» The Linux Foundation

Publishing Source Code for FOSS Compliance: Lightweight Process and Checklists

February 2012

By Ibrahim Haddad (Ph.D.)

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

Open Compliance Program

On August 10, 2010, The Linux Foundation launched the Open Compliance Program (OCP) with some noteworthy goals in mind:

- To boost adoption of Linux and other FOSS by making license compliance ever-easier to achieve
- To increase awareness and understanding of FOSS compliance responsibilities
- To make available free resources that can help companies establish their FOSS compliance programs

The Open Compliance Program now offers comprehensive training, educational materials, compliance tools, an online community (FOSSBazaar), a best practices compliance checklist, a rapid alert directory of company compliance officers, and SPDX™, a standard to help companies uniformly tag and report FOSS used in their products.

This paper falls under the free educational resources made available by The Linux Foundation that focus on various practical aspects of achieving FOSS compliance in the enterprise. Our goal has been to assist organizations in recognizing and meeting their obligations when using FOSS in their commercial products.

This paper discusses the aspect of publishing source code in meeting license obligations. It presents a sample process to follow when making source code available and offers checklists that you can use prior and post source code publication.

Compliance End-to-End Management Process

Implementation of open source compliance processes can vary from company to company based on a number of factors: the underlying product development process into which compliance must fit, the size and nature of the code base, number of products turned out, the amount of externally supplied code, size and organizational structure of the company, and so on. But the core elements of compliance usually remain the same:

- Identifying the open source in the code base
- Reviewing and approving its use
- Satisfying obligations

Figure 1 offers a high-level overview of a sample end-to-end compliance process, and illustrates the various compliance steps or phases that components containing free and open source software go through before they get approved for use in a product intended for external publication. (Other ways of organizing the compliance process may well accomplish the same goals of achieving compliance.)

