

**ISO/IEC JTC 1/SC 27 N11995**

Date: 2012-11-10

**ISO/IEC DIS 27036-2**

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: ANSI

## **Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements**

*Élément introductif — Élément central — Partie 2: Titre de la partie*

### **Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard

Document subtype:

Document stage: (40) Enquiry

Document language: E

### Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

# Contents

Page

Foreword .....	v
Introduction.....	vi
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	1
4 Symbols and abbreviated terms .....	1
5 Structure of ISO/IEC 27036 Part 2.....	2
6 Information security in supplier relationship management.....	5
6.1 Agreement processes.....	5
6.1.1 Acquisition process .....	5
6.1.2 Supply process.....	7
6.2 Organisational project-enabling processes .....	9
6.2.1 Life cycle model management process .....	9
6.2.2 Infrastructure management process .....	9
6.2.3 Project portfolio management process.....	10
6.2.4 Human resource management process .....	11
6.3 Project processes.....	13
6.3.1 Project planning process .....	13
6.3.2 Project assessment and control process .....	14
6.3.3 Decision management process .....	14
6.3.4 Risk management process .....	14
6.3.5 Configuration management process.....	16
6.3.6 Information management process.....	16
6.3.7 Measurement process.....	16
6.4 Technical processes .....	17
6.4.1 Architectural design process .....	17
7 Information security in a supplier relationship instance .....	18
7.1 Supplier relationship planning process.....	18
7.1.1 Objective .....	18
7.1.2 Inputs .....	18
7.1.3 Activities.....	18
7.1.4 Outputs .....	20
7.2 Supplier selection process.....	20
7.2.1 Objectives .....	20
7.2.2 Inputs .....	21
7.2.3 Activities.....	21
7.2.4 Outputs .....	24
7.3 Supplier relationship agreement process.....	24
7.3.1 Objective .....	24
7.3.2 Inputs .....	24
7.3.3 Activities.....	25
7.3.4 Outputs .....	28
7.4 Supplier relationship management process.....	28
7.4.1 Objectives .....	28
7.4.2 Inputs .....	29
7.4.3 Activities.....	29
7.4.4 Outputs .....	31
7.5 Supplier relationship termination process .....	32

<b>7.5.1</b>	<b>Objectives .....</b>	<b>32</b>
<b>7.5.2</b>	<b>Inputs .....</b>	<b>32</b>
<b>7.5.3</b>	<b>Activities .....</b>	<b>32</b>
<b>7.5.4</b>	<b>Outputs .....</b>	<b>33</b>
<b>Annex A</b>	<b>(informative) Information security requirements guidance.....</b>	<b>35</b>
<b>Annex B</b>	<b>(informative) Cross-references between ISO/IEC 15288 clauses and ISO/IEC 27036 Part 2 clauses .....</b>	<b>38</b>
<b>Annex C</b>	<b>(informative) Cross-references between ISO/IEC 27036 Part 2 clauses and ISO/IEC 27002 controls .....</b>	<b>40</b>
<b>Bibliography</b>	<b>.....</b>	<b>42</b>

## 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27036-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

ISO/IEC 27036 consists of the following parts, under the general title *Information technology — Security techniques — Information security for supplier relationships*:

- *Part 1: Overview and concepts*
- *Part 2: Requirements*
- *Part 3: Guidelines for Information and Communication Technology (ICT) supply chain security*
- *Part 4: Guidelines for security of cloud services.*

## Introduction

Working with suppliers and acquirers is a general business practice required to many organisations for being able to operate or manufacture.

When working with one or more suppliers, a range of information security risks can be introduced on the acquirer side. These risks can be linked to supplier staff access to acquirer's assets, such as information and information systems, but also to the difficulty of managing suppliers with different business objectives and approaches to information security. These information security risks should be managed by the acquirer.

Information security risks should also be managed by the supplier when supplying products or services to one or more acquirers.

ISO/IEC 27036 Part 2:

- a) Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships;
- b) Facilitates to understand each other'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 organisation willing to evaluate the information security in supplier or acquirer relationships;
- e) Is not intended for certification purposes.

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

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

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

# Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements

## 1 Scope

This part of ISO/IEC 27036 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.

These requirements are intended to be applicable to all organisations, regardless of type, size and nature.

To meet these requirements, an organisation should have already internally implemented a number of foundational processes, or be actively planning to do so. These processes include, but are not limited to, the following: governance, business management, operational and human resources management, and information security.

**NOTE** The user of this document needs to correctly interpret each of the forms of the expression of provisions (e.g. “shall”, “shall not”, “should” and “should not”) as being either requirements to be satisfied and/or recommendations where there is a certain freedom of choice. ISO/IEC 27000 Annex A should be consulted for further clarification.

## 2 Normative references

The following referenced documents are indispensable for the application 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 27000:2009, *Information technology -- Security techniques -- Information security management systems — Overview and vocabulary*

ISO/IEC 27036-1, *Information technology -- Security techniques -- Information security for 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 Part 1 apply.

## 4 Symbols and abbreviated terms

The following symbols (and abbreviated terms) are used in this standard:

ASP            Application Service Provider

BCP            Business Continuity Plan

DBA	Database Administrator
DR	Disaster Recovery
ICT	Information and Communication Technology
ISMS	Information Security Management System
ITT	Invitation to Tender
RFP	Request for Proposal
VOIP	Voice over IP

## 5 Structure of ISO/IEC 27036 Part 2

Clause 6 defines fundamental and high-level information security requirements applicable to the acquirer and the supplier at any point during supplier relationships.

These requirements are structured according to life cycle processes specified in ISO/IEC 15288 [1]. These requirements shall be applied by the acquirer and by the supplier to ensure that these organisations are able to manage risks that can have information security impacts in supplier relationships.

NOTE: It is not the intent of clause 6 to reference all life cycle processes specified in ISO/IEC 15288, but only processes that are relevant to information security in supplier relationships.

Clause 7 defines fundamental information security requirements applicable to the acquirer and the supplier when planning, preparing, managing and terminating a supplier relationship.

