Open Source Management Maturity Model

Almost every modern application is built with open source components, and for good reason. Organizations get access to innovative technology with reduced time to market and lower costs. However, open source does carry some measure of legal risk (OSS license compliance) and security risk (OSS vulnerabilities). And yet, many companies are still using relatively immature processes and policies to manage these concerns.

At FOSSA, we have developed a maturity model based on our learnings from our customers, industry experts, and market research. Engineering, legal, and security teams can use this framework to identify gaps in their current approach to open source management and chart a path to improvement.

Overview

BEGINNER

No Open Source Management

- Open source is used, but no policies or processes are established to govern its usage
- No inventory of open source dependencies exists
- Non-existent or limited license compliance, which has legal and reputational ramifications
- No visibility into security vulnerabilities beyond reacting to publicly available advisories; high risk of security breaches and attacks

INTERMEDIATE

Ad-Hoc Open Source Management

- Some processes are in place to govern the adoption/usage of open source, but they don't cover every use case
- Open source policies might exist but are not automated
- Outdated inventory of open source dependencies
- License compliance is ad-hoc and reactive
- Sporadic scans to get visibility into vulnerabilities

ADVANCED

Continuous Open Source Management

- Well-defined processes around open source adoption, usage, and contribution
- Automated license compliance and security policies
- SBOMs can be produced quickly with depth and precision
- Automation and real-time alerts support continuous compliance with licensing requirements
- Shift-left security posture that enables continuous and early visibility into vulnerabilities

of IT leaders expect to increase their use of enterprise open source software for emerging technologies

Source: https://www.redhat.com/en/enterprise-open-source-report/2022

Benefits of Open Source

32%

Higher-quality software

Source: https://www.redhat.com/en/enterprise-open-source-report/2022

Characteristics

	BEGINNER	INTERMEDIATE	ADVANCED
Inventory / SBOM	Manual and often incomplete inventory of open source	Inventory exists but it is not up-to-date or incomplete	Accurate and up-to-date inventory. SBOMs can be exported in multiple formats, including SPDX
Policies	Policies haven't been created or implemented	Policies exist but little to no automation	Policy automation for license compliance and security with ability to meet specific needs of teams
Open Source Program Management	No processes to govern open source adoption or usage	In-house or external counsel periodically monitors software for license compliance	Established OSPO provides guidelines and best practices for open source adoption and usage
Engineering	No guidelines or processes available to engineering to guide open source contributions or adoption	Issues aren't discovered until late in the SDLC, slowing development velocity	Developer teams save time and effort by fixing issues early in the development lifecycle
Legal	Little legal oversight	Legal has to deal with frequent and ad-hoc open source issues	Legal is integrated into compliance workflows, which enables efficient collaboration with engineering to resolve licensing issues
Security	No security scans for open source code	Sporadic scans to detect vulnerabilities but issues are not addressed immediately	Every code check-in is automatically scanned for vulnerabilities with alerts triggered for issues found
Remediation and Prioritization	No prioritization or remediation available	Some guidance is provided but remediation has to be applied manually and verified; teams have to prioritize issues themselves	Automated PRs for remediation and prioritization driven by tools that automatically apply policies

Barriers to OSS Adoption

32%

Concerns about inherent security of code

Source: https://www.redhat.com/en/enterprise-open-source-report/2022

33% of codebases contained unlicensed software and 67% of codebases had license conflicts

Source: https://www.helpnetsecurity.com/2020/05/14/open-source-components-security/

FOSSA

fossa.com

About FOSSA

The FOSSA platform automates vulnerability management and license compliance so engineering, security and legal teams can collaborate seamlessly to accelerate innovation velocity and boost efficiency.

Email us at sales@fossa.com