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org

THE LINUX FOUNDATION

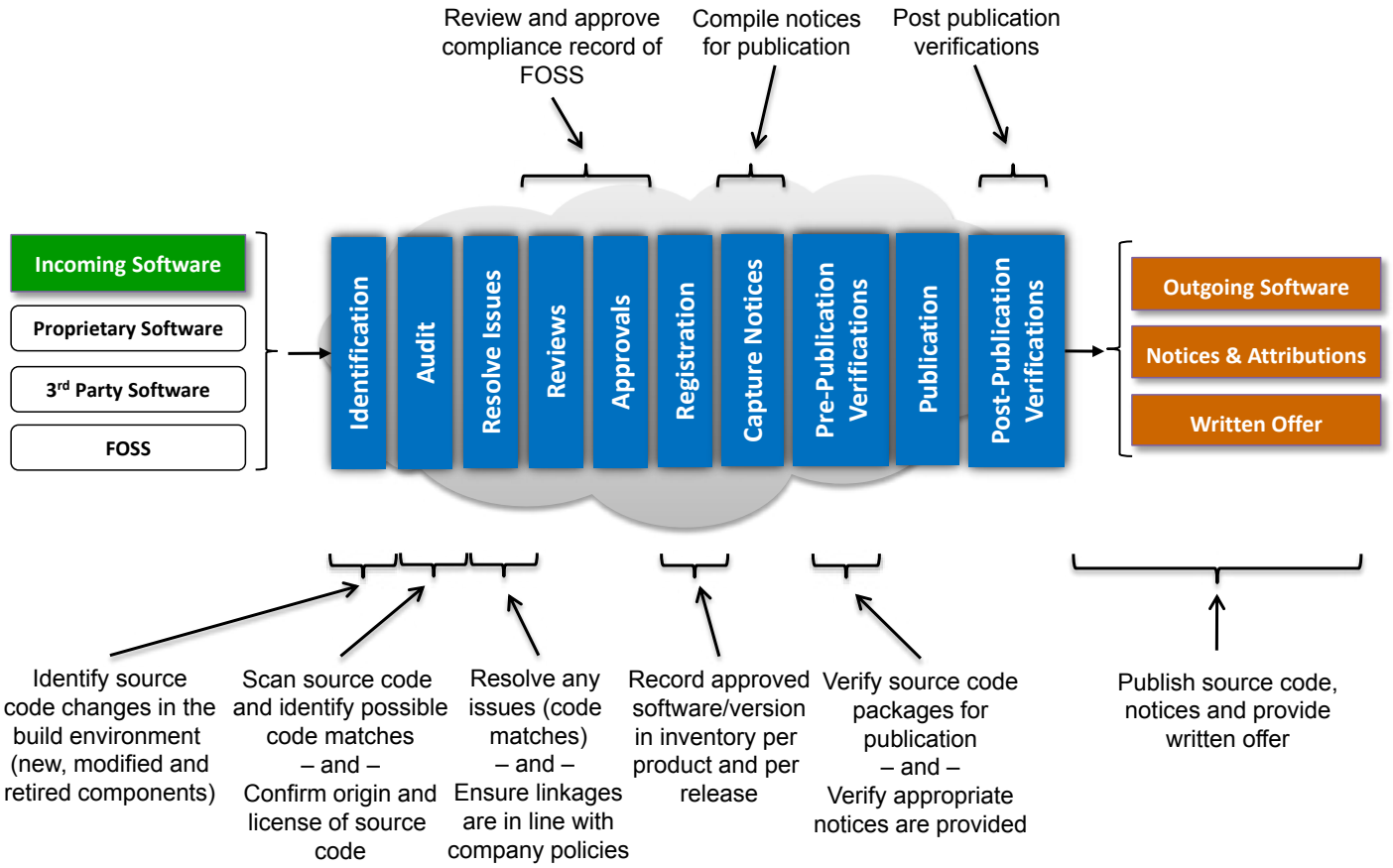

Figure 1. Sample end-to-end compliance process

The result of compliance due diligence is an identification of all FOSS used in a product intended for external publication and a plan to meet the attendant license obligations. Some of these obligations may include making source code available including any modifications applied to the original code, in addition to compilation and installation scripts (depending on the license in question).

Companies often establish a process that controls the publication of source code to ensure that the published code is the correct version, it corresponds to the binary version included in the product, the source code modifications are properly labeled, the source code is easily available on a given web site, it downloads and compiles properly and so on.

The remainder of the paper examines what happens in the last three steps of the compliance process illustrated in Figure 1, most notably the steps related to making source code publicly available: pre-publication verifications, publication, post-publication verifications.

Source Code Publishing Process

When companies incorporate FOSS into their products, they are required to respect the licenses of the FOSS. Depending on the license in question, some of the obligations may include making available (depending on license and software interaction at hand):

- Original FOSS source code for free under the same license.
- Any modifications made to the original FOSS source code for free under the same license.

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
THE LINUX FOUNDATION

- Any files linked to the original FOSS for free under the same license.
- Compilation and/or installation scripts needed to successfully compile and install the software.

Figure 2 illustrates a sample source code publication process that consists of 5 steps:

- Deciding on publication model.
- Preparing the source code packages for publication.
- Completing a pre-publication checklist to ensure that all prior steps have been successfully completed and that the source code packages are ready for release.
- Publishing the source code on a given web site.
- Completing a post-publication checklist: This checklist offers listing of verifications to be done once the source code packages are uploaded to the web site.

