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 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

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.

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.

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

ITT	invitation to tender
PII	personally identifiable information
RFP	request for proposal

5 Structure of this document

5.1 Clause 6

5.1.1 General

Clause 6 defines fundamental and high-level information security requirements applicable to the management of several supplier relationships. Any of the processes in Clause 6 can be applied to individual supplier relationships at any point in that supplier relationship life cycle based on the appropriate assessment of the risk.

The requirements are structured according to life cycle processes specified in ISO/IEC/IEEE 15288. The requirements shall be applied by the acquirer and by the supplier to ensure that these organizations are able to manage information security risks resulting from supplier relationships.

NOTE Clause 6 only references the ISO/IEC/IEEE 15288 life cycle processes that are relevant to information security in supplier relationships.

Organizations can enter into a variety of supplier relationships. Suitable relationships between acquirers and suppliers are achieved using agreements defining information security roles and responsibilities with respect to the supplier relationship.

The following agreement processes support procurement or supply of a product or service from both strategic and information security perspectives:

a) acquisition process;

b) supply process.

5.1.2 Organizational project-enabling processes

The organizational project-enabling processes are concerned with ensuring that the resources, such as the financial ones, needed to enable the project to meet the needs and expectations of the organization's interested parties are met.

The following organizational project-enabling processes support the establishment of the environment in which supplier relationships are planned or conducted:

a) life cycle model management process;

b) infrastructure management process;

c) project portfolio management process;

d) human resource management process;

e) quality management process;

f) knowledge management process.

5.1.3 Technical management processes

Technical management processes are concerned with rigorous project management and project support, covering one or more suppliers.

The following technical management processes support the establishment of the environment in which supplier relationship instances are planned or conducted:

a) project planning process;

b) project assessment and control process;

c) decision management process;

d) risk management process;

e) configuration management process;

f) information management process;

g) measurement process;

h) quality assurance process.

Technical processes are generally used by a supplier for the following purposes:

- define requirements for a product or service;
- transform these requirements into an effective product or service;
- sustain the provision of the procured or supplied product or service;
- permit consistent and quality reproduction of the procured or supplied product or service when necessary;
- dispose of the product or service when it has been decided to retire it.

NOTE ISO/IEC 27036-3 provides guidance on other technical processes in addition to the ones defined in this document.

5.2 Clause 7

Clause 7 defines fundamental information security requirements applicable to an acquirer and a supplier within the context of a single supplier relationship instance.

These requirements are structured using the following supplier relationship life cycle:

a) supplier relationship planning process;

b) supplier selection process;

c) supplier relationship agreement process;

d) supplier relationship management process;

e) supplier relationship termination process.

Requirements in Clause 7 shall be applied by the acquirer and the supplier involved in a supplier relationship to ensure that these organizations are able to manage relevant information security risks.

5.3 Relationship between Clause 6 and Clause 7

Figure 1 describes the scope of the fundamental information security requirements in connection with the processes defined in Clauses 6 and 7.

