Open Source Software License Compliance General Public Guide

Contents

Introduction

Open Source Software (OSS) has become essential to modern software development. OSS is incorporated into almost every electronic product, including super computers, cloud servers, personal computers, consumer electronics, automobiles, industrial equipment and IoT equipment. Companies are required to develop products or services with high quality and faster time–to–market even under intense competition. They also have to keep up with the latest technology trends. OSS is indispensable in this pursuit.

Much OSS is developed through the collaboration of expert developers from different organizations throughout the world. OSS is often a vehicle for advanced innovation in various fields. Software engineers who participate in Open Source development have opportunities to improve their skills and to experience this innovation firsthand.

OSS can be freely used, modified, and distributed by anyone who complies with the associated license conditions. When OSS is distributed, the distributor is require to comply with the terms and conditions of the license at the point in time when distribution occurs. There have been cases where distributors were sued and lost because they failed to satisfy their legal obligations. Thus, to reduce risks caused by using OSS, all relevant personnel must have an understanding of the basic principles of OSS.

This pamphlet has been written by the OpenChain project of The Linux Foundation, to tell as many people as possible about the basic principles of OSS.

May 2019

Learning Open Source Software

Let's learn the basics of Open Source Software (OSS).

This pamphlet explains the following:

1. What is Open Source Software?
2. What you need to do to receive the benefits of OSS
3. Risks associated with failure to comply with OSS responsibilities

Unfortunately, there have been cases where a company's failure to comply with their OSS license responsibilities resulted in litigation by the copyright holder.

4. Supply chain issues
5. What you need to do to ensure that everyone benefits from OSS

Points 3 and 4 may be intertwined. If OSS is acquired through a supply chain then all links in the supply chain must comply with the conditions of the license. If any link fails to satisfy the conditions of the license, then entities later in the supply chain will not be able to remedy the missing conditions. An employee or company acting alone cannot meet all the responsibilities and requirements by themselves.

When an item with OSS software is delivered to another party, information related to all included OSS must be provided. The following sta are required to know the proper procedures to follow when acquiring and distributing OSS:

- **Developers and engineers:** In addition to software developers, hardware engineers are deeply involved in developing device driver software, board support packages (BSP) and software development kits (SDKs) for their hardware.
- **Procurement personnel:** OSS may be included in deliverables from the supply chain, such as software, hardware modules, SoCs, semiconductor products, and products designed and developed by ODM/OEM manufacturers.
- **Sales personnel:** Sales personnel are required to understand the reasons that customers need the OSS-related information, including copyright and license information.
- **Quality assurance personnel:** OSS that is included in a product may affect its quality or introduce bugs. QA personnel need to be aware of such issues.
- **Legal/Intellectual Property personnel:** Legal and intellectual property personnel are required to know the laws, legal precedents, and legal remedies that relate to OSS license interpretation and adherence.
- **Executives and managers:** Executives and managers develop strategy around using, contributing to, and distributing Open Source; build teams to promote OSS usage; and oversee OSS processes, and investment in required software tools.

*ODM: Original Design Manufacturer OEM: Original Equipment Manufacturer

Definition of OSS

It is not easy to answer precisely "What is OSS?". Different people have different answers. However, most people would agree with the following:

> OSS is software for which the source code is provided.And the copyright holder allows others to use, inspect,modify, and share the software.

Examples of OSS

Linux is probably the most widely known example of Open Source Software. An Operating System (OS) is software that is designed to provide a platform for other software. Linux is one such operating system. Linux is everywhere. It is incorporated into almost every major computing system, including super computers, stock exchange servers, Internet servers, smartphones using the Android software stack, consumer electronics products, automobiles, and industrial equipment. Linux supports a large portion of the world's core technological infrastructure.

Linux has been developed through the collaboration of tens of thousands of developers from around the world. Linux development continues actively every day. Anyone can freely use, modify and distribute Linux, provided they abide by the conditions of the license that the Linux developers have chosen. It is very important that companies that use Linux understand and comply with the license terms for Linux.