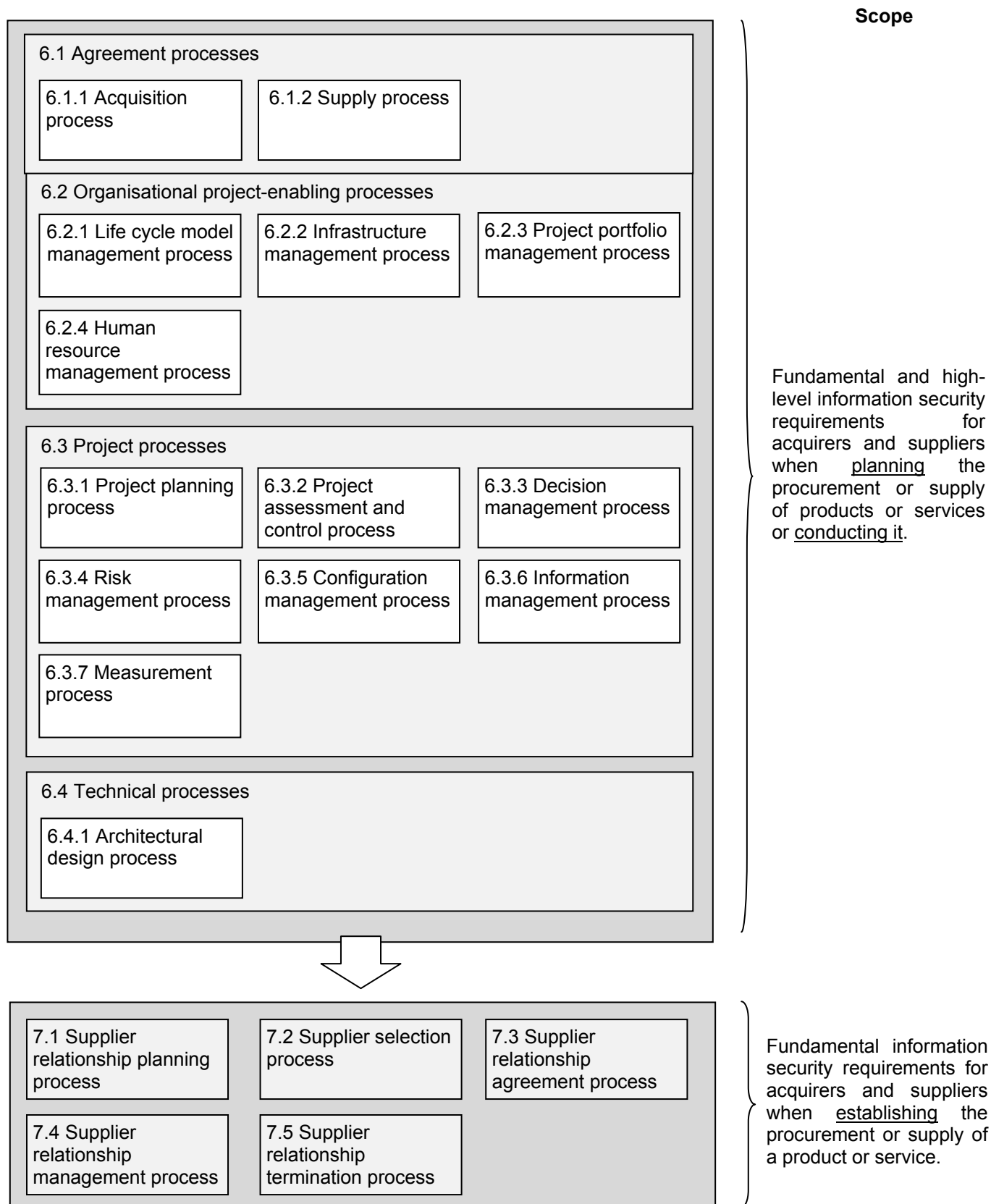
These requirements are structured given following supplier relationship life cycle processes:

- a) Supplier relationship planning process;
- b) Supplier selection process;
- c) Supplier relationship agreement process;
- d) Supplier relationship management process;
- e) Supplier relationship termination process.

These requirements shall be applied by the acquirer and by the supplier involved in a supplier relationship to ensure that these organisations are able to manage risks that can have information security impacts on the assets of both organisations, such as information and information systems.



Following figure describes the scope of the fundamental information security requirements defined in clauses 6 and 7:



**Figure 1 – Scope of fundamental information security requirements defined in clauses 6 and 7.**

Text of clauses 6.1 to 6.4, and of clauses 7.1 to 7.5 is structured in tables which need to be interpreted as follows:

<b>Acquirer</b>
Text specific to the acquirer.

<b>Supplier</b>
Text specific to the supplier.

<b>Acquirer</b>	<b>Supplier</b>
Text which shall be applied by both acquirer and supplier, unless explicitly stated.	
Text specific to the acquirer.	Text specific to the supplier.

There are three informative annexes.

Annex A provides guidance supporting the establishment of information security requirements defined in clauses 6 and 7.

Annex B provides cross-references between clauses of ISO/IEC 15288 that are relevant to supplier relationships and clauses of ISO/IEC 27036 Part 2.

Annex C provides cross-references between clauses of ISO/IEC 27036 Part 2 and information security controls listed in ISO/IEC 27002 [2] and that are relevant to supplier relationships.

## 6 Information security in supplier relationship management

### 6.1 Agreement processes

Organisations can enter into a variety of supplier relationships. Suitable relationships between acquirers and suppliers are achieved using agreements defining information security roles and responsibilities.

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

- a) Acquisition process;
- b) Supply process.

#### 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:

Acquirer
<ul style="list-style-type: none"> <li>— Establish a supplier relationship strategy that: <ul style="list-style-type: none"> <li>— Is based on the information security risk tolerance of the acquirer;</li> <li>— Defines the information security foundation to use when planning, preparing, managing and terminating the procurement of a product or service.</li> </ul> </li> </ul>

##### 6.1.1.2 Activities

Following minimum activities shall be executed by the acquirer to meet the objective defined at clause 6.1.1.1:

Acquirer
<ul style="list-style-type: none"> <li>a) Define, implement, maintain and improve a supplier relationship strategy containing the following: <ol style="list-style-type: none"> <li>1. Management motives, needs and expectations from procuring products or services; <p>NOTE: These statements should be expressed from business, operational, legal and regulatory aspects.</p> </li> <li>2. Management commitment to allocate necessary resources for it;</li> <li>3. An information security risk management framework to use for assessing information security risks accompanying the procurement of a product or service; <p>NOTE: clause 6.3.4 defines information security requirements for the establishment of an information security risk management framework.</p> </li> <li>4. A framework to use when defining information security requirements during the supplier relationship planning process;</li> </ol> </li> </ul>

### Acquirer

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 may be procured.

NOTE: Annex A provides guidance that should be used when defining these requirements.

This framework shall also include the following:

- a. Methods for suppliers to provide evidence for adherence to the defined information security requirements;
  - b. Methods for the acquirer to validate suppliers' adherence to the defined information security requirements;
  - c. 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 and which shall include the following:

- a. Methods for assessing the information security maturity required to a supplier;

Following elements can be requested to the supplier to evaluate its information security maturity:

- Past security-relevant performance;
- Evidence of pro-active management of information security (e.g. holding an ISO/IEC 27001 certification);
- Evidence of documented and tested business continuity and ICT continuity plans.

- b. Methods to be used for assessing evidence provided by a supplier based on the defined information security requirements;

- c. Methods for assessing supplier acceptance of the following:

- Information security requirements defined in the supplier relationship plan;
- Commitment to support the acquirer in its compliance monitoring and enforcement activities;
- Transition of the product or service that may be procured when it has been previously operated or manufactured by the acquirer or by a different supplier;
- Termination of the product or service supply.

- d. Requirements on supplier characteristics, such as the following, which shall be defined in accordance to business, legal, regulatory, architectural, policy and contractual aspects of the acquirer:

- Financial strength of the supplier for being able to supply the product or service;
- Location of the supplier and from which the product or service will be supplied to particularly reduce the risk of legal and regulatory breaches.

