



FOSSBazaar

A Governance Initiative to manage Free and Open Source Software life cycle

Table of contents

Executive summary	2
What is FOSS Governance	3
The importance of open source governance	3
Why FOSS Governance is needed in the enterprise	4
Best practices for an effective open source governance strategy	5
FOSSBazaar	6
Conclusion	7
For more information	8



Open source is a vital part of today's IT landscape—but to manage its complexities and mitigate its risks—an effective governance strategy is just as vital.

Executive summary

With the rapid usage expansion of open source software across the industry, a growing set of issues regarding acquisition, licensing, code use and reuse, and distribution is emerging. Risks related to deployments and respect of open source licenses need to be properly managed by organizations using open source software.

FOSSBazaar, an open initiative focusing on these open source governance issues, was launched in early 2008. This initiative is supported by a public web site, FOSSBazaar.org, which provides enterprises with a wide variety of resources and information to help them implement and improve their open source governance programs.

The challenge is not that open source software is inherently risky, but that it is often misconstrued as inherently “free” of risk by virtue of being open source. In fact, open source technology and associated licensing carry their own complexities that require oversight just like traditional software. Traditional software governance, however, does not generally address these complexities.

With an effective governance strategy, enterprises gain control over the complexities and mitigate the open source software risks at every point it touches the IT environment. In the following pages, the importance of proper open source software governance, for maximizing its benefits, while mitigating deployments risks across the enterprise will be reviewed. Guidance, access to tools, resources and information for managing FOSS use and expansion based on practical experience will be provided with an expectation to assist potential users in assessing their open source usage and implementing relevant governance strategies.

What is Open Source Governance?

Open Source Software (OSS) or Free and Open Source Software (FOSS) Governance refers to the best practices (process and policies) and related tools to help users to acquire, deploy, keep track of and manage open source software in IT environments.

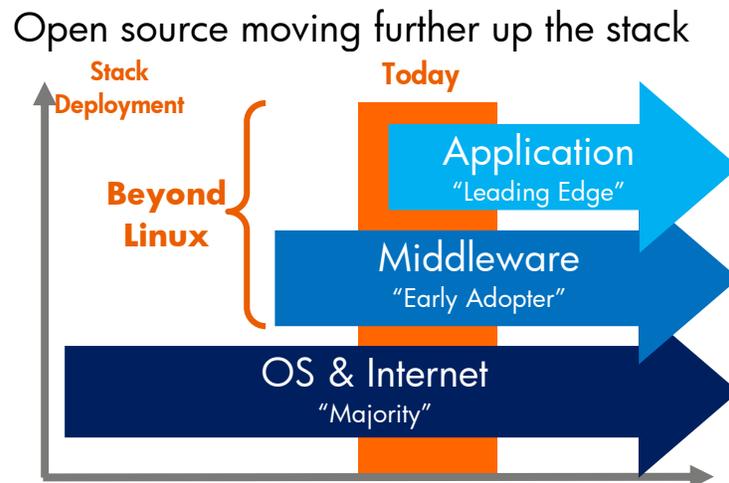
The importance of open source governance

You would be hard pressed to find an enterprise today that does not use open source software. In fact many analysts affirm that most companies use more open source software than they realize.

Acceptance and adoption of open source software is already widespread, it is even found in much commercial software, and it is expanding rapidly. According to a recent survey conducted Forrester Research nearly half (46%) of those using open source frameworks still claim they are not using open source¹.

The open source model initially developed to serve low-level software requirements continues to penetrate all software domains, far beyond operating systems, databases, and development tools to include applications and integration servers and Service-Oriented Architecture (SOA)-specific technologies.

Figure 1: Open Source Market Trends



The reason for such broad adoption is clear: enterprises want to save money—in some cases millions of dollars—and they want to enjoy those savings while delivering high service quality and flexibility within their business technology infrastructure. Global peer review

1. Forrester Research, Enterprise Open Source Use In 2007, From: Enterprise And SMB Software Survey, North America And Europe, Q3 2007, June 2008



and open access to source code are seen as major contributors to meeting these objectives. Accordingly, analysts predict that, over the next few years, the vast majority of Global 2000 organizations will have formal open source acquisition and management strategies.

