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.

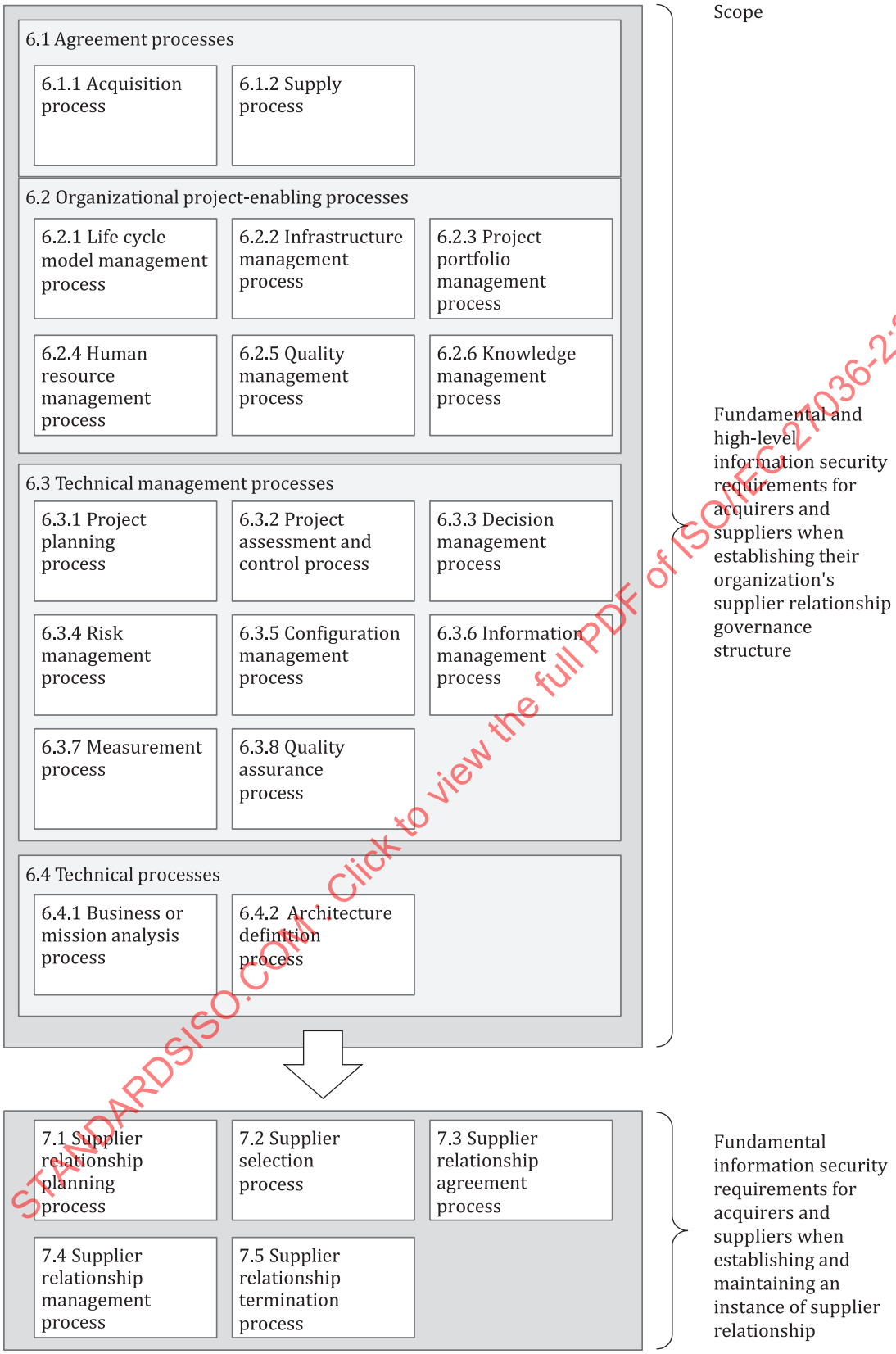

Figure 1 — Scope of fundamental information security requirements defined in Clauses 6 and 7

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;

Table 2 *(continued)*

Supplier
iii) information security incident management procedure; iv) processes for sharing information about information security changes, incidents and other relevant events among the supplier and acquirers; v) process for handling corrective actions; vi) termination plan to terminate the supply of a product or service;
b) appoint an individual responsible for handling the information security aspects of the acquirer relationship strategy and ensure that this individual is appropriately and regularly trained;
c) ensure the acquirer relationship strategy is reviewed at least once a year, whenever significant business, legal, regulatory, architectural, policy and contractual changes occur, or when a supplier relationship is established that can significantly impact the supplier.

6.2 Organizational project-enabling processes

6.2.1 Life cycle model management process

The acquirer and the supplier shall establish the life cycle model management process when managing information security in supplier relationships.

NOTE The purpose of this process is to define, maintain and ensure availability of policies, life cycle processes, life cycle models and procedures for use by the organization. There are no specific information security objectives and activities for acquirers or suppliers to consider when internally establishing this process.

6.2.2 Infrastructure management process

6.2.2.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the infrastructure management process:

— Provide the enabling infrastructure to support the organization in managing information security within supplier relationships.

6.2.2.2 Activities

The minimum activities shown in Table 3 shall be executed by the acquirer and the supplier to meet the objective defined in 6.2.2.1.

Table 3 — Infrastructure management process activities

Acquirer	Supplier
a) Define, implement, maintain and improve physical and logical security infrastructure capabilities for protecting acquirer's or supplier's assets, such as information and information systems.	
b) Define, implement, maintain and improve contingency arrangements to ensure that the procurement or the supply of a product or service can continue in the event of its disruption caused by natural causes or by humans. These arrangements should be based on information security risk assessments and associated treatment plans resulting from the procurement or the supply of a product or service, and should include: 1) the provision of alternative, secure facilities for the product or service supply to continue; 2) escrow of information and proprietary technologies, such as application source code and cryptographic keys, using a trusted third party; 3) recovery arrangements to ensure continued availability of information stored at contractor or subcontractor premises;	

Table 3 *(continued)*

Acquirer	Supplier
4) alignment with business continuity constraints expressed by an acquirer or a supplier. NOTE The following International Standards provide requirements and guidelines on contingency arrangements: — ISO/IEC 27031; — ISO 22313; — ISO 22301.	