Acquirer
<p>6. High-level information security requirements to use when defining the following:</p> <ul style="list-style-type: none"> <li>a. Transition plan to transfer a product or service procured to a supplier to a different supplier;</li> <li>b. Information security change management procedure;</li> <li>c. Information security incident management procedure;</li> <li>d. Compliance monitoring and enforcement plan;</li> <li>e. Termination plan to terminate the procurement of a product or service.</li> </ul> <p>b) Appointment of an individual responsible for handling the information security aspects of the supplier relationship strategy; and</p> <p>Care should be taken by the acquirer to ensure that this individual is correctly and regularly trained.</p> <p>c) Ensure the supplier relationship strategy is reviewed at least once a year and whenever significant business, legal, regulatory, architectural, policy and contractual changes occur.</p> <p>NOTE: The supplier relationship strategy should also be reviewed when a product or service is procured that can significantly impact the acquirer.</p>

## 6.1.2 Supply process

### 6.1.2.1 Objectives

Following objectives shall be met by the supplier for successfully managing information security within the supply process:

Supplier
<ul style="list-style-type: none"> <li>— Establish an acquirer relationship strategy that analyses advantages and feasibility to supply products or services;</li> <li>— Define the information security foundation to use when planning, preparing, managing and terminating the supply of a product or service.</li> </ul>

### 6.1.2.2 Activities

Following minimum activities shall be executed by the supplier to meet objectives defined at clause 6.1.2.1:

Supplier
<p>a) Define, implement, maintain and improve an acquirer relationship strategy containing the following:</p> <ul style="list-style-type: none"> <li>1. Management motives, needs and expectations from supplying of products or services;</li> </ul> <p>NOTE: These statements should be expressed from business, operational and legal aspects.</p>

### Supplier

2. Management commitment to allocate necessary resources for it;
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: clause 6.3.4 defines information security requirements for the establishment of an information security risk management framework.

4. An information security management framework by:
  - a. Defining, implementing, maintaining and improving an information security management within the organisation;

NOTE: An ISMS establishment based on ISO/IEC 27001 can serve to ensure adequate information security management within the organisation and to demonstrate its level to acquirers.

- b. Ensuring that information security requirements stated in existing acquirer tender documents and supplier relationship agreements have been identified for ensuring the supplier information security conformity to these requirements;

Any gap shall be addressed to satisfy acquirer's information security requirements of existing supplier relationship agreements.

- c. Defining a process to accept, interpret, apply and measure acquirer information security requirements.

5. Methods for:

- a. Demonstrating supplier's capacity to supply a product or service;
  - b. Providing evidence of adherence to information security requirements defined by acquirers.

6. High-level information security requirements to use when defining the following:

- a. Transition plan to support the transfer of a product or service when it has been previously operated or manufactured by an acquirer or by another supplier;
  - b. Information security change management procedure;
  - c. Information security incident management procedure;
  - d. Processes for sharing information about information security changes, incidents and other relevant events among the supplier and acquirers;
  - e. Process for handling corrective actions;
  - f. Termination plan to terminate the supply of a product or service.

- d) Appointment of an individual responsible for handling the information security aspects of the acquirer relationship strategy; and

Care should be taken by the supplier to ensure that this individual is correctly and regularly trained.

- e) Ensure the acquirer relationship strategy is reviewed at least once a year and whenever significant business, legal, regulatory, architectural, policy and contractual changes occur.

Supplier
NOTE: The acquirer relationship strategy should also be reviewed when a supplier relationship is established that can significantly impact the supplier.

## 6.2 Organisational project-enabling processes

The organisational 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 organisation's interested parties are met.

In particular, following organisational project-enabling processes support the establishment of the environment in which supplier relationships are conducted or planned:

- a) Life cycle model management process;
- b) Infrastructure management process;
- c) Human resource management process.

### 6.2.1 Life cycle model management process

Acquirer	Supplier
<p>— The acquirer and the supplier shall establish the life cycle model management process when managing information security in supplier relationships.</p> <p>Note: The purpose of this process is to define, maintain, and assure availability of policies, life cycle processes, life cycle models, and procedures for use by the organisation. There are no specific information security requirements and recommendations to consider by each of these organisations when internally establishing this process.</p>	

### 6.2.2 Infrastructure management process

#### 6.2.2.1 Objective

The following objective shall be met by each of the following organisations for successfully managing information security within the infrastructure management process:

Acquirer	Supplier
<p>— Provide the enabling infrastructure to support the organisation in managing information security within supplier relationships.</p>	

#### 6.2.2.2 Activities

Following minimum activities shall be executed by each of the following organisations to meet the objective defined at clause 6.2.2.1:

Acquirer	Supplier
----------	----------

Acquirer	Supplier
<p>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; and</p> <p>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 or man-made causes.</p> <p>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 include:</p> <ol style="list-style-type: none"> <li>1. The provision of alternative, secure facilities for the product or service supply to continue;</li> <li>2. Escrow of information and proprietary technologies, such as application source code and cryptographic keys, using a trusted third party;</li> <li>3. Recovery arrangements to ensure continued availability of information stored at subcontractor premises; and</li> </ol> <p>NOTE: These arrangements should only be considered when the supplier supplies services to an acquirer.</p> <ol style="list-style-type: none"> <li>4. Alignment with business continuity constraints expressed by an acquirer or supplier.</li> </ol> <p>NOTE: Following International Standards provide requirements and guidelines on contingency arrangements:</p> <ol style="list-style-type: none"> <li>1. ISO/IEC 27031 [3]</li> <li>2. ISO 22313 [4]</li> <li>3. ISO 22301 [5]</li> </ol>	

### 6.2.3 Project portfolio management process

#### 6.2.3.1 Objective

The following objective shall be met by each of the following organisations for successfully managing information security within the portfolio management process:

Acquirer	Supplier
<p>— Establish a process for considering information security implications and dependencies within each individual project for those projects where suppliers or acquirers are involved.</p>	

#### 6.2.3.2 Activities

Following minimal activities shall be executed by each of the following organisations to meet the objective defined within clause 6.2.3.1:

Acquirer	Supplier
<p>— 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</p>	



Acquirer	Supplier
<p>them to acquirer's or supplier's assets, such as information and information systems;</p> <p>NOTE: A supplier having very limited access to the acquirer's assets, such as information and information systems, may be categorised as not critical, while a supplier developing critical business software for the acquirer may be categorised as critical.</p>	
<p>— 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; and</p>	
<p>— Ensure that project closeout involving a supplier or acquirer integrates information security activities documented in a termination plan.</p>	

## 6.2.4 Human resource management process

### 6.2.4.1 Objective

The following objective shall be met by each of the following organisations for successfully managing information security within the human resource management process:

Acquirer	Supplier
<p>— Ensure the acquirer and the supplier are provided with necessary human resources having competences regularly maintained and consistent with information security needs in supplier relationships.</p>	

### 6.2.4.2 Activities

Following minimum activities shall be executed by each of the following organisations to meet the objective defined at clause 6.2.4.1:

Acquirer	Supplier
<p>a) Consider the following in the information security training and awareness programme, part of the human resource management process:</p> <ol style="list-style-type: none"> <li>1. Information security guidelines and rules, such as the information security policy and information classification, in particular for personnel dealing with supplier relationships;</li> </ol>	
<ol style="list-style-type: none"> <li>2. Information security requirements generally defined in a supplier relationship agreement, for demonstrating the existence of such requirements that meet acquirer needs and expectations;</li> <li>3. Suppliers' past performance in regards to their level of conformity with acquirer's information security requirements, for demonstrating potential lack of compliance.</li> </ol>	
<p>b) Identify and assess personnel with regard to their access to and ability to disclose information within a</p>	

Acquirer	Supplier
	<p>supplier relationship, such as sensitive information or intellectual property that should not be disclosed;</p> <ul style="list-style-type: none"> <li>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.</li> <li>d) Train these personnel on information security aspects of supplier relationships to particularly ensure that the handling of sensitive information is correctly understood;</li> <li>e) Ensure that detailed criminal and background checks have been performed for personnel assuming key positions in supplier relationships, where permissible by law; and</li> <li>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 organisation.</li> </ul>

### 6.3 Project processes

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

In particular, following project processes support the establishment of the environment in which supplier relationship instances are conducted or planned:

- 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.

#### 6.3.1 Project planning process

##### 6.3.1.1 Objective

The following objective shall be met by each of the following organisations for successfully managing information security within the project planning process:

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

##### 6.3.1.2 Activities

Following minimum activities shall be executed by each of the following organisations to meet the objective defined at clause 6.3.1.1:

Acquirer	Supplier
a) Include the following as part of the project planning process: <ol style="list-style-type: none"> <li>1. 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;</li> <li>2. Integration of information security into relevant project roles, responsibilities, accountabilities, and authorities;</li> <li>3. Securing sensitive internal information that can be impacted by supplier relationships, such as financial, intellectual property, customer or staff information; and</li> <li>4. Resources, such as financial ones, that are required to ensure protection of assets.</li> </ol>	

**6.3.2 Project assessment and control process**

Acquirer	Supplier
<p>— The acquirer and the supplier shall establish a project assessment and control process when managing information security in supplier relationships.</p> <p>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 requirements and recommendations to consider by each of these organisations when internally establishing this process.</p>	

**6.3.3 Decision management process**

Acquirer	Supplier
<p>— The acquirer and the supplier shall establish a decision management process when managing information security in supplier relationships.</p> <p>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 requirements and recommendations to consider by each of these organisations when internally establishing this process.</p>	

**6.3.4 Risk management process****6.3.4.1 Objective**

The following objective shall be met by each of the following organisations for successfully managing information security within the risk management process:

Acquirer	Supplier
<p>— Continuously address information security risks in supplier relationships and throughout their life cycle.</p>	

**6.3.4.2 Activities**

Following minimum activities shall be executed by each of the following organisations to meet the objective defined at clause 6.3.4.1:

Acquirer	Supplier
<p>a) Define, implement, maintain and improve an information security risk management framework that can be used for identifying and assessing information security risks that accompany:</p> <ol style="list-style-type: none"> <li>Existing instances of procurement or supply of product or service;</li> <li>Suppliers or acquirers involved in these instances;</li> <li>The procurement or supply of a product or service.</li> </ol>	

Acquirer	Supplier
<p>NOTE: ISO/IEC 27005 [6], ISO 31000 [7] and ISO/IEC 15288 provide guidance on risk management.</p> <p>Care should be taken to ensure that this framework is defined:</p> <ol style="list-style-type: none"> <li>Following the organisation's business or mission and considering legal, regulatory, architectural, policy and contractual requirements applicable to the organisation.</li> </ol>	
<ol style="list-style-type: none"> <li>Considering the assessment of suppliers in terms of:               <ol style="list-style-type: none"> <li>Past history, such as previous and current business arrangements and dispute information;</li> <li>Contractual agreements, such as supplier relationship agreements and non-disclosure agreements;</li> <li>Information security implications of the product or service procurement, including acquirer's assets handled, underlying technology infrastructure, business dependency and sub-contractors used;</li> <li>Supplier capability to demonstrate its maturity in information security.</li> </ol> <p>The following should be particularly considered when defining the method for assessing suppliers:</p> <ol style="list-style-type: none"> <li>The type of assessment to apply to suppliers, such as a self-assessment or an independent assessment performed by a third party;</li> <li>The level of details of the assessment and its frequency of execution.</li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>Considering the assessment of acquirers in terms of:               <ol style="list-style-type: none"> <li>Past history, such as previous and current business arrangements and dispute information;</li> <li>Contractual agreements, such as supplier relationship agreements and non-disclosure agreements;</li> <li>Information security implications of the product or service supply.</li> </ol> </li> </ol>
<p>b) Apply this information security risk management framework:</p> <ol style="list-style-type: none"> <li>To classify existing instances of procurement or supply of product or service;</li> <li>To classify suppliers or acquirers involved in these instances;</li> <li>When:           <ol style="list-style-type: none"> <li>Defining the supplier or acquirer relationship strategy;</li> <li>Planning to procure or supply a product or service.</li> </ol> </li> </ol> <p>NOTE: In case the organisation holds an ISO/IEC 27001 [8] 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 continuously information security risk assessment and treatment.</p>	

**6.3.5 Configuration management process**

Acquirer	Supplier
<p>— If applicable, the acquirer and the supplier shall establish a configuration management process when managing information security in supplier relationships.</p> <p>NOTE: When implementing the configuration management process, it is recommended to consider ISO/IEC 27002 providing guidance in change management and change control procedures.</p>	

**6.3.6 Information management process**

Acquirer	Supplier
<p>— The acquirer and the supplier shall establish an information management process considering the sensitivity of information that can be exchanged during supplier relationships.</p> <p>NOTE: An ISMS establishment based on ISO/IEC 27001 can serve as a basis for applying adequate information security of information exchanges, in particular in case of information security changes and incidents happening during supplier relationships.</p>	

**6.3.7 Measurement process****6.3.7.1 Objective**

The following objective shall be met by each of the following organisations for successfully managing information security within the measurement process:

Acquirer	Supplier
<p>— 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.</p>	

**6.3.7.2 Activities**

Following minimum activities shall be executed by each of the following organisations to meet the objective defined at clause 6.3.7.1:

Acquirer	Supplier
<p>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.</p> <p>NOTE: ISO/IEC 27004 [9] provides guidance on information security measurement that can be applied to develop and implement specific measures related to information security in supplier relationships.</p> <p>Care should be taken to ensure that this framework is defined following the organisation's business or mission and considering legal, regulatory, architectural, policy and contractual requirements applicable to the organisation.</p>	

Acquirer	Supplier
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.	

## 6.4 Technical processes

Technical Processes are generally used by a supplier for following purposes:

- a) Define requirements for a product or service;
- b) Transform these requirements into an effective product or service;
- c) Sustain the provision of the procured or supplied product or service;
- d) Permit consistent reproduction of the procured or supplied product or service when necessary; and
- e) Dispose of the product or service when it has been decided to retire it.

