INTERNATIONAL STANDARD

ISO/IEC 27036-3

Second edition
2023-06

Cybersecurity — Supplier relationships —

Part 3: Guidelines for hardware, software, and services supply chain security

Cybersécurité — Relations avec le fournisseur —

Partie 3: Lignes directrices pour la sécurité de la chaîne de fourniture en matériel, logiciels et services

Reference number
ISO/IEC 27036-3:2023(E)

© 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

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Structure ... **2**

5 Key concepts ... **2**
5.1 Business case for hardware, software, and services supply chain security ... 2
5.2 Hardware, software, and services supply chain risks and associated threats ... 3
5.3 Acquirer and supplier relationship types ... 3
5.4 Organizational capability ... 4
5.5 System life cycle processes ... 4
5.6 ISMS processes in relation to system life cycle processes ... 5
5.7 ISMS controls in relation to hardware, software, and services supply chain security ... 6
5.8 Essential hardware, software, and services supply chain security practices ... 6

6 Hardware, software, and services supply chain security in life cycle processes ... **7**
6.1 Agreement processes ... 7
6.1.1 Acquisition process ... 7
6.1.2 Supply process ... 9
6.2 Organizational project-enabling processes ... 11
6.2.1 Life cycle model management process ... 11
6.2.2 Infrastructure management process ... 11
6.2.3 Project portfolio management process ... 12
6.2.4 Human resource management process ... 12
6.2.5 Quality management process ... 13
6.2.6 Knowledge management process ... 13
6.3 Technical management processes ... 13
6.3.1 Project planning process ... 13
6.3.2 Project assessment and control process ... 14
6.3.3 Decision management process ... 14
6.3.4 Risk management process ... 14
6.3.5 Configuration management process ... 15
6.3.6 Information management process ... 16
6.3.7 Measurement process ... 16
6.3.8 Quality assurance process ... 16
6.4 Technical processes ... 16
6.4.1 Business or mission analysis process ... 16
6.4.2 Stakeholder needs and requirements definition process ... 16
6.4.3 System requirements definition process ... 17
6.4.4 System architecture definition process ... 18
6.4.5 Design definition process ... 19
6.4.6 System analysis process ... 19
6.4.7 Implementation process ... 19
6.4.8 Integration process ... 20
6.4.9 Verification process ... 20
6.4.10 Transition process ... 21
6.4.11 Validation process ... 22
6.4.12 Operation process ... 23
6.4.13 Maintenance process ... 23
6.4.14 Disposal process ... 24

Annex A (informative) **Correspondence between the controls in ISO/IEC 27002 and this document** ... **26**

© ISO/IEC 2023 – All rights reserved

Annex B (informative) **Essential elements of a software bill of materials** **29**
Bibliography **34**

© 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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity, and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27036-3:2013), which has been technically revised.

The main changes are as follows:

— the structure and content have been aligned with the most recent version of ISO/IEC/IEEE 15288;

— former Annex A has been removed;

— Annex B has been added.

A list of all parts in the ISO/IEC 27036 series can be found on the ISO and IEC websites.

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

Hardware and software products and information technology services are developed, integrated, and delivered globally through deep and physically dispersed supply chains. The supply chain can be a point-to-point or a many-to-many structure and can also be referred to as a supply network. Hardware and software are assembled from many components provided by many suppliers. Information technology services throughout the entire supplier relationship are also delivered through multiple tiers of outsourcing and supply chaining. Acquirers do not have visibility into the practices of hardware, software, and service providers beyond first or possibly second link of the supply chain. With the substantial increase in the number of organizations and people who "touch" a hardware, software, or service, the visibility into the practices by which these products and services are put together has decreased dramatically. This lack of visibility, transparency, and traceability into the hardware, software and service supply chain poses risks to acquiring organizations.

This document provides guidance to hardware, software and service acquirers and suppliers to reduce or manage information security risk. This document identifies the business case for hardware, software, and service supply chain security, specific risks and relationship types, as well as how to develop an organizational capability to manage information security aspects and incorporate a life cycle approach to manage risks supported by specific controls and practices. Its application is expected to result in:

— increased hardware, software, and services supply chain visibility and traceability to enhance information security capability;

— increased understanding by the acquirers of where their products or services are coming from, and of the practices used to develop, integrate, or operate these products or services, to enhance the implementation of information security requirements;

— in case of an information security compromise, the availability of information about what may have been compromised and who the involved actors may be.

This document is intended to be used by all types of organizations that acquire or supply hardware, software, and services. The guidance is primarily focused on the initial link of the first acquirer and supplier, but the principal steps should be applied throughout the chain, starting when the first supplier becomes an acquirer. This change of roles and applying the same steps for each new acquirer-supplier link in the chain is the essential intention of this document. By following this document, information security implications can be communicated among organizations in the chain. This helps identify information security risks and their causes, and may enhance the transparency throughout the chain. Information security concerns related to supplier relationships cover a broad range of scenarios. Organizations desiring to improve trust within their hardware, software, and services supply chain should define their trust boundaries. They should evaluate the risk associated with their supply chain activities, and then define and implement appropriate risk identification and mitigation techniques to reduce the vulnerabilities being introduced through their hardware, software and services supply chain.

The framework and controls outlined in ISO/IEC 27001 and ISO/IEC 27002 provide a useful starting point for identifying appropriate requirements for acquirers and suppliers. The ISO/IEC 27036 series provides further detail on how to establish and monitor supplier relationships. This document has been structured to be harmonized with ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207.

© ISO/IEC 2023 – All rights reserved

Cybersecurity — Supplier relationships —

Part 3: Guidelines for hardware, software, and services supply chain security

1 Scope

This document provides guidance for product and service acquirers, as well as suppliers of hardware, software and services, regarding:

a) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered hardware, software, and services supply chains;

b) responding to risks stemming from this physically dispersed and multi-layered hardware, software, and services supply chain that can have an information security impact on the organizations using these products and services;

c) integrating information security processes and practices into the system and software life cycle processes, as described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, while supporting information security controls, as described in ISO/IEC 27002.

This document does not include business continuity management/resiliency issues involved with the hardware, software, and services supply chain. ISO/IEC 27031 addresses information and communication technology readiness for business continuity.

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.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27036-1, *Cybersecurity — Supplier relationships — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27036-1 and the following 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
software bill of materials
SBoM
inventory of software components, sub-components and dependencies with associated information

© ISO/IEC 2023 – All rights reserved