Open source due diligence & advisory services

Pre-deal due diligence assistance and post-deal consulting for open source license compliance and vulnerability management

Why does it matter?

The use of open source software (OSS) is becoming increasingly prevalent in today's development environment, with estimates ranging from 50% of the entire code base to as high as 85% to 90%. With such proliferation of OSS components in today's code bases, it is imperative that OSS due diligence be performed when the target is a technology company or has external-facing technology products and applications.

Pre deal, corporate buyers and private equity (PE) firms need to have a detailed understanding of their targets' OSS assets to understand the various license and security risks. Post deal, they need to ensure that these risks are being addressed and managed effectively.

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 or externally facing products.

OSS vulnerabilities
The use of OSS comes with some type of exploitable vulnerability. With nearly 90% of software attacks aimed at the application layer, lack of careful oversight can be a significant risk to any organization.

Risks
Depending upon how restrictive the license, the use of OSS components in the target's code base could lead to obligations such as requirement to share the technology's source code externally. This can have an adverse effect on the value of target's Intellectual Property (IP).

Risks
Left untracked, OSS can leave a target's applications and data at risk to known vulnerabilities like Heartbleed. In cases where the vulnerabilities are known, patching can be delayed as it may require reengineering applications. This leaves the target exposed.

KPMG Open Source Advisory Services assists global corporate and PE buyers to discover and understand the use and impact of OSS components in their target's applications. Utilizing Flexera's FlexNet Code Insight tool, we conduct a thorough scan and review of the target's critical code. Our approach strategically aligns with a buyer's business priorities, compliance, and security needs.

Coming out of the review, buyers will get a detailed software bill of materials (BOM) of the target's critical product and application code base. This will provide the buyer with a deep understanding of the OSS foot print, known vulnerabilities that may need to be patched, and risks around licensing that may need to be addressed.

In addition, we can analyze the target's OSS usage maturity to similar organizations as compared to the leading industry practices and develop a roadmap to move it up the OSS usage maturity scale. Accordingly, we can help buyers establish or enhance the target's open source governance, policy and processes and supporting technologies.

Our services

Two broad use cases for our services are as follows:

Pre deal

- Analyze target's OSS maturity to help the buyer understand the state of OSS governance and organizational structure, associated policies and processes, etc.
- Conduct a scan and analysis of the target's critical code to help a buyer develop a detailed understanding of OSS licensing, operational, and security risks.

Post deal

- Perform deeper and wider code scans and analysis to uncover additional licensing, operational, and security risks
- Help to establish or improve target's OSS governance, policies, process and technology
- Perform OSS code scan managed services
- Assist with OSS scan tool selection and implementation

Post-deal services are OSS scan tool agnostic; i.e., KPMG can work with any OSS scan tool in buyer's or target's environment.

Why KPMG

We can perform additional value-added services beyond code review:

Security vulnerability analysis

Increasingly, the use of OSS in the source code can bring with it significant exploitable vulnerabilities (e.g., the Equifax hack). KPMG's deep security experience and capabilities can help identify the commonly known security vulnerabilities in the target's code and prevent potential security hacks.

Remediation advice

Post acquisition, KPMG can offer remediation advice to the buyer and target to address the security vulnerability and OSS licensing risks identified.

OSS governance and process review

KPMG can analyze the target's OSS governance structure, policy, and processes to provide the buyer with an understanding of the maturity and the controls around the target's OSS development environment.

Code quality and architecture review

KPMG can also perform:

- Key OSS dependencies analysis (OSS version currency and proliferation risks, support risks)
- Code quality assessment
- Application and design quality
- Application enhancement and migration consulting

OSS due diligence assistance can be performed in conjunction with KPMG's Information Technology (IT) and Technology due diligence services to provide the buyer with a report of the target's mission-critical technologies.

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

March 2019

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