The “free” availability of open source software is often perceived as a bonanza because the code itself is typically available at no cost. Indeed there is little to keep developers from making software choices on an individual basis, without corporate or even departmental oversight. The ease with which open source software can be acquired and integrated into products and in the IT environment is a very appealing factor in its widespread use. But this “free and easy” world of open source software can rapidly lead to chaos and an unsustainable situation from both technical and legal perspectives. A large use of open source software brings with it a growing set of issues regarding acquisition, licensing, code use and reuse, and distribution. Therefore, proper open source software governance is becoming increasingly important—in fact, essential—as a means of ensuring the long-term viability of open source projects across the enterprise.

Why is FOSS Governance needed in the Enterprise?

The Governance of open source software differs from the usual software asset management practices used by IT procurement for commercial software in a number of ways, for example:

- Many developers make the decision to leverage community resources to take advantage of the large number of open source technologies that are out there and they can download them directly from the web.
- It is important to identify and manage open source software in IT environments because it is usually already there. Often, even customers that do not think they are using open source technology actually are. For example,
 - Apache, PHP, Python, Perl, Tomcat, Hibernate, and, of course, Linux are widely used in today’s data centers.
 - Many traditional ISVs now incorporate and distribute open source software with their applications.
- Another key reason to govern the open source is to minimize the legal risk. It is important to be prepared—have company policies defining the use of open source software and know that open source software is being used according to these guidelines.
- And finally, there are many open source licenses.
 - There are 60+ approved OSI licenses. And there are 180 known open source licenses that HP tracks. (OSI—“Open Source Initiative”—is a community organization that has defined guidelines for what is open source and it approves licenses.)

Commercial Software acquisition goes simply through procurement processes for approval; with open source the usage of the software itself must be reviewed and understood. For example: there might be times when certain projects are fine for use but in others, i.e. embedding open source with proprietary software, might infringe upon distribution clauses. This adds a level of complexity. Best practices and streamlined processes are needed to define adequate open source approaches depending on target utilization—internal use,

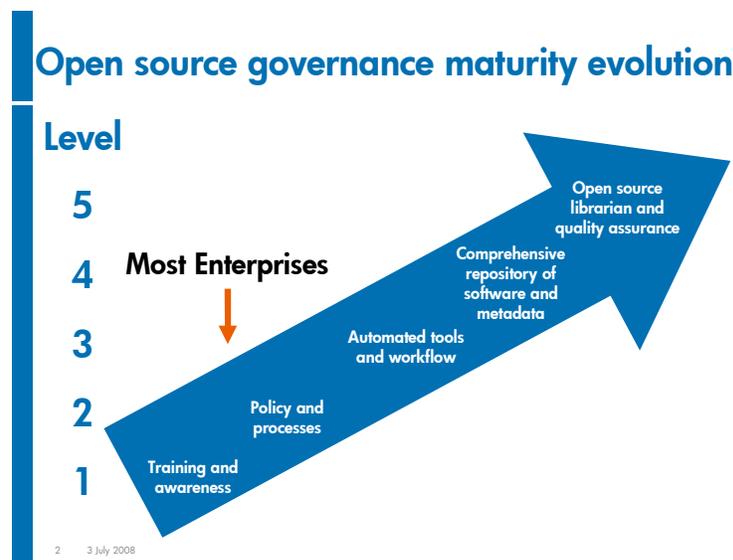
embedded use, corporate/employee contribution, and redistribution (including agents, outsourcers/offshorers, and so on).

Best practices for an effective open source governance strategy

At the foundation of any governance strategy is the creation and enforcement of a comprehensive open source policy that allows enterprises to track open source software throughout its lifecycle. As Gartner states, “A well-defined, articulated, enforced adoption policy is critical to effectively managing open source in a mainstream enterprise. This policy must establish a clear chain of command where employees conform to establish open source solutions as ‘approved’ software assets.”²

To gain full control of its FOSS life cycle a company will need to gradually refine the processes, policies and tools it is using. The various steps to implement a comprehensive FOSS Governance can be embodied in a governance maturity model as shown in figure 2, in such a model each implementation step contain the necessary elements to help an organization to gradually refine its open source governance practices.

Figure 2: The open source governance maturity model



The resulting best practices include:

- Creating an open source program office
- Developing a comprehensive open source policy
- Creating an open source review board for open source use and participation
- Driving education and enforcement

² Mark Driver, Gartner, Inc., “Establish an Enterprise Open source Policy to Maximize Value and Minimize Risk.” Publication date: December 13, 2006; ID number: G00144406



These aspects are detailed in "[Best Practices in Open Source Governance](#)" white paper available on fossbazaar.org.