NOTE: ISO/IEC 27036 Part 3 provides guidance on other technical processes in addition to the one defined here.

### 6.4.1 Architectural design process

#### 6.4.1.1 Objective

The following objective shall be met by each of the following organisations for successfully managing information security within the architectural design process:

Acquirer	Supplier
— Establish an architectural design process addressing information security of supplier relationships.	

#### 6.4.1.2 Activities

Following minimum activities shall be executed by each of the following organisations to meet the objective defined at clause 6.4.1.1:

Acquirer	Supplier
a) Define, implement, maintain and improve the product or service that can be procured or supplied using standards and generally accepted architecture and specifications to facilitate its selection and migration.	

## 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:

Acquirer
<ul style="list-style-type: none"> <li>— Establish a supplier relationship plan that documents the decision adopted by the management to initiate the procurement of a product or service, as well as the information security considerations related to this procurement.</li> </ul>

#### 7.1.2 Inputs

Following minimum inputs shall be considered by the acquirer when executing information security activities related to the supplier relationship planning process:

Acquirer
<ul style="list-style-type: none"> <li>— Supplier relationship strategy;</li> <li>— Management motives, needs and expectations from the procurement of the product or service;</li> <li>— Intended scope of the product or service planned to be procured.</li> </ul> <p>If applicable:</p> <ul style="list-style-type: none"> <li>— Existing supplier relationship management documentation, such as supplier relationship plans and agreements.</li> </ul>

#### 7.1.3 Activities

Following minimum activities shall be executed by the acquirer to meet the objective defined at clause 7.1.1:

Acquirer
<p>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;</p> <p>The acquirer shall ensure this information security risk assessment:</p> <ol style="list-style-type: none"> <li>1. Is commensurate to the criticality of the product or service planned to be procured;</li> <li>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.</li> </ol>



### Acquirer

Care should be taken to consider potential information security impacts of the product or service to be procured in regards to the information security risks associated with existing supplier relationships, particularly if there is a high dependency upon suppliers.

- b) Identify and evaluate options for the treatment of identified and assessed risks;
- c) Define and implement an information security risk treatment plan for identified and assessed risks to be mitigated to an acceptable risk level;
- d) Advise the business of the information security risk assessment and treatment plan as input to the supplier relationship agreement negotiations;

NOTE: When information security risks are high or costs for mitigating them are unacceptable, the decision to procure a product or a service should be reconsidered. This procurement should not take place when the identified information security risks cannot be reduced to an acceptable risk level by introducing applicable controls, which have been selected to mitigate identified risks.

- e) Define a supplier relationship plan for the product or service planned to be procured and which follow the supplier relationship strategy.

In particular, the supplier relationship plan shall contain the following:

1. Specifications of the product or service planned to be procured, in particular its scope, audience, type and nature;

All affected assets, such as servers, databases, applications, network infrastructure, shall be identified with their associated owners.

Inputs on their information classification, applicable legal and regulatory requirements shall be ensured as applicable, namely:

- a. Acquirer's information classification;
- b. Export control;
- c. Personal data protection legislation and labour laws;
- d. Intellectual property of third parties; and
- e. Other legal and regulatory requirements, such as tax laws, product liability, 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.

2. Information security roles and responsibilities assigned within the acquirer's organisation and specific to the product or service that may be procured;
3. Acquirer's information which can be shared with potential suppliers for the product or service that may be procured;

NOTE: Acquirer's information should have a designated owner, responsible for its dissemination and for ensuring that related handling rules are correctly applied.

4. Minimum information security requirements that shall be agreed with the supplier selected for the procurement of the product or service.

Acquirer
<p>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.</p> <p>These requirements should also be defined considering the criticality of the product or service that may be procured and the following:</p> <ul style="list-style-type: none"> <li>a. Information classification made by the acquirer;</li> <li>b. Information security requirements defined in existing supplier relationship plans and agreements.</li> </ul> <p>All defined requirements shall be classified with “SHALL” to differentiate them from recommendations.</p> <p>NOTE: Annex A provides guidance that should be used when defining information security requirements for the product or service that may be procured.</p>

#### 7.1.4 Outputs

Following minimum outputs shall be produced by the acquirer when executing information security activities related to the supplier relationship planning process:

Acquirer
<ul style="list-style-type: none"> <li>— Information security risk assessment and treatment plan associated with the product or service that may be procured;</li> <li>— 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;</li> </ul> <p>The decision to not procure a product or service shall also be documented with the information security reasons that have induced this decision.</p> <ul style="list-style-type: none"> <li>— Supplier relationship plan.</li> </ul>

## 7.2 Supplier selection process

### 7.2.1 Objectives

Following objectives shall be met by each of the following organisations for successfully managing information security within the supplier selection process:

Acquirer	Supplier
<ul style="list-style-type: none"> <li>— Select a supplier that provides adequate information security for the product or service that may be procured.</li> </ul>	<ul style="list-style-type: none"> <li>— Respond to the acquirer's tender document considering the information security risks associated with the product or service to supply and the information security requirements defined in the acquirer's tender document (e.g. ITT, RFP).</li> </ul>

### 7.2.2 Inputs

Following minimum inputs shall be considered by each of the following organisations when executing information security activities related to the supplier selection process:

Acquirer	Supplier
<ul style="list-style-type: none"> <li>— Supplier relationship strategy;</li> <li>— Supplier relationship plan.</li> </ul> <p>If applicable:</p> <ul style="list-style-type: none"> <li>— Existing supplier selection criteria defined for other procured products or services;</li> <li>— Existing confidentiality agreements defined for other procured products or services.</li> </ul>	<ul style="list-style-type: none"> <li>— Acquirer relationship strategy;</li> <li>— Acquirer's confidentiality agreement;</li> <li>— Acquirer's tender document.</li> </ul>

### 7.2.3 Activities

Following minimum activities shall be executed by each of the following organisations to meet objectives defined at clause 7.2.1:

Acquirer	Supplier
<p>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;</p> <p>The supplier selection criteria shall cover the following:</p> <ol style="list-style-type: none"> <li>1. Acceptance from the supplier of the information security requirements defined in the tender document;</li> <li>2. Supplier's maturity in information security;</li> </ol> <p>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 business continuity plans for ensuring its capacity to support concurrent activations by acquirers of incident plans or recovery plans.</p> <ol style="list-style-type: none"> <li>3. Terms under which the supplier allows being audited by the acquirer or by an authorised</li> </ol>	<p>a) Review the confidentiality agreement to ensure it protects supplier's assets, such as information and information systems, transmitted during the supplier selection process;</p> <p>In the absence of a confidentiality agreement proposed by the acquirer, the supplier should submit such document to the acquirer before any further exchange of assets that can impact the product or service that may be supplied.</p> <p>NOTE: Existing confidentiality agreements should be used as a support for preparing the confidentiality agreement of the product or service that may be supplied.</p> <p>b) Agree and sign with the acquirer this confidentiality agreement to gain access to its tender document;</p> <p>c) Validate that the development and supply of the product or service follow commonly accepted business and technical standards, and good practice;</p> <p>d) Identify and evaluate information security risks that accompany the potential supply of the product or service based on the information</p>

