Establishing Free and Open Source Software Compliance Programs: Challenges and Solutions

By Ibrahim Haddad, Ph.D.

JULY 2010

Establishing Free and Open Source Software Compliance Programs: Challenges and Solutions

By Ibrahim Haddad Ph.D.

Executive Summary

This white paper is a second in a series that focus on the practical aspects of ensuring free and open source software (FOSS) compliance in the enterprise. The first paper entitled “FOSS Compliance: The Basics You Must Know”, available from the Linux Foundation web site[1], provided a discussion on the multi-source development model, the need for compliance, objectives and benefits, the consequences of non-compliance, possible compliance failures, how to avoid them and lessons learned.

This paper picks up from where the first paper left off and provides a discussion on the following topics:

- The elements of a successful compliance program that will allow a company to capture, govern and track all software components (proprietary, 3rd party commercial and FOSS) included in its commercial products.
- The list of common challenges related to establishing and maintaining compliance programs and how to overcome these challenges and ensure successful compliance program implementation

1 http://www.linuxfoundation.org/collaborate/publications

Introduction

FOSS initiatives and projects provide companies with a vehicle to accelerate innovation through collaboration with the global community of FOSS developers. However, accompanying the benefits of teaming with the FOSS community are important responsibilities: Companies must ensure compliance with applicable FOSS license obligations.

The first half of this paper discusses the elements of a successful compliance program that allows companies to capture, govern, and track all FOSS components included in their commercial products. The second half of the paper lists the common challenges companies face when establishing and maintaining their compliance programs and proposes various solutions to overcome these challenges.

Element of a Compliance Program

The compliance program provides a structure around all aspects of FOSS including selection, approval, use, distribution, audit, inventory, training, community engagement, and public communication.

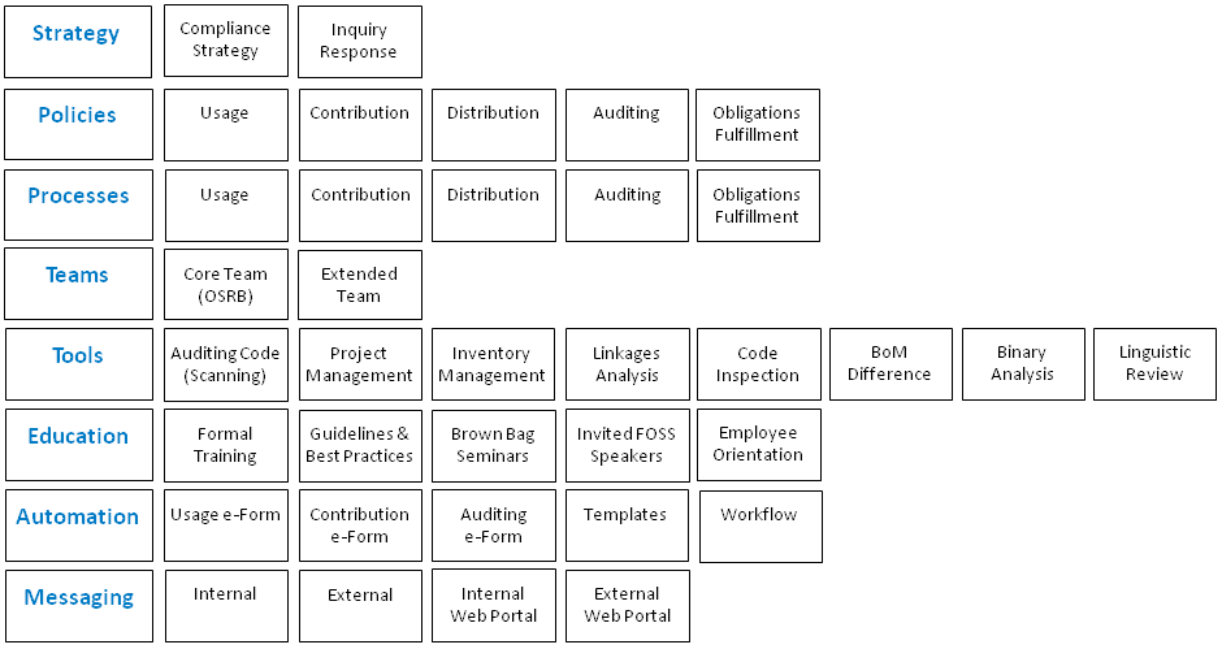

FIGURE 1. ESSENTIAL ELEMENTS OF A SUCCESSFUL COMPLIANCE PROGRAM

Figure 1 illustrates the core elements needed in a successful FOSS compliance program that includes:

