Best practices in open source governance
Managing the selection and proliferation of open source software across your enterprise

Table of contents

The importance of open source governance .................................................. 2
Executive summary .................................................................................. 3
Best practices for an effective open source governance strategy .................. 3
  Create an open source program office ...................................................... 4
  Assemble an open source review board ................................................... 5
  Drive education throughout the enterprise .............................................. 6
Considerations for developing open source usage guidelines ................. 6
  Usage .................................................................................................. 6
  Oversight ......................................................................................... 6
  Communication ............................................................................... 6
Open source governance services available from HP .............................. 6
  Open Source Governance Workshop .................................................... 7
  Open Source Governance Assessment Service .................................... 7
  Open Source Compliance Service ....................................................... 8
Conclusion ............................................................................................ 8
For more information ........................................................................... 8
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, HP continues to affirm that most companies use more open source software than they realize.

Acceptance and adoption of open source is already widespread across many industries, including commercial software development, and it is expanding rapidly. 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 leveraging high quality and flexibility within their business technology infrastructure. Global peer review 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.

To many, the “free” availability of open source software would seem like a bonanza. Because the code itself is typically available at no cost, there is little to keep developers from making software choices on an individual basis, without corporate or even departmental oversight. And the ease with which open source software can be acquired and integrated into products 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. 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.

In the following pages, we review the importance of open source software governance, summarizing the potential risks that open source technology could introduce into your enterprise and providing guidance on managing its use and proliferation based on our experience.1 HP has addressed these risks by implementing a comprehensive open source governance program across its organizations. We offer here a set of recommendations, derived from this program, that you can leverage to implement an open source governance initiative in your enterprise. In addition, we offer a broad set of professional services to assist you in assessing your open source environment and implementing appropriate governance strategies.

1 A more detailed discussion can be found in the HP white paper “Open source software governance: critical business considerations and strategies” (HP part number: 4AA1-3991ENW).
Executive summary

HP has long embraced the use of open source—and, before this term emerged, other forms of “shared” source—software, both internally and as part of our full suite of product offerings. We recognize open source as a vital part of today’s IT landscape, and we appreciate the value that it has brought to our business and our customers. Nevertheless, as the use of open source expanded within HP, we identified a growing set of issues regarding acquisition, licensing, code use and reuse, and distribution. We needed to manage the risk to our company and respect the licenses of the open source software used within our enterprise. As a result, we undertook a program of open source governance to control and manage our open source software throughout its entire lifecycle. Today, this proactive approach to managing open source is being replicated in more and more companies around the world.

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 open source governance strategy, you can gain control over the complexities and mitigate the risks with proper processes for managing open source software at every point it touches your enterprise. This allows you to address important issues, including:

- **Acquisition and tracking**—to improve awareness of when open source software enters your organization and to properly track its maturity, suitability, and support model; this also improves your ability to apply updates and patches, provide adequate service and support, and comply with licensing, as well as assess the impact of potential third-party intellectual property and patent claims
- **Licensing**—to gain a clearer picture of different open source licenses and potential interactions in order to avoid violations that could result in litigation or loss of business
- **Code derivation and reuse**—to leverage existing open source code and maintain a proper separation between open source and closed source software when the open source license requires it (sometimes referred to as code “provenance”)
- **Source reliability**—to create trusted sources for open source software, preventing the introduction of malware or otherwise exposing vulnerabilities

As a major user of open source software throughout our own IT infrastructure, HP has faced many of these issues. More importantly, we have solved them internally, leveraging in-house expertise and many years of experience to develop policies, procedures, and tools that many other organizations are now seeking to emulate. In the following pages, we will share our approach to open source governance.

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 you 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

For the past six years, HP has implemented open source governance policies and procedures, advancing our open source governance strategy to a highly mature level. (See Figure 1)

---
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
Drawing on many insights gained over the years, HP is now sharing its internal best practices for open source governance, which you can now adopt in your enterprise. These 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

By thoroughly understanding the issues and implementing a comprehensive system of governance based on the best practices presented in this paper, your company can better appreciate the benefits of open source software with confidence that the interests of your enterprise are protected.