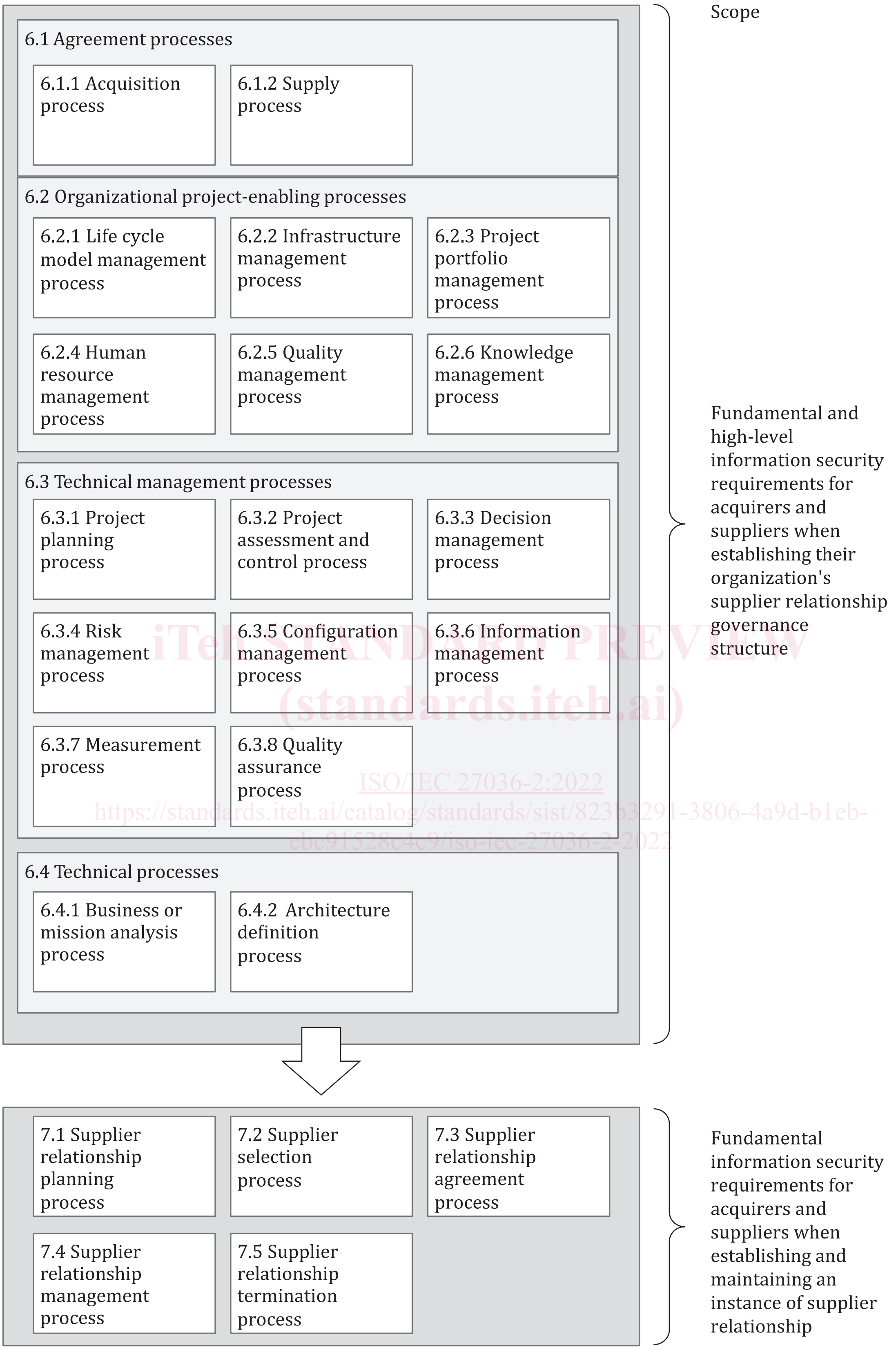
Scope
6.1 Agreement processes
6.1.1 Acquisition process
6.1.2 Supply process
6.2 Organizational project-enabling processes
6.2.1 Life cycle model management process
6.2.2 Infrastructure management process
6.2.3 Project portfolio management process
6.2.4 Human resource management process
6.2.5 Quality management process
6.2.6 Knowledge management process
6.3 Technical management processes
6.3.1 Project planning process
6.3.2 Project assessment and control process
6.3.3 Decision management process
6.3.4 Risk management process
6.3.5 Configuration management process
6.3.6 Information management process
6.3.7 Measurement process
6.3.8 Quality assurance process
6.4 Technical processes
6.4.1 Business or mission analysis process
6.4.2 Architecture definition process
Fundamental and high-level information security requirements for acquirers and suppliers when establishing their organization's supplier relationship governance structure
7.1 Supplier relationship planning process
7.2 Supplier selection process
7.3 Supplier relationship agreement process
7.4 Supplier relationship management process
7.5 Supplier relationship termination process
Fundamental information security requirements for acquirers and suppliers when establishing and maintaining an instance of supplier relationship

Figure 1 — Scope of fundamental information security requirements defined in Clauses 6 and 7

Some of the text of 6.1 to 6.4 and of 7.1 to 7.5 is structured in tables which shall be interpreted as follows:

Acquirer
Text specific to the acquirer.

Supplier
Text specific to the supplier.

Acquirer	Supplier
Text specific to both the acquirer and the supplier, unless explicitly stated.	
Text specific to the acquirer.	Text specific to the supplier.

5.4 Annexes

Annex A provides correspondence between subclauses of ISO/IEC/IEEE 15288 that are relevant to supplier relationships and subclauses of this document.

Annex B provides correspondence between subclauses of this document and information security controls listed in ISO/IEC 27002 that are relevant to supplier relationships.

Annex C provides the consolidated list of objectives that are stated in Clauses 6 and 7 for the acquirer and the supplier.

6 Information security in supplier relationship management

6.1 Agreement processes

6.1.1 Acquisition process

6.1.1.1 Objective

The following objective shall be met by the acquirer for successfully managing information security within the acquisition process:

- Establish a supplier relationship strategy that:
  - is based on the information security risk tolerance of the acquirer;
  - defines the information security foundation to use when planning, preparing, managing and terminating the procurement of a product or service.