- Strategy and inquiry response strategy
- Policies and processes for using, contributing, distributing, auditing FOSS and for fulfilling license obligations
- Compliance teams (core and extended)
- Tools to assist in compliance verification and assurance
- Educational programs and training
- Automation to ensure efficient program execution
- Messaging, internally within your organization and externally towards the FOSS community
- Relationships with the FOSS projects and FOSS organizations

In the following sections, we will provide a brief overview of each of these essential elements in a FOSS compliance program.

Compliance Strategy

A compliance strategy drives a business-based consensus on the main aspects of the policy and process implementation. If you do not start with that high-level consensus, driving agreement on the details of the policy and investments in the process tends to be very hard if not impossible. The compliance strategy establishes what must be done to ensure compliance and offers a governing set of principles for how personnel interact with FOSS. It includes a formal process for the approval, acquisition, and use of FOSS, and a method for releasing software containing FOSS or licensed under a FOSS license.

Inquiry Response Strategy

An inquiry response strategy establishes what must be done when the company receives a compliance inquiry or when the company's compliance efforts are being challenged. Several companies received negative publicity and/or were sued because they ignored requests to provide compliance information, did not know how to handle compliance inquires, lacked or had a poor compliance program, or simply refused to cooperate because they assumed the FOSS licenses are not enforceable. We know that none of these approaches is fruitful or beneficial to any of the parties involved. Therefore, companies should not ignore compliance inquiries, and instead, they should acknowledge the receipt of the inquiry, inform the reporter that they will be looking into it, and provide a certain date on when to expect a follow-up.

Informal compliance inquiries can include requests such as:

- A request for accessing source code following a written offer to provide source code licensed under GPL, LGPL and/or other licenses that require making such an offer to the end users
- A request for information regarding use of a specific FOSS project in a product
- A request for an update to the attribution and/or copyright notice that possibly was lacking or incomplete
- A request to provide missing files from the FOSS packages made available as part of meeting the license obligations

Figure 2 presents a sample process that illustrates the steps a compliance inquiry should go through from the time a company receives the inquiry until the inquiry is resolved. The following sub-sections describe what happens in each step of the compliance inquiry process.

