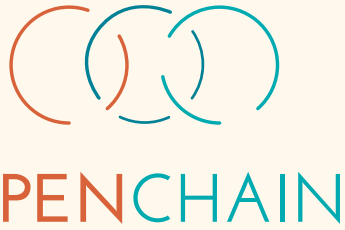

Managing Your Open Source Software Supply Chain:

A Guide From The OpenChain Project

Second Edition

Table of Contents

Introduction

This document is designed to help companies in the supply chain understand and manage Open Source Software (open source). The OpenChain Project maintains the OpenChain ISO/IEC 5230:2020 for open source license compliance and OpenChain ISO/IEC 18974:2023 for open source security assurance. These standards can help companies manage open source. You can learn more about the OpenChain Project and its standards at www.openchainproject.org.

Open source has become essential to modern software development and is incorporated into almost every electronic product, from consumer to industrial devices, from cloud to embedded software. Open source is an indispensable part of helping companies to bring products or services to market.

Much open source is developed through the collaboration of expert developers from individuals and organizations throughout the world.

Open source can be used, modified, and distributed by anyone who complies with the associated license conditions. When open source is distributed within the supply chain, the distributor is required to comply with the terms and conditions of the license. There have been cases where suppliers were sued because they failed to satisfy their legal obligations. This document is designed to help introduce the best practices needed to prevent issues occurring and to solve them when they do occur. It leads to further resources available through the OpenChain Project and other Linux Foundation Projects.

Like all other software, security issues sometimes occur with open source. By understanding how open source is created, used, and maintained, it is possible to identify, prevent and address many of these issues before they become a concern. The key thing is for all relevant personnel to understand the basic principles of open source.

Please note that this document is designed to provide insight based on experience shared from our global community. It does not contain legal advice.

Learning Open Source

Let's learn the basics of open source

Let's first explain the following:

1. What is Open Source?

2. What you need to do to receive the benefits of open source

3. Risks associated with failure to comply with open source responsibilities

4. Supply chain issues

5. What you need to do to ensure that everyone benefits from open source

Unfortunately, there have been cases where a company's failure to comply with their open source license responsibilities resulted in litigation by the copyright holder. Points 3 and 4 may be intertwined. If open source is acquired through a supply chain then all links in the supply chain must comply with the conditions of the license(s). If any link fails to satisfy the conditions, then entities later in the supply chain will also not be able to, nor be able to remedy the missing conditions.

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

- 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: open source may be included in deliverables from the supply chain, such as software, hardware modules, SoCs, semiconductor products, and products designed and developed by an Original Design Manufacturer (ODM) or Original Equipment Manufacturer (OEM).
- Sales personnel: Sales personnel are required to understand the reasons that customers need the open source-related information, including copyright and license information. This additionally ties directly into requirements from governments, such as SBOM guidance from NTIA, CISA and the White House Executive Order in the United States.
- Quality assurance personnel: open source 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 open source license interpretation and adherence.
- Executives and managers: Executives and managers develop strategy around using,

contributing to, and distributing open source; build teams to promote open source usage; and oversee open source processes, and investment in required software tools.

Definition of open source

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

The Open Source Initiative (OSI) is an organization that promotes open source. It defines criteria for what constitutes open source and approves different licenses as valid open source licenses.

https://opensource.org/licenses https://opensource.org/osd (Open Source Definition)

Most open source software is licensed under an OSI-approved license. Some software that is licensed under a non-OSI-approved license may still be treated as open source provided that it complies with the Open Source Definition.

The OpenChain Specifications define "open source" more broadly, to ensure that they cover software components for which the source code is available under licences which do not meet the open source definition (called "source available" licences).

Examples of open source

Linux is probably the most widely known example of open source, supporting a large portion of the world's core technological infrastructure. It is developed through the collaboration of tens of thousands of developers from around the world. Anyone can freely use, modify and distribute Linux, provided they abide by the conditions of the license that the Linux developers have chosen. There are a huge number of other open source projects that power modern infrastructure, including Kubernetes, Android Open Source Project and PyTorch, with many thousands of libraries used as components to build other software.

