» The Open Compliance Program

Free and Open Source Software Compliance: Who Does What

A Guide to the Roles and Responsibilities of Individuals and Teams Involved in Ensuring FOSS Compliance

By Ibrahim Haddad (Ph.D.), The Linux Foundation

A White Paper By The Linux Foundation
http://www.linuxfoundation.org

Introduction

Ever since companies started integrating FOSS in their products, there has been the need to ensure compliance with applicable FOSS licenses. Different companies have used various ways to structure their teams responsible for fulfilling this function. Some companies have opted for a centralized team (Open Source Program Office) lead by an individual who has engineering, legal and operational experience. Other companies have opted for a cross functional team that consists of a dedicated Open Source Compliance Officer who has access to various individuals and teams that contribute to the compliance effort without being part of a centralized team. In this paper, we examine the later model of FOSS compliance team and discuss the roles and responsibilities of individuals and teams involved in the compliance process.

FOSS Compliance

FOSS compliance means that users of FOSS must observe all the copyright notices and satisfy all the license obligations for the FOSS they use in a commercial product. Companies using FOSS in commercial products must exercise due diligence to comply with the terms of FOSS licenses while at the same time protecting their intellectual property, and that of 3rd party suppliers, from unintended disclosure.

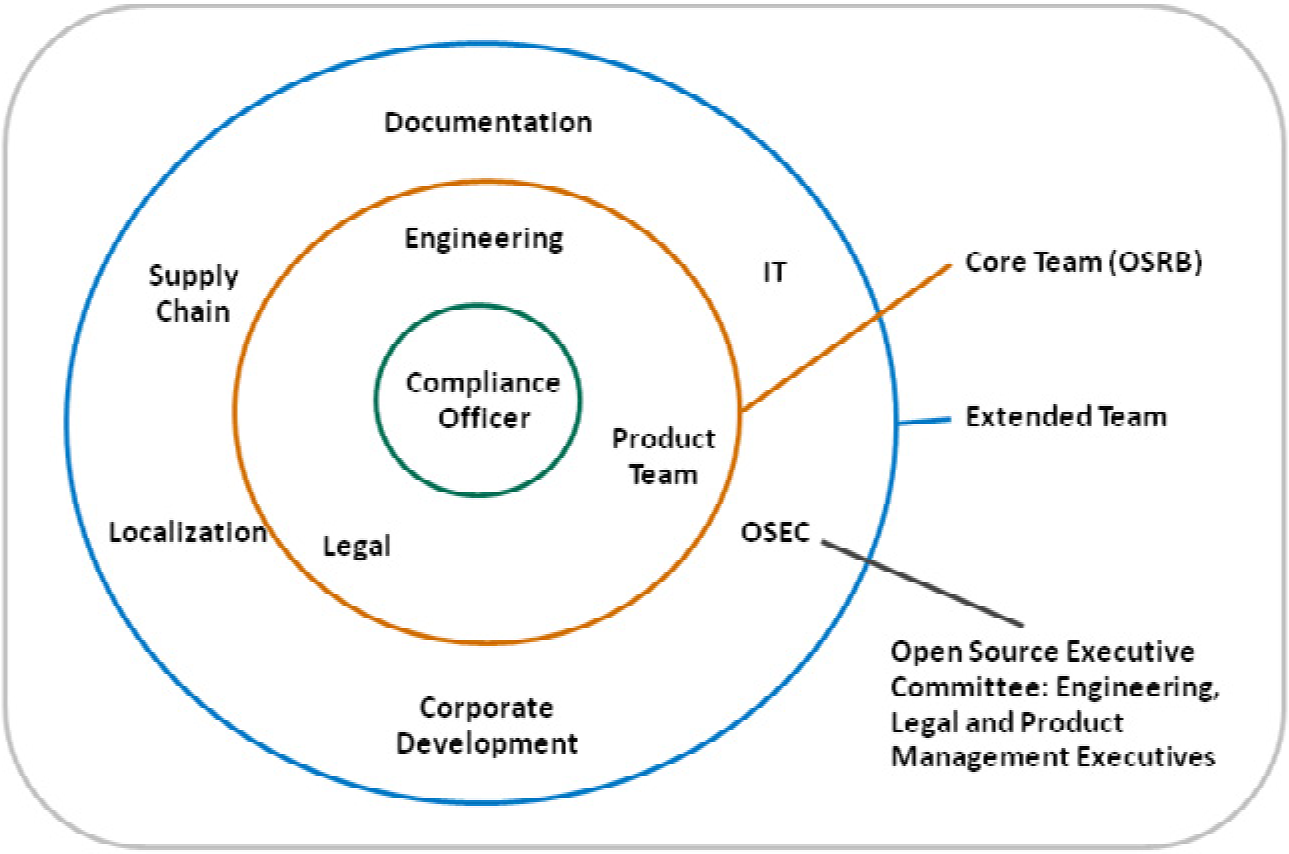

Figure 1: Teams and individuals involved in FOSS compliance

Figure 1 presents a break down of the different departments responsible for achieving FOSS compliance. There are two teams involved in achieving compliance: core team and extended team. The core team is called the Open Source Review Board (OSRB) and 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 an as-needed basis, based on tasks they receive from the core team or the OSRB.