In addition to Linux, there are a huge number of other OSS projects. These include the Apache project used for HTTP servers, the widely used compiler GNU Compiler Collection (GCC), and the Eclipse integrated development environment, to name just a few.

OSS and license

A copyright holder of OSS does not waive their copyright in the code, but grants users certain rights to the software based on the user's adherence to the conditions of the software's license. In some cases, a copyright holder may grant users a patent license. It is critical for users of Open Source software to understand the license of each piece of OSS they use.

Almost all OSS licenses disclaim liability for OSS developers. In almost all cases, the OSS developers do not take responsibility for usage of OSS; but require users, product integrators, and vendors to take this responsibility on themselves.

Not all software is covered by copyright. If you need to judge whether a particular piece of OSS is copyrighted material or not, you should consult with a lawyer or intellectual property expert.

What is granted by license (copyright)

With some OSS licenses, the copyright holder grants others the right to use or distribute the software. This license grant occurs without direct communication between the copyright holder and the user, but this right-of-use is only granted if the user adheres with conditions provided by the copyright holder in the license. When a user fails to comply with these license conditions, a serious issue arises.

What is granted by license (patent)

With some OSS licenses, the copyright holder of OSS grants others the right to freely use the patents that are practiced by the software and owned by the copyright holder. Not every OSS license grants such a patent license. Examples of licenses that include such patent grants are the Apache license, and the GNU General Public License (GPL) version 3.

Typical OSS license

The Open Source Initiative (OSI) is an organization that promotes OSS. It defines the criteria for what constitutes OSS and approves dozens of dierent licenses as valid OSS licenses.

https://opensource.org/licenses
https://opensource.org/osd

Most OSS is licensed under an OSI-approved license. In addition, some software that is licensed under non-OSIapproved license may be treated as Open Source software as well. Whether such software should be treated as OSS (or handled some other way) should be determined by agreement between the software supplier and the recipient.

What you need to do to receive the benefits of OSS

When you use OSS, the most important thing to know is your obligations related to distribution of the software.

Almost all OSS licenses define the followings:

- The OSS developer disclaims liability for the effects of using the software
- Some obligations must be fulfilled when the software is distributed by an individual or legal entity (distributor).

In the following sections, a distributor can mean either an individual or a legal entity such as a company.

Anyone who complies with the conditions of the license may freely use and distribute the software.

However, the conditions differ from license to license. Some licenses require only that a license notice and a copyright notice be included in the source publication. Other licenses require the disclosure of the source code and a written oer to obtain it. Some licenses have terms that aect what other OSS the first software may be used in combination with. A distributor is required to comply with all of the obligations defined in the license.

There are several ways to distribute software. One way is to sell a product that incorporates the OSS software. Another way is by providing a site from which the software may be downloaded. When an item that contains OSS is distributed, the entity that is distributing it is required to comply with the license for that OSS.

Examples of OSS distribution

There are several different ways OSS may be distributed. In every case, the distributor is required to comply with the OSS license.

1. One way to distribute OSS is to develop a product using an SDK (software development kit) provided by a semiconductor vendor. If OSS that is included in the SDK is incorporated into a product during development, then this means that the semiconductor vendor is distributing OSS via inclusion in the SDK, and the product developer is distributing OSS via inclusion in the product. In this case, the product vendor has responsibilities to fulfill to comply with the license. But they are dependent on the semiconductor vendor. If the semiconductor vendor does not provide appropriate information about the OSS included in the SDK, the product vendor cannot comply with the OSS license.
2. Another way that OSS might be distributed is when an ODM or OEM is entrusted with the design and development of a product for manufacturers. The ODM or OEM may incorporate OSS into the product, which the product distributor needs to know about.

   Even though an OEM or ODM made the product, the brand owner of the product distributes the OSS incorporated into the product. The brand owner is required to comply with the OSS license. If the ODM or OEM manufacturer does not provide appropriate information about OSS, the brand owner of the product cannot comply with the OSS license.
3. Other ways of distributing OSS include shipping a product, releasing mobile application software, or providing an update of software for a previously shipped device.