6.2.3 Project portfolio management process

6.2.3.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the project portfolio management process:

— Establish a process for considering information security and overall business mission implications and dependencies for each individual project for those projects where suppliers or acquirers are involved.

6.2.3.2 Activities

The minimum activities shown in Table 4 shall be executed by the acquirer and the supplier to meet the objective defined in 6.2.3.1.

Table 4 — Project portfolio management process activities

Acquirer	Supplier
a) Define, implement, maintain and improve a process for identifying and categorizing suppliers or acquirers based on the sensitivity of the information shared with them and on the access level granted to them to acquirer's or supplier's assets, such as information and information systems; NOTE A supplier having very limited access to the acquirer's assets, such as information and information systems, can be categorized as not critical, while a supplier developing critical business software for the acquirer can be categorized as critical.	
b) define, implement, maintain and improve a process for ensuring that information security considerations are integrated into the evaluation of supplier performance as a part of each individual project;	
c) ensure that project closeout involving a supplier or an acquirer integrates information security activities documented in a termination plan.	

6.2.4 Human resource management process

6.2.4.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the human resource management process:

— Ensure the acquirer and the supplier are provided with necessary human resources including screening requirements, confidentiality requirements, training and awareness to ensure personnel competences are regularly maintained and consistent with information security needs in supplier relationships.

6.2.4.2 Activities

The minimum activities shown in Table 5 shall be executed by the acquirer and the supplier to meet the objective defined in 6.2.4.1.

Table 5 — Human resource management process activities

Acquirer	Supplier
a) Consider the following in the information security training and awareness programme as part of the human resource management process:	
1) information security guidelines and rules, such as the information security policy and information classification, for personnel dealing with supplier relationships;	
2) information security requirements generally defined in a supplier relationship agreement, for demonstrating the existence of such requirements that meet acquirer's needs and expectations;	
3) suppliers' past performance in regard to their level of conformity with acquirer's information security requirements, for demonstrating potential lack of compliance;	
b) identify and assess personnel with regard to their access to and ability to disclose or modify information within a supplier relationship, such as sensitive information or intellectual property that should not be disclosed or modified;	
c) ensure that identified personnel, especially those engaged in the information security or in the decision of the procurement or supply of a product or service, have adequate competencies and qualifications;	
d) train these personnel on information security aspects of supplier relationships to particularly ensure that the handling of sensitive information is correctly understood;	
e) ensure that detailed criminal and background checks have been performed for personnel assuming key positions in supplier relationships, where permissible by law;	
f) designate contact points and their backups for critical aspects of each supplier relationship including operations and maintenance to ensure minimum impact when personnel leave the organization.	

6.2.5 Quality management process

The acquirer and the supplier shall establish a quality management process when managing information security in supplier relationships.

NOTE The purpose of this process is to ensure that products and services meet organization quality objectives and achieve customer satisfaction. There are no specific information security objectives and activities for acquirers and suppliers to consider when internally establishing this process.

6.2.6 Knowledge management process

The acquirer and the supplier shall establish the knowledge management process when managing information security in supplier relationships.

NOTE The purpose of this process is to create the capability and assets that enable the organization to exploit opportunities to re-apply existing knowledge. There are no specific information security objectives and activities for acquirers or suppliers to consider when internally establishing this process.

6.3 Technical management processes

6.3.1 Project planning process

6.3.1.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the project planning process:

— Establish a project planning process addressing information security of supplier relationships.

6.3.1.2 Activities

The minimum activities shown in Table 6 shall be executed by the acquirer and the supplier to meet the objective defined in 6.3.1.1.

Table 6 — Project planning process activities

Acquirer	Supplier
— Include the following as part of the project planning process: — impacts on project costs, plans and schedule of information security requirements defined for assets used within the procurement or supply of a product or service; — integration of information security into relevant project roles, responsibilities, accountabilities and authorities; — securing sensitive internal information that can be impacted by supplier relationships, such as financial, operational, intellectual property, PII for customers or staff; — resources, such as financial ones, that are required to ensure protection of assets.	

6.3.2 Project assessment and control process

The acquirer and the supplier shall establish a project assessment and control process when managing information security in supplier relationships.

NOTE The purpose of this process is to determine the status of the project and direct project plan execution to ensure that the project performs according to plans and schedules, within projected budgets, to satisfy technical objectives. There are no specific information security objectives and activities for acquirers or suppliers to consider when internally establishing this process (adapted from ISO/IEC/IEEE 15288).

6.3.3 Decision management process

The acquirer and the supplier shall establish a decision management process when managing information security in supplier relationships.

NOTE The purpose of this process is to select the most beneficial course of project action where alternatives exist. There are no specific information security objectives and activities for acquirers or suppliers to consider when internally establishing this process (adapted from ISO/IEC/IEEE 15288).

6.3.4 Risk management process

6.3.4.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the risk management process:

— Continuously address information security risks in supplier relationships and throughout their life cycle including re-examining them periodically or when significant business, legal, regulatory, architectural, policy and contractual changes occur.

6.3.4.2 Activities

The minimum activities shown in Table 7 shall be executed by the acquirer and the supplier to meet the objective defined in 6.3.4.1.

