RECOMMENDED OPEN SOURCE COMPLIANCE PRACTICES FOR THE ENTERPRISE

IBRAHIM HADDAD, PHD

THE LINUX FOUNDATION

Ibrahim Haddad, PhD

Recommended Open Source Compliance Practices for the Enterprise

Printed in the United States of America

April 2019

1 Letterman Drive
Building D
Suite D4700
San Francisco CA 94129

ABSTRACT

Open source software provides significant economies to be gained through shared and transparent development, which offers access to source code, the ability to customize the source code based on specific needs, results in faster time-to-market for products and services, and provides access to a large pool of innovators. As such, open source software provides major competitive advantages when used appropriately, and when users comply with its licensing terms.

With an incredibly high adoption rate and the increasing rapid adaptation of source code, enterprises are often on the lookout for better ways to maintain proper license compliance for the hundreds and thousands of open source components included in their products and services. This paper offers practical recommendations to help them improve their open source compliance practices.

Contents

Chapter 1

INTRODUCTION

Open source initiatives and projects provide companies with a vehicle to accelerate innovation through collaboration with a global community of developers. Accompanying the benefits of teaming with the open source community is a very important responsibility: Ensuring compliance with applicable open source licenses.

In its simplest definition, open source compliance means that users of open source software must observe the copyright notices and satisfy the license obligations for the open source software they use. In addition, companies integrating open source software into their commercial products, software solutions, or services, want to protect their own intellectual property and that of third-party software suppliers from unintended disclosure. The result of these requirements is a situation where enterprises need to identify the origins of all source code used in the product or service and all applicable licenses, and prepare to fulfill the license obligations when the product is released or the service goes live.

Companies that use open source software in their products or software stacks typically establish an open source management program to ensure compliance with all open source licenses. Such a program provides a structure around all aspects of open source software including selection, approval, use, distribution, audit, inventory, training, community engagement, and public communication.

A license compliance program helps achieve four main objectives, as illustrated in Figure 1.

1. **Comply with the terms of open source licenses**
2. **Facilitate the usage of open source in products and services**
3. **Comply with the licensing terms of third party commercial software**
4. **Protect your product/service differentiation (intellectual property)**

Figure 1: Objectives of an open source compliance program

Figure 2 illustrates the core elements needed in a successful open source compliance program. For a detailed discussion on the implementation of such a program, please refer to the newly updated second edition of "**Open Source Compliance in the Enterprise**". This ebook offers a practical guide for enterprises on how best to use open source code in products and services, and to participate in open source communities in a legal and responsible way.

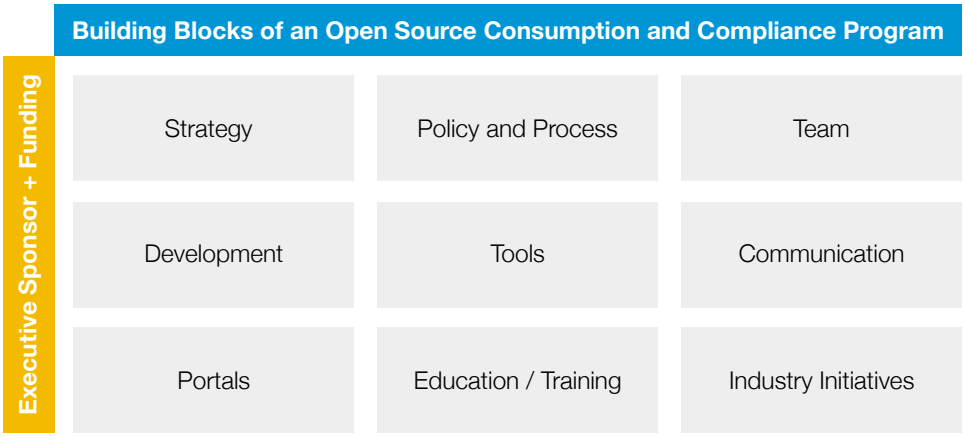

Figure 2: Core building blocks of an open source management program

Figure 3 illustrates the three fundamental processes that comprise the core of open source compliance:

1. Identifying open source software coming into the enterprise
2. Reviewing and approving its intended use
3. Satisfying the license obligations of open source software used in products and services.