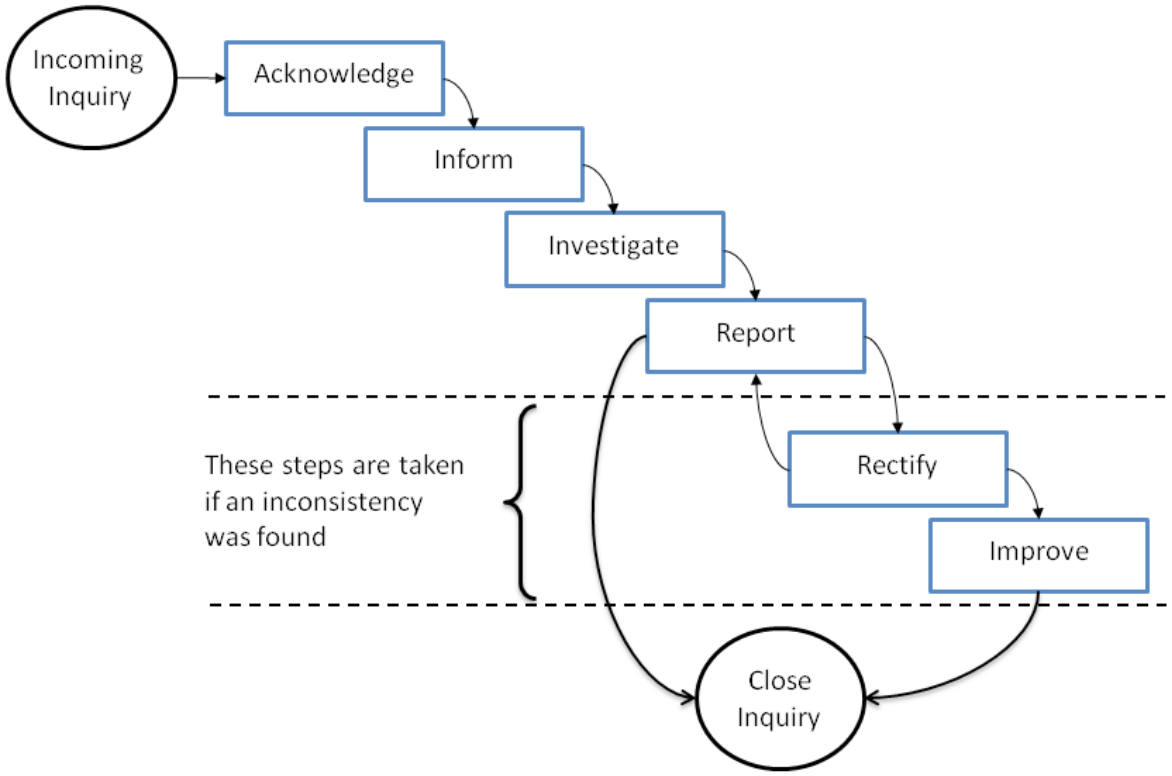

FIGURE 2. PROCESS OF RESPONDING TO INCOMING COMPLIANCE INQUIRIES

Acknowledge

Once you receive the compliance inquiry, you should reply informing the inquirer that you have received their email and that you will look into it and get back to them in a timely fashion. It is important to understand the reporter, their motivation and to verify if their accusation is accurate or even current. Furthermore, not every reporter understands licenses fully and sometimes there may be mistakes in their submissions. If you were missing information as submitted by the inquirer, you would request additional information from them to help you isolate the precise problem. The minimum set of information reported should include:

- The name of the product affected
- The name and version of the software component in question
- The reason why a violation is believed to exist
- A statement regarding what license this code is under

Inform

Companies must keep an open a dialog with the compliance inquiry reporter. As a company that maintains rigid compliance practices, you should highlight your compliance program and practices, and

show good faith efforts toward compliance. Inform the inquirer about your compliance program and practices and assure them that you will investigate their concern. It is also advisable to send updates of your internal investigation when they are available.

- Confirm you have received the report
- Confirm that you treat compliance inquiries seriously and consider achieving compliance as part of the development process
- Highlight your compliance program
- Inform the reporter that you are investigating and will report back on your findings within x number of days

Investigate

In this step, you investigate the reported allegation. Ideally, you can refer back to compliance records for the specific product and software component in question, review it, and verify that the compliance record agrees or disagrees with the inquiry.

Report

After concluding the internal investigation (within acceptable time delays) through the review of the compliance due diligence completed for the specific software component (or product) in question, you need to provide the reporter with the results.

Close Inquiry

If the compliance inquiry was a false alarm, you will close the compliance inquiry ticket without any further action after ensuring that the inquirer is satisfied with your response.

Rectify

If the investigation uncovers a compliance issue, you will report back to the inquirer with the assurance that you will take all the necessary steps needed to bring your product back to compliance while specifying a date by which you expect to complete this task. It is your responsibility to resolve the issue with the reporter, while being collaborative and showing good will. You need to understand the obligations under the applicable license and show how and how soon you will meet the obligations.

Improve

If there is a compliance issue, you will call for an OSRB meeting to discuss the case, learn how this non-compliance occurred, and improve existing process and practices to ensure that such errors do not happen again.

Policies and Processes

A policy is a set of rules for the use and management of FOSS in your organization. Processes are detailed specifications as to how a company will implement these rules on a daily basis. Compliance policies and processes govern the various aspects of using, contributing, auditing, and distribution of FOSS.

Figure 3 illustrates an example end-to-end compliance process that includes the various steps a software component goes through before the OSRB approves its acceptance in the build system and integration with the software product. We will have a separate paper that discusses policies and processes invoked when FOSS is included in a commercial product, in addition to a detailed discussion around the compliance end-to-end process.