Table 7 — Risk management process activities

<table>
<tr><th>Acquirer</th><th>Supplier</th></tr>
<tr><td colspan="2">a) Integrate information security risk management into the organization's existing risk management framework that can be used in identifying, assessing, and treating information security risks that accompany:
1) existing instances of procurement or supply of product or service;
2) suppliers or acquirers involved in these instances;
3) the procurement or supply of a product or service.
NOTE ISO/IEC 27005, ISO 31000 and ISO/IEC/IEEE 15288 provide guidance on risk management.
Care should be taken to ensure that this framework is defined:
— following the organization's business or mission and considering legal, regulatory, architectural, policy and contractual requirements applicable to the organization;</td></tr>
<tr><td>— considering the assessment of suppliers in terms of:
— past history, such as previous and current business arrangements and dispute information;
— contractual agreements, such as supplier relationship agreements and non-disclosure agreements;
— information security implications of the product or service procurement, including acquirer's assets handled, underlying technology infrastructure, business dependency and sub-contractors used;
— supplier capability to demonstrate its maturity in information security;
— considering the following when defining the method for assessing suppliers:
— the type of assessment to apply to suppliers, such as a self-assessment or an independent assessment performed by a third party;
— the level of details of the assessment and its frequency of execution.</td><td>— considering the assessment of acquirers in terms of:
— past history, such as previous and current business arrangements and dispute information;
— contractual agreements, such as supplier relationship agreements and non-disclosure agreements;
— information security implications of the product or service supply, including:
— information security requirements given in the tender document or supplier relationship agreement;
— information security risks of the supplier which emerge from the acquirer's access to supplier's information in the case where, for example, the acquirer applies a level of control on the provider's production process with access to the supplier's sensitive information.</td></tr>
<tr><td colspan="2">b) Apply this information security risk management framework:
1) to categorize existing instances of procurement or supply of product or service;
2) to categorize suppliers or acquirers involved in these instances;
3) when:
i) defining the supplier or acquirer relationship strategy;
ii) planning to procure or supply a product or service.
If the organization holds an ISO/IEC 27001 certification, it is recommended to include the assets resulting from the procurement or supply of a product or service in the ISMS asset inventory to ensure continuous information security risk assessment and treatment.</td></tr>
</table>

6.3.5 Configuration management process

If applicable, the acquirer and the supplier shall establish a configuration management process when managing information security in supplier relationships.

NOTE The purpose of this process is to establish and maintain the integrity of all identified outputs of a project or process and make them available to concerned parties. There are no specific information security objectives and activities to consider by each of these organizations when internally establishing this process (adapted from ISO/IEC/IEEE 15288).

When implementing the configuration management process, it is recommended to consider ISO/IEC 27002, which provides guidance in change management and change control procedures.

6.3.6 Information management process

The acquirer and the supplier shall integrate information security into an existing information management process to consider the sensitivity of information that can be exchanged during supplier relationships.

NOTE 1 The purpose of this process is to provide relevant, timely, complete, valid and, if required, confidential information to designated parties. There are no specific information security objectives and activities to consider by each of these organizations when internally establishing this process (adapted from ISO/IEC/IEEE 15288).

NOTE 2 Establishing an ISMS based on ISO/IEC 27001 can serve as a basis for applying adequate information security of information exchanges, in case of information security changes and incidents happening during supplier relationships.

6.3.7 Measurement process

6.3.7.1 Objective

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

— Collect, analyse and report information security measures related to the procurement or supply of a product or service to demonstrate the maturity of information security in supplier relationships and to support effective management of processes.

6.3.7.2 Activities

The minimum activities shown in Table 8 shall be executed by the acquirer and the supplier to meet the objective defined in 6.3.7.1.

Table 8 — Measurement process activities

Acquirer	Supplier
a) Define, implement, maintain and improve an information security measurement framework that can be used for assessing the procurement or supply of product or service. NOTE ISO/IEC 27004 provides guidance on information security measurement that can be applied to develop and implement specific measures related to information security in supplier relationships. It is recommended to define this framework based on the organization's business or mission and considering legal, regulatory, architectural, policy and contractual requirements applicable to the organization.	
b) Apply this information security measurement framework when preparing a supplier relationship instance to agree with the other party about what is to be measured, how the measures are to be reported, the frequency of reporting and the actions to be undertaken if the measures do not meet specified criteria.	

6.3.8 Quality assurance process

The acquirer and the supplier shall establish the quality assurance process when managing information security in supplier relationships.

NOTE The purpose of this process is to ensure the effective application of the organization's quality management process to the project. There are no specific information security objectives and activities for acquirers or suppliers to consider when internally establishing this process.

6.4 Technical processes

6.4.1 Business or mission analysis process

6.4.1.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the business or mission analysis process:

— Establish a process for considering information security during the business and mission analysis process.

6.4.1.2 Activities

The minimum activities shown in Table 9 shall be executed by the acquirer and the supplier to meet the objective defined in 6.4.1.1.

Table 9 — Business or mission analysis process activities

Acquirer	Supplier
— Integrate information security considerations into the business or mission analysis process to ensure business or mission requirements and information security concerns are appropriately balanced in managing supplier relationships.	

6.4.2 Architecture definition process

6.4.2.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the architecture definition process:

— Establish a technical framework for sustained procurement of product or service that satisfies the purpose of supplier relationships.

6.4.2.2 Activity

The minimum activities shown in Table 10 shall be executed by the acquirer and the supplier to meet the objective defined in 6.4.2.1.

Table 10 — Architecture definition process activities

Acquirer	Supplier
— Establish a process to define, implement, maintain and improve the information security requirements of the product or service that can be procured or supplied to facilitate sustained and consistent application.	

7 Information security in a supplier relationship instance

7.1 Supplier relationship planning process

7.1.1 Objective

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

— Document the decision adopted by management to initiate the procurement of a product or service, as well as the information security considerations related to this procurement.

7.1.2 Inputs

The minimum inputs shown in Table 11 shall be considered by the acquirer when executing information security activities related to the supplier relationship planning process objective defined in 7.1.1.

Table 11 — Supplier relationship planning process inputs

	Acquirer
a)	Supplier relationship strategy.
b)	Management motives, needs and expectations from the procurement of the product or service.
c)	Intended scope of the product or service planned to be procured.
d)	Findings from relevant reports such as risk assessment, privacy impact assessment, threat report, penetration test.
If applicable:	
e)	Existing supplier relationship management documentation, such as supplier relationship plans and agreements.

7.1.3 Activities

The minimum activities shown in Table 12 shall be executed by the acquirer to meet the supplier relationship planning process objective defined in 7.1.1.