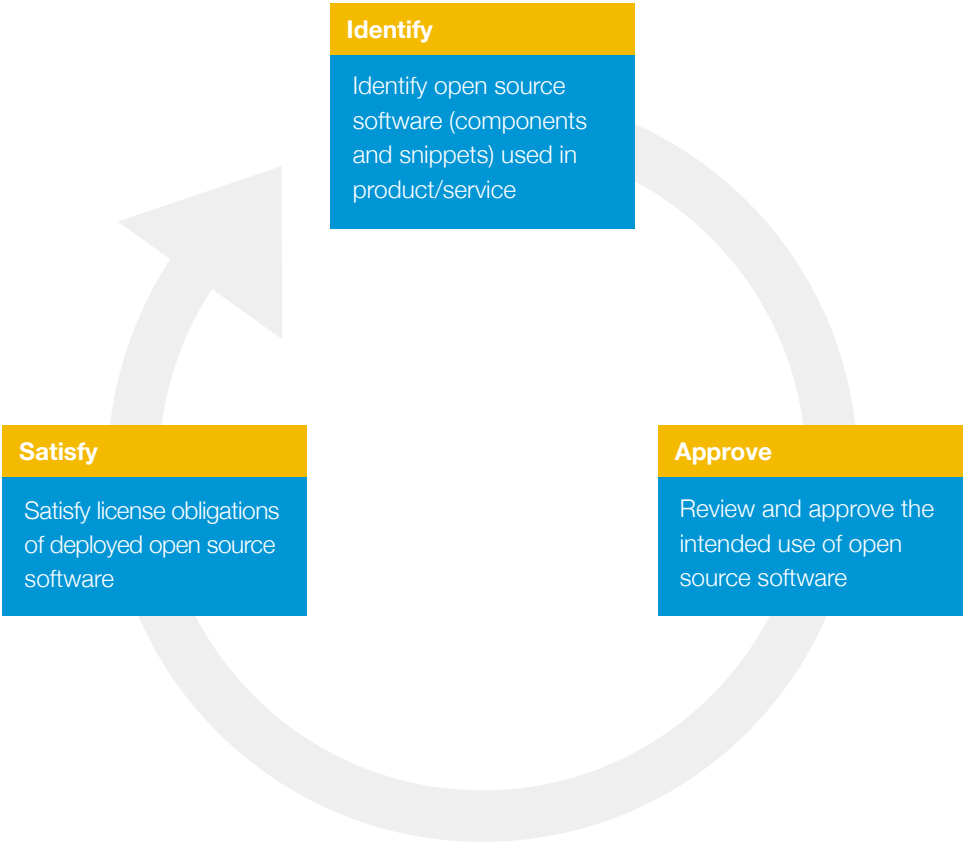

Figure 3: The main three ongoing activities in an open source compliance program

Figure 4 examines these three fundamental processes, their inputs, and outputs.

Identify:
The goal of this initial step is to monitor the ingress and incorporation of open source in a software portfolio, regardless of whether that incorporation

was as a standalone package or embedded within third-party or company-developed software. The output of this step is a detailed software bill of materials that identifies all open source software (packages and snippets), their origin, license, and any licensing conflicts identified by the software composition analysis tools resulting from mixing code licensed under conflicting terms.

Approve:
This step has two primary goals:

1. Review the output from the previous step, understand the licenses that govern the use, modification, and distribution of the source code in question, and

2. Make a decision on the approval or disapproval of the use of the identified open source software, each per its own unique context.

Once approval is granted, product teams are notified so they understand their responsibilities and begin preparations to fulfill the license obligations.

Satisfy:
In this final step, the license, copyright, and attribution notices for all approved open source software (whole components and snippets) are prepared and passed to the appropriate departments to be included in the product documentation. Similarly, open source packages destined for publication in fulfillment of license obligations have been flagged and will be ready for publication when the product/service goes live.

