BLACKDUCK

INTRODUCTION TO OPEN SOURCE GOVERNANCE & COMPLIANCE

WHY OPEN SOURCE?

Open source software is pervasive in today's software lifecycle and supply chain. Open source is used to build applications, products, and services. Software developers can choose from freely downloadable code components to speed development and slash budgets by thousands, or even millions, of dollars.

The embrace of cloud computing, mobile, and distributed development has forced organizations to increase the pace and intensity of application development. At the same time, development managers are under pressure to deliver solutions faster, with fewer resources. For mobile development in particular, open source offers extremely practical benefits. Many companies face tremendous pressure to quickly deploy high- quality mobile applications, and open source helps organizations achieve this goal.

What's more, the fastest-growing and most agile companies are built on open source, from Facebook and Twitter to Amazon and Google. Apple, the most valuable company in the world, built the iPhone, iPad, and MacBook with open source code.

The benefits are clear: the industry-standard cost per line of code (LoC) ranges from $10 to $20, and the average component used by a Global 2000 company contains 50,000 lines of code. Therefore, the use of open source could save from $500,000 to $1 million per project.

The price and performance advantages of open source have been the main drivers of its adoption. But the full benefits of open source are only realized when organizations have visibility into, and control over, its use in the enterprise.

WHY ARE VISIBILITY & CONTROL SO CRITICAL?

According to Gartner, fewer than half the organizations using open source today have effective programs in place to manage it. Poor management of open source can expose organizations to security, legal, and operational risks. Uncontrolled use of open source can introduce code that contains security vulnerabilities, does not comply with corporate policies, or is not properly licensed. To avoid these risks, organizations must develop policies based on best practices and automate the management of open source component use.

OPEN SOURCE SOFTWARE'S COMPETITIVE ADVANTAGE:

CHEAPER
FASTER
INNOVATIVE
FLEXIBLE

Legal Risk

Business, security, and IT leaders must understand the obligations associated with open source licenses and develop policies to prevent their organizations from violating these obligations. Organizations can gain control over open source component use by automating the governance and compliance process as part of application development lifecycles.

Ignoring license compliance can result in bad publicity, copyright infringement, and even stop shipment orders, damaging company reputations and immediately impacting revenue streams.

Operational Risk

Low-quality components can cause down- and upstream failures. By automating the selection of open source components, developers can make better component choices. For instance, developers can decide whether to use a component based on:

- Community activity – how many commits and committers a particular component has
- Version – how far the requested version is behind the current version

Security Risk

Managing application security is essential in today's complex IT environment. All external code is susceptible to security vulnerabilities and should be actively monitored, both in development and post-deployment.

By leveraging the latest vulnerability data, security vulnerabilities associated with a component can be identified. And after components have been selected and deployed, continually monitoring their use assures that vulnerabilities are quickly addressed.

> " IT leaders must understand, embrace, manage, and direct how and where open source will play a role in their strategic IT road maps to maximize the business value and minimize the risks associated with these technologies."
>
> –Gartner

HOW DO YOU GET STARTED?

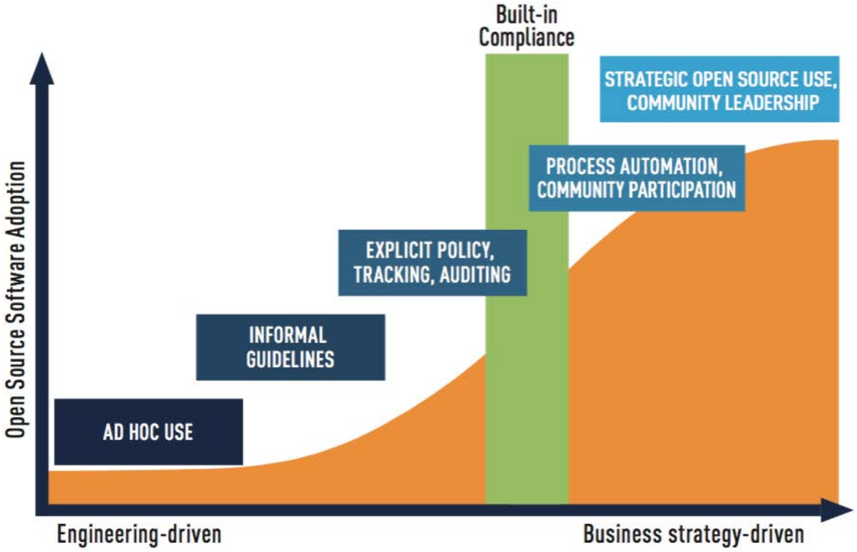
The first step to managing open source is to understand how much you have and where it's used. This can be achieved with the help of software that scans and audits code. Audits should not be a one-time event, but rather should be done on an ongoing basis. This helps ensure long-term compliance with risk management policies and external license obligations. Next, it makes sense to implement a governance program that encompasses all third-party code, whether from a commercial vendor, an open source project, or an outsourced supplier.