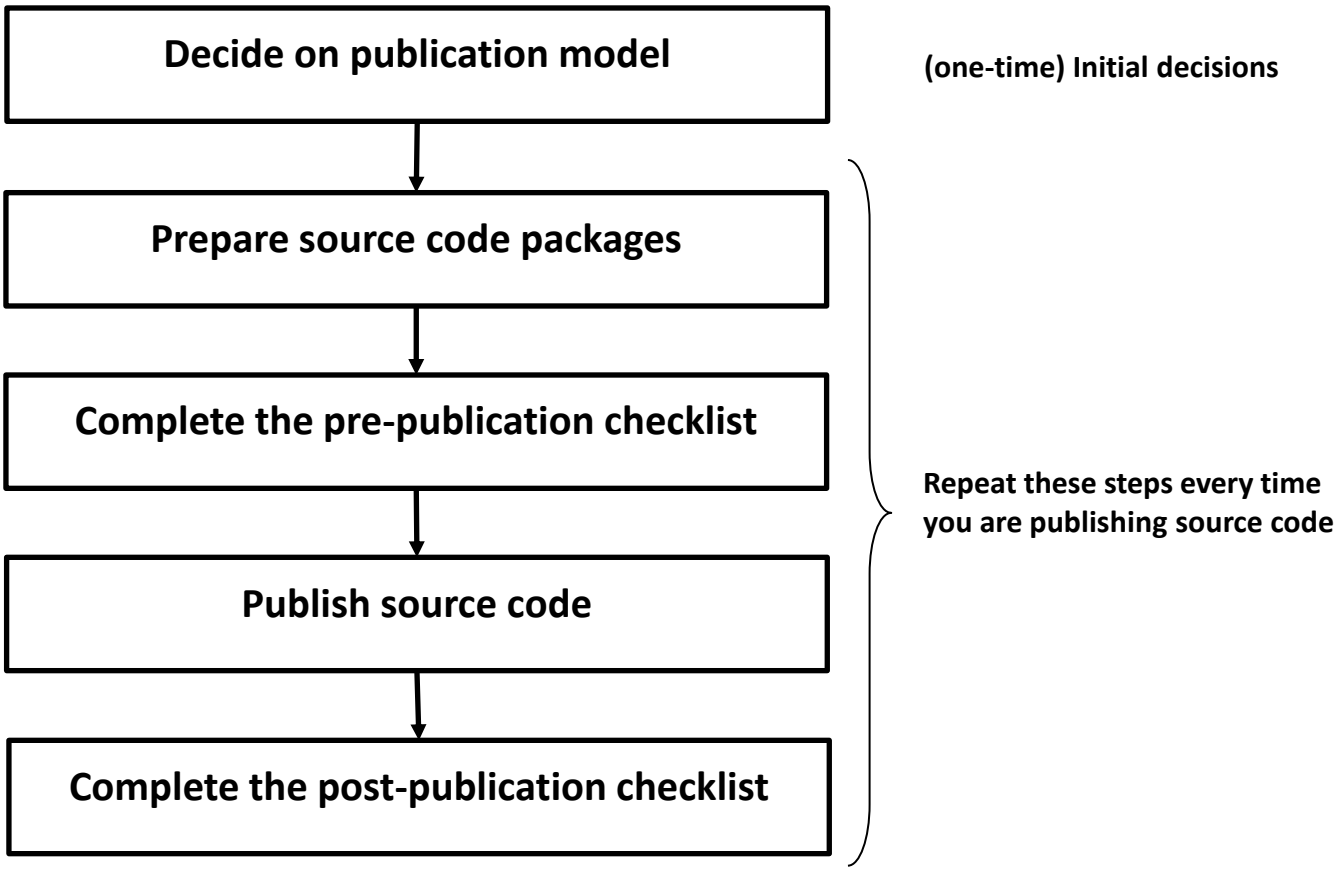

Figure 2. Generic process for publishing source code

Deciding on the Publication Model

There are two common publications models: the first is referred to as Instant Compliance, where the source code is made available to end users when the product ships by posting the source code packages on a web site accessible by the general public. The end users of the product will then be able to access the web site and download the FOSS used in that product. This is the easiest and recommended model to follow.

The second model is referred to as On-Demand, where source code is made available to end

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
THE LINUX FOUNDATION

users only after receiving a request from the product's end users asking for the specific source code packages they're eligible to have access to.

Preparing the Source Code Packages

You need to decide on how to package your source code, either as a flattened or un-flattened package. There are several aspects related to preparing the source code packages for publishing on a web site. Some are related to how packages are presented, some are related to highlighting the source code modifications, and others are related to the actual mode of publication. The following sub-sections discuss all of these aspects.

Preparing the Source Code Packages

A flattened package is a source code package that you downloaded from the web, unzipped and you directly applied your modifications to it.