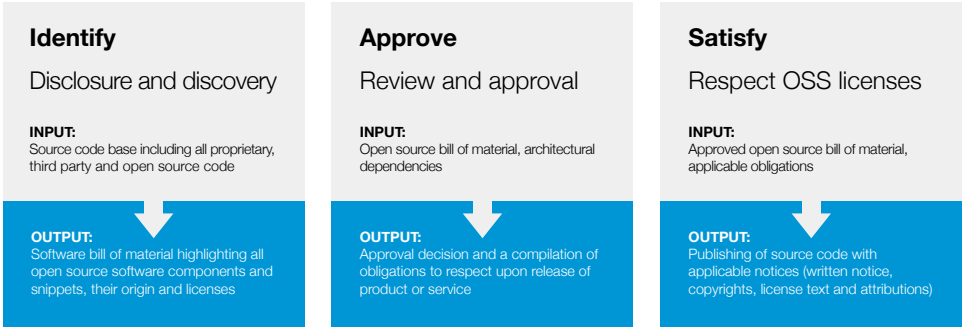

Figure 4: The inputs and outputs of the three fundamental open source compliance processes

With this lengthy introduction and context setting, we come to the point where we present the recommended practices that enterprises can implement to improve and strengthen their open source compliance program:

- Set up an Open Source Review Board (OSRB)
- Set up an automated system to identify open source software
- Get software suppliers to comply with open source licenses
- Scale your open source legal support
- Integrate open source compliance checkpoints in business and development processes
- Provide checklists for the various open source compliance tasks
- Develop and deploy supporting checklists
- Benchmark open source compliance activities
- Get involved in key compliance open source compliance initiatives

In the next sections, we explore each of these recommended practices and discuss how they enable open source compliance efforts.

Chapter 2

ESTABLISH AN OPEN SOURCE REVIEW BOARD

The open source review board (OSRB) consists of representatives from Legal and Product/Engineering teams, in addition to the open source compliance officer or a representative from the Open Source Program Office. The primary duty of the OSRB is to review and approve the planned use of open source software in products and services.

Figure 5 provides a high-level overview of the responsibilities of each participant in the OSRB.

Open Source Legal Counsel	• Review and approve usage, modification, distribution of open source software. • Provide legal guidance related to open source licenses. • Contribute to the creation of compliance training. • Contribute to improving the compliance program. • Review and approve content of web portals in relation to license compliance. • Review and approve the list of obligations for used open source software. • Sign off on product release from an open source compliance perspective.
Product / Engineering Representative	• Enforce compliance policies and processes within their organizations. • Integrate compliance practices in the software development processes. • Contribute to improving the compliance program from engineering perspective. • Follow technical open source compliance guidelines. • Collaborate with OSRB members to respond to compliance inquiries. • Conduct design, architecture and code reviews. • Prepare open source packages and notices destined for publications. • Sign off on product release from an open source compliance perspective.
Representative of the Open Source Program Office or Compliance Officer	• Drive open source compliance activities. • Coordinate source code scans and audits. • Participate in engineering reviews and distribution readiness assessment. • Coordinate the publication of open source software packages and notices. • Contribute to training efforts and improving the compliance program. • Contribute to facilitating the automation and discovery of open source software. • Sign off on product release from an open source compliance perspective.

Figure 5: Primary responsibilities of the core compliance team

In addition to the members of the ORSB, achieving open source compliance is a cross-disciplinary activity that involves various departments and individuals within any given organization (Figure 6).

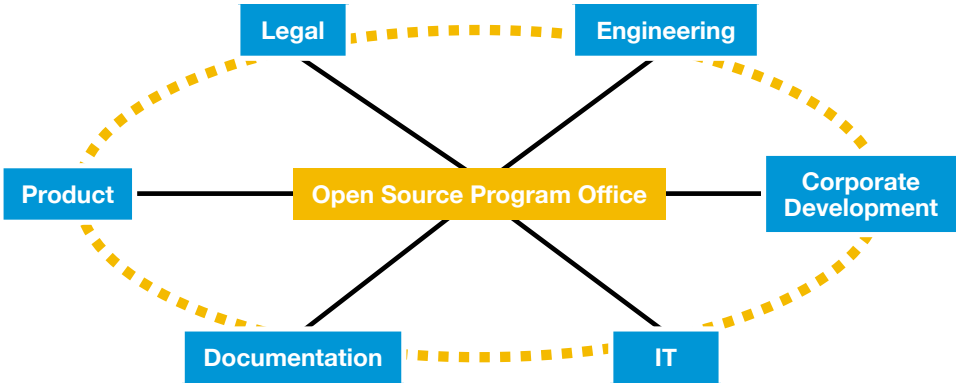

Figure 6: Open source compliance is the responsibility of several teams

Figure 7 provides a brief description of the core responsibilities of supporting teams helping the OSRB with the task of ensuring open source compliance.

