OPENCHAIN

OpenChain Conformance 2016-H1 Conformance Check

Table of Contents

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 free/open source software (FOSS) is delivered with trusted and consistent compliance information.
- **Mission**: 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 Conformance 2016-H1 Specification available under http://openchain.wpengine.com/wp-content/uploads/2016/09/openchain_spec_2016_h1.pdf. It is designed to assess the status of OpenChain conformance in relation to a specific version of the specification.

Definitions

The definitions used in this document correspond to the definitions used in the OpenChain Conformance 2016-H1 Specification available under http://openchain.wpengine.com/wp-content/uploads/2016/09/openchain_spec_2016_h1.pdf.

G1: Know Your FOSS Responsibilities

		No	Yes	Reference to Specification
1.a.	Do you have rules that govern FOSS license compliance of the Supplied Software distribution?			1.1
1.b.	Are these rules internally communicated?			1.1
1.c.	Are these rules documented?			1.1.1
1.d.	Is your Software Staff aware of the rules that govern FOSS license compliance of the Supplied Software distribution?			1.1.2
1.e.	Do you document, how you make your Software Staff aware of the existing procedures that govern FOSS license compliance of the Supplied Software distribution?			1.1.2
1.f.	Do you make your software staff aware of the existence of the FOSS policy using at least one of the following methods?			1.1.2
1.f.i	Training,			
1.f.ii	Internal documentation,			
1.f.iii	Other practical communication methods?			
1.g.	Have 85% or more of the Software Staff attended a FOSS training within the last 24 months?			1.2.3
1.h.	Does this training cover all of the following topics:			1.2.1
1.h.i	Basics of IP law pertaining to FOSS and FOSS licenses,			
1.h.ii	FOSS licensing concepts (including the concepts of permissive and copyleft licenses),			
1.h.iii	FOSS project licensing models,			
1.h.iv	Software Staff roles and responsibilities pertaining to FOSS compliance specifically and the FOSS policy in general,			
1.h.v	Process for identifying, recording and/or tracking of FOSS components contained in Supplied Software,			
1.i.	Do you use one or more of the following FOSS course materials:			
1.i.i	Slide decks,			1.2.1
1.i.ii	Online courses,			
1.i.iii	Other training material?			
1.j.	Do you track the completion of the course for all Software Staff?			
1.k.	Do you provide a written test to track the completion of the course for all Software Staff?			1.2.2

G2: Assign Responsibility for Achieving Compliance

		No	Yes	Reference to Specification
2.a.	Have you assigned an individual or a group of persons responsible for managing internal FOSS compliance?			2.1
2.b.	Is the FOSS compliance management activity sufficiently resourced regarding			
2.b.i	• Time allocated to perform the role,			2.2
2.b.ii	• Budget allocated to the role?			2.2
2.c.	Have you assigned responsibilities to develop and maintain FOSS compliance policy and processes?			2.1.2
2.d.	Is legal expertise pertaining to FOSS compliance accessible to the FOSS Compliance Role (e.g., could be internal or external)?			2.1.1
2.e.	Have you assigned individual(s) responsible for receiving external FOSS compliance inquiries (“FOSS Liaison”)?			
2.f.	Is the FOSS Liaison function publicly identified in one of the following ways:			
2.f.i	• Email address?			
2.f.ii	• Linux Foundation's Open Compliance Directory?			2.1
2.f.iii	• Another practical way?			2.1
2.g.	Can third parties reach the FOSS Liaison by way of electronic communication?			2.1
2.h.	Does the FOSS Liaison respond to FOSS compliance inquiries?			2.2.4
2.i.	Does the FOSS Liaison make commercially reasonable efforts to respond to FOSS compliance inquiries as appropriate?			
2.j.	Can the FOSS Liaison escalate FOSS compliance issues to resolve them?			

G3: Review and Approve FOSS Content

		No	Yes	Reference to Specification
3.a.	Do you identify all FOSS components and their respective Identified Licenses from which Supplied Software is comprised?			3.1
3.b.	Do you list all FOSS components and their respective Identified Licenses from which Supplied Software is comprised?			3.1
3.c.	Is there a procedure for identifying and listing all FOSS components and their respective Identified Licenses) from which Supplied Software is comprised?			3.1
3.d.	Is this procedure documented?			3.1
3.e.	Do you archive the list of FOSS components and their respective Identified Licenses from which Supplied Software is comprised?			3.1
3.f.	Is there a procedure for archiving all FOSS components and their respective Identified Licenses from which Supplied Software is comprised?			3.1
3.g.	Is this procedure documented?			3.1
3.h.	Have you set up a FOSS program?			3.2
3.i.	Is this FOSS program capable of handling at least the following typical FOSS use cases encountered by Software Staff for Supplied Software?			3.2
3.i.i	Distribution in binary form.			
3.i.ii	Distribution in source form.			
3.i.iii	Integration with other FOSS such that it may trigger copyleft obligations.			
3.i.iv	Contains modified FOSS.			
3.i.v.	Contains FOSS or other software under an incompatible license interacting with other components within the Supplied Software.			
3.i.vi	Contains FOSS with attribution requirements.			
3.j.	Are you addressing the typical FOSS use cases encountered by Software Staff for Supplied Software?			3.2.1
3.k.	Have you implemented a process to address these typical FOSS use cases?			3.2.1

G4: Deliver FOSS Content Documentation and Artifacts

		No	Yes	Not required by Identified License	**Reference to Specification**
4.a.	Does the FOSS program ensure that the Supplied Software is accompanied by the required artefacts that might include the following information, if required by the license				4.1
4.a.i	copyright notices,				
4.a.ii	copies of Identified Licenses,				
4.a.iii	modification notifications,				
4.a.iv	attribution notices,				
4.a.v	prominent notices,				
4.a.vi	source code,				
4.a.vii	written offers?				
4.b.	Do you ensure the above Distributed Compliance Artifacts are distributed with Supplied Software?				4.1.1
4.c.	Have you set up a process to ensure the above Distributed Compliance Artifacts are provided with Supplied Software?				4.1.1
4.d.	Is this process documented?				4.1.1
4.e.	Is this process available to the Software Staff?				4.1.1
4.f.	Do you archive copies of the Distributed Compliance Artifacts of the Supplied Software (e.g., legal notices, source code, SPDX documents)?				4.1.2
4.g.	Can you easily retrieve the archived copies of the Distributed Compliance Artifacts of the Supplied Software (e.g., legal notices, source code, SPDX documents)?				4.1.2
4.h.	Is the archived planned to exist 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 contributions of your employees to FOSS projects on behalf of the organization?			5.1
5.b.	Do your employees have to follow rules, when they contribute to FOSS projects on behalf of the organization?			5.1
5.c.	Are these rules captured in a written policy (“FOSS Contribution Policy”)?			5.1.1
5.d.	Is your Software Staff aware of the existence of the FOSS Contribution Policy?			5.1.2
5.e.	Do you make your Software Staff aware of the FOSS Contribution Policy using at least one of the following methods?			5.1.2
5.e.i	Training,			
5.e.ii	Internal documentation,			
5.e.iii	Another practical communication method?			
5.g.	Does the FOSS Contribution Policy cover considerations that might include the following?			5.2
5.g.i	Legal approval for license considerations ,			
5.g.ii	Business rationale or approval			
5.g.iii	Technical review of code to be contributed			
5.g.iv	Community engagement and interaction			
5.g.v	Adherence to project-specific contribution requirements			