INTERNATIONAL STANDARD

ISO/IEC 27036-2

Second edition
2022-06

Cybersecurity — Supplier relationships —

Part 2: **Requirements**

Partie 2: Exigences

Reference number
ISO/IEC 27036-2:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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 2022 – All rights reserved

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **1**
5 Structure of this document **2**
5.1 Clause 6 2
5.1.1 General 2
5.1.2 Organizational project-enabling processes 2
5.1.3 Technical management processes 2
5.2 Clause 7 3
5.3 Relationship between Clause 6 and Clause 7 3
5.4 Annexes 5
6 Information security in supplier relationship management **5**
6.1 Agreement processes 5
6.1.1 Acquisition process 5
6.1.2 Supply process 7
6.2 Organizational project-enabling processes 8
6.2.1 Life cycle model management process 8
6.2.2 Infrastructure management process 8
6.2.3 Project portfolio management process 9
6.2.4 Human resource management process 9
6.2.5 Quality management process 10
6.2.6 Knowledge management process 10
6.3 Technical management processes 11
6.3.1 Project planning process 11
6.3.2 Project assessment and control process 11
6.3.3 Decision management process 11
6.3.4 Risk management process 11
6.3.5 Configuration management process 13
6.3.6 Information management process 13
6.3.7 Measurement process 13
6.3.8 Quality assurance process 14
6.4 Technical processes 14
6.4.1 Business or mission analysis process 14
6.4.2 Architecture definition process 14
7 Information security in a supplier relationship instance **15**
7.1 Supplier relationship planning process 15
7.1.1 Objective 15
7.1.2 Inputs 15
7.1.3 Activities 15
7.1.4 Outputs 16
7.2 Supplier selection process 17
7.2.1 Objectives 17
7.2.2 Inputs 17
7.2.3 Activities 17
7.2.4 Outputs 21
7.3 Supplier relationship agreement process 21
7.3.1 Objective 21
7.3.2 Inputs 22
7.3.3 Activities 22

© ISO/IEC 2022 – All rights reserved

7.3.4 Outputs 24
7.4 Supplier relationship management process 25
7.4.1 Objectives 25
7.4.2 Inputs 26
7.4.3 Activities 26
7.4.4 Outputs 27
7.5 Supplier relationship termination process 28
7.5.1 Objectives 28
7.5.2 Inputs 28
7.5.3 Activities 28
7.5.4 Outputs 29
Annex A (informative) **Correspondence between ISO/IEC/IEEE 15288 and this document** **30**
Annex B (informative) **Correspondence between ISO/IEC 27002 controls and this document** **32**
Annex C (informative) **Objectives from Clauses 6 and 7** **34**
Bibliography **38**

© ISO/IEC 2022 – 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).

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 https://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. 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 27036-2:2014), 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 15288.

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 2022 – All rights reserved

Introduction

Organizations throughout the world work with suppliers to acquire products and services. Many organizations establish several supplier relationships to cover a variety of business needs, such as operations or manufacturing. Conversely, suppliers provide products and services to several acquirers.

Relationships between acquirers and suppliers established for the purpose of acquiring a variety of products and services may introduce information security risks to both acquirers and suppliers. These risks are caused by mutual access to the other party's assets, such as information and information systems, as well as by the difference in business objectives and information security approaches. These risks should be managed by both acquirers and suppliers.

This document:

a) specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships;

b) facilitates mutual understanding of the other party's approach to information security and tolerance for information security risks;

c) reflects the complexity of managing risks that can have information security impacts in supplier and acquirer relationships;

d) is intended to be used by any organization willing to evaluate the information security in supplier or acquirer relationships;

e) is not intended for certification purposes;

f) is intended to be used to set a number of defined information security objectives applicable to a supplier and acquirer relationship that is a basis for assurance purposes.

ISO/IEC 27036-1 provides an overview and concepts associated with information security in supplier relationships.

ISO/IEC 27036-3 provides guidelines for the acquirer and the supplier for managing information security risks specific to the ICT products and services supply chain.

ISO/IEC 27036-4 provides guidelines for the acquirer and the supplier for managing information security risks specific to the cloud services.

© ISO/IEC 2022 – All rights reserved

Cybersecurity — Supplier relationships —

Part 2: Requirements

1 Scope

This document specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.

These requirements cover any procurement and supply of products and services, such as manufacturing or assembly, business process procurement, software and hardware components, knowledge process procurement, build-operate-transfer and cloud computing services.

This document is applicable to all organizations, regardless of type, size and nature.

To meet the requirements, it is expected that an organization has internally implemented a number of foundational processes or is actively planning to do so. These processes include, but are not limited to: business management, risk management, operational and human resources management, and information security.

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 and ISO/IEC 27036-1 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/

4 Abbreviated terms

ASP	application service provider
BCP	business continuity plan
ICT	information and communication technology
ISMS	information security management system

© ISO/IEC 2022 – All rights reserved