6.1.1.2 Activities

The minimum activities shown in Table 1 shall be executed by the acquirer to meet the objective defined in 6.1.1.1.

Table 1 — Acquisition process activities

Acquirer
a) Define, implement, maintain and improve a supplier relationship strategy containing the following: 1) Management motives, needs and expectations from procuring products or services expressed from business, operational, legal and regulatory perspectives. 2) Management commitment to allocating necessary resources.

Table 1 *(continued)*

Acquirer
3) An information security risk management framework to use for assessing information security risks accompanying the procurement of a product or service.
NOTE Subclause 6.3.4 defines information security requirements for the establishment of an information security risk management framework.
4) A framework to use when defining information security requirements during the supplier relationship planning process.
This framework shall be defined following information security guidelines and rules, such as information security policy and information classification, established by the acquirer.
Information security requirements defined in this framework need to be customized to each supplier relationship instance, considering type and nature of the product or service that is procured.
This framework shall also include the following:
i) methods for suppliers to provide evidence for adherence to the defined information security requirements;
ii) methods for the acquirer to validate suppliers' adherence to the defined information security requirements and the frequency of such validation;
iii) processes for sharing information about information security changes, incidents and other relevant events among the acquirer and suppliers.
5) A supplier selection criteria framework to use when selecting a supplier, which includes the following:
i) Methods for assessing the information security maturity required from a supplier.
The following elements can be requested from the supplier to evaluate its information security maturity:
a) past security-relevant performance;
b) evidence of pro-active management of information security (e.g. holding an ISO/IEC 27001 certification relevant to the supply of the product or service);
c) evidence of documented and tested business continuity and ICT continuity plans.
ii) Methods to be used for assessing evidence provided by a supplier based on the defined information security requirements.
iii) Methods for assessing supplier acceptance of the following:
a) information security requirements defined in the supplier relationship plan;
b) commitment to support the acquirer in its compliance monitoring and enforcement activities;
c) transition of the product or service supply that may be procured when it has been previously manufactured or operated by the acquirer or by a different supplier;
d) termination of the product or service supply.
iv) Supplier-specific requirements, to be defined in accordance with business, legal, regulatory, architectural, policy and contractual expectations from the acquirer, such as:
a) financial strength of the supplier for being able to supply the product or service;
b) location of the supplier from which the product or service will be supplied.
6) High-level information security requirements to use when defining the following:
i) transition plan to transfer a product or service procured to a different supplier;
ii) information security change management procedure;
iii) information security incident management procedure;
iv) compliance monitoring and enforcement plan;
v) termination plan to terminate the procurement of a product or service.
b) Appoint an individual responsible for handling the information security aspects of the supplier relationship strategy and ensure that this individual is appropriately and regularly trained.

Table 1 *(continued)*

Acquirer
c) Ensure the supplier relationship strategy is reviewed at least once a year, whenever significant business, legal, regulatory, architectural, policy and contractual changes occur, or when a product or service being procured can significantly impact the acquirer.

6.1.2 Supply process

6.1.2.1 Objective

The following objective shall be met by the supplier for successfully managing information security within the supply process:

- Establish an acquirer relationship strategy that:
  - is based on the information security risk tolerance of the supplier;
  - defines the information security baseline to use when planning, preparing, managing and terminating the supply of a product or service.

6.1.2.2 Activities

The minimum activities shown in Table 2 shall be executed by the supplier to meet the objective defined in 6.1.2.1.

Table 2 — Supply process activities

Supplier
a) Define, implement, maintain and improve an acquirer relationship strategy containing the following: 1) management motives, needs and expectations from supplying of products or services expressed from business, operational and legal perspectives; 2) management commitment to allocate necessary resources; 3) an information security risk management framework to use for assessing information security risks that accompany the supply of a product or a service; NOTE 1 6.3.4 defines information security requirements for the establishment of an information security risk management framework. 4) an information security management framework by: i) defining, implementing, maintaining and improving information security management within the organization; NOTE 2 An ISMS establishment based on ISO/IEC 27001 can serve to ensure adequate information security management within the organization and to demonstrate its level to acquirers. ii) ensuring that the supplier information security requirements stated in existing acquirer tender documents and supplier relationship agreements conform to these requirements; any gap shall be addressed to satisfy acquirer's information security requirements of existing supplier relationship agreements; iii) defining a process to accept, interpret, apply and measure acquirer information security requirements; 5) methods for: i) demonstrating supplier's capacity to supply a product or service of acceptable quality; ii) providing evidence of adherence to information security requirements defined by acquirers; 6) high-level information security requirements to use when defining the following: i) transition plan to support the transfer of a product or service supply when it has been previously manufactured or operated by an acquirer or by another supplier; ii) information security change management procedure;