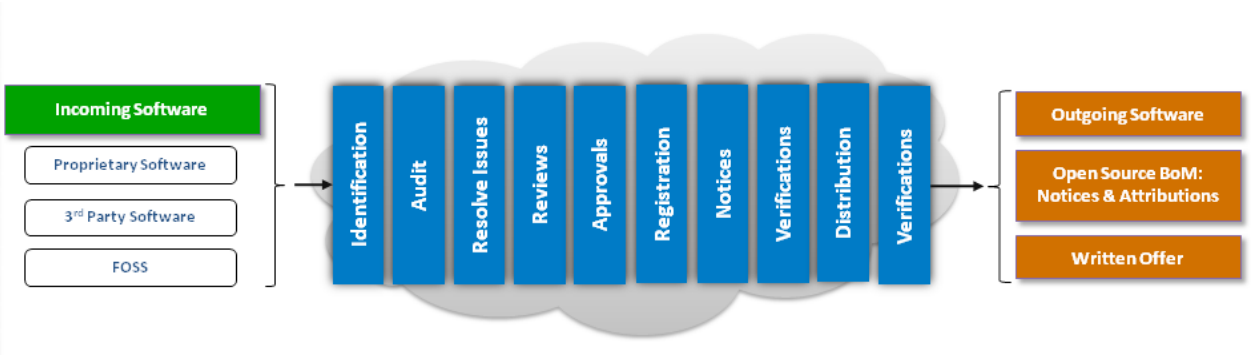

FIGURE 3. SAMPLE COMPLIANCE DUE-DILIGENCE PROCESS

Compliance Teams

Compliance teams consist of various individuals tasked with the mission of ensuring FOSS compliance. Figure 4 presents the individuals and teams responsible for achieving FOSS compliance.

