OPENCHAIN

OpenChain Specification

Version 2.0 (DRAFT) 2018.12.04

DRAFT: This is the draft of the next version 2.0 of the OpenChain specification. Recommended changes to be made over the current released version 2.0 can be found in yellow or red highlights throughout the document. We are targeting to release a new version of the specification in April 2019. The actual version number of the next release has not been finalized and therefore it is subject to change on the day of release.

Contents

0) Update Change Log (temporary section)

We provide a summary of changes made to version 1.2 of the Specification. This is a temporary section that will be removed from the specification in the final version.

- Changed version number from 1.2 to 2.0
- Overhauled the training to move from a more prescriptive to a less prescriptive requirement. Give more flexibility to an organization to define the roles and responsibilities and how to ensure those holding those roles are properly trained. We replace the term training with the two concepts used by the ISO 9001:2015 standard: Competency and Awareness.
- Considering Replacing section titles **Goal 1**, **Goal 2**, … with **Part 1**, **Part** 2, …. They don't represent goals as much as they represent attributes or aspects of a program.
- Added the ability for each organization to define the scope of the compliance program that could range from an entire corporation to a single software offering or product line. A requirement was added Section 1
- Standardized on the term Open Source. The previous specification uses both terms "Open Source" and the "FOSS (Free and Open Source)" interchangeable. It was acknowledged that the term Open Source is more widely recognized and understood for the following reasons: i) Some users of current the specification have pointed out there was confusion between the term Open Source Software and FOSS. This was particularly true for first time readers; ii) Open Source represents a superset (inclusive); iii) The large majority of major foundations use the de facto term Open Source (e.g., Apache, Eclipse, OSI, Linux, OpenStack, Cloud Foundry, …); iv) Most commercial organizations externally use the de facto term Open Source; v) It is also consistent with the term "Open Source Program Office" which represents a major target audience of the specification; vi) The term Open Source is de facto in Asia, largely used in North America and mixed but dominate in Europe; Translations would be simplified by the use of a single term;
- Program Scope Declaration (section 1.4) was added. Provide the flexibility to construct a compliance program that best fits the scope of a given organization's needs. Some organizations could choose to maintain a compliance program for a specific product line while others could choose the program scope to govern software releases of the entire organization. Large organizations may prefer the former example while smaller organizations may prefer the latter.
- Changes Section 2 to deemphasize specific roles and emphasize expected tasks to be performed instead.

1) Introduction

The OpenChain Initiative began in 2013 when a group of software supply chain open source practitioners observed two emerging patterns: 1) significant process similarities existed among organizations with mature open source compliance programs; and 2) there still remained a large number of organizations exchanging software with less developed programs. The latter observation resulted in a lack of trust in the consistency and quality of the Compliance Artifacts accompanying the software being exchanged. As a consequence, at each tier of the supply chain, downstream organizations were frequently redoing the compliance work already performed by other upstream organizations.

A study group was formed to consider whether a standard program specification could be created that would: i) facilitate greater quality and consistency of open source compliance information being shared across the industry; and ii) decrease the high transaction costs associated with open source resulting from compliance rework. The study group evolved into a work group, and in April 2016, formally organized as a Linux Foundation collaborative project.
The Vision and Mission of the OpenChain Initiative are as follows:

- **Vision**: A software supply chain where open source software (OSS) is delivered with trustworthy and consistent compliance information.

- **Mission**: Establish requirements to achieve effective management of open source software (OSS) for software supply chain participants, such that the requirements and associated collateral are developed collaboratively and openly by representatives from the software supply chain, open source community, and academia.

In accordance with the Vision and Mission, this specification defines a set of requirements that if met, would significantly increases the probability that an open source compliance program had achieved a sufficient level of quality, consistency and completeness; although a program that satisfies all the specification requirements does not guarantee full compliance. The requirements represent a base level (minimum) set of requirements a program must satisfy to be considered OpenChain Conforming. The specification focuses on the “what” and “why” qualities of a compliance program as opposed to the “how” and “when” considerations. This ensures a practical level of flexibility that enables different organizations to tailor their policies and processes to best fit their objectives.

Section 2 introduces definitions of key terms used throughout the specification. Section 3 presents the specification requirements where each one has a list of one or more Verification Materials. They represent the evidence that must exist in order for a given requirement to be considered satisfied. If all the requirements have been met for a given program, it would be considered OpenChain Conforming in accordance with version 1.2 of the specification. Verification Materials are not intended to be public, but could be provided under NDA or upon private request from the OpenChain organization to validate conformance.