Table 12 — Supplier relationship planning process activities

	Acquirer
a)	Identify and assess information security risks that accompany the potential procurement of the product or service based on the information security risk management framework which has been defined in the supplier relationship strategy. The acquirer shall ensure this information security risk assessment: 1) is commensurate to the criticality of the product or service planned to be procured; 2) covers legal and regulatory constraints impacting the product or service planned to be procured to ensure that formal permissions and licences have been obtained prior to entering into the supplier relationship. Care should be taken to consider potential information security impacts of the product or service to be procured in regard to the information security risks associated with existing supplier relationships, particularly if there is a high dependency upon suppliers.
b)	Identify the acceptable level of risk applied to the potential supplier relationship.
c)	Identify and evaluate options for the treatment of identified and assessed risks.
d)	Define and implement an information security risk treatment plan for identified and assessed risks to be mitigated to the acceptable level of risk.

Table 12 *(continued)*

Acquirer
e) Advise the business of the information security risk assessment and treatment plan as input to the supplier relationship agreement negotiations. It is recommended for the procurement to not take place if the identified information security risks cannot be reduced to the acceptable level.
f) Define a supplier relationship plan for the product or service planned to be procured and which follow the supplier relationship strategy. The supplier relationship plan shall contain the following: 1) Specifications of the product or service planned to be procured, its scope, audience, type and nature. 2) Assets, such as servers, databases, applications, network infrastructure, that have information security relevance in the use of the product or service, and their associated owners. 3) Acquirer's information classification inputs to the supplier's information classification and other information security controls. 4) Legal and regulatory requirements of the acquirer's jurisdiction, and areas of laws and regulations binding the potential supplier that should be reviewed during supplier selection process, namely: i) export control; ii) personal data protection legislation and labour laws; iii) intellectual property of third parties; iv) other legal and regulatory requirements, such as tax laws, product liability and investigatory powers. If any authorisations or licences from internal or external authorities are required for legal and regulatory compliance, these shall be obtained prior to entering into any supplier relationship agreement with the supplier. 5) Information security roles and responsibilities assigned within the acquirer's organization and specific to the product or service that may be procured. 6) Acquirer's information which can be shared with potential suppliers for the product or service that may be procured, including a designated owner, responsible for its dissemination and for ensuring that related handling rules are correctly applied. 7) Minimum information security requirements that shall be agreed with the supplier selected for the procurement of the product or service. These requirements shall be directly derived from the information security risk assessment and treatment plan, and from the information security requirements framework defined in the supplier relationship strategy. These requirements should also be defined considering the criticality of the product or service that may be procured and the following: i) information classification made by the acquirer; ii) information security requirements defined in existing supplier relationship plans and agreements. All defined requirements shall be labelled with "SHALL" to differentiate them from recommendations. The defined controls shall cover all security areas (information, ICT, personnel and physical) spanning across people, process and technology.

7.1.4 Outputs

The minimum outputs shown in Table 13 shall be produced by the acquirer when executing the information security activities related to the supplier relationship planning process objective defined in 7.1.1.

Table 13 — Supplier relationship planning process outputs

Acquirer
a) An information security risk assessment and treatment plan associated with the product or service that may be procured.
b) A documented management decision stating the approval of information security risk assessment and treatment plan and that procurement of the product or service may be initiated. The decision to not procure a product or service shall also be documented with the information security reasons that have induced this decision.
c) A supplier relationship plan.

7.2 Supplier selection process

7.2.1 Objectives

The following objectives shall be met by the acquirer and the supplier for successfully managing information security within the supplier selection process.

The acquirer shall:

— select a supplier that provides adequate information security for the product or service that may be acquired.

The supplier shall:

— respond to the acquirer's tender document considering the information security risks associated with the product or service to be supplied and the information security requirements defined in the acquirer's tender document (e.g. ITT, RFP).

7.2.2 Inputs

The minimum inputs shown in Table 14 shall be considered by the acquirer and the supplier when executing information security activities related to the supplier selection process objective defined in 7.2.1.

Table 14 — Supplier selection process inputs

Acquirer	Supplier
a) Supplier relationship strategy.	a) Acquirer relationship strategy.
b) Supplier relationship plan.	b) Acquirer's confidentiality agreement.
If applicable:	c) Acquirer's tender document.
c) Existing supplier selection criteria defined for other procured products or services.	
d) Existing confidentiality agreements defined for other procured products or services.	

7.2.3 Activities

The minimum activities shown in Table 15 shall be executed by the acquirer and the supplier to meet the supplier selection process objective defined in 7.2.1.

Table 15 — Supplier selection process activities

Acquirer	Supplier
a) Define and implement supplier selection criteria based on the supplier relationship plan containing specifications of the product or service that may be procured and on the supplier selection criteria framework defined in the supplier relationship strategy. The supplier selection criteria shall cover the following: 1) Acceptance from the supplier of the information security requirements defined in the tender document. 2) Supplier's maturity in information security. This maturity can be defined by requesting the supplier to hold an ISO/IEC 27001 certification or to provide information security documentation such as documented and tested BCPs for ensuring its capacity to support concurrent activations by acquirers of incident management and recovery plans. 3) Terms under which the supplier allows being audited by the acquirer or by an authorized third party to ascertain compliance with the defined information security requirements. 4) Terms under which the supplier provides regular assurance to the acquirer regarding maintaining information security (i.e. monthly performance reports, annual attestation, regular self-assessments, independent external assessments). 5) Transition acceptance when the product or service that may be procured has been previously operated or manufactured by the acquirer or by a different supplier. 6) Termination acceptance to maintain information security in case of supplier relationship agreement termination. 7) Capacity management of the supplier to supply the product or service that may be procured. 8) Financial strength of the supplier that may supply the product or service. 9) The location of the supplier from which the product or service will be supplied.	a) Review the confidentiality agreement to ensure it protects supplier's assets, such as information and information systems, transmitted during the supplier selection process. NOTE 1 In the absence of a confidentiality agreement proposed by the acquirer, the supplier can submit its own confidentiality agreement to the acquirer before any further exchange of assets that can impact the product or service being supplied. NOTE 2 Existing confidentiality agreements can be used as a support for preparing the confidentiality agreement of the product or service that may be supplied. b) Agree and sign an acquirer confidentiality agreement. c) Receive the acquirer's tender document. d) Validate that the development and supply of the product or service follow commonly accepted business and technical standards, and good practice. e) Identify and evaluate information security risks that accompany the potential supply of the product or service based on the information security risk management framework defined in the acquirer relationship strategy. f) Identify the acceptable level of risk for the supply of the product or service. g) Identify and evaluate options for the treatment of the identified and assessed risks. h) Define and implement an information security risk treatment plan for the identified and assessed risks to be mitigated to the acceptable risk level. It is recommended for the procurement to not take place if the identified information security risks cannot be reduced to the acceptable level. i) Review the information security requirements defined in the tender document for: 1) ensuring conformity to these requirements; 2) determining if any additional controls will need to be implemented to address them. The resources required, such as the financial ones, for implementing these controls need to be assessed to ensure that the supplier is willing to respond to the tender document.

