OPENCHAIN

Conformance Handbook for OpenChain Specification 1.1

Revision 1

Miriam Ballhausen, Shane Coughlan

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.

Our Goals

Vision

The vision for the project is to enable a software supply chain where free/open source software (FOSS) is delivered with trusted and consistent compliance information.

Mission

The mission is to establish requirements to achieve effective management of free/open source software (FOSS) 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.

This conformance check corresponds to the OpenChain Specification 1.1[1]. It is designed to assess the status of OpenChain conformance.

---

[1] See https://wiki.linuxfoundation.org/_media/openchain/openchainspec-1.1.draft.pdf

Definitions

The definitions used in this document correspond to the definitions used in the OpenChain Specification 1.1.[2]

[2] See https://wiki.linuxfoundation.org/_media/openchain/openchainspec-1.1.draft.pdf

G1: Know Your FOSS Responsibilities

		No	Yes	Reference to Specification
1.a.	Do you have a documented policy that governs FOSS license compliance of the Supplied Software distribution (e.g., via training, internal wiki, or other practical communication method)?			1.1; 1.1.1
1.b.	Is the policy internally communicated?			1.1.
1.c.	Do you have a documented procedure that communicates the existence of the FOSS policy to all Software Staff?			1.1.2
1.d.	Do you have FOSS training materials (e.g., slide decks or online course) covering the following topics?			1.2; 1.2.1
1.d.i	The FOSS policy and where to find it.			1.2
1.d.ii	Basics of Intellectual Property law pertaining to FOSS and FOSS licenses,			1.2
1.d.iii	FOSS licensing concepts (including the concepts of permissive and copyleft licenses),			1.2
1.d.iv	FOSS project licensing models,			1.2
1.d.v	Software Staff roles and responsibilities pertaining to FOSS compliance specifically and the FOSS policy in general,			1.2
1.d.vi	Process for identifying, recording and/or tracking of FOSS components contained in Supplied Software?			1.2
1.e.	Do you track the completion of the training for all Software Staff?			1.2.2
1.f.	Have 85% or more of the Software Staff completed a FOSS training within the last 24 months?			1.2; 1.2.3
1.g	Do you have a process for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license?			1.3

1.h	Do you have a documented procedure to review and document the obligations, restrictions and rights granted by each Identified License governing the Supplied Software.			1.3.1

G2: Assign Responsibility for Achieving Compliance

		No	Yes	Reference to Specification
2.a.	Have you assigned individual(s) responsible for receiving external FOSS compliance inquiries ("FOSS Liaison")?			2.1, 2.2.1
2.b.	Is the FOSS Liaison function publicly identified (e.g. via an email address and/or the Linux Foundation's Open Compliance Directory)?			2.1.1
2.c.	Do you have a documented procedure that assigns responsibility for receiving FOSS compliance inquiries?			2.1.2, 2.2.3
2.d.	Have you assigned a person, group or function responsible for managing internal FOSS compliance? *The FOSS Compliance role and FOSS Liaison can be the same individual.*			2.2.1
2.e.	Is legal expertise pertaining to FOSS compliance accessible to the FOSS Compliance Role (e.g., internal or external)?			2.2.2
2.f.	Have you assigned responsibilities to develop and maintain FOSS compliance policy and processes?			2.2.3
2.g.	Do you have a documented procedure for handling review and remediation of non-compliant cases?			2.2.4, 2.1.2

G3: Review and Approve FOSS Content

		No	Yes	Reference to Specification
3.a	Do you have a documented procedure for identifying, tracking and archiving information about the collection of FOSS components from which a Supplied Software release is comprised?			3.1.1
3.b	Do you have FOSS component records for each Supplied Software release which demonstrates the documented procedure was properly followed?			3.1.2
3.c	Have you implemented a procedure that handles at least the following common FOSS license use cases for the FOSS components of each supplied Supplied Software release?			3.2.1
3.c.i	distributed in binary form;			3.2
3.c.ii	distributed in source form;			3.2
3.c.iii	integrated with other FOSS such that it may trigger copyleft obligations;			3.2
3.c.iv	contains modified FOSS;			3.2
3.c.v	contains FOSS or other software under an incompatible license interacting with other components within the Supplied Software;			3.2
3.c.vi	contains FOSS with attribution requirements.			3.2

G4: Deliver FOSS Content Documentation and Artifacts

		No	Yes	Reference to Specification
4.a.	Do you have a documented procedure that describes a process that ensures the Compliance Artifacts are distributed with Supplied Software as required by the Identified Licenses?			4.1.1
4.b.	Do you archive copies of the Compliance Artifacts of the Supplied Software?			4.1.2
4.c.	Can you easily retrieve the archived copies of the Compliance Artifacts of the Supplied Software?			4.1.2
4.d.	Are the copies of the Compliance Artifacts archived for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer)?			4.1.2

G5: Understand FOSS Community Engagement

		No	Yes	**Reference to Specification**
5.a.	Do you allow employees to contribute to FOSS projects on behalf of your organization?			5.1
5.b.	Do you have a documented FOSS contribution policy?			5.1.1
5.c.	Is your Software Staff aware of the existence of the FOSS Contribution Policy (e.g. via training, internal wiki, or other practical communication method)?			5.1.2
5.d.	Provided the FOSS contribution policy permits contributions, do you have a documented procedure that describes the FOSS contribution process?			5.2.1