International Standard

ISO/IEC 18974

Information technology — OpenChain security assurance specification

First edition
2023-12

Reference number
ISO/IEC 18974:2023(en)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Requirements **3**
4.1 Program foundation 3
4.1.1 Policy 3
4.1.2 Competence 3
4.1.3 Awareness 3
4.1.4 Program scope 4
4.1.5 Standard practice implementation 4
4.2 Relevant tasks defined and supported 5
4.2.1 Access 5
4.2.2 Effectively resourced 5
4.3 Open source software content review and approval 6
4.3.1 Software bill of materials 6
4.3.2 Security assurance 6
4.4 Adherence to the specification requirements 7
4.4.1 Completeness 7
4.4.2 Certification duration 7
Bibliography **8**

© ISO/IEC 2023 – All rights reserved

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by the Joint Development Foundation (JDF) (as OpenChain Security Assurance Specification 1.1) 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 and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

The OpenChain Project (see [4]) is working towards a supply chain where open source is delivered with trusted and consistent compliance information. As part of this mission, the OpenChain Project maintains ISO/IEC 5230 (see [1]), the International Standard for open source license compliance. A natural next step in support of the broader mission was to develop a guide to identify and present the minimum core set of requirements every security assurance program should satisfy with respect to the use of open source software.

For context, ISO/IEC 5230 is a process management specification that identifies inbound, internal and outbound inflection points where a process, policy or training should exist. The identification and tracking of software used and deployed is an inherent part of getting this right, and this allows the approach to also be useful for security or export control.

The OpenChain Project community noticed ISO/IEC 5230 being used in the security domain and decided to develop this security specification to satisfy market demand. This specification is intended to identify and describe the key requirements of a quality security assurance program in the context of using open source Software. It focuses on a narrow subset of primary concern: checking open source Software against publicly known security vulnerabilities like CVEs, GitHub/GitLab vulnerability reports, and so on.

This specification focuses on the “what” and “why” aspects of a quality security assurance program rather than delving into to “how” and “when.” This was a conscious decision to ensure flexibility for organizations of any size and in any market to use this specification. This approach, along with the types of processes identified, is built on more than five years of practical, global feedback around the creation and management of such programs. The result is that a company can frame a program that precisely fits their supply chain requirements, scoped to a single product or a complete legal entity, and take this solution to market quickly and effectively.

This specification was derived from [5]. That reference document went through a final approval process via the OpenChain Project’s normal voting practice to transform into this published security specification. The scope of this specification may expand over time based on community feedback.

Clause 4 defines the requirements that a program must satisfy to achieve a core level of security assurance. Each 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 specification is maintained by the OpenChain Project. Information about participation in that maintenance is available at https://www.openchainproject.org/community.

© ISO/IEC 2023 – All rights reserved

Information technology — OpenChain security assurance specification

1 Scope

This specification contains the key requirements of a quality open source software security assurance program that establishes 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.

Free Software Definition, Free Software Foundation, www.gnu.org/philosophy/free-sw.html

The Minimum Elements For a Software Bill of Materials (SBOM), The United States Department of Commerce, July 12, 2021, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

Open Source Definition, Open Source Software Initiative, www.opensource.org/osd

3 Terms and definitions

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

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

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

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

3.1
component record
data set containing supplier name, component name, version of the component, other unique identifiers, dependency relationship, author of SBOM data and timestamp, as defined by NTIA minimum elements for SBoM

3.2
customer agreement
agreement that the processes used to find, track or fix security issues are regarded as sufficient and correct by relevant customers or user organizations if applicable

3.3
common vulnerabilities and exposures
CVE
disclosed computer software security issues and flaws in a public database

Note 1 to entry: When someone refers to a CVE, they mean a security flaw that has been assigned a CVE ID number within the database. The CVE database is sponsored by the US Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA).

© ISO/IEC 2023 – All rights reserved