1	IT	• Create/acquire new tools needed for ensuring compliance • Provide support and maintenance for the tools and automation infrastructure used by the compliance program
2	Corporate Development	• Request/supervise open source compliance due diligence be completed before a merger or an acquisition • Ensure compliance records when receiving source code from outsourced development centers
3	Documentation	• Include open source license information and notices in the product documentation
4	Open Source Executive Committee	• Review and approve proposals to release proprietary source code under an open source license
5	Software Procurement	• Mandate third party software providers to disclose open source in licensed or purchased software components • Assist with ingress of third party software bundled with and/or includes open source software

Figure 7: Core responsibilities of supporting teams in ensuring open source compliance

Chapter 3

KNOW WHAT'S IN YOUR CODE

The core of the open source compliance effort is to identify open source code and their respective licenses, so organizations can meet the applicable license obligations. An open source policy and a process guide this core activity. Compliance policies and processes govern the various aspects of using, contributing, auditing, and publication of open source software. If we take the basic process illustrated in Figure 3 and expand it, we would be looking at an end-to-end compliance process. Figure 8 presents such a process that has as inputs source code originating from multiple sources. The source code goes through a series of steps and the final output of the process includes a written offer, a list of notices (copyrights, attributions, licenses), and the source code packages destined for publication in fulfillment of license obligations..

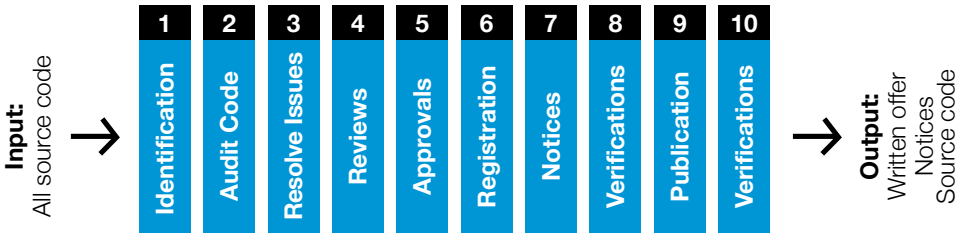

Figure 8: End-to-end sample open source compliance process

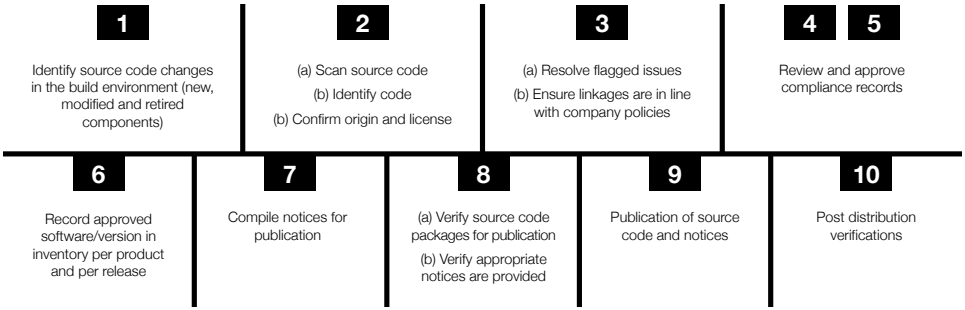

Figure 9: Inside the process

Figure 8 provides a detailed example of an end-to-end compliance process that includes the various steps a software component goes through before the OSRB approves its acceptance in the build system and integration with the software product.

Figure 9 provides a brief description of what happens in each of these steps.

Chapter 4

IMPROVE YOUR SOFTWARE SOURCING PRACTICES

It is crucial to get your software providers involved in open source compliance. Software providers must disclose open source code included in their deliverables and offer all notices including applicable source code.