The below diagram illustrates five levels of open source adoption. Organizations with mature processes don't worry about compliance; compliance is built in. They can instead focus on leveraging open source for strategic advantage.

KNOW YOUR CODE

Open source is an essential component in the development of today's software applications and services, and there is no sign of this changing in the future. Security threats to applications built on open source will also continue to increase, and license compliance challenges will remain prevalent for many organizations.

To realize the benefits of open source without being blindsided by security vulnerabilities or held back by compliance issues, organizations need to know what is going into their applications. Innovative tools are available today to catalog all open source in organizations' software portfolios – from whole platforms such as Linux, Android and Hadoop, to individual code components, all the way down to the level of code snippets cut and pasted into internally- developed application code.


Built-in Compliance
STRATEGIC OPEN SOURCE USE, COMMUNITY LEADERSHIP
PROCESS AUTOMATION, COMMUNITY PARTICIPATION
EXPLICIT POLICY, TRACKING, AUDITING
INFORMAL GUIDELINES
AD HOC USE
Open Source Software Adoption
Engineering-driven
Business strategy-driven

Stages of Open Source Adoption

These tools, when employed on demand or integrated into software development workflows, provide critical information for companies to act upon, without slowing development or delaying time to market.

They allow organizations to develop robust processes to determine:

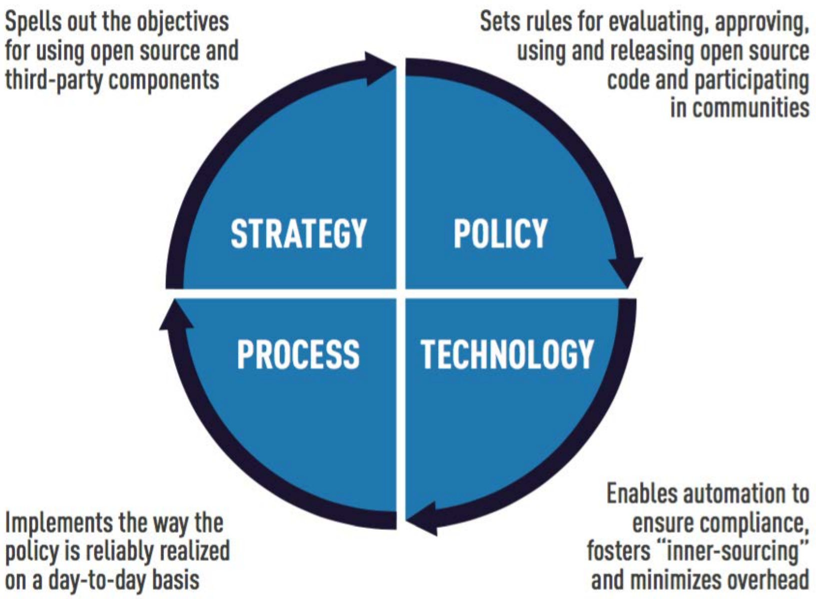
- Exactly what open source software resides in, or is deployed along with, applications
- Where this open source software is located in build trees and system architectures
- Whether the code exhibits any known security vulnerabilities
- Full details of the organization's open source risk profile

THE BLACK DUCK HUB: YOUR COMPREHENSIVE SOLUTION

The Black Duck Hub helps security and development teams secure and manage open source code. The Black Duck Hub is an automated solution that maps known security vulnerabilities in scanned open source code, creates a bill of materials (including open source license information) and constantly monitors scanned code for new vulnerabilities.

Find out what's in your code. Get a live demo of the Black Duck Hub today.

An effective governance program has four main elements:



Spells out the objectives for using open source and third-party components

Sets rules for evaluating, approving, using and releasing open source code and participating in communities

Implements the way the policy is reliably realized on a day-to-day basis

Enables automation to ensure compliance, fosters "inner-sourcing" and minimizes overhead

ABOUT BLACK DUCK SOFTWARE

Organizations worldwide use Black Duck Software's industry-leading products to automate the processes of securing and managing open source software, eliminating the pain related to security vulnerabilities, license compliance and operational risk. Black Duck is headquartered in Burlington, MA, and has offices in San Jose, CA, Vancouver, London, Belfast, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing. For more information, visit www.blackducksoftware.com.

CONTACT

To learn more, please contact: sales@blackducksoftware.com or +1 781.891.5100
Additional information is available at: www.blackducksoftware.com