An un-flattened package is a source code package that you downloaded from the web, and then you created your own set of patches that will be applied against the original source code package during build time.

Highlighting the modifications to the original source code

For flattened packages, you need to provide the original downloaded source code package that includes the modifications you introduced to the source code. Following this method, you need to mark the source code modifications you introduced and update the change log file to mention the changes you applied to the code.

In the case of un-flattened packages, there is no extra work to do since you are already providing your modifications as their own patch file. The patch file includes all the code changes that you apply against the original downloaded package. Following this method, you will need to make available to end users the original package and a compressed file that includes all of your patches.

Distributing a single versus multiple packages

One additional decision you need to make is how to present the source code packages on your web site. Some companies choose to bundle all the source code packages for a given product into a single file that is named after the product name and version number it corresponds to. Other companies choose a different path by creating a web page for each product and listing on that page the original FOSS source code packages and the corresponding patch files.

Static versus live publication

Static publication refers to making available the source code packages in a compressed format such as a tar or tgz files. On the other hand, a live publication is making available the source in a live repository (within git for instance) to make it easier for the developers community to browse the source code and examine your modifications on your web site without having to download the packages locally. The live publication would only work if you are using flattened source code packages.

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org

THE LINUX FOUNDATION

Pre-Publication Checklist

The pre-publication checklist is a set of conditions that must be met before releasing the source code to the public. It includes the following (listed in random order):

- ❑ The product containing the FOSS package is ready to ship or has shipped very recently.
- ❑ The FOSS package has been approved for usage in that specific product.
- ❑ The modifications that were introduced to the FOSS package have been reviewed to ensure:
  - Each modified source code file contains an additional entry for a copyright notice, disclaimer and a generic "change log" entry
  - No product code names are used in the source code as variable names or in the comments. In general, it is poor coding practice to key off product names to make run-time decisions.
  - No references to future products or future product plans are mentioned in the source code comments.
  - No obscene, vulgar, or blasphemous language should be used in comments.
  - No references to individuals, email addresses, and internal URLs.
- ❑ The FOSS package is tested to compile on an generic machine that does not have the company computing environment setup on it.
- The product manual is updated to:
  - Mention that the product includes FOSS.
  - Offer proper copyright and attribution notices.
  - Indicate how to access the code of the FOSS package (written offer) either through a web page download or by contacting your company via email or snail mail as a specified address provided in the product manual.
- ❑ Existing license, copyright and attribution notices for the FOSS package included are not disturbed.
- ❑ The source code package corresponds to the binary that goes with the product and that it includes:
  - Build and installation instructions (when applicable).
  - A copy of the license text.

Publication

Publication of source code is the step in the process where someone in the company updates the external open source web site and uploads the source code packages and make them available to the general public.

Post-Publication Checklist

The post-publication checklist includes the following:

- ❑ Verify that the packages have been uploaded to the web site.
- ❑ Verify that the packages are accessible from an external computer (a computer not connected to your company's network).
- ❑ Verify that the packages can be uncompressed without errors.
- ❑ Verify that the packages compile and build without errors.

If any errors were found in this phase, a correction action is taken and packages will be uploaded

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org

THE LINUX FOUNDATION

again to the web site and re-verified.

Conclusion

This paper provides a practical discussion on the process of making source code available as part of meeting FOSS license obligations. Our hope with this paper is to provide some insight on how to set a proper process and checklists in place to ensure fast, effective and correct execution of a source code publication process.

The next paper is this series will provide guidance on how to avoid being non-compliant. For a listing of all of our compliance papers, visit http://www.linuxfoundation.org/publications/compliance.

About the Author

Ibrahim Haddad, Ph.D., is the Director of Technology and Alliances at The Linux Foundation and Contributing Editor for the Linux Journal.

Linux Foundation Resources

Linux Training

The Linux Foundation offers two training courses to enable organizations effectively work with open source developers:

LF 205: How to Participate in the Linux Community: Working with the kernel development community is not particularly hard, but it does require an understanding of how that community works. This course is intended to bring attendees up to speed quickly on how kernel development is done and how to be a part of the process with a minimum of pain and frustration.