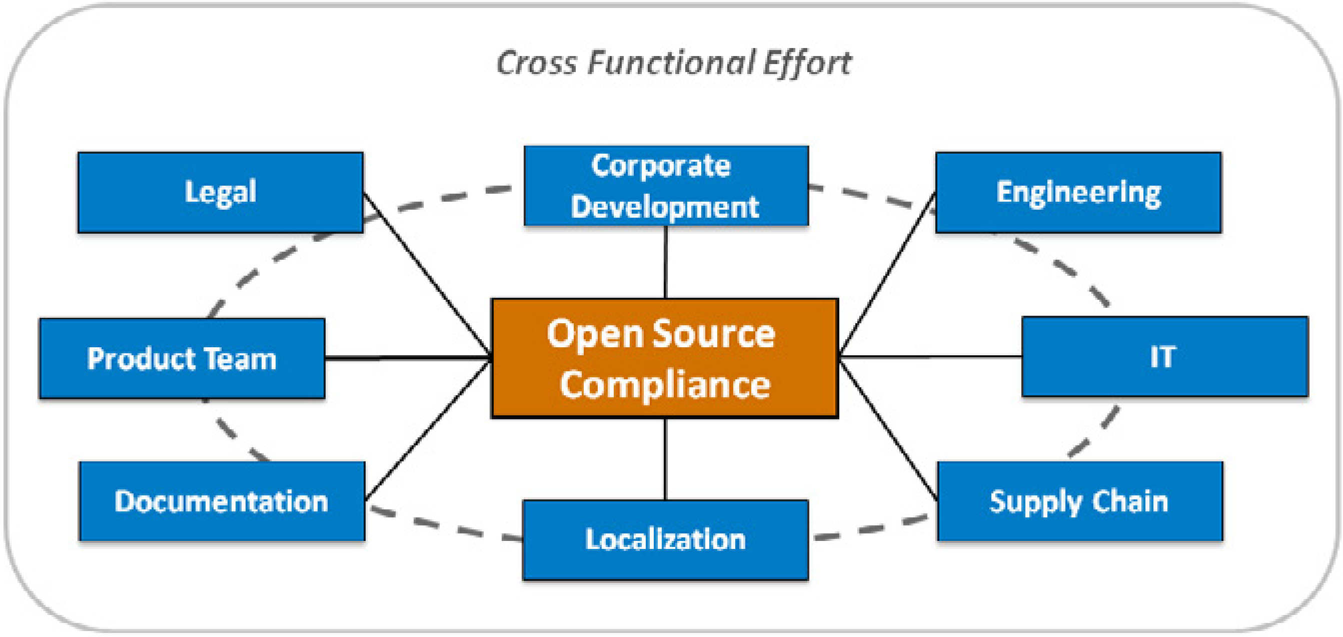

Figure 2: FOSS compliance is a cross functional effort

Open Source Review Board

Mission

The mission of the OSRB consists of:

1. Ensuring compliance with both third party software and FOSS licensing obligations
2. Facilitating effective usage of FOSS in commercial products within the company
3. Protecting product differentiation while complying with FOSS licensing obligations
4. Ensuring that FOSS license obligations do not extend to proprietary software or third party software

OSRB Participants

Members of the Core Team (OSRB)	Primary Responsibilities
Legal Representative	• Review and approve usage, modification, distribution of FOSS • Provide legal guidance • Contribute to creation of the FOSS training • Contribute to creation and improvement of the compliance program • Review and approve content of web portals in relation to compliance • Review and approve the list of obligations to fulfill for each software component included in a product • Sign off on product release from a compliance perspective
Engineering and Product Team Representative	• Follow compliance policies and processes • Integrate compliance practices in the software development process • Contribute to improving the compliance program • Follow technical compliance guidelines • Respond quickly to all compliance related questions • Conduct design, architecture and code reviews • Prepare FOSS packages for distribution • Sign off product release from a compliance perspective
Compliance Officer[1]	• Drive all compliance activities • Coordinate source code scans and audits • Participate in engineering reviews, code inspections, distribution readiness assessment • Coordinate distribution of FOSS packages • Contribute to creating compliance training • Contribute to improving the compliance program • Contribute to the creation of new tools to facilitate the automation and discovery of FOSS in the development environment

Table 1: Primary responsibilities of the core compliance team

Responsibilities

The OSRB responsibilities include the following:

1. Compliance End-to-End Management

The OSRB is responsible for establishing the end-to-end compliance process which covers all aspects related to using FOSS in a commercial product in addition to creating and maintaining compliance policies, processes, guidelines, templates and forms used in the compliance program.