Acquirer	Supplier
<p>third party to ascertain compliance with the defined information security requirements;</p> <p>4. 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;</p> <p>5. Termination acceptance to maintain information security in case of supplier relationship agreement termination;</p> <p>6. Capacity management from the supplier to supply the product or service that may be procured,</p> <p>7. Financial strength of the supplier that may supply the product or service; and</p> <p>8. The location of the supplier and from which the product or service will be supplied.</p> <p>Care should be particularly taken to identify this location in order to:</p> <p>a. Identify any potential legal and regulatory risks caused by the difference in laws and regulations between the acquirer and the supplier;</p> <p>NOTE: Investigations related to the foreign legislation need be performed in the case of cross jurisdictional procurement.</p> <p>b. Ensure that legal and regulatory obligations applying to the supplier cannot adversely impact the supplier relationship agreement in terms of information security; and</p> <p>c. Evaluate environmental threats, such as local crime rates or geopolitical issues, and their potential impacts.</p> <p>NOTE: 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.</p> <p>b) Prepare a confidentiality agreement to be signed by the supplier that may supply the product or service to protect acquirer's assets, such as information and information systems, transmitted during the supplier selection process;</p> <p>This confidentiality agreement shall be signed by the acquirer and the potential supplier before any</p>	<p>security risk management framework defined in the acquirer relationship strategy;</p> <p>Care should be taken by the supplier to ensure that the potential supply of a product or service will also not increase the impact or likelihood of information security risks linked to existing business activities and supplier relationships.</p> <p>e) Identify and evaluate options for the treatment of the identified and assessed risks;</p> <p>f) Define and implement an information security risk treatment plan for the identified and assessed risks which have been selected to be mitigated to an acceptable risk level;</p> <p>Identified and assessed information security risks the supplier has selected not to mitigate shall be notified to the acquirer.</p> <p>NOTE: When information security risks are high or costs for mitigating them are unacceptable, the decision to supply a product or service should be reconsidered. This supply should not take place when the identified information security risks cannot be reduced to an acceptable risk level by introducing applicable controls, which have been selected to mitigate identified risks.</p> <p>g) Review the information security requirements defined in the tender document for:</p> <ol style="list-style-type: none"> <li>1. Ensuring conformity to these requirements;</li> <li>2. Determining if any additional information security controls will need to be implemented to address them.</li> </ol> <p>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.</p> <p>h) Review the terms under which audits will be executed by the acquirer or by an authorised third party to ascertain compliance with the information security requirements defined by the acquirer;</p> <p>i) Decide to respond or not to the tender document based on the following:</p> <ol style="list-style-type: none"> <li>a. Supplier's information security risk assessment and treatment plan related to the potential supply of the product or service;</li> </ol>

Acquirer	Supplier
<p>exchange of assets which relates to the product or service that may be procured.</p> <p>NOTE: Existing confidentiality agreements should be used as a support for preparing the confidentiality agreement of the product or service that may be procured.</p> <p>c) Prepare and provide a tender document, such as an ITT or a RFP, to the potential supplier;</p> <p>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.</p> <p>In particular, the tender document shall contain the following:</p> <ol style="list-style-type: none"> <li>1. Specifications (e.g. scope, audience, type and nature) of the product or service to be procured;</li> <li>2. Information security requirements that the supplier shall follow while supplying the product or service;</li> <li>3. Service levels or key performance indicators to follow during the product or service supply; and</li> <li>4. Potential penalties that may be imposed by the acquirer in case of non-compliance to the information security requirements.</li> </ol> <p>NOTE: As far as possible, the tender document should only contain public or declassified information. Such document should only contain information necessary for allowing the supplier to respond with rationale. Highly sensitive information should never be included in a tender document under any circumstances.</p> <p>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; and</p> <p>NOTE: For procurement of non-customised services (e.g. ASP services), the acquirer should validate that the information security management, controls, implementation and/or service levels provided by the supplier meet the supplier selection criteria.</p> <p>e) Select a supplier based on the evaluation of these response documents.</p> <p>NOTE: Acquirers should prefer a supplier that provides greater transparency throughout the product or service supply chain and assurances that acquirer's information</p>	<p>b. The gap to be addressed to satisfy acquirer's information security requirements defined in the tender document.</p> <p>j) Assign an individual responsible for integrating appropriate information security language that addresses information security requirements and criteria into the response document.</p>

Acquirer	Supplier
security requirements defined in the tender document will be met.	

#### 7.2.4 Outputs

Following minimum outputs shall be produced by each of the following organisations when executing information security activities related to the supplier selection process:

Acquirer	Supplier
<ul style="list-style-type: none"> <li>— Supplier selection criteria;</li> <li>— Confidentiality agreement;</li> <li>— Tender document;</li> <li>— Response documents evaluation results;</li> <li>— Acquirer' selection of the potential supplier which has met supplier selection criteria.</li> </ul>	<ul style="list-style-type: none"> <li>— Signed acquirer's confidentiality agreement;</li> <li>— Response document to the acquirer's tender document.</li> </ul>

### 7.3 Supplier relationship agreement process

#### 7.3.1 Objective

The following objective shall be met by each of the following organisations for successfully managing information security within the supplier relationship agreement process:

Acquirer	Supplier
<ul style="list-style-type: none"> <li>— Establish and agree on a supplier relationship agreement addressing information security roles and responsibilities of the acquirer and the supplier, as well as the following: <ul style="list-style-type: none"> <li>— Transition process when the product or service has been previously operated or manufactured by a party different from the supplier;</li> <li>— Information security change management;</li> <li>— Information security incident management;</li> <li>— Termination process.</li> </ul> </li> </ul>	

#### 7.3.2 Inputs

Following minimum inputs shall be considered by each of the following organisations when executing information security activities related to the supplier relationship agreement process:

Acquirer	Supplier
— Supplier relationship strategy.	— Acquirer relationship strategy.
— Acquirer's tender document; — Supplier's response document.	

