INTERNATIONAL STANDARD

ISO/IEC 5230

First edition
2020-12

Information technology — OpenChain Specification

Reference number
ISO/IEC 5230:2020(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document should be noted (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 and IEC 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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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 Joint Development Foundation (as OpenChain Specification) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

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 Terms and definitions

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

2.1
compliance artifacts
a collection of artifacts that represent the output of a compliance program and accompany the supplied software

Note: The collection may include (but is not limited to) one or more of the following: attribution notices, source code, build and install scripts, copy of licenses, copyright notices, modification notifications, written offers, open source component bill of materials, and SPDX documents.

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

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

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) or the Free Software Definition published by the Free Software Foundation (see gnu.org/philosophy/free-sw.html) or similar license

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

2.6
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.

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

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

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/

3 Requirements

3.1 Program foundation

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 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 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.

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 program participants fulfilling each role

- Ensure that program participants 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:

Ensure that the program participants have obtained a sufficient level of competence for their respective roles and responsibilities.

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 - which should include the program's objectives, one's contribution within the program, and implications of program non-conformance.

Rationale:

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

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.