Table 15 *(continued)*

Acquirer	Supplier
10) Subcontractor transparency acceptance regarding whether the use of subcontractors by the supplier is allowed or not including any information security requirements that need to be followed in the event subcontracting is allowed such as: i) notifying the acquirer of any use of subcontractors including any other parties used in the supply chain who may also have access/exposure to the acquirer's information; ii) identifying/listing the subcontractor personnel who will be working on the project; iii) notifying the acquirer of any changes to subcontracting arrangements; iv) assurance requirements of subcontractors including regularity of such assurances; v) auditing requirements of subcontractors; vi) confidentiality requirements of subcontractors. Care should be particularly taken to identify this location in order to: — identify any potential legal and regulatory risks caused by the difference in laws and regulations between the acquirer and the supplier; NOTE 3 Investigations related to the foreign legislation are performed in the case of cross-jurisdictional procurement. — ensure that legal and regulatory obligations applying to the supplier cannot adversely impact the supplier relationship agreement in terms of information security; — evaluate environmental threats, such as local crime rates or geopolitical issues, and their potential impacts. NOTE 4 Existing supplier selection criteria defined for other procured products or services can be also used when defining and implementing supplier selection criteria of the product or service that may be supplied.	j) Review the terms under which audits will be executed by the acquirer or by an authorized third party to ascertain compliance with the information security requirements defined by the acquirer. k) Decide to respond or not to the tender document based on the following: 1) supplier's information security risk assessment and treatment plan related to the potential supply of the product or service; 2) the gap to be addressed to satisfy the acquirer's information security requirements defined in the tender document. l) Assign an individual responsible for integrating appropriate information security language that addresses information security requirements and criteria into the response document.

Table 15 *(continued)*

Acquirer	Supplier
b) Prepare a confidentiality agreement to be signed by the potential supplier to protect acquirer's assets, such as information and information systems, transmitted during the supplier selection process. NOTE 5 If appropriate, this confidentiality agreement can be signed by the acquirer and the potential supplier before any exchange of information which relates to the product or service that may be procured. NOTE 6 Existing confidentiality agreements can be used as a support for preparing the confidentiality agreement of the product or service that may be procured. c) Prepare and provide a tender document including information security requirements, such as an ITT or an RFP, to the potential supplier. The tender document shall be produced based on the supplier relationship plan and shall contain information sufficient for enabling the supplier to prepare its proposal with rationale. The tender document shall contain the following: 1) specifications (e.g. scope, audience, type and nature) of the product or service to be procured; 2) information security requirements that the supplier shall follow while supplying the product or service; 3) service levels or key performance indicators to follow during the product or service supply; 4) potential penalties that can be imposed by the acquirer in case of non-compliance with the information security requirements. Include only information necessary for the supplier to respond to the tender document, such as public or declassified information. Do not include highly sensitive information in a tender document. d) Collect response documents which have been transmitted by potential suppliers in response to the tender document and evaluate them based on supplier selection criteria. Care should be taken to validate that the information security management, controls, implementation and service levels provided by the supplier meet the supplier selection criteria for procurement of non-customised services (e.g. ASP services).	

Table 15 *(continued)*

Acquirer	Supplier
e) Identify the acceptable level of risk for the procurement of the product or service. Identify and evaluate options for the treatment of the identified and assessed risks. Define and implement an information security risk treatment plan for the identified and assessed risks which have been selected to be mitigated to the acceptable risk level. It is recommended for the procurement to not take place if the identified information security risks cannot be reduced to the acceptable level. f) Select a supplier based on the evaluation of these response documents such that this provides greater transparency throughout the product or service supply chain and assurances that acquirer's information security requirements defined in the tender document will be met.	

7.2.4 Outputs

The minimum outputs shown in Table 16 shall be produced by the acquirer and the supplier when executing the information security activities related to the supplier selection process objective defined in 7.2.1.

Table 16 — Supplier selection process outputs

Acquirer	Supplier
a) Supplier selection criteria. b) A confidentiality agreement. c) A tender document. d) An information security risk assessment and treatment plan associated with the product or service. e) Response documents evaluation results. f) Acquirer's selection of the potential supplier which has met the supplier selection criteria.	a) If appropriate, a signed acquirer's confidentiality agreement. b) An information security risk assessment and treatment plan associated with the product or service that may be supplied. c) A response document to the acquirer's tender document.

7.3 Supplier relationship agreement process

7.3.1 Objective

The following objective shall be met by the acquirer and the supplier for successfully managing information security within the supplier relationship agreement process:

— Establish and agree on a supplier relationship agreement addressing the following:

  — information security roles and responsibilities of the acquirer and the supplier;

  — security controls required across information security, ICT security, personnel security and physical security;

— a transition process when the product or service has been previously operated or manufactured by a party different from the supplier;

— information security change management;

— information security incident management;

— compliance monitoring and enforcement;

— a termination process.

7.3.2 Inputs

The minimum inputs shown in Table 17 shall be considered by the acquirer and the supplier when executing information security activities related to the supplier relationship agreement process objective defined in 7.3.1.