### 7.3.3 Activities

Following minimum activities shall be executed by each of the following organisations to meet the objective defined at clause 7.3.1:

Acquirer	Supplier
<p>a) Define with the other party the supplier relationship agreement specific to the planned supply of the product or service;</p> <p>This agreement shall:</p> <ol style="list-style-type: none"> <li>Conform to the acquirer's tender document and to the supplier's response document;</li> </ol> <p>It means that this agreement shall particularly contain the following:</p> <ol style="list-style-type: none"> <li>The information security requirements the supplier shall comply with;</li> <li>The service levels or key performance indicators to follow during the product or service delivery.</li> </ol> <p>NOTE: 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).</p> <ol style="list-style-type: none"> <li>Address information security roles and responsibilities of both acquirer and supplier within the scope of the product or service supply;</li> </ol> <p>NOTE: Defined roles and responsibilities should be assigned to competent individuals within the acquirer or supplier that are correctly and regularly trained in information security.</p> <ol style="list-style-type: none"> <li>Address the information security aspects of supplier's subcontracting arrangements impacting the product or service supply;</li> <li>Address the transition of the product or service supply when it has been previously operated or manufactured by the acquirer or by a different supplier to ensure its continuity;</li> </ol> <p>A transition plan shall be defined by specifying the information security requirements to follow by both acquirer and supplier during the transition of the product or service supply.</p> <p>The definition of this plan shall conform to associated high-level information security requirements defined in the acquirer and supplier relationship strategies.</p> <p>The transition plan shall be agreed by both acquirer and supplier, and documented in the supplier relationship agreement.</p> <ol style="list-style-type: none"> <li>Address the handling of changes and incidents, breaches or other events that can impact acquirer's and supplier's information security, and within the scope of the product or service supply;</li> </ol>	

Acquirer	Supplier
<p>In particular:</p> <ol style="list-style-type: none"> <li>An information security change management procedure shall be defined, agreed by both acquirer and 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;</li> <li>An information security incident management procedure shall be defined, agreed by both acquirer and 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.</li> </ol> <p>NOTE: ISO/IEC 27035 [10] provides guidance on information security incident management.</p> <p>The definition of both procedures shall conform to associated high-level information security requirements defined in the acquirer and supplier relationship strategies.</p> <p>6. State how:</p> <ol style="list-style-type: none"> <li>The acquirer will monitor and enforce the supplier's compliance against the defined information security requirements; and</li> <li>The supplier will commit to the compliance requirements.</li> </ol> <p>In particular, following elements shall be defined and implemented by each of the following organisations, and documented in the supplier relationship agreement:</p> <ul style="list-style-type: none"> <li>— On acquirer side: <ul style="list-style-type: none"> <li>— 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: <ul style="list-style-type: none"> <li>— The types of monitoring activities, such as information security risk analysis and audit, their frequency of execution and how their results will be reported; and</li> <li>— The management and follow-up of corrective actions initiated by the supplier.</li> </ul> </li> </ul> </li> <li>— On supplier side: <ul style="list-style-type: none"> <li>— A process for identifying, initiating, managing, recording, reporting and closing down corrective actions resulting from results of acquirer monitoring and enforcement activities.</li> </ul> <p>This process shall comply with the associated high-level information security requirements defined in the acquirer relationship strategy.</p> </li> </ul> <ol style="list-style-type: none"> <li>Address the intellectual property ownership of the product or service that may be supplied, and associated assets which will be created by both acquirer and supplier;</li> <li>Address conditions, such as the supplier's ability to fulfil information security requirements defined in the supplier relationship agreement, under which both acquirer and supplier have the right to terminate this agreement during its execution period;</li> <li>Address penalties imposed upon the acquirer or supplier in case of non-compliance to the information security requirements defined in the supplier relationship agreement; and</li> </ol>	



Acquirer	Supplier
<p>10. Define information security obligations and service continuity requirements in regards to the supplier relationship termination execution;</p> <p>A termination plan shall be defined, agreed by both acquirer and supplier and documented in the supplier relationship agreement.</p> <p>The definition of the termination plan shall conform to associated high-level information security requirements defined in the acquirer and supplier relationship strategies.</p> <p>In particular, the termination plan shall cover the following:</p> <ul style="list-style-type: none"> <li>a. Definition of information security requirements to be followed by both acquirer and supplier if it has been decided to transfer the product or service supply from the supplier back to the acquirer or to another supplier;</li> <li>b. 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: <ul style="list-style-type: none"> <li>— Returned to the acquirer or forwarded to another supplier;</li> <li>— Returned to the supplier; or</li> <li>— Destroyed or retained by the acquirer or supplier.</li> </ul> </li> <li>c. 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;</li> <li>d. Destruction mechanisms to apply to the assets that have been identified to be destroyed;</li> </ul> <p>NOTE: Destruction can be required upon time frames agreed by both acquirer and supplier or set by legislation or regulation. It can be enforced by the security protection mechanisms defined and agreed by both acquirer and supplier and which apply to retained assets. A specific non-disclosure agreement may also be defined and agreed by both acquirer and supplier for ensuring the protection of retained assets after the termination of the supplier relationship.</p> <ul style="list-style-type: none"> <li>e. Assurance capabilities demonstrating that the destruction of selected assets has taken place. Assurance should be supported by a certificate of destruction;</li> </ul> <p>NOTE: Both acquirer and supplier can also require independent verification that assets have been properly destroyed.</p> <ul style="list-style-type: none"> <li>f. 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;</li> <li>g. Commitment not to disclose sensitive information during a period of time after the termination of the supplier relationship agreement;</li> <li>h. The time scale of the termination procedure execution.</li> </ul> <p>NOTE: A number of different business areas representing commercial, technical and procurement activities need to be involved in the supplier relationship agreement negotiations, because of security-related impacts across organisations. Their involvement should ensure that this agreement considers interests of a maximum number of organisational units impacted by the supplied product or service and is more comprehensive in terms of addressing information security risks and concerns.</p> <p>b) Approve with the other party the defined supplier relationship agreement.</p>	

### 7.3.4 Outputs

Following minimum outputs shall be produced by each of the following organisations when executing information security activities related to the supplier relationship agreement process:

Acquirer	Supplier
<p>— Signed supplier relationship agreement;</p> <p>NOTE: The signed supplier relationship agreement should be stored in such way that protection is made for its traceability and integrity as well availability and confidentiality.</p> <p>— Information security change management procedure;</p> <p>— Information security incident management procedure;</p> <p>— Termination plan.</p> <p>If applicable:</p> <p>— Transition plan.</p> <p>NOTE: Common information exchange methods (e.g. network connectivity, messaging and file formats, software versions, cryptographic standards) should also be established to enable communications between acquirer and supplier with adequate confidentiality, integrity and availability.</p>	
— Acquirer's compliance monitoring and enforcement plan.	— Corrective actions handling process.

## 7.4 Supplier relationship management process

### 7.4.1 Objectives

Following objectives shall be met by each of the following organisations for successfully managing information security within the supplier relationship management process:

Acquirer	Supplier
<p>— Maintain information security during the execution period of the supplier relationship in accordance with the supplier relationship agreement and by particularly considering the following:</p>	
<p>— Transition the product or service supply when it has been previously operated or manufactured by the acquirer or by a different supplier;</p>	<p>— 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;</p>
<p>— Train personnel impacted by the information security requirements defined in the supplier relationship agreement;</p> <p>— Manage changes and incidents that can have information security impacts on the product or service supply;</p>	
<p>— Monitor and enforce compliance of the supplier with security provisions defined</p>	<p>— Support the acquirer in the compliance</p>

<b>Acquirer</b>	<b>Supplier</b>
in the supplier relationship agreement.	monitoring and enforcement activities.

#### 7.4.2 Inputs

The outputs listed in clause 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.