Open source and licenses

A copyright holder of open source 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 to understand the license of each piece of open source they use.

Almost all open source licenses disclaim liability for the open source developers. In almost all cases, the open source developers do not take responsibility for the usage of open source; 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 open source is copyrighted material or not, you should consult with a lawyer or intellectual property expert.

What is granted by licenses (copyright)

Open source licenses are a grant by the copyright holder giving other people the right to use or distribute 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, serious legal issues arise.

What is granted by licenses (patents)

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

What you need to do to receive the benefits of open source

When you use open source, the most important thing to know is the license conditions related to distribution of the software.

Almost all open source licenses define the following:

- The open source developer disclaims liability for the effects of using the software
- Some conditions 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 offer to obtain it. Some licenses have terms that affect what other open source the software may be used in combination with. A distributor is required to comply with all of the conditions defined in the license.

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

Examples of open source distribution

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

1. One way to distribute open source is to develop a product using an SDK (software development kit) provided by a e.g. semiconductor vendor. If open source that is included in the SDK is incorporated into a product during development, then this means that the semiconductor vendor is distributing open source via inclusion in the SDK, and the product developer is distributing open source 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 open source included in the SDK, the product vendor cannot comply with the open source license.

2. Another way that open source might be distributed is when an Original Design Manufacturer (ODM) or Original Equipment Manufacturer (OEM) is entrusted with the design and development of a product for manufacturers. The ODM or OEM may incorporate open

source into the product, which the product distributor needs to know about. Even though an OEM or ODM made the product, the companies responsible for the distribution of the product to market must pay attention to open source incorporated into the product. These companies are required to comply with the open source license. If the ODM or OEM manufacturer does not provide appropriate information about open source, the distributing company cannot comply with the open source license.

3. Other ways of distributing open source include shipping a product, releasing mobile application software, or providing an update of software for a previously shipped device. If open source is included in a product, mobile application, or software update, this constitutes distribution of open source. The entity who ships the product or releases the software is required to comply with the open source license.

4. JavaScript used in web pages constitutes distribution: An interesting case of open source 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 open source, then this constitutes distribution and the license terms will apply.

5. Some licenses (such as AGPL or the Open Software License) impose conditions on use of the software where the functionality of that software is made available to third parties (e.g. a user accessing a SaaS service provided by the software). These so-called "deemed distribution" licenses require that (in certain circumstances) the end-user is entitled to the source code of the software under the relevant open source license, even if the executable software code is not distributed to them in providing the service.

Conditions to be fulfilled when open source is distributed

The conditions that need to be fulfilled when open source is distributed vary from license to license. It is important to identify all of the open source 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 have few conditions. 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 open source can read it.

Reciprocal licenses

The GPL license, the LGPL license, the AGPL license, and the Common Development and Distribution 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 conditions to be met as well. To distribute software under a reciprocal license you must understand these conditions. If needed, you should consult with your legal and intellectual property staff.

Considerations around patents

In some cases, an open source 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 open source. If you have such a patent, that you cannot grant your users a license to, you must not distribute open source covered by such license terms.

Risks caused by failure to comply

Litigation by an open source copyright holder against a company for failure to comply with the license.

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

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 suffered litigation on products that had been made by an ODM manufacturer.

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

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

What is lost in litigation

When a company is involved in litigation, one of the addition areas of damage 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 open source 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 open source community

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

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

A good relationship with the open source community may enable a company to have its own new ideas adopted into the open source. The open source community may improve software based on your ideas and requirements. Also, engineers in your company may have the opportunity to collaborate with highly skilled open source 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 open source developers, the community may help your engineers find and resolve bugs, as the software is developed.

Contributing to open source communities

There are many ways to contribute to open source projects and 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 open source, such as The Linux Foundation.