Table 17 — Supplier relationship agreement process inputs

Acquirer	Supplier
a) Supplier relationship strategy. b) Acquirer's tender document. c) Supplier's response document.	a) Acquirer relationship strategy.

7.3.3 Activities

The minimum activities shown in Table 18 shall be executed by the acquirer and the supplier to meet the supplier relationship agreement process objective defined in 7.3.1.

Table 18 — Supplier relationship agreement process activities

Acquirer	Supplier
a) Define with the other party the supplier relationship agreement specific to the planned supply of the product or service. This agreement shall: 1) Conform to the acquirer's tender document and to the supplier's response document. This means that this agreement shall particularly contain the following: i) the information security requirements the supplier shall comply with; ii) the service levels or key performance indicators to follow during the product or service delivery. NOTE 1 Content of the supplier relationship agreement can be derived from the tender document, or from the response document, in the case of non-customisable services (e.g. ASP service). 2) Address information security roles and responsibilities of both the acquirer and the supplier within the scope of the product or service supply. It is recommended to assign defined roles and responsibilities to competent individuals within the acquirer or supplier that are correctly and regularly trained in information security. 3) Address the information security aspects of supplier's subcontracting arrangements impacting the product or service supply.	

Table 18 *(continued)*

Acquirer	Supplier
4) Address the transition of the product or service supply when it has been previously manufactured or operated by the acquirer or by a different supplier to ensure its continuity. A transition plan shall be defined by specifying the information security requirements to be followed by both the acquirer and the supplier during the transition of the product or service supply. The definition of this plan shall conform to associated high-level information security requirements defined in the acquirer and supplier relationship strategies. The transition plan shall be agreed by both the acquirer and the supplier and documented in the supplier relationship agreement. 5) Address the handling of changes and incidents, breaches or other events that can impact the acquirer's and the supplier's information security, and that are within the scope of the product or service supply, including: i) an information security change management procedure shall be defined, agreed by both the acquirer and the supplier, and documented in the supplier relationship agreement to ensure required changes that affect information security are in a timely manner approved by the acquirer and applied by the supplier; ii) an information security incident management procedure shall be defined, agreed by both the acquirer and the supplier, and documented in the supplier relationship agreement to ensure that information security incidents that arise during the product or service supply are identified, immediately reported and investigated, considering legal, regulatory and contractual considerations and requirements. NOTE 2 The ISO/IEC 27035 series provides guidance on information security incident management. The definition of both procedures shall conform to associated high-level information security requirements defined in the acquirer and supplier relationship strategies. 6) State how: i) the acquirer will monitor and enforce the supplier's compliance against the defined information security requirements; iii) the supplier will commit to the compliance requirements. The following elements shall be defined and implemented by each of the following organizations, and documented in the supplier relationship agreement: — on the acquirer side: — a plan specific for compliance monitoring and enforcement which complies with the associated high-level information security requirements defined in the supplier relationship strategy and which describes: — the types of monitoring activities, such as information security risk analysis and audit, their frequency of execution and how their results will be reported; — the management and follow-up of corrective actions initiated by the supplier; — on the supplier side: — a process for identifying, initiating, managing, recording, reporting and closing down corrective actions resulting from results of acquirer monitoring and enforcement activities. This process shall comply with the associated high-level information security requirements defined in the acquirer relationship strategy. 7) Address the intellectual property ownership of the product or service that may be supplied, and associated assets which will be created by both the acquirer and the supplier. 8) Address conditions under which the acquirer or supplier has the right to terminate this agreement during its execution period, such as the supplier's inability to fulfil information security requirements defined in the supplier relationship agreement. 9) Address penalties imposed upon the acquirer or the supplier in case of non-compliance to the information security requirements defined in the supplier relationship agreement.	

Table 18 *(continued)*

Acquirer	Supplier
10) Define information security obligations and service continuity requirements in regard to the supplier relationship termination execution. A termination plan shall be defined, agreed by both the acquirer and the supplier and documented in the supplier relationship agreement. The definition of the termination plan shall conform to associated high-level information security requirements defined in the acquirer and supplier relationship strategies. The termination plan shall cover the following: i) definition of information security requirements to be followed by both the acquirer and the supplier if it has been decided to transfer the product or service supply from the supplier back to the acquirer or to another supplier; ii) identification of assets (e.g. acquirer's information and information systems, supplier's information and information systems, records) that are used within the product or service supply for selecting those that will be: a) returned to the acquirer or forwarded to another supplier; b) returned to the supplier; c) destroyed or retained by the acquirer or supplier; iii) transmission mechanisms to apply to the assets that have been identified to be returned to the acquirer or forwarded to another supplier, or returned to the supplier; iv) destruction mechanisms to apply to the assets that have been identified to be destroyed; NOTE 3 Destruction can be required upon time frames agreed by both the acquirer and the supplier or set by legislation or regulation. It can be enforced by the security protection mechanisms defined and agreed by both the acquirer and the supplier and which apply to retained assets. A specific non-disclosure agreement can also be defined and agreed by both the acquirer and the supplier for ensuring the protection of retained assets after the termination of the supplier relationship. v) assurance capabilities demonstrating that the destruction of selected assets has taken place; assurance should be supported by a certificate of destruction; NOTE 4 Both the acquirer and the supplier can also require independent verification that assets have been properly destroyed. vi) a hand-over period with associated training that will be applied in the case a decision is made to transfer the product or service supply back to the acquirer or to forward it to another supplier; vii) A commitment not to disclose sensitive information during a period of time after the termination of the supplier relationship agreement; viii) the timescale of the termination procedure execution. NOTE 5 To ensure that supplier relationship agreement comprehensively addresses information security risks and concerns across the organization, a maximum number of operational units representing commercial, technical and procurement activities impacted by the supplied product or service need to be involved in the supplier relationship agreement negotiations. b) Approve with the other party the defined supplier relationship agreement.	