   If OSS is included in a product, mobile application, or software update, this constitutes distribution of OSS. The entity who ships the product or releases the software is required to comply with the OSS license.
4. JavaScript used in web pages constitutes distribution:

   An interesting case of OSS distribution may occur when a web page is transferred to a user's machine.

   JavaScript that is included in web pages is transferred from the web server to the browser on the user's machine, as part of the page data, when the user accesses the page. If the JavaScript program is OSS, then this constitutes distribution and the license terms will apply.

Obligations to be fulfilled when OSS is distributed

The obligations that need to be fulfilled when OSS is distributed vary from license to license. It is important to identify all of the OSS and associated licenses in a product or program that is distributed.

This is required to clearly understand all the different license terms that must be satisfied.

Permissive licenses

The MIT license, the BSD license and the Apache license require few obligations. These licenses require the distribution of the software's copyright notice and the license text. The notice should be clearly displayed in a place where the person receiving the OSS can read it.

Reciprocal licenses

The GPL license, the LGPL license, the AGPL license, and the Mozilla Public License require disclosure of the source code for the associated software. (The license and the copyright in the source code must not be removed.) If the distributor has modified the source code, then all source code modifications must also be disclosed. Reciprocal licenses aim to foster an environment where people can share modifications and improvements among all users and developers of the software.

In addition to the disclosure of the source code, these licenses generally require other obligations to be met as well. To distribute software under a reciprocal license you must understand these obligations. If needed, you should consult with your legal and intellectual property staff.

Patents that you cannot grant

In some cases, an OSS license may require a distributor to grant their users a license for patents embodied in the software that the distributor uses or adds to the OSS. If you have such a patent, that you cannot grant your users a license to, you must not distribute OSS covered by such license terms.

Risks caused by failure to comply

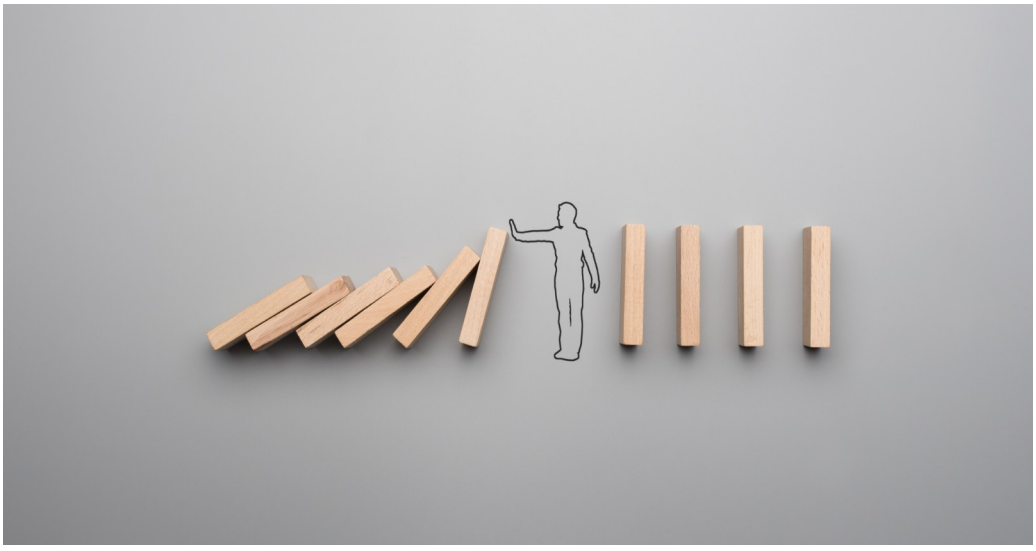
Litigation by an OSS copyright holder against a company for failure to comply with the license has occurred.

Unfortunately, it has occurred that failure to comply with the OSS license resulted in litigation against the user (and distributor) by the OSS copyright holders. In at least one case, a judgement required the defendant to suspend the shipment of their products containing OSS.

