Free and Open Source Software Compliance: An Operational Perspective

Philip Koltun [a]

Director of Open Compliance Program, The Linux Foundation

DOI: 10.5033/ifosslr.v3i1.61

Abstract
FOSS compliance involves many operational considerations that go beyond legal matters and the purview of the Law Department. Compliance policies, processes, training, and tools enable a company to use FOSS effectively. Essential compliance elements include identification of FOSS used in products; review and approval of planned FOSS use; and satisfaction of license obligations. The Linux Foundation's Open Compliance Program provides many resources to assist with compliance.

Keywords
Compliance; Free and Open Source Software

Introduction

Free and open source software (FOSS) *compliance* refers to the aggregate of policies, processes, training, and tools that enables a company to effectively use FOSS and contribute to open communities while respecting copyrights, complying with license obligations, and protecting the company's intellectual property and that of its customers and suppliers.

Companies initiate open compliance programs for a variety of reasons. Sometimes, it's recognition that a new product will use FOSS and that compliance must occur. Sometimes, interest in increased community involvement sparks awareness of license obligations. Sometimes, a company has already distributed a product that uses FOSS and compliance concerns are raised internally by knowledgeable engineers or externally by the license enforcement community.

If we think of a force-field analysis for initiating a compliance program, the forces driving a company include newfound awareness of obligations; desire to collaborate; commitment to being a good corporate citizen; and community pressure. Forces that tend to restrain implementation of a

compliance initiative include inertia, lack of knowledge, lack of leadership, and lack of resources. See Figure 1.

Fig. 1: Force-Field Analysis for Compliance Program Implementation

Restraining forces can be overcome by education and advocacy from strategists and FOSS enthusiasts in a company. The Linux Foundation's Open Compliance Program provides training, white papers, tools, and other aids to overcome challenges posed by lack of knowledge and resources.[1]

For a product being distributed externally, compliance involves three core activities: identification of FOSS; review and approval of planned use of FOSS; and satisfaction of license obligations for the included FOSS. Each of these activities is discussed below.

Identification of FOSS

First, identification of all FOSS in a product comes from the dual processes of disclosure and discovery. With *disclosure,* engineers and product managers of the company and its external suppliers typically identify FOSS based on prior knowledge of where the code came from. *Discovery* refers to audits (either manual or automated) that are used to identify FOSS code and its origin.

Reliance only on disclosure can be problematic. Few products these days are written from scratch. Most evolve from legacy products and externally acquired source code (either FOSS or commercially licensed software), with new code being written to implement differentiating features and functionality. Sometimes millions of lines of code may be included in a product, some of it pre-dating the engineers currently working for the company. It's unlikely that any one individual or team will know all of the code and where it came from. So it is hardly surprising that disclosure alone would be incomplete or inaccurate.

1 http://www.linuxfoundation.org/programs/legal/compliance

Review and Approval

Reviewing and approving planned FOSS use is the second essential step in compliance, typically requiring a panel of skilled and knowledgeable individuals known as an Open Source Review Board (OSRB). An OSRB must review FOSS use in context, so a product architectural diagram will be needed to show how the software components (including FOSS) interface and interact. The OSRB examines licensing implications of the architecture, compatibility of components from a license perspective, and resultant license obligations. Therefore, an OSRB must incorporate the expertise of skilled software architects and licensing experts with direct insight into company product development plans and history. FOSS community contacts are also highly beneficial.

Someone should monitor whether the OSRB has the resources needed to provide adequate cycle time on review decisions. That is, given the nature and complexity of planned FOSS use, will it be possible to reach approval decisions in the timeframe needed by product teams? Metric collection can provide insight into the rate of reviews, the number of issues identified and their priority, and the closure rate.

Satisfaction of Obligations

The third essential step concerns satisfaction of obligations. Many organizational actions must come together to assure FOSS license obligations can be met. Obligation fulfillment typically involves inclusion of attributions, copyright notices, and license text along with the product when it is distributed externally. Providing complete and corresponding source code or an offer of source code may also be required, depending on the FOSS licenses involved. Individuals or teams responsible for product documentation and localization activities must perform necessary tasks to assure that documentation obligations are met.