7.3.4 Outputs

The minimum outputs shown in Table 19 shall be produced by the acquirer and the supplier when executing the information security activities related to the supplier relationship agreement process objective defined in 7.3.1.

Table 19 — Supplier relationship agreement process outputs

Acquirer	Supplier
a) A signed supplier relationship agreement. Store the signed supplier relationship agreement in such a way that its traceability, integrity, availability and confidentiality is maintained and protected.	
b) Completed confidentiality agreements.	
c) An information security change management procedure.	
d) An information security incident management procedure.	
e) A termination plan.	
If applicable:	
f) A transition plan.	
Establish common information exchange methods (e.g. network connectivity, messaging and file formats, software versions, cryptographic standards) to enable communications between the acquirer and the supplier with adequate confidentiality, integrity and availability.	
g) Acquirer's compliance monitoring and enforcement plan and procedures.	g) Acceptance of the compliance monitoring and enforcement plan. h) A corrective actions handling process.

7.4 Supplier relationship management process

7.4.1 Objectives

The following objectives shall be met by each of the following organizations for successfully managing information security within the supplier relationship management process.

The acquirer shall:

— maintain information security during the execution period of the supplier relationship in accordance with the supplier relationship agreement and by particularly considering the following:

  — transition the product or service supply when it has been previously operated or manufactured by the acquirer or by a different supplier;

  — train personnel impacted by the information security requirements defined in the supplier relationship agreement;

  — manage changes and incidents that can have information security impacts on the product or service supply;

  — monitor and enforce compliance of the supplier with information security provisions defined in the supplier relationship agreement.

The supplier shall:

— maintain information security during the execution period of the supplier relationship in accordance with the supplier relationship agreement and by particularly considering the following:

  — support the acquirer in the transition of the product or service supply when it has been previously operated or manufactured by the acquirer or by a different supplier;

  — train personnel impacted by the information security requirements defined in the supplier relationship agreement;

  — manage changes and incidents that can have information security impacts on the product or service supply;

  — support the acquirer in the compliance monitoring and enforcement activities.

7.4.2 Inputs

The outputs listed in 7.3.4 shall be considered by the acquirer and the supplier as minimum inputs when executing information security activities related to the supplier relationship management process.

The minimum inputs shown in Table 20 shall be considered by the acquirer and the supplier when executing information security activities related to the supplier relationship management process objective defined in 7.4.1.

Table 20 — Supplier relationship management process inputs

Acquirer	Supplier
a) Decision concerning who will perform the supplier's compliance monitoring and enforcing activities. b) Previous results of suppliers' compliance monitoring and enforcing activities and trends over time.	a) Previous results of compliance monitoring and enforcing activities performed by acquirers of supplied products or services.

7.4.3 Activities

The minimum activities shown in Table 21 shall be executed by the acquirer and the supplier to meet the supplier relationship management process objective defined in 7.4.1.

Table 21 — Supplier relationship management process activities

Acquirer	Supplier
a) Ensure that the other party has received the supplier relationship agreement and fully understands the information security aspects contained therein. b) Operate transition of the product or service in accordance with the agreed transition plan and notify the other party in a timely manner in case unexpected events occur during this activity. c) Manage information security changes and incidents in accordance with the agreed procedures. d) Train on a regular basis personnel that can be involved in the supplier relationship agreement execution. e) Manage other changes, such as the following, when notified by the other party, which are not covered by the information security change management procedure and which can impact the supply of the procured product or service: 1) change in organization's business, mission or environment; 2) change related to organization's financial strength; 3) change of organization's ownership, or creation of joint ventures; 4) change of location from which the product or service is procured or supplied; 5) change of organization's information security level, such as the achievement or loss of an ISO/IEC 27001 certification; 6) change in the ability to support required business continuity capabilities; 7) change in legal, regulatory and contractual requirements applicable to the organization. The management of these changes will require the notified party to do the following: — Ensure that information security risks associated to this change have been identified and assessed, along with the options for their respective treatment. — Ensure that a risk treatment plan for identified and assessed information security risks to be mitigated has been defined, agreed upon by involved parties and implemented. It is recommended to terminate the procurement or supply of a product or service when the identified information security risks cannot be reduced to the acceptable level. — Agree with the other party on the changes to the supplier relationship agreement, which includes the following: — information security change management procedure;	

Table 21 *(continued)*

Acquirer	Supplier
— information security incident management procedure; — termination plan. — Approve the updated supplier relationship agreement.	
f) Ensure compliance monitoring and enforcement activities meet the associated plan and the corrective actions handling process. In case of changes in information security risks or of audit nonconformities, the acquirer with the support of the supplier shall: 1) identify and assess information security impacts resulting from these changes or audit nonconformities; 2) determine if information security aspects defined in the supplier relationship agreement shall be reconsidered; 3) determine what corrective actions should be implemented within a defined and agreed time scale to retrieve an acceptable information security level within the scope of the procured product or service; 4) agree with the supplier on: i) the changes to be made to the information security aspects defined in the supplier relationship agreement; ii) the implementation of corrective actions; 5) approve the updated supplier relationship agreement.	f) Support acquirer's compliance monitoring and enforcement activities in accordance with the associated plan and the corrective actions handling process. This means particularly that the supplier shall: 1) Approve the selection of the acquirer personnel or of the third party that will perform the information security risk assessment or audit to verify the supplier's compliance with the supplier relationship agreement. NOTE The supplier can refuse the candidate proposed by the acquirer for performing the information security risk assessment or audit only for valid reasons. 2) Assist the acquirer in performing the following activities resulting from changes in information security risks or from audit nonconformities: i) reconsider information security aspects defined in the supplier relationship agreement; ii) define corrective actions that should be implemented within a defined time scale to continue providing acceptable information security for acquirer's information and information systems. The handling of these corrective actions shall conform to the corrective actions handling process. 3) Agree with the acquirer on: i) the changes to be made to the information security aspects defined in the supplier relationship agreement; ii) the implementation of corrective actions. 4) Approve the updated supplier relationship agreement.

7.4.4 Outputs

The minimum outputs shown in Table 22 shall be produced by the acquirer and the supplier when executing the information security activities related to the supplier relationship management process objective defined in 7.4.1.