Supply chain issues

Open source 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 open source 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 conditions 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. 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 open source 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 program to ensure open source compliance. The OpenChain Project created ISO/IEC 5230:2020 to explain the key requirements of this type of program, and to make it clear that even small teams can address open source compliance cheaply and effectively. At its most basic level, ISO/IEC 5230:2020 helps a company check its compliance process and improve it where necessary based on 30 years of industry knowledge. Free self-certification is available on the OpenChain Project website and there are also options for third-party certification if a company or its customers require it.

Get Certified: https://www.openchainproject.org/get-started

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 open source 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 open source component it receives, along with the software.

If information about an open source component is not received, the component should not be incorporated into a product.

Different roles in a company have different responsibilities for open source compliance

Software developers

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

- Open source 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 open source 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 open source contained in incoming software so that the company can record details for license compliance or other purposes. For example, they should check if open source is included in an SDK provided by a semiconductor vendor.

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

Sales personnel

Sales personnel are required to communicate with customers regarding open source. A customer may have special requirements related to the use of open source. For example, a company may have an open source policy that precludes it from using open source with

specific licenses.

It is important that sales personnel learn of customers' requirements regarding open source and communicate this information to internal software developers.

Legal / Intellectual property personnel

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

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

Executives and Managers

To use open source effectively 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 open source-related issues. This includes investments in human resources, training, and development environments.

Delivery of open source software

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

This document has explained the importance of maintaining the list of open source and of complying with open source licenses.

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

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

When open source is included in software deliverables, you must clearly identify such software, and its license. For example, the license may change between different versions of an open source component. The name and specific version of each component is therefore 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 open source license requires the distributor to disclose source code, please provide the source code. The source code and any associated materials that is specifically required depends on the open source license. For example, version 3 of the GPL/LGPL 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 may be required by customers

The following information may be required with your deliverables that include open source.

- List of open source components

For each open source 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 a choice of more than one) the license your company is distributing the open source under
- Information of modifications you made to the software

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

- The actual license text and copyright notices

For open source where the license requires disclosure of source code:

- The required source code plus potentially other items such as the scripts used compilation and installation (check the individual license terms)

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

The preceding information is 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) is a project hosted by the Linux Foundation that has developed a standardized format for exchanging license information. The SPDX format was published as ISO/IEC 5962:2021 after many years as a de-facto industry standard. Anyone can use SPDX and it is recommended for use throughout the supply chain. Please find information about it at https://spdx.org

Source code scanning tools

There are scanning tools that can detect open source 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 itself is available under an open source license and can be freely used by anyone. There are also other open source and commercial scanning tools available. Some tools can generate reports e.g. based on the SPDX specification which is useful for generating information that can be directly included in the deliverables to a customer. It is recommended to use tools such as these to verify open source licenses in software packages during development and before shipping.

Additional considerations

Suppliers should be aware of and potentially include processes to address regulation from government such as the United State's White House Executive Order [1], the NTIA Minimum Requirements [2], the European Union's Cyber Resilience Act (CRA) [3] and the EU Product Liability Directive [4].

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

[3] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[4] https://single-market-economy.ec.europa.eu/single-market/goods/free-movement-sectors/liability-defective-products_en (2022 draft revision)

About OpenChain Project

The OpenChain Project is building a supply chain where open source is delivered with trusted and consistent process management information. It maintains OpenChain ISO/IEC 5230:2020, the international standard for open source license compliance, and ISO/IEC 18974:2023, the international standard for open source security assurance.

There is an extensive global community of over 1,000 companies collaborating around the OpenChain Project to make the supply chain quicker, more effective and more efficient. For more information, please visit us at https://www.openchainproject.org/

About The Linux Foundation

The Linux Foundation is the world's leading home for collaboration on open source software, hardware, standards, and data. Linux Foundation projects are critical to the world's infrastructure, including Linux, Kubernetes, Node.js, ONAP, PyTorch, RISC-V, SPDX, OpenChain, and more. The Linux Foundation focuses on leveraging best practices and addressing the needs of contributors, users, and solution providers to create sustainable models for open collaboration. For more information, please visit us at https://www.linuxfoundation.org/