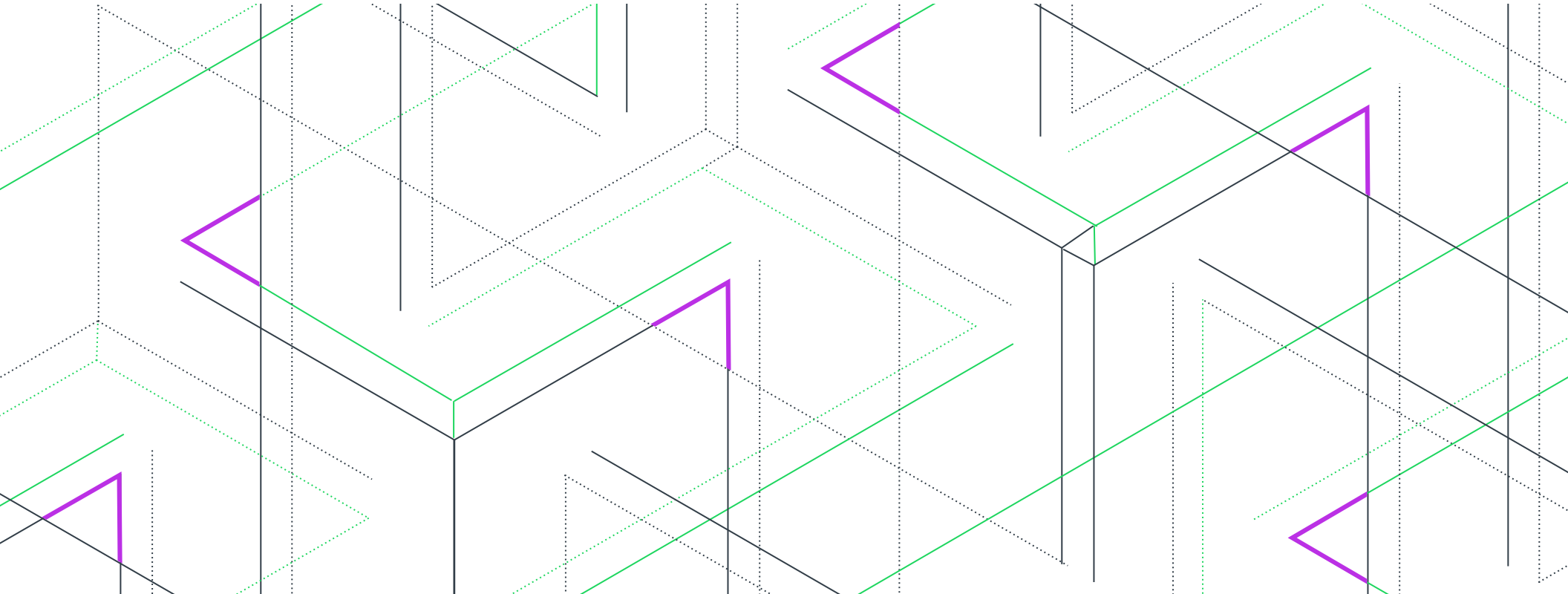
EBOOK

revenera

Software Composition Analysis Maturity Model

Strengthen Open Source Compliance and Security



Open source software (OSS) offers tremendous benefits in speeding up product development. In fact, research indicates as much as 96% of commercial applications contain open source components.

As the value increases, so has the opportunity for license compliance and security risks, putting a spotlight on the need for a process to manage the use of OSS.

Revenera's Software Composition Analysis (SCA) Maturity Model offers a framework to assess your current state of license compliance and security, and provide you with actionable next steps, including:

- Where to start
- A benchmark with peers for comparison
- A process maturity and business value assessment
- Specific, must-have improvements to put in place now

The model consists of four levels of maturity for license compliance and security. The model can be applied to all industries.

Process Maturity and Business Value ↑

Optimized **LEVEL 4**	Are we optimized for growth, scalability, digital transformation, and change management?
Automated **LEVEL 3**	Have we automated processes for scale and best user experience?
Enabled **LEVEL 2**	Are we using standard vulnerability management, OSS license compliance and obligation management processes across all products?
Reactive **LEVEL 1**	Are our applications secure, compliant and centrally managing obligations?

Key Software Composition Analysis Business Processes

License Management → Vulnerability Management → Obligation Management → Component Management

The model assesses business processes in four key dimensions of Software Composition Analysis.