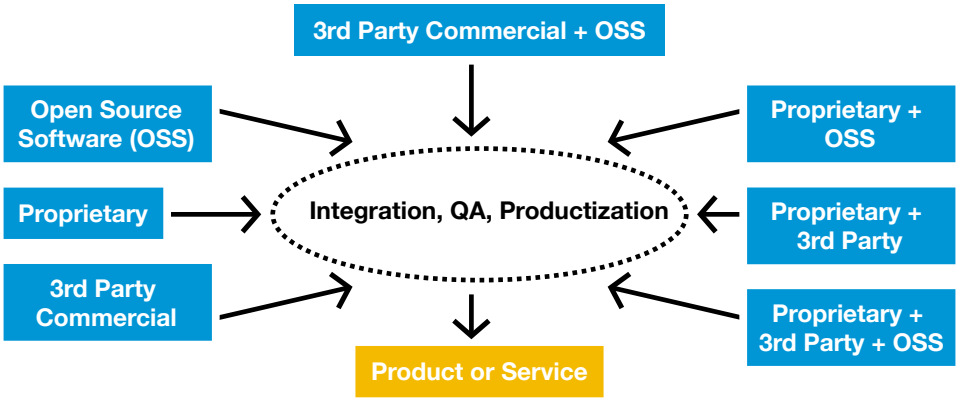

Figure 10: Multisource development model

Figure 10 illustrates the multi-source development model and the various combinations of sources for incoming source code. Under this model, a product or a software stack could now consist of any combination of proprietary software, third-party commercial, and third-party open source software. For instance, software component A can include proprietary source code in addition to 3rd party proprietary source code, while software component B can include proprietary source code in addition to source code from an open source project.

Companies are now in a state where they must update their supply chain (software procurement) procedures to address the acquisition and use of open source software. Supply Chain personnel are usually involved in moving software from the suppliers to your company. They can support open source compliance activities in two primary ways:

- Mandate that third-party software providers disclose any open source they use in their deliverables, and
- Assist with licensing-in third-party software bundled with and/or integrated with open source packages.

A recommended practice in this area is to mandate that third-party software providers disclose any open source used in their offering, along with a statement on how they plan to meet the applicable open source license obligations. If third-party software includes open source, Supply Chain must ensure that open source license obligations are satisfied since—after initial ingress—those obligations become your responsibility as the distributor of a product or service that includes open source.

Chapter 5

OFFER EASILY ACCESSIBLE OPEN SOURCE LEGAL SUPPORT

Most organizations create open source compliance programs and set up core teams to ensure proper compliance. It can be the case that open source legal support is a bottleneck in some companies as you have hundreds and thousands of developers witting and integrating open source code, and very few legal staff responsible for providing needed legal support. Scaling that open source legal support requires some out-of-the-box thinking but it can be achieved with the help of the following practical methods.

LICENSE PLAYBOOKS

An easy-to-read and digest summary of open source licenses intended for software developers. They provide easy to understand information about these licenses such as license grants, restrictions, obligations, patent impact, and more. The availability of such playbooks for most used open source software licenses minimizes the number of basic questions sent to the legal counsel and provides developers with immediate guidance, information, and answers to common inquiries.

LICENSE COMPATIBILITY MATRIX

License compatibility is a term that refers to the situation of determining if a certain license has compatible terms with another license. GPL compatibility refers to the situation of determining if a certain license has compatible terms with the GPL. Development teams often encounter the license compatibility problem when combining source code originating from different software components licensed under incompatible licenses. When the development team is combining code incoming under different licenses, they can refer to the license compatibility matrix to verify if there is a licensing conflict joining the source code in a single software component. If

the development team is using source code licensed under a license that is not in the matrix, they can get advice from the Legal Counsel on next steps.

LICENSE CLASSIFICATION

In an effort to reduce the number of questions received by the open source legal counsel and to increase license and compliance process education, some companies opt to classify the most used licenses in their products under a few categories. Figure 11 presents a simple example of a license classification system, where most used open source licenses fall into four categories.

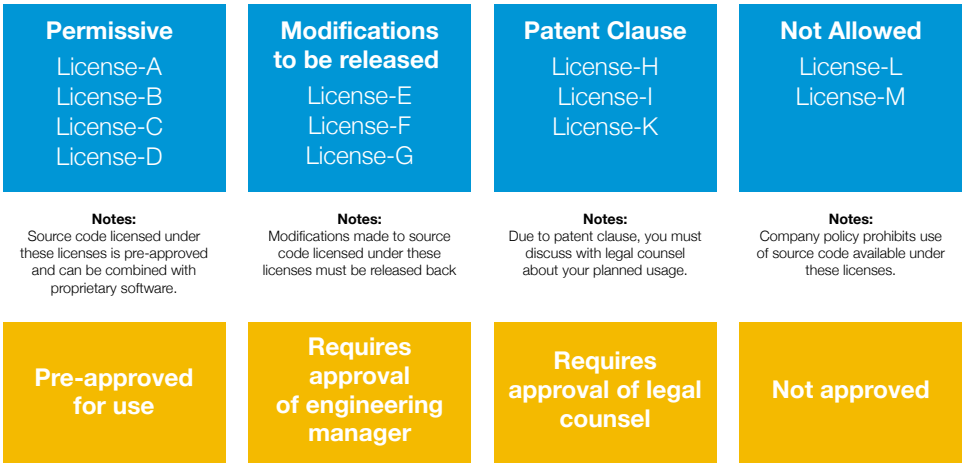

Figure 11: Example license categories (for illustration purposes only)