As part of the process to satisfy source code obligations, the company should place into a software repository the complete source code corresponding exactly to each FOSS package used in a given product release. The complete source code may include any associated interface definition files, plus the scripts used to control compilation and installation of the executable. Verification activities should assure that source code used to produce product binaries has been cleansed of any inappropriate comments and that all FOSS packages in the product have been approved by the OSRB.

The company should also define a code distribution mechanism that satisfies the requirements of particular FOSS licenses. A web portal is often created to provide online access to source code used in company products, though other distribution mechanisms beyond a portal may be required. Responsibility for maintaining the portal must be assigned and staffed appropriately, and the portal should be organized in a clear and meaningful way to provide users easy access to products' licensing information and FOSS source code.

It's also crucial that the company responds to all external compliance requests for source code in a timely manner. Response actions should be given high priority and issues escalated to an appropriate level of management if there are problems with compliance. A company must establish a process for

responding to compliance requests promptly and fully and for tracking compliance requests to closure.

Compliance is an Operational Process

The foregoing discussion should illustrate that compliance involves many operational considerations that go beyond legal matters and the purview of the Law Department. Compliance problems, when they occur, are usually attributable to operational problems, not legal misinterpretations. Typical compliance problems include failure to provide source code (or an offer of source code) at all; providing incomplete source code or an incorrect version; omitting required attribution notices or doing so inaccurately; and so on. The root cause of these problems most likely traces to one or more disconnects involving people and processes: The engineers who know about the FOSS inclusion are disconnected from the people who understand the obligations. Or, the people who understand the obligations are disconnected from the people who manage product release and generate documentation. Or, the steps for FOSS review and obligation satisfaction are not integrated into the product development and release processes and schedule. And so on.

When a company distributes a product externally, it bears the responsibility for satisfying FOSS license obligations, including those for code obtained from third party suppliers. Compliance of third party software suppliers represents a special challenge for a company. Supplied code usually comes in the form of binaries rather than source, in order to protect the supplier's intellectual property. So the company lacks the ability to examine the supplier's source code for FOSS inclusion. Moreover, the company's business teams have specialized interests in the supplier and its software: Typically, Business Development is interested in differentiating features; Engineering is interested in obtaining the code and testing the functionality; Supply Chain is interested in the cost and the deal. Who will look out for FOSS inclusion and compliance?

As a result, a company must require FOSS disclosure and obligation satisfaction from its suppliers. A company should also satisfy itself about its suppliers' FOSS compliance practices. Does a supplier have a policy on FOSS use, compliance training for its teams, automated code scanning to facilitate discovery and recognition of FOSS, a procedure to prepare a FOSS bill of materials, and so on? Key questions a company must consider in regard to its suppliers include whether to insist on an automated FOSS code scan and the manner in which license obligations will be satisfied. The Linux Foundation's Self-Assessment Checklist can be used effectively to assess supplier compliance practices and engage suppliers in discussion about compliance.[2]

Ultimately, an effective compliance program must integrate compliance activities into day-to-day business processes so that identification, review and approval, and obligation satisfaction steps are routinely accomplished in time for product release. Key elements of a compliance program include company policy, employee training, assignment of compliance responsibility, staffing of the compliance function, and automation to enhance efficiency and accuracy.

When a company implements an effective compliance process, it benefits in numerous ways besides meeting its license obligations. A company engaged in compliance activities achieves a better

2 http://www.linuxfoundation.org/programs/legal/compliance/self-assessment-checklist

understanding of its product and platform content; an opportunity to optimize FOSS use; enhanced ability to engage in collaborative communities; and improvement of its product development practices. Notable among these development practices are improved configuration management, supplier management, and verification capabilities.

First Steps

First steps taken to implement a compliance program depend, of course, on the company's product plans and current situation. Figure 2 illustrates a typical sequence of actions.