Additional clarification on how to interpret the specification can be obtained by reviewing the Specification Frequently Asked Questions (FAQs) located at:
https://www.openchainproject.org/specification-faq

2) Definitions

Compliance Artifacts - a collection of artifacts which represent the output of the Open Source management program for a Supplied Software release. The collection may include (but are not limited to) one or more of the following: source code, attribution notices, copyright notices, copy of licenses, modification notifications, written offers, Open Source component bill of materials, SPDX documents and so forth.

Open Source Software (Open Source) ~~FOSS~~ ~~(Free and Open Source Software)~~ - software subject to one or more licenses that meet the Open Source Definition published by the Open Source Initiative (OpenSource.org) or the Free Software Definition (published by the Free Software Foundation) or similar license.

Open Source ~~FOSS~~ Liaison - a designated person who is assigned to receive external Open Source ~~FOSS~~ inquires.

Identified Licenses - a set of ~~FOSS~~ Open Source Software licenses identified as a result of following an appropriate method of identifying licenses that govern the Supplied Software.

OpenChain Conforming Program (Program) - a program that satisfies all the requirements of this specification.

Software Staff - any employee or contractor that defines, contributes to or has responsibility for preparing Supplied Software. Depending on the organization, that may include (but is not limited to) software developers, release engineers, quality engineers, product marketing and product management.

SPDX or Software Package Data Exchange - the format standard created by the SPDX Working Group for exchanging license and copyright information for a given software package. A description of the SPDX specification can be found at www.spdx.org.

Supplied Software - software that an organization delivers to third parties (e.g., other organizations or individuals).

Verification Materials - evidence that must exist in order for a given requirement to be considered satisfied.

3) Requirements

~~Goal 1.0: Know Your Open Source Responsibilities~~Program Foundation

1.1 Policy

A written Open Source policy exists that governs Open Source license compliance of the Supplied Software distribution. The policy must be internally communicated.

Verification Material(s):

- ☐ 1.1.1 A documented Open Source policy.
- ☐ 1.1.2 A documented procedure that makes Software Staff aware of the existence of the Open Source policy (e.g., via training, internal wiki, or other practical communication method).

Rationale:

To ensure steps are taken to create, record and make Software Staff aware of the existence of a Open Source policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.

~~Mandatory Open Source training for all Software Staff exists such that:~~
~~The training, at a minimum, covers the following topics:~~
~~The Open Source policy and where to find a copy;~~
~~Basics of Intellectual Property law pertaining to Open Source and Open Source licenses;~~
~~Open Source licensing concepts (including the concepts of permissive and copyleft licenses);~~
~~Open Source project licensing models;~~
~~Software Staff roles and responsibilities pertaining to Open Source compliance specifically and the Open Source policy in general; and~~
~~Process for identifying, recording and/or tracking of Open Source components contained in Supplied Software.~~
~~Software Staff must have completed Open Source training within the last 24 months to be considered current ("Currently Trained"). A test may be used to allow Software Staff to satisfy the training requirement.~~

1.2 Competence

The organization shall:

- **Identify the roles and the corresponding responsibilities of those roles that affects the performance and effectiveness of the Program;**
- **Determine the necessary competence of person(s) fulfilling each role**
- **Ensure that these persons are competent on the basis of appropriate education, training, and/or experience;**
- **Where applicable, take actions to acquire the necessary competence**
- **Retain appropriate documented information as evidence of competence**

Verification Material(s):

- ~~1.2.1 Open Source training materials covering the above topics (e.g., slide decks, online course, or other training materials).~~
- ~~1.2.2 Documented method for tracking the completion of the training for the Software Staff.~~
- ~~1.2.3 At least 85% of the Software Staff are Currently Trained, as per the definition above. The 85% may not necessarily refer to the entire organization, but to the totality Software Staff governed by the OpenChain Conforming program.~~
- 1.2.1 A documented list of roles with corresponding responsibilities for the different participates in the Open Source compliance program;
- 1.2.2 A documented that identifies the competencies for each role
- 1.2.3 Documented evidence of assessed competence for each program participant

Rationale:
~~To ensure the Software Staff have recently attended Open Source training and that a core set of relevant Open Source topics were covered in the training. The intent is to ensure a core base level set of topics are covered but a typical training program would likely be more comprehensive than what is required here.~~
To ensure that the program participants have obtain a sufficient level of competence for their respected roles and responsibilities.

1.3 Awareness

The organization shall ensure that persons doing work are aware of:

a) The Open Source policy;
b) Relevant Open Source objectives;
c) Their contribution to the effectiveness of the Open Source compliance program;
d) The implications of not conforming to the Open source compliance program requirements.