LF 271: Practical Guide to Open Source Development: This course prepares organizations to maximize their effectiveness and shorten the time to value when participating in open source development projects. This course builds upon years of best practices and extensive experience in commercial participation in open source projects to help organizations approach the open development model in a structured and methodical manner, maximizing the likelihood of success. The course provides extensive examples from the Linux kernel community, and includes specific best practices for working with upstream.

Linux Foundation Labs

If you have a collaborative software project you need hosted at a neutral party, the Linux Foundation may be able to help. The Linux Foundation assists companies and communities by hosting collaborative software projects. The Linux Foundation provides three main services to Lab projects:

- The technical, operational and legal infrastructure so that project leaders can focus on technological innovation.
- Guidance and consulting on open source best practices gleaned from the two decades of experience of Linux and the ability to collaborate and network with the large and growing Linux Foundation community.
- By providing these services to companies and developers, the Linux Foundation provides a much needed framework for advancing and accelerating technology that allows project

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org

THE LINUX FOUNDATION

hosts to focus on innovation.

- There are two main criteria that must be met in order for the Linux Foundation to host a lab project:
- Use of open source governance best practices including license and contribution agreement choices in keeping with the ideals of Linux
- Project must either use Linux or have the potential to enhance the Linux ecosystem

If you have a project that may fit this criteria, please contact us:

http://www.linuxfoundation.org/labs.

Open Compliance Program

The Linux Foundation's Open Compliance Program was established to boost adoption of Linux and other open source by making license compliance ever-easier to achieve, to increase awareness and understanding of open source compliance responsibilities, and to make available free resources that can help companies establish their compliance programs. The program offers comprehensive training, compliance educational materials (white papers, compliance blog, webinars), compliance tools, an online compliance community (FOSSBazaar), a best practices checklist, a rapid alert directory of company compliance officers, and SPDXTM, a standard to help companies uniformly tag and report software used in their products.

Events

The Linux Foundation produces a number of technical events around the world that provide a venue to bring together developers to solve problems in a real-time environment.

Publications

The Linux Foundation produces a wide range of publications that are available for free download. These publications are divided into three categories: Open Source Compliance, Workgroups (such as Tizen, OpenMAMA, LSB, SPDX, FOSSology, etc.) and Community. The Linux Foundation publications are available from http://www.linuxfoundation.org/publications.

Compliance Resources

- **Open Compliance Program:** http://www.linuxfoundation.org/programs/legal/compliance
- **Professional and Comprehensive Compliance Training:** The Linux Foundation offers hands-on training from compliance experts for individuals and companies responsible for achieving compliance with open source licenses and establishing an open source compliance program, as well as for those who simply want to learn more about compliance. Options available include live onsite training in addition to instructor-led live remote training. http://www.linuxfoundation.org/programs/legal/compliance/training-and-education
- **Open Compliance Program Self-Assessment Checklist:** An extensive checklist of practices found in industry-leading compliance programs. Companies can use this checklist as a confidential internal tool to assess their progress in implementing a rigorous compliance process and help them prioritize their process improvement efforts. http://www.

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
THE LINUX FOUNDATION

linuxfoundation.org/programs/legal/compliance/self-assessment-checklist

- **Compliance Publications:** http://www.linuxfoundation.org/publications
- **Open Compliance Directory and Rapid Alert System:** http://www.linuxfoundation.org/programs/legal/compliance/directory
- **Compliance Tools:** http://www.linuxfoundation.org/programs/legal/compliance/tools
- **The Software Package Data Exchange™:** The SPDX™ specification is a standard format for communicating the components, licenses and copyrights associated with a software package. http://www.spdx.org/
- **FOSSBazaar:** An open community of technology and industry leaders who are collaborating to accelerate adoption of free and open source software in the enterprise. http://fossbazaar.org/

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org

THE LINUX FOUNDATION

The Linux Foundation promotes, protects, and advances 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/.