[1] In most companies, the Compliance Officer is called Director of Open Source, Director of Open Source Program Office, Director of Open Source Management or variation of these titles. The person in any of these roles is responsible for Open Source strategy, compliance and driving contributions. However, for the purpose of this paper, we will only focus on the compliance aspect and therefore call the person in this role a Compliance Officer.

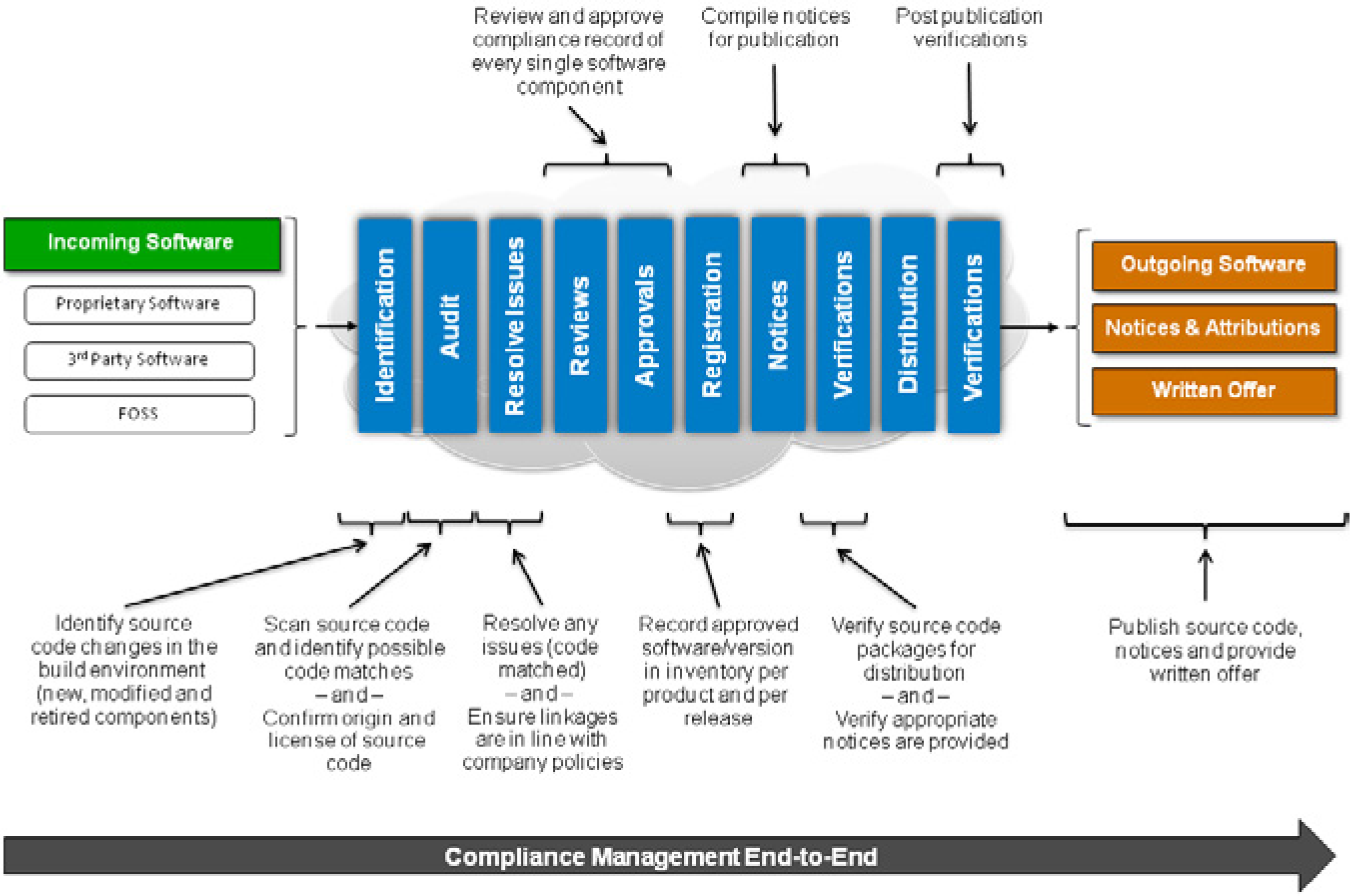
Review and approve compliance record of every single software component
Compile notices for publication
Post publication verifications
Incoming Software
Proprietary Software
3rd Party Software
FOSS
Identification
Audit
Resolve Issues
Reviews
Approvals
Registration
Notices
Verifications
Distribution
Verifications
Outgoing Software
Notices & Attributions
Written Offer
Identify source code changes in the build environment (new, modified and retired components)
Scan source code and identify possible code matches – and – Confirm origin and license of source code
Resolve any issues (code matched) – and – Ensure linkages are in line with company policies
Record approved software/version in inventory per product and per release
Verify source code packages for distribution – and – Verify appropriate notices are provided
Publish source code, notices and provide written offer
Compliance Management End-to-End