The above license categories are a simple way to classify licenses making it easier for developers to know the course of action when integrating code under these licenses. An example would be a developer who would like to use an open source package licensed under:

- License A **– Action:** Use without any problem
- License E **– Action:** Get approval of engineering manager
- License I **– Action:** Get approval of Legal Counsel

- License M **– Action:** Use of this license is prohibited by policy
- Other **– Action:** Ask a manager on the course of action

For further reading on this topic, we recommend reading "**Practical Advice to Scale Open Source Legal Support**". The paper examines the role of legal counsel in ensuring open source compliance and offers practical advice that a legal counsel can provide to the software development team. Such practical advice will enable software developers to make daily decisions related to open source licenses without having to go back to the legal counsel for every single question.

Chapter 6

INCORPORATE COMPLIANCE CHECKPOINTS IN PROCESSES

It is necessary to incorporate compliance practices into the development processes to ensure the success of open source compliance efforts. You can achieve this via a number of ways.

1. **Compliance for every internal release:** Update process management to ensure that open source compliance activities are included early enough in the product development cycle to enable the organization to meet its release timelines. Following this model, incremental compliance for future releases becomes straightforward as well.

2. **Updating supply chain procedures:** Tailoring Supply Chain's supplier selection procedures to ensure that open source compliance requirements are considered when performing due diligence on suppliers and their deliverables.

3. **Enforcement of verification:** Using verification steps to ensure that you have met all compliance requirements before any external distribution occurs.

4. **Training employees:** Providing open source compliance training to all staff.

5. **Adopting SPDX to report license information:** Providing license information in SDPX format to minimize any possible errors and standardize the way you report that information.

Chapter 7

DEVELOP AND DEPLOY CHECKLISTS

Checklists are very useful tools to ensure consistency and completeness in carrying out compliance tasks. It is highly recommended to establish checklists for compliance milestones and targeted checklist based on staff responsibilities.

Examples of checklists include:

- A checklist before approving integration of incoming code into the product's source code repository
- A checklist to ensure the fulfillment of obligations
- A checklist for developers
- A checklist for engineering managers
- A checklist for compliance staff
- A checklist for open source legal staff
- A checklist for software procurement staff

To illustrate the point, we provide a sample checklist that showcases various tasks that must be checked before the organization publishes source code packages in fulfillment of license obligations for open source code that was included in a shipping product:

Pre-Distribution Checklist

- Verify the modifications that were introduced to the open source packages are documented and included in the open source releases notes as part of the changelog.
- Ensure that each modified source code file contains an additional entry for a copyright notice, disclaimer, and a generic "changelog" entry.

- Confirm all contents of the source code package have been reviewed by Engineering and confirmed by OSRB.
- Ensure the open source package compiles on a non-corporate standard Linux machine. The goal with this step is to ensure that the open source package you are about to publish compiles on a generic end-user system.
- Update the product manual to:
    - Mention that the product includes open source software.
    - Include a listing of all licenses that correspond to the different open source software included in the product.
    - Offer proper copyright and attribution notices.
    - Indicate how to access the code of the open source package (written offer) either through a web page download or by contacting your company via email or postal mail at a specified address provided in the product manual.
- Perform a linguistic review to ensure that there aren't any inappropriate comments in the source code.
    - Note: Some companies forget to go through a linguistic review, and when the code is published, they face embarrassment from exposure of inappropriate comments left in the source code. Another important reason to perform a linguistic review is to ensure that the source code and comments do not refer to future product code names or capabilities.
- Ensure that existing license, copyright and attribution notices are not disturbed.
- Verify that the source code to be distributed corresponds to the binary that goes with the product, that the source code builds into the same library distributed with the product, and that appropriate instructions are included in the source distribution (derived binaries are usually identical except for time/date stamp).