FOSSBazaar

FOSSBazaar is an open community formed by HP, Coverity, DLA Piper, Google, the Linux Foundation, Novell, Olliance Group, OpenLogic, SourceForge, Krugle, Ars Aperta and BT. As a workgroup of the Linux Foundation, FOSSBazaar is dedicated to empowering individuals and enterprises to understand potential issues related with the use of free and open source software (FOSS), the processes that can properly govern the implementation and deployment of FOSS, and tools that can be used for these efforts across the lifecycle of an open source project.

FOSSBazaar.org is the first open community website dedicated to the selection, acquisition, and deployment of FOSS in IT enterprises. It is the platform used by the community for the learning, sharing, and evolving of industry best practices for maximizing the benefits and reducing the risks of deploying open source software. Managers in business, government, and education, who want to assess the benefits and risks associated with using FOSS in their IT environments, can find useful information to get started, or enhance their FOSS governance practices.

FOSSBazaar.org also operates like a portal that can direct interested parties to commercial vendor services that address multiple FOSS governance needs.

FOSSBazaar.org resources include:

White papers including:

- Best Practices in Open Source Governance
- FOSS Governance Fundamentals
- IP Management Best Practices in Open Source
- Copyright Basics
- Copyright Ownership

Many tools including:

- FOSS Governance Maturity Self-Assessment survey
- Open Source Policy Workshop
- Open Source Best Practices Scorecard
- OSS Discovery: Find installed open source software
- FOSSology

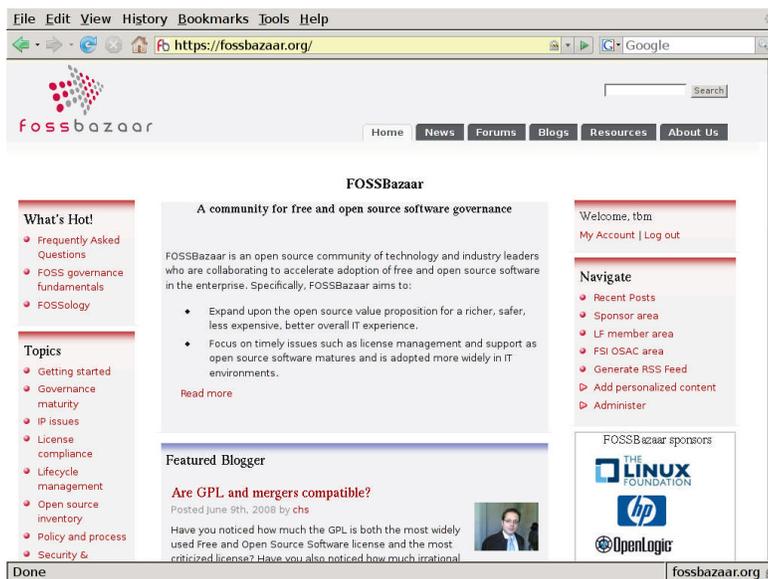
Active blogs:

- Not Enough support? No, too many support choices!
- Open source strategy or policy?
- Use Open Source To Save Money
- Obstacles for making FOSS development truly global

Hot forums:

- General/getting started
- Legal/Licensing
- Policy/Process
- Lifecycle Management
- Support options

Figure 3: The FOSSBazaar home page



Conclusion

While the free availability of open source software is an attractive asset for developers, this same freedom makes it difficult to track the use of open source and ensure compliance with licensing across enterprises. Governance of open source software is key to mitigating potential and real risks associated with large deployments of Free and Open Source Software and enabling IT environments to gain greater value from open source community projects.

By gaining a greater understanding of the issues associated with open source software, and by addressing those issues with a comprehensive governance program, enterprise customers can get into a stronger position to deploy more agile, secure and lower cost IT infrastructure for a better business competitive advantage.

The FOSSBazaar community provides a set of best practices and tools for the governance of free and open source to enterprises around the world through its website FOSSBazaar.org. Potential users are invited to go to this sites where they will find useful information and tools and are invited join the community to share their experience.



For more information

For more information on how FOSSBazaar can help you address the risks and maximize the value of open source software for your enterprise, visit: www.fossbazaar.org