**Create an open source program office**

Faced with widespread but relatively uncontrolled dissemination of open source software throughout multiple divisions worldwide, HP conducted a comprehensive audit as a first step in its open source governance strategy. To oversee this process, we created an open source program office—a central point of responsibility where all open source activities would be understood for consistent communication inside and outside the company.
The audit identified all open source software in use throughout the enterprise, whether it was for internal IT infrastructure, for redistribution to customers, part of an open source project, or embedded in other HP products. We also had to work with our partners and suppliers to determine the use of open source software in third-party products being integrated or distributed with HP products. Once this information was well understood, we then analyzed the licenses for each piece of software to understand the license rights and verify that the open source software component was being used in compliance with its associated license requirements.

Based on the information gained from the audit and combined with internal business objectives, we created a policy manual detailing every aspect of open source acquisition, use, and licensing. The policy manual provides guidelines for how to work with the open source community, shows what to look for when bringing open source software into the enterprise, relates important issues related to each use case, and details procedures for working with third parties or competitors on a community project.

Assemble an open source review board
To help educate our employees and enforce open source policies, HP also assembled a review board. Our open source review board is a virtual team of open source experts, including IT, legal, engineering, and community members. It provides a centralized resource to answer questions and monitor open source activity within our enterprise. The responsibility of the board is to review:

- Free and open source software used in company products, solutions, and services
- Group and individual participation in open source projects
- Company software released under an open source license
- Internal use of open source software for IT infrastructure

To govern effectively, any employee wishing to introduce a proposal for using open source software must now follow an established workflow overseen by the review board. (See Figure 2)
Given the complexity surrounding open source licensing and the potential interaction between open source and proprietary code, it is not surprising that open source proposals following this workflow inside HP required intensive manual analysis. In some cases, attorneys on the review board were spending weeks to analyze complex proposals.

To streamline the workflow processes, HP has continually applied technology to automate the process, as well as to analyze the licenses and the reusability of the code. The ultimate goal of the process is to facilitate open source use and participation while mitigating risks. We now view the workflow and tools as a resource rather than a burden on the system.

**Drive education throughout the enterprise**

In the course of the many years that HP has invested in evolving its open source governance best practices, we have built an extensive knowledge base that open source participants can tap into to maximize the effectiveness of their projects. We also conduct in-depth training with our developers and engineers to help them understand the issues and our policies governing open source software. Through education, clear procedures, and automated tools, we have made open source policies as easy as possible for everyone to follow. But to underscore the seriousness of these policies, we enforce them strictly, and violations are considered grounds for dismissal.

By maintaining this level of control, HP has been able to reduce our risks significantly while making open source software a vital part of our business, as well as an integral part of the value we deliver to our customers and partners.

**Considerations for developing open source usage guidelines**

As you develop your own open source policies and guidelines, HP recommends that you do so using a cross-functional team composed of legal, research and development, and business managers. With a diverse team, you will be able gain a broad perspective of the issues affecting the interests of your enterprise. Areas that this team may wish to address include:

**Usage**

- **Corporate use of open source**—the business need for open source and what part it plays in your infrastructure and development projects, including when and where it is appropriate or not appropriate to use it
- **Employee open source contributions**—where and when such contributions are appropriate or not appropriate

**Oversight**

- **Open source governance**—a complete set of policies, procedures, and tools to manage the acquisition, use, licensing, and distribution of open source software
- **Relationships with open source community**—how your organization works with the community, with best practices for managing that relationship
- **Licensing, copyrights, and patent guidelines**—corporate policies for licensing open source projects and protecting proprietary assets

**Communication**

- **Awareness, documentation, communication, and compliance**—strategies to train, educate, and enforce governance policies
- **Employee and manager responsibilities**—specifying the roles and responsibilities of everyone in supporting your open source governance strategy
Open source governance services available from HP

Addressing the risks and challenges surrounding open source software with an effective governance strategy may seem like a daunting task. Rest assured, you are not alone. Leveraging the experience we have from developing our own governance program, HP offers a set of consulting services to help you target the issues within your own enterprise, develop a plan for addressing those issues, and implement a governance program tailored to your specific needs and objectives. Our services include:

Open Source Governance Workshop
The HP Open Source Governance Workshop is a one-day interactive workshop to guide your core open source team (designed for five to ten attendees) through the top issues of managing open source in the enterprise. The workshop is targeted at a cross-organizational audience, including auditing, legal, procurement, operational risk management, technology strategy, and line-of-business departments. We present an overview of the HP framework for open source governance policies, processes, and tools for governance automation, covering the following topics:

• Open source policy and guidelines—This session covers background and rationale behind various aspects of a corporate open source policy, including motivations and business justifications for and against the use of open source within an enterprise. In addition, the various aspects of participation in open source communities are discussed: employee participation on personal vs. company time, projects that are appropriate to open source—and ones that are not—and business reasons.

• Open source processes—During this session, we draw from our experience in running an internal open source review board and program office to provide details on various processes involved with open source compliance and governance.

• Legal aspects of OSS governance—This session provides details on a variety of legal considerations pertaining to working with open source software in the enterprise, including open source license characteristics and bridging the legal and technical communities.

Open Source Governance Assessment Service
The HP Open Source Governance Assessment Service is typically an 8-week consulting engagement designed to help you identify how and where open source software is used across your enterprise, and to establish a foundation for defining compliance requirements. The assessment service provides a gap analysis where your organization’s current practices are compared against industry best practices, and we offer a set of recommendations to address the identified gaps. Optionally, a financial impact analysis of the use of open source software in your organization can be included. The following format is used to deliver this service:

• Phase 1: project planning and initiation—This phase lays the foundation for your open source governance program by reviewing your current documentation and policies, establishing a project team, and formalizing a project plan, which includes identifying critical success factors and metrics.

• Phase 2: data discovery—In this phase, we gather key information in regard to the licenses attached to the open source software used across your enterprise through a process of personal interviews and use of the HP license discovery tool.

• Phase 3: data analysis and open source maturity assessment—During the next phase, all the data gathered in Phase 2 is consolidated and analyzed, and a financial impact analysis is developed from the results. We also review the project status and conduct working sessions to determine your open source maturity level.

• Phase 4: develop recommendations and high-level roadmap—Based on the research and analysis performed, we then identify key open source initiatives for maturity improvement, develop a high-level plan for improving open source governance in your enterprise, and present our recommendations to your corporate management.
Open Source Compliance Service
The HP Open Source Compliance Service is an extended consulting engagement that works with your core open source team to develop open source policies, establish an open source program office, implement processes to manage open source in your enterprise, and conduct training. The Open Source Compliance Service is normally conducted as a follow-up engagement to the Assessment Service with the objective of implementing its recommendations. The processes implemented during this service will typically leverage the HP governance tools portfolio to discover, analyze, and monitor the use of open source in your organization on an ongoing basis.

Conclusion
As we have seen, there are numerous issues related to the acquisition, licensing, and distribution of open source software. Because of our deep involvement in the open source community, HP is highly sensitive to and knowledgeable about these topics. We leverage open source technology, both for internal consumption and for integration in our products; we support best-of-breed open source software from partners in our customer solutions; and we contribute code to the community on a regular basis to help fuel its growth. It is, therefore, incumbent on us to manage the risks associated with open source—for HP and for our customers.

Any enterprise using open source software today must recognize that it has this same responsibility. 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, ensure compliance with licensing, and protect against malware. Governance of open source software is the key to mitigating the many risks and enabling your enterprise to gain greater value from its development projects.

HP has developed a set of best practices and tools for open source governance that we now share with enterprises around the world. Through workshops and consulting engagements, we can work with your open source team to assess your current use of open source, plan and implement a governance program, and conduct training to educate employees and managers. By calling on HP, you can bring to your organization a wealth of knowledge and experience in open source that will help you avoid common pitfalls and move forward with an effective open source governance strategy.

By gaining a greater understanding of the issues associated with open source software, and by addressing those issues with a comprehensive governance program, you will put yourself in a stronger position to mitigate the risks and maximize the value of open source software for your enterprise.

For more information
For more information on how HP can help you address the risks and maximize the value of open source software for your enterprise, contact an HP representative, or visit: www.opensource.hp.com

To learn more, visit www.hp.com

© Copyright 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA1-4698ENW, September 2007