

This is a preview of "BS ISO/IEC 5230:2020". [Click here to purchase the full version from the ANSI store.](#)



BSI Standards Publication

Information technology — OpenChain Specification

This is a preview of "BS ISO/IEC 5230:2020". [Click here to purchase the full version from the ANSI store.](#)

National foreword

This British Standard is the UK implementation of ISO/IEC 5230:2020.

The UK participation in its preparation was entrusted to Technical Committee ICT/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 13810 8

ICS 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2020.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

This is a preview of "BS ISO/IEC 5230:2020". [Click here to purchase the full version from the ANSI store.](#)

First edition
2020-12

Information technology — OpenChain Specification



Reference number
ISO/IEC 5230:2020(E)

© ISO/IEC 2020

This is a preview of "BS ISO/IEC 5230:2020". [Click here to purchase the full version from the ANSI store.](#)



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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

This is a preview of "BS ISO/IEC 5230:2020". Click here to purchase the full version from the ANSI store.

Contents

Foreword.....	iv
Introduction.....	v
1 Scope.....	1
2 Terms and definitions	1
3 Requirements.....	2
3.1 Program foundation.....	2
3.1.1 Policy.....	2
3.1.2 Competence	2
3.1.3 Awareness	3
3.1.4 Program scope.....	3
3.1.5 License obligations.....	4
3.2 Relevant tasks defined and supported.....	4
3.2.1 Access.....	4
3.2.2 Effectively resourced.....	4
3.3 Open source content review and approval.....	5
3.3.1 Bill of materials	5
3.3.2 License compliance	6
3.4 Compliance artifact creation and delivery	6
3.4.1 Compliance artifacts.....	6
3.5 Understanding open source community engagements.....	7
3.5.1 Contributions	7
3.6 Adherence to the specification requirements	7
3.6.1 Conformance	7
3.6.2 Duration.....	7
Annex A (informative) Language translations of this specification	9

This is a preview of "BS ISO/IEC 5230:2020". Click here to purchase the full version from the ANSI store.

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.

This is a preview of "BS ISO/IEC 5230:2020". [Click here to purchase the full version from the ANSI store.](#)

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 \(FAQs\)](#).

This is a preview of "BS ISO/IEC 5230:2020". [Click here to purchase the full version from the ANSI store.](#)

This is a preview of "BS ISO/IEC 5230:2020". Click here to purchase the full version from the ANSI store.

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.