Verification Material(s):
- 1.3.1 Documented evidence of assessed awareness for each program participant including implications of non-conformance.

Rationale:
To ensure program participants have obtain a sufficient level of awareness for their respected roles and responsibilities.

1.4 Program Scope

Different compliance programs may be governed by different levels of scope. For example, a program could govern a single product line, an entire department or an entire organization. The scope designation needs to be declared for each program seeking conformance.

Verification Material(s):
- 1.4.1 A written statement that clearly defines the scope of the program.

Rationale:
Provide the flexibility to construct a compliance program that best fits the scope of an organization's needs. Some organizations could choose to maintain a compliance program for a specific product line while others could choose the program scope to govern software releases of the entire organization. Large organizations may prefer the former example while smaller organizations may prefer the latter.

1.5~~3~~ License Obligations

A process exists for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license.

Verification Material(s):

- ☐ 1.3.1 A documented procedure to review and document the obligations, restrictions and rights granted by each Identified License.

Rationale:
To ensure a process exists for reviewing and identifying the license obligations for each Identified License for the various use cases.

2.0: Relevant Tasks Defined and Supported~~Assign Responsibility for Achieving Compliance~~

2.1 Maintain a process to effectively respond to external Open Source inquiries. Publicly identify a means by which a third party can make an Open Source compliance inquiry.

~~**2.1 Identify External Open Source Liaison Function ("Open Source Liaison").**~~
~~**Assign individual(s) responsible for receiving external Open Source inquiries;**~~
~~**Open Source Liaison must make commercially reasonable efforts to respond to Open Source compliance inquiries as appropriate; and**~~
~~**Publicly identify a means by which one can contact the Open Source Liaison**~~

Verification Material(s):

- ☐ 2.1.1 Publicly visible method any third party **make an Open Source compliance inquiry** (e.g., via a published contact email address, or the Linux Foundation's Open Compliance Directory).
- ☐ 2.1.2 An internal documented procedure ~~that assigns responsibility for~~for responding to ~~receiving~~ third party Open Source compliance inquiries.

Rationale:
To ensure there is a reasonable way for third parties to contact the organization with regard to Open Source compliance inquiries and that ~~this~~ the organization is prepared to effectively respond~~responsibility has been effectively assigned~~.

2.2 Identify and Resource Open Source Compliance Task(s).

- **Assign accountability to ensure the successful execution of Open Source compliance tasks.**
- **Open Source compliance tasks are sufficiently resourced:**
  - **Time to perform the tasks have been allocated; and**
  - **Commercially reasonable budget has been allocated.**
- **A process exists for reviewing and updating the policy and supporting tasks;**
- **Legal expertise pertaining to Open Source compliance is accessible to those who may need such guidance; and**
- **A process exists for the resolution of Open Source compliance issues.**

~~**2.2 Identify Internal Open Source Compliance Role(s).**~~
~~Assign individual(s) responsible for managing internal Open Source compliance. The Open Source Compliance role and the Open Source Liaison may be the same individual.~~
~~Open Source compliance management activity is sufficiently resourced:~~
~~Time to perform the role has been allocated; and~~
~~Commercially reasonable budget has been allocated.~~
~~Assign responsibilities to develop and maintain Open Source compliance policy and processes;~~
~~Legal expertise pertaining to Open Source compliance is accessible to the Open Source Compliance role (e.g., could be internal or external); and~~
~~A process exists for the resolution of Open Source compliance issues.~~

Verification Material(s):

- ☐ 2.2.1 Document with name of persons, group or function in Open Source Compliance role(s) identified.
- ☐ 2.2.2 The identified roles have been properly staffed and adequate funding provided.

- ☐ 2.2.2 Identification of legal expertise available to address Open Source Compliance matters which could be internal or external.
- ☐ 2.2.3 A documented procedure that assigns internal responsibilities for Open Source compliance.
- ☐ 2.2.4 A documented procedure for handling the review and remediation of non-compliant cases.

Rationale:
To ensure Open Source compliance responsibilities ~~have been~~are effectively ~~assigned~~supported and resourced.

Goal 3: Review and Approve Open Source Content

3.1 A process exists for creating and managing an Open Source component bill of materials which includes each component (and its Identified Licenses) from which the Supplied Software is comprised.

Verification Material(s):

- ☐ 3.1.1 A documented procedure for identifying, tracking and archiving information about the collection of Open Source components from which a Supplied Software release is comprised.
- ☐ 3.1.2 Open Source component records for each Supplied Software release which demonstrates the documented procedure was properly followed.