In December of 2009 there was a lawsuit related to Open Source software called "Busybox". The Busybox program is widely incorporated into embedded systems and is licensed under the GPL version 2 license. In this case, 14 companies were the subject of the lawsuit, including some in the consumer electronics industry. The remarkable thing about this case was that companies suered litigation on products that had been made by an ODM manufacturer.

In every case, it was the distributor's failure to comply with the OSS license that resulted in the litigation. To avoid litigation, an entity working with OSS should:

- Identify every piece of OSS in the software to be distributed
- Understand the obligations defined by the OSS license, and comply with them.



What is lost in litigation

When a company is litigated, one of the largest damages to the company is to its reputation (reputational risk). A bad reputation of not complying with software licenses may cause a company to lose the trust of other companies. The more that a company understands the importance of its trust relationships, and endeavors to build trust throughout its industry, the more serious that company is about avoiding risks to its reputation.

To respond to litigation requires a lot of work and expense. In the absence of litigation, the human resources involved in legal, procurement, engineering, and compliance could be used in more constructive tasks. This means that a company spending time responding to litigation might miss out on other business opportunities that those human resources could be working on. In particular, employing a competent lawyer for OSS litigation is very expensive.

A settlement or a legal judgement may require payment of money or a fine. In the extreme, a judgement could result in the suspension of shipment of a product, which could be quite damaging and costly.

Building a good relationship with the OSS community

To reduce the risk of litigation, it is essential to understand OSS principles and to comply with the obligations of the OSS licenses. In addition, it is highly recommended to contribute to the OSS community and to build good relationships with the developers of the OSS that you use.

If you understand why the authors selected a specific Open Source license for their software, and the intent of the OSS community that supports an OSS project, it will help you move beyond just fulfilling the letter of the OSS license. Understanding the intent of the developers is one of the most important benefits of having a good relationship with the OSS community.

A good relationship with the OSS community may enable a company to have its own new ideas adopted into the OSS. The OSS community may improve software based on your ideas and requirements. Also, engineers in your company may have the opportunity to collaborate with highly skilled OSS developers, and this could result in more satisfaction and skill for your engineers.

As the system software increases in size and functionality, it becomes more and more complex. It is harder and harder to produce software without bugs. However, if a company has a good relationship with OSS developers, the community may help your engineers find and resolve bugs, as the software is developed.

Contributing to OSS communities

There are many ways to contribute to OSS communities: proposing bugfixes and new features, translating documents, providing places and forums where community members can communicate, and sponsoring and participating in projects and trade associations that support OSS, such as the Linux Foundation.

Supply chain issues

OSS compliance cannot be achieved by one person acting alone.

As software becomes larger and more complex, the supply chain for software also tends to become larger and more complex. A modern software supply chain may include an OSS community, a software supplier, a semiconductor vendor that provides an SDK, and a final product vendor. If any member of a large and complex software supply chain fails to comply with license obligations or fails to provide the appropriate license information, it will cause a large impact to a vendor who is obligated to comply with the license (Figure 1). Compliance failure could result in product shipment being suspended. If the vendor does not know about the failure before shipping, the vendor may receive an inquiry regarding the failure from a copyright holder or a third party, which it cannot respond to.

However, if software compliance is managed appropriately in the upstream supply chain, these problems can be avoided. To facilitate compliance with OSS licenses, all participants in the supply chain must do their duty, build trust throughout the supply chain, and communicate appropriate information regarding included software.

It is recommended that each company in the supply chain establish a team to ensure OSS compliance in the chain. The Linux Foundation's OpenChain project provides a Self Certification program that companies can use for this purpose. The Self Certification helps a company check its compliance process. The certification test is available in several languages and anyone can use it for free.