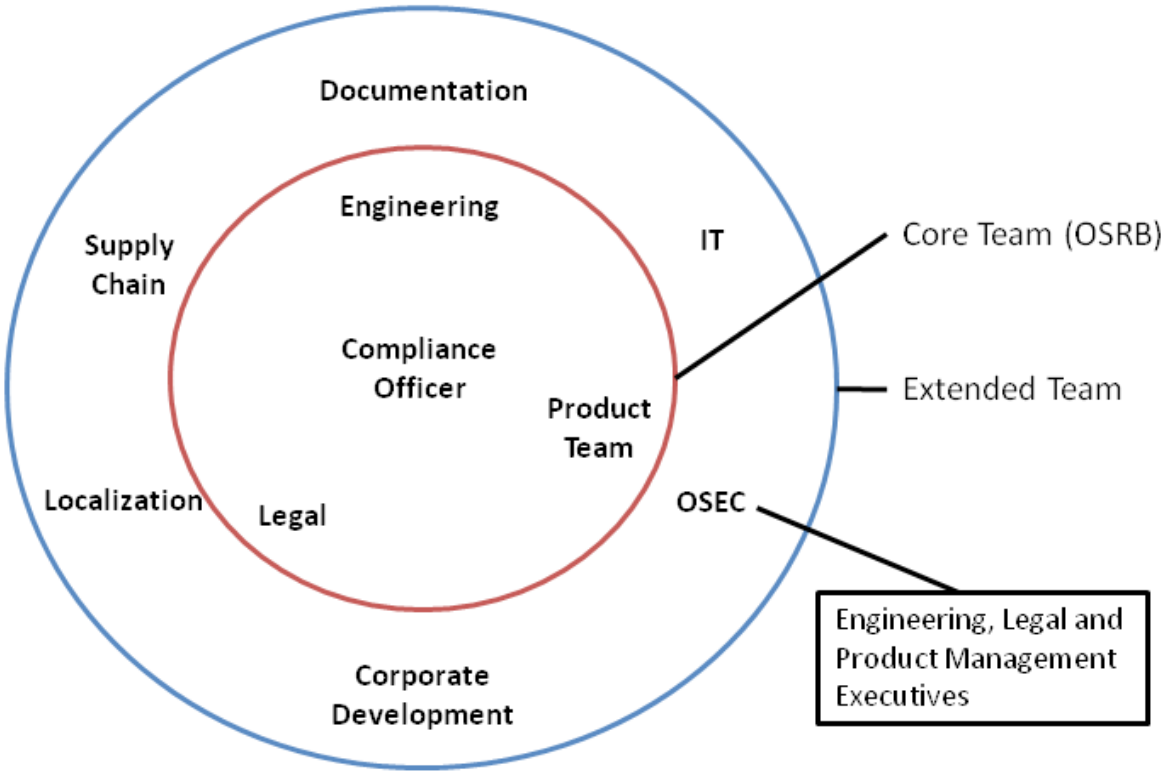

FIGURE 4. INDIVIDUALS AND TEAMS INVOLVED IN FOSS COMPLIANCE

There are two teams involved in achieving compliance: core team and extended team (Figure 4). The core team, often called the Open Source Review Board (OSRB), consists of representatives from engineering and product teams, one or more legal counsels, and the Compliance Officer. The extended team consists of various individuals across multiple departments that contribute on an on-going basis to the compliance efforts: Documentation, Supply Chain, Corporate Development, IT, Localization and the Open Source Executive Committee (OSEC). However, unlike the core team, members of the extended team are only working on compliance on-demand, based on tasks they receive from the OSRB. In a future paper, we will discuss in details the roles and responsibilities of each individual or team involved in ensuring FOSS compliance.

Tools

The OSRB deploys and uses several tools to automate and facilitate the auditing of source code and the discovery of source code and licenses. These tools include:

- A compliance project management tool to manage the compliance project, track tasks and resources
- A software inventory tool to keep track of every single software component, version, products that uses it, linkage method, and other important information
- A source code and license identification tool to identify source code included in the build system and their licenses
- A dependency checker tool to identify the interactions of any given software component with other software components used in the product
- A source code peer review tool to review the changes introduced to the original source code before it gets published as part of meeting license obligations
- A bill of material (BoM) difference tool to identify the changes introduced to the BoM of any given product given two different builds
- In a future paper, we will discuss these tools and explain how they contribute to ensuring FOSS compliance in a very efficient and accurate way.

Web Presence

Companies use portals in two directions: inwards, inside the company, and outwards as a window to the world and the FOSS community. The internal portal houses the compliance policies, guidelines, documentation, training, and hosts discussion forums, announcements, and access to mailing lists. The external portal offers a platform for the company towards the world, the FOSS community, and a venue to post all the source code of FOSS packages they use, in fulfillment of their license obligations.

Education

Education is an essential building block in a compliance program to ensure that employees have a good understanding of the policies governing the use of FOSS. All personnel involved in the development, quality assurance, release and maintenance of software need to understand the compliance program.

The goal of providing FOSS and compliance training is to raise awareness of FOSS policies and strategies and to build a common understanding around the issues and facts of FOSS licensing. Training also serves as a venue to publicize and promote the compliance policy and processes within the organization and to promote a culture of compliance.

There are formal and informal training methods; formal methods may include instructor-led training courses where employees have to pass an exam to pass the course; i nformal methods may include webinars, brown bag seminars, and presentations given to new hires as part of the new employee orientation session.

Informal Training

- Brown bag seminars: Brown bag seminars are usually presentations done during lunchtime by either company employee (in-house legal counsel, FOSS expert, compliance officer, etc.) or an invited speaker (most commonly a prolific FOSS developer). The goal of these seminars is to present and evoke discussions about the various aspects of incorporating FOSS in a commercial product. These sessions can also include discussions of the company's compliance program, policies, and processes.
- New employee orientation: In some instances, the Compliance Officer presents on company's compliance efforts, rules, policies, and processes to all new employees as part of the new employee orientation session. As such, on their first day, new employees would receive a 30 minutes training on FOSS and compliance. As a result, the new employees will have all the necessary information they need: who to talk to, what internal web site to visit, how to sign-up for FOSS and compliance training, etc.