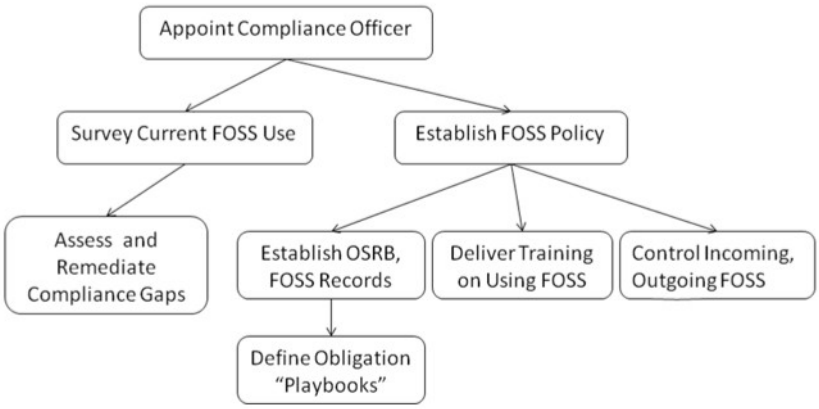

Fig. 2: Initial Actions in a Compliance Program

First and foremost, someone must bear overall responsibility for leading the compliance initiative and achieving product compliance. Commonly now, this person holds the title of Open Source Compliance Officer. Ideally, the Compliance Officer possesses insight into FOSS licensing and community interactions, software design, company product architecture and plans, and company business processes. Interpersonal relationships with key company decision-makers are also essential.

Even though compliance is a business function driven by Engineering and Product Management, attorneys nonetheless play an important contributory role and must be engaged as partners in the compliance undertaking. The Law Department typically advises on licensing and interprets FOSS licenses and their obligations. In most cases, engineers do not have time or expertise to read lengthy licensing texts and need a quick summary of commonly-used FOSS licenses that highlights the key compliance obligations. The Law Department also advises on licensing conflicts arising from planned use of software under incompatible licenses. They can help resolve issues that may be associated with the use of particular FOSS and advise and direct the engineering and product teams in the event of any compliance inquiries. Ultimately, the Law Department may have authority to stop product shipment in the event of any compliance issues that warrant such serious action.

Compliance Resources

The Linux Foundation's Open Compliance Program is the industry's only neutral, comprehensive software compliance initiative. By marshaling the resources of its members and leaders in the compliance community, the Linux Foundation brings together the individuals, companies and legal entities needed to expand the use of FOSS while decreasing legal costs and reducing fear, uncertainty, and doubt.

Inevitably, this short overview of compliance barely touches on important details of what must be done and how to implement those practices and avoid common pitfalls. Companies seeking greater insight into compliance practices can take Linux Foundation compliance training courses; download freely available Linux Foundation compliance white papers and the Self-Assessment Checklist; participate in the SPDX® working group; participate in the FOSSBazaar community and discuss compliance best practices; and access other helpful resources. More information can be found at http://www.linuxfoundation.org/programs/legal/compliance.

Conclusion

Compliance is a goal, but it is also the outcome of many interrelated activities and supporting processes, tools, artifacts, and infrastructure. The three fundamental elements of compliance consist of FOSS identification; review and approval of planned FOSS use; and satisfaction of obligations. But these core elements must be shored up by a company policy on FOSS use; training on compliance responsibilities and requirements; and other supports such as staffing, project management discipline, recordkeeping and automated tools. Essential processes must be defined and used regularly; skilled staff must be deployed to perform these processes; and the conditions must be established for a successful compliance program. Many helpful resources on compliance are available from The Linux Foundation's Open Compliance Program.

About the author

Philip Koltun *is director of The Linux Foundation's Open Compliance Program, which provides training, tools, and other resources to make FOSS license compliance ever-easier to achieve. Previously, he defined and implemented comprehensive open source compliance programs for Motorola and NAVTEQ, including policies and procedures, training, OSRB function, 3rd party supplier compliance, and compliance tool introduction.*