Figure 3: Example end-to-end compliance process

End-to-End Compliance Process

The sample end-to-end compliance process (Figure 3) involves the following:

1. Identifying all software planned for inclusion in the product
2. Scanning and auditing all the source code components
3. Resolving any identified issues as part of the scan and audit activity
4. Reviewing the compliance record by Legal, Engineering and the Compliance Officer
5. Getting the approval of the OSRB to include the specific software component in the product
6. Registering the approved software component in the software inventory system
7. Compiling all the obligations and notices related to the use of FOSS
8. Performing a pre-distribution verification of all previous steps
9. Distributing any applicable software components and making available applicable notices
10. Performing a post-distribution verifications

The detailed responsibilities of the OSRB include:

- Review incoming requests from engineering and product teams for using FOSS and determine approval
- Perform audits on all software included in the product which involves the following tasks:
  - Run the source code scanning tool over the software base
  - Analyze the results and resolve all the possible matches and licensing conflicts as flagged by the scanning tool
  - Create the final audit report and ensure that all identified issues have been closed

  Depending on the size of the company, the auditing responsibilities can be assigned to the OSRB or to an auditing team that reports to the compliance officer.
- Perform architecture review to analyze the interaction between the FOSS source code, proprietary code and third party source code. The goal of this review is to ensure that architectural guidelines are respected and that the interactions between FOSS, proprietary and third party software are within the acceptable legal guidelines.
- Perform linkage analysis review to determine if any FOSS license obligations migrate to proprietary or third party software.
- Perform code inspections as part of the pre-distribution verification to ensure that FOSS license, copyright notices have been intact, and that engineers have updated the change logs to reflect the changes introduced to the source code
- Compile a list of license obligations that must be for using the FOSS in question and pass it to appropriate departments for fulfillment. Once the OSRB has approved the usage of FOSS in a product, as part of the approval process, the OSRB compiles the list of obligations and passes it to the various other individuals and teams to ensure its fulfillment. As part of the pre- distribution process, the OSRB performs final checks before the product ships, including verifying the fulfillment of obligations.
- Sign off on product distribution from a FOSS compliance perspective

2. Training

The OSRB is responsible for developing and offering FOSS and compliance training to ensure that:

- Employees have a good understanding of the company's FOSS policies and compliance practices.
- Employees are educated on some of the most common FOSS licenses and the issues surrounding using FOSS in commercial products.

In addition, the OSRB provides guidance on FOSS questions incoming from company staff and engineers.

3. Web Presence

The OSRB hosts the FOSS internal and external web portals. The internal portal houses the compliance policies, guidelines, documentation, training, and may also host forums for discussions, announcements and provide access to mailing lists. The external portal offers the company a window to the world and the FOSS community and a venue to post all the source code of FOSS packages they use, in fulfillment of their license obligations.

4. Compliance Inquiries

The OSRB is responsible for responding to compliance inquiries received by the company in relation to FOSS compliance. Figure 4 illustrates a sample process a compliance inquiry might go through. We discussed this topic in an earlier paper. As a reminder, companies should not ignore compliance inquiries. 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.