License Management

To manage open source license dependencies and reduce the impact of legal risk

Vulnerability Management

To prevent security defects due to third-party component usage

Obligation Management

To manage obligations related to the use of open source software, based on associated licenses and company policies

Component Management

To achieve insight into how or what components are used, and include this insight in usage and product roadmap decisions

LEVEL 1: Reactive

LICENSE MANAGEMENT

Recognition that manually managing open source license dependencies impacts legal risk

VULNERABILITY MANAGEMENT

Realization that vulnerability management is needed to prevent security defects due to third-party component usage

OBLIGATION MANAGEMENT

Understanding manual obligation management is costly, inconvenient and incomplete

COMPONENT MANAGEMENT

Security/Legal decisions made with little or no insight into how or what components are used

Open source use is skyrocketing. Management realizes the need for a process and tooling, but teams are not enabled to assess associated risk.

Characteristics of a Reactive Level Team

Tooling: In some cases, you use a homegrown tool for certain high risk applications to detect high-level software packages. More commonly, you ask developers to disclose the OSS they use in some projects. A bill of material is only created in response to a customer request, usually by visually identifying high-level packages in the application code.

Team: Reactive teams are beginning to understand the need for a formal or ad hoc team to determine and implement corporate policy around OSS.

Monitoring OSS: Your teams are not enabled to monitor open source components or associated vulnerabilities.

Incident management: Incident management can be seen as the true test of SCA maturity. At this maturity level, teams are not equipped to remediate vulnerabilities.

Actions to Move to Next Level

With the WannaCry and Equifax hacks still looming heavily over software organizations, there is a big push to understand and manage software vulnerabilities in both commercial software and software developed for internal users.

- Educate on a repeatable, automated process
- Create a team of people responsible for managing the process
- Change the perception that a security tool will slow down production

LEVEL 2: Enabled

LICENSE MANAGEMENT

- Reduce risk due to undisclosed OSS/third-party component use
- Cost savings from automation of component selection & self-service

VULNERABILITY MANAGEMENT

- Reduce costs from exercised vulnerabilities
- Allow better component selection due to vulnerability insights
- Reduce time to market with up-to-date vulnerability info

OBLIGATION MANAGEMENT

- Improved customer satisfaction by lower vulnerability exposure
- Improved customer satisfaction with insight into legal obligations
- Reduce legal risk from unfullfilled legal obligations

COMPONENT MANAGEMENT

- Security/Legal risk analysis informed by component usage
- Rapid response to zero day and other high importance vulnerability alerts across the enterprise

Risk assessment has improved around OSS use. Short-term success metrics for security and compliance are in place. Teams have started to implement a formal process.

Characteristics of an Enabled Team

Tooling: You likely scan your applications with a commercial code scan tool for vulnerable code one or more times before shipping. Some companies ask developers to disclose their use of OSS. You are able to consistently create BOMs with your products, but these are incomplete. Your scan and analysis is limited to high-level software packages.

Teams and training: Your ad hoc open source management team created policies and training but need to consistently evaluate open source security and compliance initiatives.

Monitoring OSS: OSS risk is considered in project plans and initiatives. You determine when a new vulnerability affects high-level packages you track and monitor.

Incident management: You are equipped to remediate some vulnerabilities and are beginning to formulate an action plan if an incident occurs.

Actions to Move to Next Level

- Document processes and controls
- Create consistency for engineering actions and priorities
- Automate process to avoid delays in shipping products on time
- Increase governance automation to simplify legal team impact; regularly report on open source risk to management

LEVEL 3: Automated

LICENSE MANAGEMENT

- Improved developer experience by automating OSS license lifecycle management
- Reduce Legal team costs via policy automation
- Minimize Legal out of compliance in all environments

VULNERABILITY MANAGEMENT

- Improved process automation for vulnerability lifecycle management as part of continuous build process
- Vulnerability Alerts allow for faster remediation and reduced customer exposure to security risk

OBLIGATION MANAGEMENT

- Improved legal and security compliance through obligation automation (especially third-party notices)
- Reduce costs of providing current version to version compliance artifacts

COMPONENT MANAGEMENT

- Data-driven roadmap decisions from in-product component use insight
- Reduce usage of low count/low quality components in lieu of vetted corporate standards

Automation is in place and high-level and deep scanning have been integrated into the development process. Remediation and component selection is easy. Product updates do not require rushed security-related patches.

Characteristics of an Automated Team

- **Tooling:** You use a commercial scan platform to scan code early in the software development lifecycle. Your teams perform automated high-level scans across the board, but realize that package level analysis may not be enough. You explore tools to get more visibility into dependencies, subcomponents and commercial code without significantly increasing people and cost.
- **Team:** Your company has a formal open source review board to set and update corporate policy. This team trains and enables developers to use open source while understanding risk. The board analyzes and reports on OSS usage.
- **Monitoring OSS:** Continuous monitoring occurs. Automated teams easily determine when a new vulnerability affects code in your organization. Process and policy are widely understood, so engineering teams easily prioritize reported issues and respond quickly to alerts.
- **Incident Management:** You have a strong communication plan if a new vulnerability is discovered. Your team is equipped to remediate vulnerabilities, although limited by the depth of scans.