https://certification.openchainproject.org/

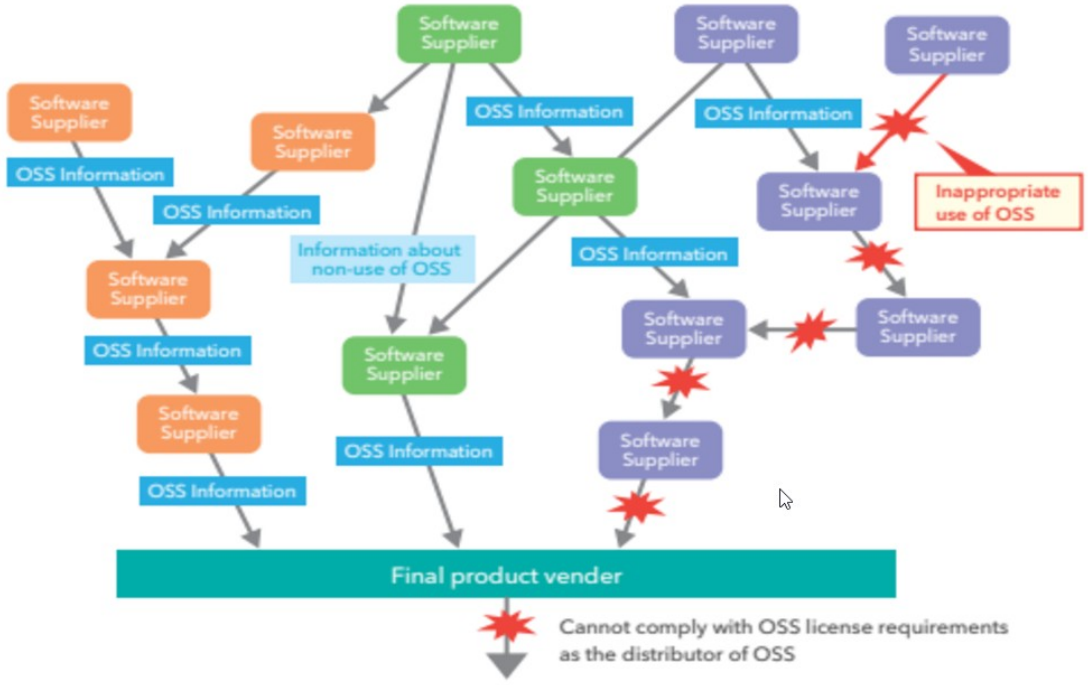


Figure 1 Software supply chain issues

Requirements for participants in the supply chain

When a supplier distributes software, the supplier is required to provide to each recipient the information that is needed to comply with the OSS license. A recipient should review the data and files carefully and verify that they are accurate.

A software distributor may include software from multiple suppliers for a single product. In this case, the distributor is required to receive information about each OSS component it receives, along with the software.

If information about an OSS component is not received, such OSS should not be incorporated into a product.

Different roles in a company have different responsibilities for OSS compliance

Software developers

Software developers should manage, record and store the configuration of the software. This includes the following:

- OSS and its license
- Linkage (e.g. libraries used by the software, dynamic or static linkage, etc.)
- Modifications. That is, the technical details of any modifications made to the software.

These items must be identified and listed. Any time the software configuration changes, the list should be updated. The license may change from one release of software to the next, for a particular project. It is recommended to create and manage the list so that each OSS item is easily referenced and reviewed. Some licenses (for example, the GPL license) require a distributor to disclose the source code. It is highly recommended that source control management software is used to track the original source code and any changes to the source code.

Software procurement personnel

Software procurement personnel must receive information about any OSS in the incoming software, for software engineers to record. OSS may be included in software like the SDK provided by a semiconductor vendor.

Procurement personnel are required to pay attention to the software in all the dierent kinds of deliverables that the company receives.

Sales personnel

Sales personnel are required to communicate with customers regarding OSS. A customer may have special requirements related to the use of OSS. For example, a

company may have an OSS policy that precludes it from using OSS with specific licenses.

It is important for sales personnel learn of customers' requirements regarding OSS, and communicate this information to internal software developers.

Legal / Intellectual property personnel

Cooperation with legal and intellectual property personnel is indispensable for understanding OSS licenses. Legal and intellectual property personnel should review the licenses that govern the OSS used by a company and advise developers as to its use:

- What approvals are needed for using OSS? (In general,OSS licenses disclaim liability for the developer of the software.)
- What is required in order to distribute the OSS?
- Can the inclusion of OSS cause a problem when the software is used by downstream recipients?