- Verify that the package adheres to the linkage relationships and interactions defined in your open source policies.
- Ensure inclusion of a copy of the license text, if not already present, in a LICENSE file in the root folder of the open source package.
- If the source code package requires special build tools or environment settings for instance, then include the details in a README file or similar.

Such checklists, especially when automated and integrated with business and development processes, are a great reminder of everything that must be done properly to ensure compliance and reduce the chance or errors.

Chapter 8

BENCHMARK YOUR COMPLIANCE ACTIVITIES

The OpenChain project offers the option of self-certifying to a set of compliance specifications, created by expert stakeholders in the field, that allows a given organization to test itself and declare its adherence to a specific level of compliance. You can learn more at **https://www.openchainproject.org/conformance**. We also cover the OpenChain project in a later section.

Chapter 9

GET INVOLVED WITH INDUSTRY INITIATIVES

Given the widespread adoption of open source software, open source compliance is now a general interest area and no longer a niche interest important to a specific set of companies. Consequently, several initiatives have been launched to support open source compliance efforts at an industry level. We cover the most prominent ones in this section and provide appropriate references for further reading.

OPENCHAIN

The OpenChain Project focuses on increasing open source compliance in the supply chain. The OpenChain Project was formally launched in October 2016 and is hosted by the Linux Foundation. It originated in discussions that occurred three years earlier and that continued at an increasing pace until a formal project was born. The basic idea was simple: Identify key recommended processes for effective open source management. The goal was equally clear: Reduce bottlenecks and risk when using third-party code to make open source license compliance simple and consistent across the supply chain. The key was to pull things together in a manner that balanced comprehensiveness, broad applicability, and real-world usability.

The OpenChain Project is building an industry standard for license compliance. It can be understood as the foundation for open source compliance in the supply chain. Engagement and adoption are free of cost and supported by a vibrant community backed by leading multinationals across multiple sectors. There are three interconnected parts to the OpenChain Project.

- A **Specification** that defines the core requirements of a quality compliance program.
- A **Conformance** method that helps organizations display adherence to these requirements.
- A **Curriculum** to provide basic open source processes and best practices.

Due to its open source origins, the OpenChain Project has an intentionally low barrier to entry. It hosts a series of public mailing lists, teleconferences on the first and third Monday of each month and workshops adjacent to major open source events. All of these activities are open to participation from any party at any time.

The OpenChain Project consists of work teams, a steering and outreach committee, and a governing board. The work teams are accessible by the activities listed above. The steering and outreach committee is accessible to members, work team leads and one elected representative from the broader community. Finally, the governing board is accessible to Platinum Member company representatives.

All participants in the OpenChain community began their involvement via the work teams and evolved their engagement over time based on their specific requirements. This path is recommended for parties considering engagement in the future. The first step is to join the main OpenChain Project mailing list and informally collaborate with the wider community. Everyone—from individuals to representatives of multinational companies—is equally welcome. To engage with the OpenChain Project community please visit the **community page**.

SPDX®

The Software Package Data Exchange® (SPDX®) specification is a standard format for communicating the components, licenses, and copyrights associated with software packages. The SPDX® specification is developed by the SPDX workgroup, which is hosted by the Linux Foundation. The effort started as a grass-roots effort by a few passionate individuals who wanted to solve the problem of communicating compliance information and grew to a much larger effort that includes representatives from more than 20 organizations, including software, systems and tool vendors, foundations and systems integrators, all committed to creating a standard for software package data exchange formats.

The SPDX® standard helps facilitate compliance with free and open source software licenses by standardizing the way license information is shared across the software supply chain. SPDX® reduces redundant work by

providing a common format for companies and communities to share important data about software licenses and copyrights, thereby streamlining and improving compliance.

The SPDX community consists of individuals and companies who are producing and consuming SPDX documents, as well as those who contribute to the SPDX specification, License List and tools. There are three SPDX teams that work on different aspects of the SPDX project. They are:

- **Technical** – Maintains and publishes the specification and tools
- **Outreach** – Supports SPDX adoption efforts
- **Legal** – Publishes and maintains the license list and associated collateral

Each team hosts its own meetings and mailing list, and in general, there are conference calls at least bi-weekly with the technical team. There is also a general **mailing list** along with a monthly meeting for everyone in the SPDX community.

