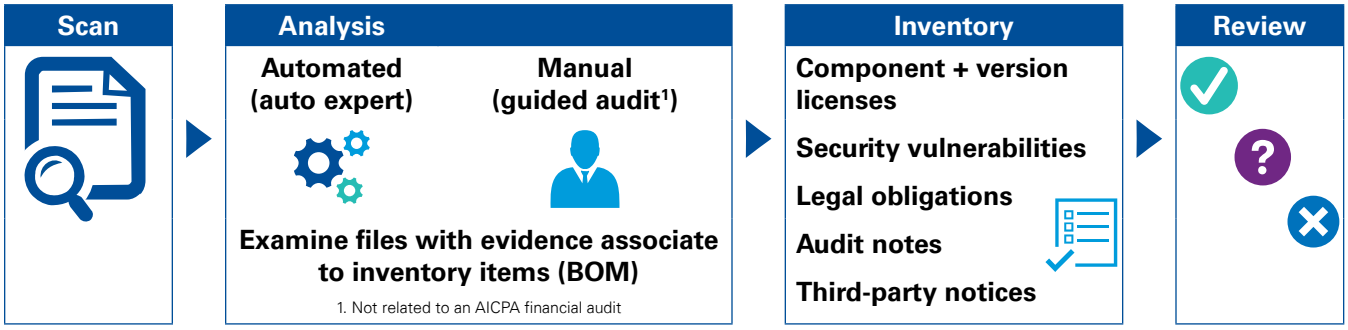
Our services

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

M&A due diligence
Preacquisition due diligence (OSS license obligation), postacquisition deep dive (OSS license obligation/ vulnerability detection assessment)

Baselines/investigations
Software bill of material (BOM), OSS license obligations, vulnerabilities detection, and SDLC process reengineering to embed continuous OSS usage monitoring

Our process



The KPMG difference

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

Contact us

Paul Baguley
Principal, Major Projects and Contract Advisory
M: 650-814-7612
T: 408-367-7608
paulbaguley@kpmg.com

Sarab Narang
Director, Major Projects and Contract Advisory
M: 408-876-0042
T: 408-367-7688
snarang@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