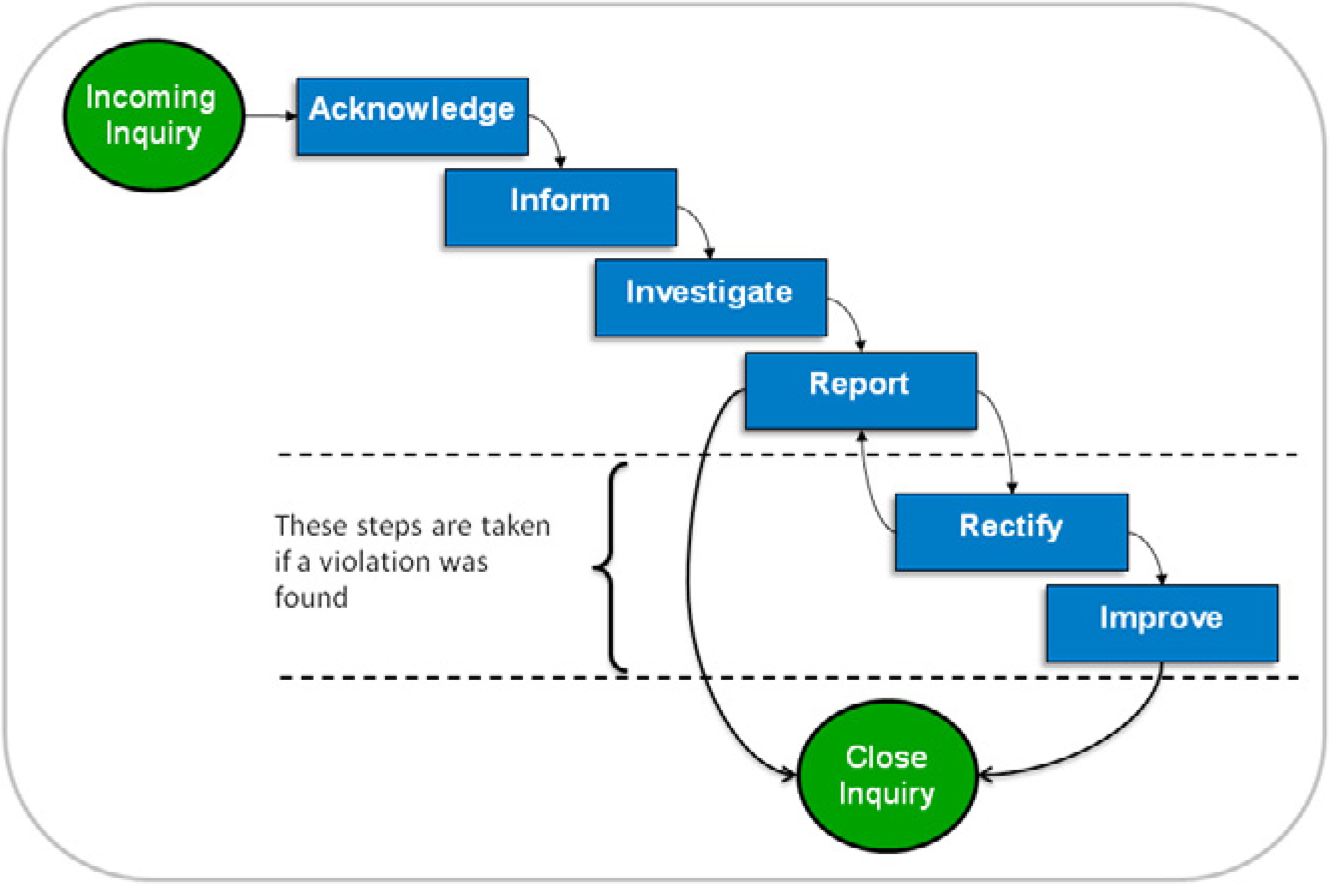

Figure 4: Example of a compliance inquiry response process

5. Updating Documentation

The OSRB updates end-user documentation to ensure appropriate notices are provided to consumers about FOSS included in the product along with a written offer on how to obtain the source code when applicable. An example of a written offer that the OSRB would add to the product document would look as follows:

> *To obtain a copy of the source code being made publicly available by FooBar, Inc. ("FooBar") related to software used in this FooBar product ("Product"), you should visit http://opensource.foobar.com or send your request in writing by email to opensource@foobar.com or by snail mail to:*
>
> *FooBar Inc.*
> *Attention: Open Source Inquiries*
> *Street Address*
> *City, State, Postal Code*
> *Country*

6. Tools

The OSRB deploys new tools to be used as part of the compliance infrastructure that will contribute to making the compliance work more efficient and highly automated. Table 2 provides examples of tools that can be used by a FOSS compliance program:

Tool	Benefits
Project Management Tool	• Track progress of every compliance ticket • Assign and track tasks
Source Code Scanning and Identification Tool	• Scan source code for possible matches with FOSS • Identify licenses of scanned source code • Create a bill of material of scanned code
Dependency Checker Tool	• Identify linkages made by software components both at static and dynamic levels
Bill of Material Difference Tool	• Identify changes to a bill of material between two releases of the same product
Binary Scanning Tool	• Execute a brute force scanning for binaries with unknown source • Identify possible matches with open source projects
Code Janitor Tool	• Clean the source code from any comments that were left unintentionally. Some companies call this process a linguistic review

Table 2: Tools used to aid in ensuring FOSS compliance

We will discuss these tools in a separate paper focused on this specific topic.

7. Releasing IP

The OSRB works with the OSEC to determine whether the company needs to distribute corresponding source code disclose or take on other obligations such as a patent non-assert, as part of using FOSS.