Formal Training

Depending on the size of the company and the extent to which FOSS is included in its commercial offerings, the company can mandate their employees working with FOSS to take formal instructor-led courses and pass the evaluation. This section provides recommendations on four essential training courses:

- Introduction to FOSS: The course provides an overview of FOSS, its characteristics in comparison to proprietary software and freeware, and presents an in-depth discussion on the FOSS development model, the FOSS community, and FOSS licenses. In addition, the course examines the benefits and risks of adopting FOSS and using it in commercial products and introduces compliance and license obligations.
- Compliance Processes and Policies: This course provides necessary background information on compliance policies, processes, and procedures. The focus of the course will be on compliance practices and techniques adopted by the company to allow you to ship a product containing FOSS while meeting all license obligations, without putting the Company's intellectual property or that of your third party software providers at risk. Furthermore, the training provides a demonstration of how to fill out the OSRB form and provide information about available FOSS guidelines.
- Working with the FOSS Community: This course provide information on the FOSS development model, best practices on interacting with the FOSS community, driving contributions to mainline, cultural aspects and general advice to working with the community.

- Engineering Guidelines for Using FOSS: This course provides guidelines for system architecture and description of how the company's policies apply to particular engineering situations (user space versus kernel space, dynamic versus static linkage, device drivers, etc.).

Education

Engineers requesting to use or contribute to FOSS will be requested to submit forms built around templates designed by the Open Source Review Board (OSRB). An efficient, automated system includes electronic forms, templates, and workflows. This automation allows the OSRB to manage all "paper work" related to compliance electronically. We will discuss this topic, along with tools, in a separate future paper.

Messaging

Messaging is an integral part of any compliance program. It consists of internal and external messaging. The single most important recommendation with respect to messaging is to be clear and consistent in your messaging, whether it is internally explaining the company's goals and concerns around FOSS to your employees, or externally toward the FOSS community.

Compliance Challenges and Solutions

In the following sections, we will discuss the challenges companies face when establishing compliance program and offer recommendations on how can to overcome these challenges via an operational focused approach. Some of the most common challenges include:

1. Creating a compliance program while achieving the right balance between processes and product ship deadlines
2. Thinking long term, while executing short term
3. Communicating compliance
4. Establishing a clean software baseline for version 1.0 products
5. Maintaining compliance for evolving products
6. Institutionalizing and sustaining compliance efforts

Challenge #1: Creating a Compliance Program

The first challenge is to create the compliance program and its supporting infrastructure while achieving the right balance between following processes and meeting product ship deadlines. There are various approaches that can help overcome this challenge and assist in the creation of a lightweight program that is not seen as a burden to the development activities.

Proposed Solutions

Executive Support

It is important to have executive level commitment to compliance. An executive sponsor for compliance is a necessity to ensure its success and continuity.

Lightweight Policies and Processes

Processes and policies are important, however, they have to be light and efficient so that the engineering teams do not regard them as overly burdensome to the development process. You must avoid requiring engineers to spend more time than necessary on compliance activities. You need to establish two important building blocks: first, a simple and clear compliance policy, and second a lightweight compliance process, both well communicated across the company.

Mandate Basic Rules

As part of putting the compliance program in place, you will need to mandate some simple rules that everyone must follow, such as:

- Mandate the OSRB usage form for any FOSS: The OSRB usage form is the entry point into the compliance due diligence for any incoming FOSS or incoming third party software to the company. It is essential that engineers fill out the OSRB usage form for every FOSS project they intend to use in any product.
- Mandate compliance code inspections as part of the software development process
- Mandate design reviews as part of the existing software development process.
- Mandate architecture reviews and code inspections to understand how software componentsare inter-related and to discover license obligations that can propagate from FOSS to proprietary software.
- Mandate due diligence on software received from third party software providers: If a FOSS package is included in a third party component in a product, the engineer selecting the third party software, the third party software management team and the third party software vendor should work together to prepare the usage form for submission to the OSRB.

Integrate Compliance in the Development Process

The most successful way to establish compliance is to incorporate the compliance process and policies, checkpoints and activities as part of the existing software development process. This method ensures that compliance is part of the software development process and not an activity that is either an overhead to development, or an activity that is trying to catch up with development (in terms of speed and coverage).

Challenge #2: Long-Term Goals versus Short-Term Execution

Figure 1 described the essential elements needed for a successful compliance program. Some may be overwhelmed by the amount of work needed to implement such a complete program. In reality, it is actually not all that difficult because you do not have to implement everything mentioned in Figure 1 at the same time.

The priority of all companies is to ship the product on time while building and expanding their internal FOSS compliance infrastructure. Therefore, you should expect to build your compliance infrastructure as you go and keeping in mind its scalability for future activities and products.