Actions to Move to Next Level

- Continue consistent use of documentation, processes and controls
- Reinforce engineering actions to continuously monitor, prioritize and remediate issues
- Ship products with third-party disclosures
- Start to examine code from suppliers and partners to also monitor associated risk

LEVEL 4: Optimized

LICENSE MANAGEMENT

- Continuous management of OSS compliance with complete transparency between vendors & customers
- Complete compliance through deep analysis including binary and source

VULNERABILITY MANAGEMENT

- Better customer protection due to vulnerability alerts for installed base/ previous versions
- Insight into supply chain vulnerabilities using deep analysis

OBLIGATION MANAGEMENT

- Increase customer confidence by providing compliance to customers and community
- Reduce reword costs by including obligation management in policy decisions

COMPONENT MANAGEMENT

- Visibility of technology and language change over time across the enterprise
- Data can be used to best support high-value OSS ecosystems and components

A powerful combination of infrastructure, automation and education is in place for full protection. Your team understands that some projects have more risk exposure than others and a deeper analysis is necessary. Processes are in place around how to treat code from partners and suppliers for security and compliance.

Characteristics of an Optimized Team

Much of the tooling, teams and training, incident management and OSS monitoring aspects for an optimized team are the same as for the automated team. The difference is in the breadth and depth of scans and analysis. Optimized teams either analyze or expect analysis of code received from vendors.

You're On It! Protection in Place

Full use of scalability and visibility to empower rapid adoption of OSS. Consistent feedback loop in place. Full visibility into component usage and obligation data for enterprise-wide planning insights. Powerful breadth and depth of scans and analysis.

Start the Conversation

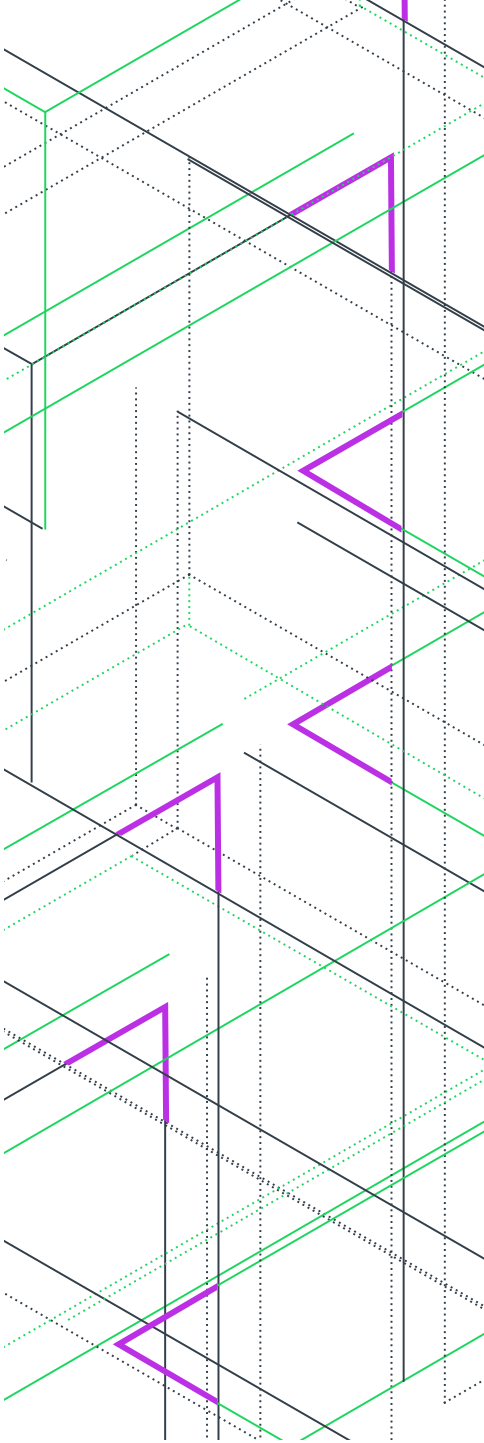
Open source software risk management means making sure all of the components in your products are license compliant and secure based on your company's policies. This maturity model provides a framework for building a structure throughout your organization for governance, risk and control.

Instead of defining a pass/fail metric, the SCA model provides a practical, staged approach to open source management. Take advantage of this opportunity to create clear short- and long-term goals to increased control and transparency of your open source usage.

NEXT STEPS

Concerned about the compliance and security of your applications?

CONTACT US >



Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**

1.800.809.5659 | +44.870.871.1111 | revenera.com

revenera™