FOSSology

The FOSSology Project is a FOSS project built around an open and modular architecture for analyzing software. Existing modules include license analysis, meta data extraction, and MIME type identification. FOSSology analyzes a given set of software packages, and reports items such as the software licenses used by these packages.

Legal Representative

The Legal representative is a member of the OSRB and provides legal advice and guidance to engineering teams on FOSS legal questions and issues. The Legal representative must approve the usage of a FOSS after reviewing the compliance ticket and evaluating the risk factors based on the feedback provided by engineering and the compliance officer. Other than the responsibilities defined as part of its OSRB role, the Legal representative carries the following responsibilities:

1. Advise on Licensing

The OSRB Legal representative interprets FOSS licenses and their obligations, and provides FOSS license advice to engineering and product teams. In most cases, engineers do not have time to read lengthy licensing text and need a quick summary of most used FOSS licenses that highlights the key points. It has proven to be very helpful when Legal provided such sheets for FOSS licenses that describe very briefly for each license, the license grant, the limitations and obligations. Legal representative also provides advise on licensing conflicts in relation to incompatible or conflicting license obligations.

License Compatibility

As mentioned earlier, the Legal Counsel provide advice on license compatibility issues. As example of license compatibility, as illustrated at the Free Software Foundation web site (http://www.fsf.org/licensing/licenses), is the following:

> A license p is compatible with a license q (or is q-compatible) if
> A work licensed under p can be distributed under the terms of q.

A practical example:

> The X11 license is compatible with the GPL version 2, because works licensed under the X11 license, can be distributed under the terms of the GPL.

2. Resolve IP Issues Associated With the Use of FOSS

The OSRB Legal representative works with OSEC to review and approve the release of software under FOSS terms or the release of proprietary source code as FOSS.

3. Approve updates to product documentation with respect to FOSS notices

The OSRB Legal representative updates the corporate end user license agreement to include appropriate references to FOSS. Commercial products are distributed under an end user license agreement. Legal must update that specific end user license agreement to reflect that the product contains FOSS and as part of the agreement provide information on how the end user can contact the company to receive information on how to access the source code of applicable FOSS (such as GPL source code).

Engineering and Product Teams Representative

Engineering and product teams may have one or more representatives that participate in the OSRB and track down all compliance related tasks (sometimes called tickets) assigned to engineering. In parallel, engineering and product teams have several responsibilities with respect to FOSS compliance:

1. Submit Requests to Use FOSS

The engineering and product teams decide what external software to bring into the product baseline, including third party and FOSS. Their primary responsibility from a compliance perspective is to submit complete OSRB usage forms for any FOSS that is planned for inclusion in a product. The OSRB usage form provides information regarding the open source project and describes the intended use of the FOSS in question and helps construct and maintain a good record of software origin.

2. Follow Technical Compliance Guidelines

The engineering and product teams should follow the OSRB’s technical guidelines to architect, design, and implement source code. The OSRB guidelines typically cover:

- Common mistakes and how to avoid them
- Rules to follow when using libraries to avoid linkages issues that might arise
- Development in kernel space versus user space
- Specific engineering situations that are applicable to FOSS compliance

3. Conduct Design Reviews

Engineering teams should continuously conduct design reviews to discover and remedy any compliance issues in a timely manner. The Compliance Officer drives the design reviews and invites different engineering participants depending on the software component in question.

4. Cooperate With OSRB

Engineering teams must respond promptly to provide information requested by the OSRB and be prompt in closing internal compliance tickets.

5. Maintain a Change Log in Each Modified FOSS

As part of meeting the FOSS license obligations and depending on the FOSS license in questions, some licenses impose the obligation of providing a change log that describes the changes that were introduced to the FOSS package (such as those licensed under the GPL). An example of a change log at the beginning of the source code file looks as follows:

```
/*
* Date          Author            Comment
*
* 01/05/2010    Ibrahim Haddad    Fixed memory leak in play_record()
*/
```

Some companies prefer not to include the name of their employees in change log files. In that case, the change log file would look like:

```
/*
* Date          Author            Comment
*
* 01/05/2010    Foobar Inc.       Fixed memory leak in play_record()
*/
```

6. Prepare Source Code Packages for Distribution

Engineering teams prepare the source code packages that will be distributed to source code requests as part of meeting the FOSS license obligations, in addition to any build scripts or utilities needed to build the FOSS that corresponds to the binaries in the software release.

7. Integrate Compliance Milestones as Part of the Development Process

This exercise take places in collaboration with the OSRB and the Compliance Officer.