Table 22 — Supplier relationship management process outputs

Acquirer	Supplier
a) Information security risk assessment and audit reports related to compliance monitoring and enforcement activities.	
If applicable:	
b) An information security risk assessment related to changes which are not covered by the information security change management procedure.	
c) A transition plan execution report.	
d) Information security changes history and associated reports.	
e) Information security incidents history and associated reports.	
f) An approved updated supplier relationship agreement.	
Protect the approved updated supplier relationship agreement to maintain its traceability and integrity as well availability and confidentiality, when stored.	
g) A list of corrective actions which have been agreed upon and the current status (e.g. open, withdrawn or implemented).	

7.5 Supplier relationship termination process

7.5.1 Objectives

The following objectives shall be met by the acquirer and the supplier for successfully managing information security within the supplier relationship termination process:

a) protect the product or service supply during its termination to avoid any information security, legal and regulatory impacts after the notice of termination;

b) terminate the product or service supply in accordance with the termination plan.

7.5.2 Inputs

The minimum inputs shown in Table 23 shall be considered by the acquirer and the supplier when executing information security activities related to the supplier relationship termination process objective defined in 7.5.1.

Table 23 — Supplier relationship termination process inputs

Acquirer	Supplier
a) Management decision from the acquirer or supplier to terminate the product or service supply.	
b) Last available version of the supplier relationship agreement, which shall contain a termination plan.	
If applicable:	
c) Existing non-disclosure agreements established with suppliers.	

7.5.3 Activities

The minimum activities shown in Table 24 shall be executed by the acquirer and the supplier to meet the supplier relationship termination process objective defined in 7.5.1.

Table 24 — Supplier termination management process activities

Acquirer	Supplier
a) Clarify with the party having decided to terminate the product or service supply if there are any information security motivations behind this decision. If any, the party being notified of the product or service supply termination shall do the following: 1) identify and assess information security risks associated to given information security motivations, along with the options for their respective treatment; 2) ensure that a risk treatment plan for identified and assessed risks to be mitigated has been defined and implemented. If a sudden termination is needed, activate the acquirer's BCP depending on the importance of the product or service supply for which the decision to terminate it has been taken.	
b) Decide with the supplier whether the product or service supply shall be cancelled or transferred back to the acquirer or another supplier.	
c) Define and implement a communication plan to inform internal personnel and third parties impacted by the product or service supply about its termination.	
d) Appoint an individual responsible for handling the product or service supply termination in accordance with the termination plan.	
e) Ensure an up-to-date inventory of assets that are used within the supply of the product or service exists.	
f) Select and agree with the other party on the assets that will be: 1) returned to the acquirer or forwarded to another supplier; 2) returned to the supplier; 3) destroyed or retained by the acquirer or supplier.	
g) Execute the termination of the product or service supply in accordance with the termination plan.	
h) Ensure that logical and physical access rights granted to the other party for accessing and handling internal assets required for the product or service supply are removed in a timely manner.	
i) Agree with the other party on the achievement of the supplied product or service termination.	

7.5.4 Outputs

The following minimum outputs shall be produced by each of the following organizations when executing information security activities related to the supplier relationship termination process.

The minimum outputs shown in Table 25 shall be produced by the acquirer and the supplier when executing the information security activities related to the supplier relationship termination process objective defined in 7.5.1.

Table 25 — Supplier relationship termination process outputs

Acquirer	Supplier
a) A communication plan related to the product or service supply termination.	
b) The appointment of an individual responsible for the termination of product or service supply.	
c) An up-to-date inventory of assets that are used within the product or service supply.	
d) A termination plan execution report.	
If applicable:	
e) An information security risk assessment and treatment plan associated with information security motivations given for terminating the product or service supply.	
f) A transition plan execution report.	
g) Assets destruction certificates.	
h) A report on the logical and physical access rights removal execution.	
j) Any signed/completed confidentiality agreements for any ongoing confidentiality requirements.	

Annex A
(informative)

Correspondence between ISO/IEC/IEEE 15288 and this document

Table A.1 shows the correspondence between the subclauses of ISO/IEC/IEEE 15288 and this document.

Table A.1 — Correspondence between ISO/IEC/IEEE 15288 and this document

ISO/IEC/IEEE 15288	This document
6.1 Agreement processes	6.1 Agreement processes
6.1.1 Acquisition process	6.1.1 Acquisition process
—	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
6.1.2 Supply process	6.1.2 Supply process
—	7.2 Supplier selection process
—	7.3 Supplier relationship agreement process
—	7.4 Supplier relationship management process
—	7.5 Supplier relationship termination process
6.2 Organizational project-enabling processes	6.2 Organizational project-enabling processes
6.2.1 Life cycle model management process	6.2.1 Life cycle model management process
6.2.2 Infrastructure management process	6.2.2 Infrastructure management process
6.2.3 Project portfolio management process	6.2.3 Project portfolio management process
6.2.4 Human resource management process	6.2.4 Human resource management process
6.2.5 Quality management process	6.2.5 Quality management process
6.2.6 Knowledge management process	6.2.6 Knowledge management process
6.3 Technical management processes	6.3 Technical management processes
6.3.1 Project planning process	6.3.1 Project planning process
6.3.2 Project assessment and control process	6.3.2 Project assessment and control process
6.3.3 Decision management process	6.3.3 Decision management process
6.3.4 Risk management process	6.3.4 Risk management process
6.3.5 Configuration management process	6.3.5 Configuration management process
6.3.6 Information management process	6.3.6 Information management process
6.3.7 Measurement process	6.3.7 Measurement process
6.3.8 Quality assurance process	6.3.8 Quality assurance process
6.4 Technical processes	6.4 Technical processes
6.4.1 Business or mission analysis process	6.4.1 Business or mission analysis process
6.4.2 Stakeholder needs and requirements definition process	6.4.2 Architecture definition process
6.4.3 System requirements definition process	—
6.4.4 Architecture definition process	—
6.4.5 Design definition process	—