ISO #####-#:####(E)

ISO TC ###/SC ##/WG #

Secretariat: XXXX

Information technology — OpenChain Specification

PAS Submission

Version 2.1 DRAFT 2019-11-09

DRAFT: This is the draft of the next version 2.1 of the OpenChain specification. Other than putting the previous 2.0 version into ISO format, only very minor changes to the content are expected to be made to this version. We plan to finalize this version around December 15th. *This section will be removed prior to submitting for ISO approval*.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by the Linux Foundation and was submitted to Joint Technical Committee ISO/IEC JTC 1, *Information technology*, under the “PAS Transposition Process”.

This edition is the first.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document defines the key requirements of a quality open source license compliance program. The objective is to provide a benchmark that builds trust between organizations exchanging software solutions comprised of open source software. Specification conformance provides assurance that a program has been designed to produce the required compliance artifacts (i.e., legal notices, source code and so forth) for each software solution. This document focuses on the "what" and "why" aspects of a program rather than the "how" and "when". This ensures flexibility for different organizations of different sizes in different markets to choose specific policy and process content that fits their size, goals and scope. For instance, an OpenChain conformant program may address a single product line or the entire organization.

This introduction provides the context for all potential users. Clause 2 defines key terms used throughout this document. Clause 3 defines the requirements that a program must satisfy to achieve conformance. A requirement consists of one or more verification materials (i.e., records) that must be produced to satisfy the requirement. Verification materials are not required to be made public, though an organization may choose to provide them to others, potentially under a Non-Disclosure Agreement (NDA).

This document was developed as an open initiative with feedback received from more than 200 contributors. Insight into its historical development can be obtained by reviewing the Specification mailing list and Frequently Asked Questions (FAQs).

Information technology — OpenChain Specification

1 Scope

This document specifies the key requirements of a quality open source license compliance program in order to provide a benchmark that builds trust between organizations exchanging software solutions comprised of open source software.

~~2 Normative references~~

~~The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.~~

~~*Software Package Data Exchange*® (SPDX®), www.spdx.org~~

~~3~~2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

~~3~~2.1
compliance artifacts
a collection of artifacts that represent the output of the program ~~for~~ that accompany the supplied software

Note: The collection may include (but is 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, and SPDX documents.

~~3~~2.2
identified licenses
a set of open source Software licenses identified as a result of following an appropriate method of identifying open source components from which the supplied software is comprised

~~3~~2.3
OpenChain conformant
a program that satisfies all the requirements of this document

~~3~~2.4
open source
software subject to one or more licenses that meet the Open Source Definition published by the Open Source Initiative (see opensource.org/osd)~~[2]~~ or the Free Software Definition published by the Free Software Foundation (see gnu.org/philosophy/free-sw.html)~~[1]~~ or similar license

~~3~~2.5
program
the set of policies, processes and personnel that ~~manage~~ comprise an organization's open source license compliance activities

~~3~~2.6
~~software staff~~program participants

any organization employee or contractor that defines, contributes to or has responsibility for preparing supplied software

Note: Depending on the organization, that may include (but is not limited to) software developers, release engineers, quality engineers, product marketing and product management.

~~3~~2.7
SPDX
the format standard created by the Linux Foundation's SPDX (Software Package Data Exchange) Working Group for exchanging license and copyright information for a given software package (see spdx.org)

~~3~~2.8
supplied software
software that an organization distributes to third parties (e.g., other organizations or individuals)

~~3~~2.9
verification materials
materials that demonstrate that a given requirement of the specification is satisfied

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

~~4~~3 Requirements

~~4.1~~3.1 Program foundation

~~4.1.1~~3.1.1 Policy

A written open source policy shall exist that governs open source license compliance of the supplied software. The policy shall be internally communicated.

Verification material(s):

- 3.1.1.1 A documented open source policy.
- 3.1.1.2 A documented procedure that makes ~~software staff~~program participants 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~~program participants aware of the existence of an 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.

~~4.1.2~~3.1.2 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)~~program participants fulfilling each role

- Ensure that program participants ~~these persons~~ are competent on the basis of appropriate education, training, and/or experience;
- Where applicable, take actions to acquire the necessary competence; and
- Retain appropriate documented information as evidence of competence.

Verification material(s):

- 3.1.2.1 A documented list of roles with corresponding responsibilities for the different participants in the program.
- 3.1.2.2 A document that identifies the competencies for each role.
- 3.1.2.3 Documented evidence of assessed competence for each program participant.

Rationale:

~~To e~~Ensure that the ~~identified participants fulfilling program roles have~~program participants have obtained a sufficient level of competence for their respective roles and responsibilities.

~~4.1.3~~3.1.3 Awareness

The organization shall ensure that the program participants are aware of:

- The open source policy;
- Relevant open source objectives;
- Their contribution to the effectiveness of the program; and
- The implications of not following the Program's requirements.

Verification material(s):

- 3.1.3.1 Documented evidence of assessed awareness for the program participants - ~~each program personnel~~ which should includ~~e~~ing the program's objectives, one's contribution within the program, and implications of program non-conformance.

Rationale:

To ensure the program participants ~~program personnel~~ have obtained a sufficient level of awareness for their respective roles and responsibilities within the program.

~~4.1.4~~3.1.4 Program scope

Different 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.

Verification material(s):

- 3.1.4.1 A written statement that clearly defines the scope and limits of the program.

Rationale:

To provide the flexibility to construct a program that best fits the scope of an organization's needs. Some organizations could choose to maintain a program for a specific product line while others could implement a program to govern the supplied software of the entire organization.

~~4.1.5~~3.1.5 License obligations

A process shall exist for reviewing the identified licenses to determine the obligations, restrictions and rights granted by each license.