8. Take FOSS Training

All engineers must take the available FOSS training. 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 and the business and legal risks of incorporating FOSS in products. Training also servers as a venue to publicize and promote the compliance policy and processes with the organization and to promote a culture of compliance. There are formal and informal training methods: formal methods such as instructor-led training courses where employees have to pass a knowledge exam to pass the course. Informal methods include webinars, "brown bag" seminars and presentation given to new hires as part of the new employee orientation session.

9. Monitor the FOSS projects

The goal with this activity is to determine whether any bug fixes or security patches have become available and take responsibility for updating the FOSS component used in the product.

Software Freedom Law Center – Practical Guide to GPL Compliance

On August 26, 2008, the Software Freedom Law Center published a guide on how to be compliant with the GNU General Public License (GPL) and related licenses. The guide focuses on avoiding compliance actions and minimizing the negative impact when enforcement actions occur. It introduces and explains basic legal concepts related to the GPL and its enforcement by copyright holders. It also outlines business practices and methods that lead to better GPL compliance. It also recommends proper post-violation responses to the concerns of copyright holders. The guide is available from http://softwarefreedom.org.

Compliance Officer

The compliance officer, also called OSRB Chair, chairs the OSRB and manages the overall compliance program. The compliance officer must possess the following expertise:

- Solid understanding of FOSS licenses and obligations to discuss with legal counsels
- Knowledge of industry practices (FOSS compliance and FOSS development model)
- Knowledge and experience in establishing corporate wide programs, policies and processes
- Technical knowledge and depth to be able to discuss with engineers
- Historical perspective on FOSS
- Knowledge of FOSS community consensus and practices
- Contacts in the FOSS community and in the FOSS organizations that could be called upon for clarification

In addition to the responsibilities associated with participation in the OSRB, the Compliance Officer carries the following duties:

- Drives the compliance due diligence end-to-end process and acts as the compliance program manager ensuring all compliance related tasks are resolved and there are no compliance issues blocking product ship
- Coordinates source code scans and drive all auditing issues to closure
- Participates in engineering design reviews, code inspections and distribution readiness assessment to assure that the engineering and product teams follow all compliance processes and policies and conforms to the approved OSRB usage form
- Coordinates the source code distribution of FOSS packages with engineering and product team, including preparing and verifying distribution checklist for each FOSS package
- Acts as liaison between OSEC and OSRB
- Escalates compliance issues to OSEC
- Acts as liaison between the engineering and product teams and the OSRB and OSEC in regard to usage plan approval processes

- Reports on compliance activities to the OSEC including flagging any issues that stand in the way of shipping a product

FOSS Compliance Extended Team

The extended team consists of various individuals and teams that act as supporting functions to the OSRB and contributing to the achievement of compliance.

Members of the Extended Team	Primary Responsibilities
Open Source Executive Committee (OSEC)	• Decide on FOSS strategy • Review and decide on the approval to release IP • Review and decide on the approval to release proprietary source code under a FOSS license
Documentation Team	• Include FOSS license information and notices in the product documentation
Localization Team	• Translate FOSS license information and notices in the product documentation
Supply Chain Team (Business Development)	• Mandate third party software providers to disclose FOSS in what is being delivered • Assist with licensing-in third party software that is bundled with FOSS packages
IT	• Provide support and maintenance for the tools and automation infrastructure used by the compliance program • Create new tools based on OSRB request
Corporate Development	• Request FOSS compliance to be completed before a merger or an acquisition • Request FOSS Request FOSS compliance to be completed when receiving source code from outsourced development centers or third party software vendors

Table 3: Primary responsibilities of the extended compliance team

Open Source Executive Committee

The Open Source Executive Committee (OSEC) consists of engineering, legal and product marketing executives in addition to the Compliance Officer. The OSEC is responsible for setting the FOSS strategy, reviewing and approving licensing proprietary source code under a FOSS license.

Documentation

The documentation team is responsible for ensuring the inclusion of a written offer to provide source code for included FOSS and that appropriate notices (copyrights and attributions) are included in the product documentation.

Localization

The localization team is responsible for translating the FOSS licenses and notices into the supported languages depending on the countries in which the product will be available. The industry practice is to keep FOSS licenses in their native language. The Free Software Foundation (FSF) does not provide or approve any translations of the GNU GPL, LGPL, AGPL, and FDL into other languages. The reason is that verifying the translation is a difficult and expensive task and often involves the help of bilingual lawyers in other countries. In addition, if a translation error occurs, the results could be catastrophic.