Rationale:

To ensure a process exists for creating and managing a Open Source component bill of materials used to construct the Supplied Software. A bill of materials is needed to support the systematic review of each component's license terms to understand the obligations and restrictions as it applies to the distribution of the Supplied Software.

3.2 The Open Source management program must be capable of handling common Open Source license use cases encountered by Software Staff for Supplied Software, which may include the following use cases (note that the list is neither exhaustive, nor may all of the use cases apply):

- **distributed in binary form;**
- **distributed in source form;**
- **integrated with other Open Source such that it may trigger copyleft obligations;**
- **contains modified Open Source;**
- **contains Open Source or other software under an incompatible license interacting with other components within the Supplied Software; and/or**
- **contains Open Source with attribution requirements.**

Verification Material(s):

- ☐ 3.2.1 A documented procedure for handling the common Open Source license use cases for the Open Source components of the Supplied Software.

Rationale:

To ensure the program is sufficiently robust to handle an organization's common Open Source license use cases. That a procedure exists to support this activity and that the procedure is followed.

Goal 4: Deliver ~~Open Source Content Documentation and~~Compliance Artifacts

4.1 A process exists for creating the set of Compliance Artifacts for each Supplied Software release.

Verification Material(s):

- 4.1.1 A documented procedure that ensures the Compliance Artifacts are prepared and distributed with the Supplied Software release as required by the Identified Licenses.

- 4.1.2 Copies of the Compliance Artifacts of the Supplied Software release are archived and easily retrievable, and the archive is planned to exist for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer).

Rationale:
To ensure the complete collection of Compliance Artifacts accompany the Supplied Software as required by the Identified Licenses along with other reports created as part of the Open Source review process.

Goal 5: Understand Open Source Community Engagement

5.1 A written policy exists that governs contributions to Open Source projects by the organization. The policy must be internally communicated.

Verification Material(s):

- ☐ 5.1.1 A documented Open Source contribution policy;
- ☐ 5.1.2 A documented procedure that makes all Software Staff aware of the existence of the Open Source contribution policy (e.g., via training, internal wiki, or other practical communication method).

Rationale:
To ensure an organization has given reasonable consideration to developing a policy with respect to publicly contributing to Open Source. The Open Source contribution policy can be made a part of the overall Open Source policy of an organization or be its own separate policy. In the situation where contributions are limited or not permitted at all, a policy should exist making that position clear.

5.2 If an organization permits contributions to Open Source projects then a process exists that implements the Open Source contribution policy outlined in Section 5.1.

Verification Material(s):

- ☐ 5.2.1 Provided the Open Source contribution policy permits contributions, a documented procedure that governs Open Source contributions.

Rationale:
To ensure an organization has a documented process for how the organization publicly contributes Open Source. A policy may exist such that contributions are not permitted at all. In that situation it is understood that no procedure may exist and this requirement would nevertheless be met.

Goal 6: ~~Certify~~Verify Adherence to OpenChain Requirements

6.1 In order for an organization to ~~be~~ have an OpenChain ~~Certified~~Conforming Program, it must affirm that ~~it has an Open Source management~~the program that meets the criteria described in this OpenChain Specification version 1.3~~2~~.

Verification Material(s):

- 6.1.1 An affirmation of the existence of ~~an Open Source management~~a program that meets all the requirements of this OpenChain Specification version 1.3~~2~~.

Rationale:
To ensure that if an organization declares that it has a program that is OpenChain Conforming, that such program has met all the requirements of this specification. The mere meeting of a subset of these requirements would not be considered sufficient.

6.2 Conformance with this version of the specification will last 18 months from the date conformance validation was achieved. Conformance validation requirements can be found on the OpenChain project's website.

Verification Material(s):

- 6.2.1 The organization affirms the existence of a ~~Open Source management~~ program that meets all the requirements of this OpenChain Specification version 1.3~~2~~ within the past 18 months of achieving conformance validation.

Rationale:
It is important for the organization to remain current with the specification if that organization wants to assert program conformance over time. This requirement ensures that the program's supporting processes and controls do not erode if ~~the~~ an ~~conforming~~ organization continues to assert program conformance over time.

Appendix I: Language Translations

To facilitate global adoption we welcome efforts to translate the specification into multiple languages. Because OpenChain functions as an open source project translations are driven by those willing to contribute their time and expertise to perform translations under the terms of the CC-BY 4.0 license and the project's translation policy. The details of the policy and available translations can be found on the OpenChain project specification webpage.