Proposed Solutions

- Plan a complete compliance infrastructure to meet your long-term goals, and then implement the pieces needed for short-term execution. For instance, if you are just starting to develop a product that includes FOSS and do not have any compliance infrastructure yet, your immediate concern may be, for example, establishing a compliance team, process and policy, tools and automation,

and training your employees. Once you kick off these activities (in that order) and you have a good grip on the build system (from a compliance perspective), you can move to the other program elements.

- Establish lightweight policies and processes (discussed earlier)
- Incorporate compliance as part of the development process (discussed earlier)

Challenge #3: Communicating Compliance

Communication is essential to ensure the success of the compliance activities. There are two aspects of the communication activities: internal to the company and external towards the FOSS community and the industry.

Internal Communication

Companies need internal compliance communication to ensure that employees are aware of what is involved when they include FOSS in a commercial product and to ensure that they are educated about the company's compliance policies, processes, and guidelines. Internal communications can take one of several forms:

- All-hands meetings are a great venue for executives to show their support and endorsement to the compliance activities and to ask their employees to follow company policies and processes.
- Formal training mandated to all employees working with FOSS.
- Hosting brown-bag FOSS and compliance seminars are a successful way to bring additional compliance awareness.
- Establishing an internal FOSS portal that will host the company's compliance policies and procedures, FOSS related publications and presentations, mailing lists, and a discussion forum related to FOSS and compliance.
- Some companies issue a company-wide FOSS newsletter periodically that focuses on compliance and news around FOSS.

External Communication

Furthermore, companies need external compliance communications to ensure that the FOSS community is aware of their efforts to meet the license obligations of the FOSS they are using in their commercial product. External communications can take one of several forms:

- Web site dedicated for FOSS: The web site is a main channel for distribution of FOSS packages (and modification) and usually hosts a discussion forum or mailing lists.
- Reaching out and supporting FOSS organizations such as the Free Software Foundation: Such activities are important to help the company build relationship with FOSS organization, understand the roles of these organizations, and contribute to their efforts.
- Participation in FOSS events and conferences: Participation can be at various levels ranging from sponsoring an event, to contributing presentations and publications, or simply sending engineers to attend and meet FOSS developers and foster new relationships with the FOSS community members.

Challenge #4: Establishing Clean Software Baseline

One of the initial challenges with compliance programs is to find out exactly what FOSS is in use, how it is licensed and where in your products or platform it is being used. Furthermore, the challenge revolves around establishing a clean software baseline for your product or software platform. This is an intensive activity over a period of time that can extend for months depending on how soon you started the compliance activities in parallel to the development activities.

Proposed Solutions

Companies achieve initial compliance through the collection of the following activities:

- Early submission and review of OSRB usage forms
- Audits on the source code
- Due diligence on the use of FOSS by third party software providers
- Design review and code inspections to analyze the interaction between FOSS, proprietary code and third party software components
- Update documentation to inform users how to obtain a copy of the FOSS

If a company fails to establish base line compliance, it is almost a guarantee that future revisions of the same product (or other products built using the initial base line) will have compliance issues.

- Offer a simple but enforced policies and light weight processes (discussed earlier)
- Include compliance checkpoints as part of the software development process (discussed earlier)
- Ensure availability of a dedicated compliance core team that consists of the Compliance Officer,
- Legal Counsel and Engineering representatives (we will discuss roles and responsibilities in a future paper)
- Utilize tools and automation to support efficient processing of compliance tickets

Challenge #5: Maintaining Compliance

There are several challenges in maintaining open source compliance, similar to those faced when establishing baseline compliance. In fact, many of the steps are the same but just on a smaller scale. Maintaining compliance is a continuous effort and is a comparatively small incremental effort that depends on discipline and commitment to build compliance activities into existing engineering and business processes.

Figure 5 illustrates the concept of incremental compliance whereby you need to ensure compliance of whatever source code changes that took place in between the initial compliant base line and the current version.