Executives and Managers

To use OSS eectively and appropriately requires the cooperation of different staff inside a company.

Executives and managers may need to facilitate coordination between internal organizations and may decide to establish a dedicated team to manage OSS-related issues. This includes investments in human resources, training, and development environments.

OSS information required to be delivered with software

To ensure that everyone benefits from OSS, people must know what information regarding OSS must be provided with software deliverables.

This pamphlet has explained the importance of maintaining the list of OSS and of complying with OSS licenses.

What information regarding OSS should be provided with software deliverables? This section explains the specific information that must be distributed with OSS. Because the required information varies depending on business and company policy, please communicate with each recipient company for details.

When no OSS is included in software deliverables, you should clearly communicate that “the deliverable does not include any OSS” to recipients. The recipient may then act accordingly.

When OSS is included in software deliverables, you must clearly identify such software, and its license. For example, the license may change between dierent versions of OSS. The name and version of each OSS component is indispensable information. For each component it is helpful to provide the download location or main project source site or web site for the software. This allows recipients to verify the information about the software, its version and license.

When the OSS license requires the distributor to disclose source code, please provide the source code. The source code that is specifically required depends on the OSS license. For example, version 3 of the GPL/LGPL 3 license requires that in addition to the source code for the software, you must also provide information needed to re-install a modified binary based on the code.

Information that must be distributed with OSS

The following information must be distributed with your

deliverables that include OSS.

- List of OSS components

For each OSS component:

- Information which identifies the software (version number, origin of the source code (for example, website URL) and how the software can be obtained)
- List of applicable licenses, and (if more than one) the license your company is distributing the OSS under
- Any modifications you made to the software

For OSS where the license requires the distributor to provide license and copyright notices:

- The actual license text and copyright notices

For OSS where the license requires disclosure of source code:

- The required source code (In the case of GPL, in addition to the source code you must also provide the scripts used for generation of the executables created from the source)

In some cases, where an OSS component itself includes a secondary piece of OSS, you must provide information for the secondary OSS component as well.

The preceding information is fairly general. One customer may require certain pieces of information, while a different customer may require other information instead. It is important to communicate with your customers regarding the pieces of information they require and the format of them.

SPDX project

SPDX® (Software Package Data Exchange®) project, hosted by the Linux Foundation, has a standardized format for exchanging license information.

Anyone can use this format, and it is highly recommended for use throughout the supply chain. Please find information about this format at:

https://spdx.org/

Source code scanning tools

There are scanning tools that can detect OSS in software packages and automatically generate some information. For example, the FOSSology project hosted by the Linux Foundation has developed such a scanning tool. The FOSSology tool is available under an OSS license and can be freely used by anyone. There are also other scanning tools available, with commercial licenses. It is recommended to use tools such as these to verify OSS licenses in software packages during development and before shipping.

Some scanning tools have the ability to generate reports based on the SPDX specification. These scanning tools are useful for generating information that can be directly included in the deliverables to a customer.

About OpenChain Project

The OpenChain Project builds trust in open source by making open source license compliance simpler and more consistent. The OpenChain Specification defines a core set of requirements every quality compliance program must satisfy. OpenChain Conformance allows organizations to display their adherence to these requirements. The OpenChain Curriculum supports this process by providing extensive reference material for eective open source training and management. The result is that open source license compliance becomes more predictable, understandable and ecient for all participants in the software supply chain.

https://www.openchainproject.org/

About The Linux Foundation

The Linux Foundation is dedicated to building sustainable ecosystems around open source projects to accelerate technology development and industry adoption.

Founded in 2000, The Linux Foundation provides unparalleled support for open source communities through financial and intellectual resources, infrastructure, services, events, and training. Working together, The Linux Foundation and its projects form the most ambitious and successful investment in the creation of shared technology.

https://www.linuxfoundation.org/