Verification material(s):

- 3.1.5.1 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 an organization may encounter (as defined in §3.3.2).

~~4.2~~3.2 Relevant tasks defined and supported

~~4.2.1~~3.2.1 Access

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.

Verification material(s):

- 3.2.1.1 Publicly visible method that allows any third party to make an open source license compliance inquiry (e.g., via a published contact email address, or the Linux Foundation's Open Compliance Directory).
- 3.2.1.2 An internal documented procedure for responding to third party open source license 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 the organization is prepared to effectively respond.

~~4.2.2~~3.2.2 Effectively resourced

Identify and Resource Program Task(s):

- Assign accountability to ensure the successful execution of program tasks.
- Program tasks are sufficiently resourced:
  - Time to perform the tasks have been allocated; and
  - Adequate funding has been allocated.
- A process exists for reviewing and updating the policy and supporting tasks;
- Legal expertise pertaining to open source license compliance is accessible to those who may need such guidance; and
- A process exists for the resolution of open source license compliance issues.

Verification material(s):

- 3.2.2.1 Document with name of persons, group or function in program role(s) identified.
- 3.2.2.2 The identified program roles have been properly staffed and adequate funding provided.
- 3.2.2.3 Identification of legal expertise available to address open source license compliance matters which could be internal or external.
- 3.2.2.4 A documented procedure that assigns internal responsibilities for open source compliance.
- 3.2.2.5 A documented procedure for handling the review and remediation of non-compliant cases.

Rationale:

To ensure: i) program responsibilities are effectively supported and resourced and ii) policies and supporting processes are regularly updated to accommodate changes in open source compliance best practices.

~~4.3~~3.3 Open source content review and approval

~~4.3.1~~3.3.1 Bill of materials

A process shall exist for creating and managing a bill of materials that includes each open source component (and its identified licenses) from which the supplied software is comprised.

Verification material(s):

- 3.3.1.1 A documented procedure for identifying, tracking, reviewing, approving, and archiving information about the collection of open source components from which the supplied software is comprised.
- 3.3.1.2 Open source component records for the supplied software that demonstrates the documented procedure was properly followed.

Rationale:

To ensure a process exists for creating and managing an open source component bill of materials used to construct the supplied software. A bill of materials is needed to support the systematic review and approval of each component's license terms to understand the obligations and restrictions as it applies to the distribution of the supplied software.

~~4.3.2~~3.3.2 License compliance

The program shall be capable of managing common open source license use cases encountered by ~~software staff~~program participants for supplied software, which may include the following use cases (note that the list is neither exhaustive, nor might 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):

- 3.3.2.1 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.

~~4.4~~3.4 Compliance artifact creation and delivery

~~4.4.1~~3.4.1 Compliance artifacts

A process shall exist for creating the set of compliance artifacts for the supplied software.

Verification material(s):

- 3.4.1.1 A documented procedure that describes the process under which the compliance artifacts are prepared and distributed with the supplied software as required by the identified licenses.
- 3.4.1.2 A documented procedure for archiving copies of the compliance artifacts of the supplied software - where the archive is planned to exist for a reasonable period of time[1] since the last offer of the supplied software; or as required by the identified licenses (whichever is longer). Records exist that demonstrate the procedure has been properly followed.

Rationale:

To ensure reasonable commercial efforts have been instituted in the preparation of the compliance artifacts that accompany~~ies~~ the supplied software, as required by the identified licenses.

~~4.5~~3.5 Understanding open source community engagements

~~4.5.1~~3.5.1 Contributions

If an organization considers contributions to open source projects, then

- a written policy shall exist that governs contributions to open source projects;
- the policy shall be internally communicated; and
- a process shall exist that implements the policy

Verification material(s):

If an organization permits contributions to open source projects, then the following shall exist:

- 3.5.1.1 A documented open source contribution policy;
- 3.5.1.2 A documented procedure that governs open source contributions; and
- 3.5.1.3 A documented procedure that makes all ~~software staff~~program participants aware of the existence of the open source contribution policy (e.g., via training, internal wiki, or other practical communication method).

Rationale:

When an organization permits open source contributions, the intent is that the organization has given reasonable consideration to developing and implementing a contribution policy. The open source contribution policy can be made a part of the overall open source policy or be its own separate policy.

~~4.6~~3.6 Adherence to the specification requirements

~~4.6.1~~3.6.1 Conformance

In order for a program to be deemed OpenChain conformant, the organization shall affirm that the program satisfies the requirements presented in this document.

[1] Determined by domain, legal jurisdiction and/or customer contracts

Verification material(s):

- 3.6.1.1 A document affirming the program specified in §3.1.4 satisfies all the requirements of this document.

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 document. The mere meeting of a subset of these requirements is not considered sufficient.

~~4.6.2~~3.6.2 Duration

A program that is OpenChain conformant with this version of the specification shall last 18 months from the date conformance validation was obtained. The conformance validation registration procedure can be found on the OpenChain project's website.

Verification material(s):

- 3.6.2.1 A document affirming the program meets all the requirements of this document, within the past 18 months of obtaining conformance validation.

Rationale:

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

Annex A
(informative)

Language translations of this specification

To facilitate global adoption, efforts to translate the specification into different languages are most welcome. Because OpenChain functions as an open source project, translations are prepared by those willing to contribute their time and expertise to perform the translations. Translations are i) offered under the terms of the CC-BY-4.0 license and ii) consistent with the project's translation policy. The details of the policy and available translations can be found on the OpenChain project's wiki.

~~Bibliography~~

~~[1] *Free Software Definition*, Free Software Foundation, www.fsf.org~~

~~[2] *Open Source Definition*, Open Source Initiative, www.OpenSource.org~~