If you want to provide translations of FOSS license, it is recommended that you label these translations as unofficial. In this regard, the FSF gives permission to publish translations of the GNU GPL, LGPL, AGPL, and FDL into other languages on two conditions:

1. The translations must be labeled as unofficial to inform people that they do not count legally as substitutes for the authentic version
2. You agree to install changes at FSF's request, if they identify that changes are necessary to make the translation clearer

According to the FSF, to label translations as unofficial, you need to add the following text at the beginning, both in English and in the language of the translation. Replace "language" with the name of that language, and "GNU General Public License" and "GPL" with the name and abbreviation of the license you are translating, if it is not the GPL:

> *This is an unofficial translation of the GNU General Public License into language. It was not published by the Free Software Foundation, and does not legally state the distribution terms for software that uses the GNU GPL—only the original English text of the GNU GPL does that. However, we hope that this translation will help language speakers understand the GNU GPL better.*
>
> *- Free Software Foundation (http://www.gnu.org/licenses/translations.html)*

Supply Chain

Supply chain personnel (including business development managers) are usually involved in moving software from the suppliers to your company. Therefore, it is important for companies to update their supply chain procedures (and deal flow process) to address the acquisition and use of FOSS to give them visibility into what FOSS is delivered to them by their software providers.

A best practice in this area is to mandate third party software providers to disclose (through a source code scan report) FOSS used in their offering along with a statement on how they plan to meet the applicable FOSS license obligations. If the third party software includes FOSS, the company's supply chain personnel must ensure that FOSS license obligations are satisfied since this responsibility transfer to the company as distributor of a product that includes FOSS. It is not sufficient to point at the supplier and inform the FOSS community that meeting FOSS license obligations is the responsibility of the supplier. Therefore, companies must know what goes into all of the product's software, including software provided by outside suppliers.

Furthermore, agreements relating to outsourced development of software should also be updated to reflect compliance procedures and to ensure that other provisions of these agreements. Supply chain personnel should mandate that all source code received from outsourced development centers must go through the compliance process to discover all FOSS being used and ensure proper actions to fulfill license obligations.

IT

IT provides support and maintenance for the tools and automation infrastructure used by the compliance program. This includes the servers hosting the various tools, the tools themselves, mailing lists and web portals. In addition, IT may get requests from the OSRB to develop tools that will be used to improve the effectiveness or efficiency of the compliance activities.

Corporate Development

Company policies regarding merger and acquisition transactions need to be updated to account for FOSS. If a company is considering an acquisition, it should structure its compliance program so that it can offer a level of disclosure and representations that will be requested by the acquirer. Corporate development must mandate that source code be evaluated from a compliance perspective prior to any acquisition to avoid surprises that might derail discussions or affect the company's valuation. For the acquiring company, comprehensive code evaluation assures accurate valuation of software assets and mitigates the risk of unanticipated licensing issues undermining future value. In addition, the acquiring company may include provisions in the purchase agreement requiring the disclosure of FOSS that is subject to the transaction. Diligence practices should be updated to require FOSS disclosure and include guidance regarding the review of any disclosed FOSS and licenses.

Other areas where Corporate Development is involved with compliance are transactions such as spin-offs, joint ventures, strategic alliances and OEM distributor agreements. In some cases, the compliance due diligence may result a decision not to proceed with the transaction given that the compliance situation is far from ideal.

Conclusion

This paper provides a practical and detailed discussion on the roles and responsibilities of the individual and team responsibilities in a comprehensive program to ensure FOSS compliance. Our hope with this paper is to provide some insight on how to structure your FOSS compliance team to be as effective as possible and well integrated within the organization and not regarded as a separate entity adding overhead to the development process. The paper also has some indirect benefit of providing you with the areas of competence that you need to look for when you are hiring individuals to be part of the company's compliance efforts.

The next paper is this series will examine a detailed compliance process from software intake phase to releasing a product. Stay tuned!

Acknowledgment

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) and to Philip Koltun (The Linux Foundation Director of Open Compliance Program) for their reviews and valuable input.

About the Author

Dr. Ibrahim Haddad manages The Linux Foundation's Mobile Linux initiatives and works with the community to facilitate a vendor-neutral environment for advancing the Linux platform for next-generation mobile computing devices.

About the Open Compliance Program

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 open source software while decreasing legal costs and FUD. The Open Compliance Program offers comprehensive training and informational materials, open source tools, an online community (FOSSBazaar), a best practices checklist, a rapid alert directory of company's compliance officers and a standard to help companies uniformly tag and report software used in their products. The Open Compliance Program is led by experts in the compliance industry and backed by such organizations as the Adobe, AMD, ARM Limited, Cisco Systems, Google, HP, IBM, Intel, NEC, Novell, Samsung, Software Freedom Law Center, Sony Electronics and many more. More information can be found at http://www.linuxfoundation.org/programs/legal/compliance.

The Linux Foundation promotes, protects and standardizes Linux by providing unified resources and services needed for open source to successfully compete with closed platforms.

To learn more about The Linux Foundation, the Open Compliance Program or our other initiatives please visit us at http://www.linuxfoundation.org/.

THE LINUX FOUNDATION