TODO GROUP

The TODO Group is a collection of companies who collaborate on the policies, practices, and pragmatics of running an open source program office, including the open source compliance function. Their collaboration is managed as a community project under the Linux Foundation, and they are a resource to companies who are just starting to get their open source programs established.

The TODO group publishes **guides** for open source program offices, and its members frequently present at open source conferences on best practices. Visit todogroup.org to learn more and reach out to **info@todogroup.org** to find out how to join.

Summary

Open source compliance is often more of an operational and logistical challenge than a legal challenge. Achieving compliance requires the proper policies and processes, training, tools and proper staffing that enables an organization to effectively use open source and contribute to open source projects and communities, while respecting the copyrights of their respective holders, complying with license obligations, and protecting the organization's intellectual property and that of its customers and suppliers.

About two decades ago, I came across open source compliance as a system designer working at Ericsson Research focusing on bringing open source technologies and integrating them in our R&D efforts. Back then, compliance practices were very heavy on the legal side and involved analysis of open source licenses and the various possible interpretations, understanding the implications of using a specific license, and so on. Some of these are still true to some extent, but since then, compliance practices have improved dramatically and in the process, we have learned much

Open source compliance today is a far different problem than what it was two decades ago. Today, it is more about scaling, automation, and building trust within the software supply chain. In this paper, we introduced practical recommendations for companies to improve their open source enterprise compliance practices. For detailed discussions on building open source compliance programs, please download "**Open Source Compliance in the Enterprise**".

Linux Foundation Resources

Assessment of Open Source Practices as Part of Due Diligence in Merger and Acquisition Transactions

This **e-book** is intended as a tool to help evaluate the open source practices of an organization as part of the due diligence process. The checklist presents a set of recommended practices distilled from the experiences of organizations committed to encouraging the use of open source while fully complying with license obligations.

Open Source Compliance in the Enterprise (2nd Edition)

Open Source Compliance in the Enterprise is a practical guide for enterprises on how to best use open source in products and services, and participate in open source communities in a legal and responsible way.

Practical GPL Compliance

Practical GPL Compliance is a compliance guide for startups, small businesses, and engineers, particularly focused on complying with the versions of the GNU General Public License (GPL). Its goal is to provide practical information and quickly address common issues.

Open Source Audits in Merger and Acquisition Transactions

This **e-book** provides an overview and practical guide to open source audits in merger and acquisition transactions, and offers basic guidelines to improve open source compliance preparedness.

OpenChain Curriculum

The **OpenChain Curriculum** helps organizations meet the training and process requirements of the OpenChain Specification. It is also a general open source training and–because of its public domain licensing–you can re-use it for internal or external purposes without any restrictions.

Free Training: Compliance Basics for Developers

A **free online open source compliance course** from the Linux Foundation targeted for developers.

Software Package Data Exchange (SPDX)

SPDX is a standard format for communicating the components, licenses, and copyrights of software packages.

TODO Group

TODO Group is an open **group of companies** who want to collaborate on practices, tools, and other ways to run successful and effective open source projects and programs: **http://todogroup.org/**.

ACKNOWLEDGMENTS

The author would like to express his sincere appreciation to Jessica Wilkerson (Director of Research at the Linux Foundation) for her valuable reviews and feedback.

FEEDBACK

Suggestions for improvement will be appreciated. Please send **comments** to the author directly.

ABOUT THE AUTHOR

Ibrahim Haddad (Ph.D.) is the Executive Director of the **Deep Learning Foundation** that supports and sustains open source innovation in artificial intelligence, machine learning, and deep learning. He previously served as Vice President of R&D and Head of the Open Source Division at Samsung Electronics. At Samsung, he established the global open source division, set and executed Samsung's open source strategy, launched internal and external R&D collaboration projects, supported M&A and corporate VC activities, and represented Samsung in various foundations and consortia. Throughout his career, Haddad has held several technology and portfolio management roles at Ericsson Research, the Open Source Development Lab, Motorola, Palm, Hewlett-Packard and The Linux Foundation. Haddad graduated with Honors from Concordia University (Montréal, Canada) with a Ph.D. in Computer Science, where he was awarded the J. W. McConnell Memorial Graduate Fellowship and the Concordia University 25th Anniversary Fellowship.

Twitter: **@IbrahimAtLinux**
Web: **IbrahimAtLinux.com**
LinkedIn: **linkedin.com/in/ibrahimhaddad**