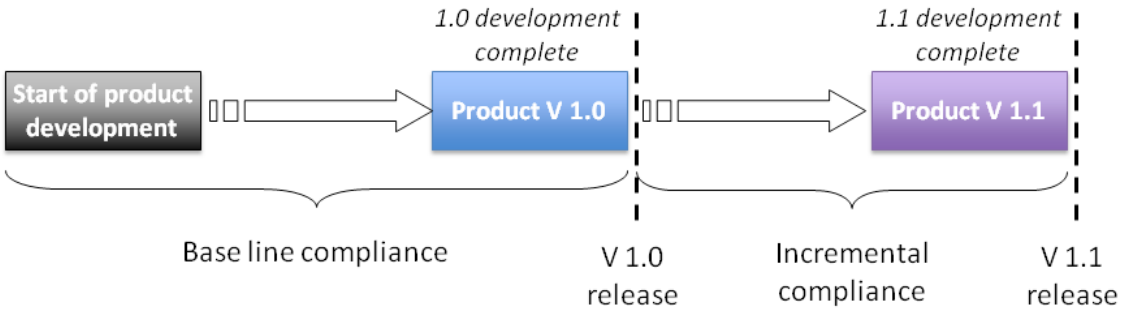

FIGURE 5. EXAMPLE OF INCREMENTAL COMPLIANCE

Proposed Solutions

Companies achieve initial compliance through the collection of the following activities:

- Early submission and review of OSRB usage form
- Continuous enforcement of the basic rules, e.g. engineers must receive approval before integrating a FOSS component in the build system
- Continuous audits of all source code integrated in the code base regardless of its origins (FOSS, third party or proprietary)
- Continuous improvements of tools used in ensuring compliance and automating as many activities as possible to ensure high efficiency in executing the compliance program

Challenge #6: Institutionalization and Sustainability

One of the challenges facing companies is to keep compliance activities going as the company grows and ships more products using FOSS components. Companies can take several steps to ensure the institutionalization of compliance within the company's development culture and to ensure its sustainability.

Proposed Solutions

- Sponsorship: Executive level commitment is essential to ensure sustainability of compliance activities. There has to be a company executive who is the compliance champion that ensures corporate support for the compliance function.
- Consistency: Achieving consistency across the company is key in large companies that consist of multiple business units.
- Measurement and analysis: Measure and analyze the impact and effectiveness of the compliance activities, processes, and procedures with the goal of studying the performance and improving the compliance program. This will help you communicate the productivity advantages that accrue from each program element when educating about the compliance program.

- Streamlining compliance processes: The scope and nature of a company's use of FOSS is dynamic, it is dependent on products, technologies, mergers, acquisitions, offshore development activities and many other factors. Therefore, it is a necessity to continuously review compliance policies and processes and introduce improvements. Furthermore, the FOSS license interpretations and legal risks continue to evolve. In such a dynamic environment, the compliance program must evolve as well.
- Enforcement: A compliance program is of no value unless it is enforced. A compliance program should include mechanisms for ongoing monitoring of adherence to the program and for enforcing policies, procedures, and guidelines throughout the company. One way to enforce the compliance program is to integrate it within the software development process and ensure that a certain percentage of the employees' performance evaluation depends on how well they are committed to FOSS compliance.
- Staffing: ensure propose staffing is allocated to the compliance function as well as adequate compliance training provided to every employee in the organization.

Conclusions

In this paper, we provide an overview of the various elements that contribute to the success of FOSS compliance and discuss top challenges that a company has to deal with when establishing and maintaining their compliance programs and how to overcome these challenges.
This series of papers aims to increase public awareness of the various issues surrounding FOSS compliance from an operational perspective, and does not aim to provide a legal discussion on the topic. Compliance management, or compliance due diligence, consists of a set of actions that control the intake and distribution of FOSS used in commercial products. The result of compliance due diligence is an identification of all FOSS used in the product and a plan to meet the FOSS license obligations. This topic will be discussed in a future paper. Stay tuned.

Acknowledgements

The author would like to express his gratitude to Karen Copenhaver (Legal Director of the Linux Foundation and Partner in Choate, Hall & Stewart LLP 's Business & Technology practice) for her reviews and valuable input.

About the Author

Ibrahim Haddad is Director of Technology and Alliances at the Linux Foundation focusing on Mobile Linux initiatives and advancing the Linux platform for next-generation mobile computing devices.