Following inputs are also recommended to be considered by each of the following organisations:

<b>Acquirer</b>	<b>Supplier</b>
<ul style="list-style-type: none"> <li>— Decision concerning who will perform the supplier's compliance monitoring and enforcing activities;</li> <li>— Previous results of suppliers' compliance monitoring and enforcing activities and trends over time.</li> </ul>	<ul style="list-style-type: none"> <li>— Previous results of compliance monitoring and enforcing activities performed by acquirers of supplied products or services.</li> </ul>

#### 7.4.3 Activities

Following minimum activities shall be executed by each of the following organisations to meet objectives defined at clause 7.4.1:

<b>Acquirer</b>	<b>Supplier</b>
<ul style="list-style-type: none"> <li>a) Ensure that the other party has received the supplier relationship agreement and fully understand contained information security aspects;</li> <li>b) Operate transition of the product or service in accordance to the agreed transition plan and notify the other party in a timely manner in case of unexpected events occur during this activity;</li> <li>c) Manage information security changes and incidents in accordance to the agreed procedures;</li> <li>d) Train on a regular basis internal personnel that can be involved in the termination plan execution;</li> <li>e) Manage other changes, such as the following, 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:               <ul style="list-style-type: none"> <li>1. Change in organisation's business, mission or environment;</li> <li>2. Change related to organisation's financial strength;</li> <li>3. Change of organisation's ownership, or creation of joint ventures;</li> <li>4. Change of location from which product or service is procured or supplied;</li> <li>5. Change of organisation's information security level, such as the achievement or loss of an ISO/IEC 27001 certification;</li> </ul> </li> </ul>	

Acquirer	Supplier
<p>6. Change in the ability to support required business continuity service capabilities; and</p> <p>7. Change in legal, regulatory and contractual requirements applicable to the organisation.</p> <p>The management of these changes will require the notified party to do the following:</p> <ol style="list-style-type: none"> <li>1. Ensuring that information security risks associated to this change have been identified and assessed, along with the options for their respective treatment;</li> <li>2. Ensuring that a risk treatment plan for identified and assessed risks to be mitigated has been defined, agreed by involved parties and implemented;</li> </ol> <p>NOTE: When information security risks are high or costs for mitigating them are unacceptable, the procurement or supply of the product or service should be reconsidered. This procurement or supply should not take place when the identified information security risks cannot be reduced to an acceptable risk level by introducing applicable controls, which have been selected to mitigate identified risks.</p> <ol style="list-style-type: none"> <li>3. Agreeing with the other party the changes to be made to the supplier relationship agreement, which includes the following: <ol style="list-style-type: none"> <li>a. Information security change management procedure;</li> <li>b. Information security incident management procedure; and</li> <li>c. Termination plan.</li> </ol> </li> <li>4. Approving the updated supplier relationship agreement.</li> </ol>	
<p>f) Ensure compliance monitoring and enforcement activities meet the associated plan and the corrective actions handling process.</p> <p>In case of changes in information security risks or of audit nonconformities, the acquirer with the support of the supplier shall:</p> <ol style="list-style-type: none"> <li>1. Identify and assess information security impacts resulting from these changes or audit nonconformities;</li> <li>2. Determine if information security aspects defined in the supplier relationship agreement shall be reconsidered;</li> <li>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;</li> <li>4. Agree with the supplier: <ol style="list-style-type: none"> <li>a. The changes to be made to the information security aspects defined in the supplier relationship agreement; and</li> <li>b. The implementation of corrective</li> </ol> </li> </ol>	<p>f) Support acquirer's compliance monitoring and enforcement activities in accordance to the associated plan and the corrective actions handling process.</p> <p>It means particularly that the supplier shall:</p> <ol style="list-style-type: none"> <li>1. Approve the selection of the acquirer personnel or of the third party that will perform the information security risks assessment or audit to verify the supplier's compliance with the supplier relationship agreement;</li> </ol> <p>NOTE: The supplier may refuse the candidate proposed by the acquirer for performing the information security risk assessment or audit only for valid business reasons.</p> <ol style="list-style-type: none"> <li>2. Assist the acquirer in performing following activities resulting from changes in information security risks or from audit nonconformities: <ol style="list-style-type: none"> <li>a. Reconsider information security aspects defined in the supplier relationship agreement; and</li> <li>b. Define corrective actions that should be</li> </ol> </li> </ol>

Acquirer	Supplier
<p>actions;</p> <p>5. Approve the updated supplier relationship agreement.</p>	<p>implemented within a defined time scale to continue providing acceptable information security for acquirer information and information systems.</p> <p>The handling of these correctives actions shall conform to the corrective actions handling process.</p> <p>3. Agreeing with the acquirer:</p> <p>a. The changes to be made to the information security aspects defined in the supplier relationship agreement; and</p> <p>b. The implementation of corrective actions;</p> <p>4. Approve the updated supplier relationship agreement.</p>

#### 7.4.4 Outputs

Following minimum outputs shall be produced by each of the following organisations when executing information security activities related to the supplier relationship management process:

Acquirer	Supplier
<p>— Information security risk assessment and audit reports related to compliance monitoring and enforcement activities.</p>	
<p>If applicable:</p> <p>— Information security risk assessment related to changes which are not covered by the information security change management procedure;</p> <p>— Transition plan execution report;</p> <p>— Information security changes history and associated reports;</p> <p>— Information security incidents history and associated reports;</p> <p>— Signed updated supplier relationship agreement;</p> <p>NOTE: The signed updated supplier relationship agreement should be stored in such way that protection is made for its traceability and integrity as well availability and confidentiality.</p> <p>— List of corrective actions which have been agreed and implemented.</p>	

## 7.5 Supplier relationship termination process

### 7.5.1 Objectives

Following objectives shall be met by each of the following organisations for successfully managing information security within the supplier relationship termination process:

Acquirer	Supplier
<ul style="list-style-type: none"> <li>— Protect the product or service supply during its termination to avoid any information security, legal and regulatory impacts after the notice of termination;</li> <li>— Terminate of the product or service supply in accordance to the termination plan.</li> </ul>	

### 7.5.2 Inputs

Following minimum inputs shall be considered by each of the following organisations when executing information security activities related to the supplier relationship termination process:

Acquirer	Supplier
<ul style="list-style-type: none"> <li>— Management decision from the acquirer or supplier on termination of the product or service supply;</li> <li>— Last available version of the supplier relationship agreement, which shall contain a termination plan.</li> </ul>	
If applicable: <ul style="list-style-type: none"> <li>— Existing non-disclosure agreements established with suppliers.</li> </ul>	

### 7.5.3 Activities

Following minimum activities shall be executed by each of the following organisations to meet objectives defined at clause 7.5.1:

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; <p>If any, the party being notified of the product or service supply termination shall do the following:</p> <ol style="list-style-type: none"> <li>1. Identify and assess information security risks associated to given information security motivations, along with the options for their respective treatment;</li> <li>2. Ensure that a risk treatment plan for identified and assessed risks to be mitigated has been defined and implemented.</li> </ol> <p>NOTE 1: When information security risks are high or costs for mitigating them are unacceptable, the procurement or supply of the product or service should be reconsidered. This procurement or supply should not take place when the identified information security risks cannot be reduced to an acceptable risk level by introducing applicable controls, which have been selected to mitigate identified risks.</p>	

Acquirer	Supplier
NOTE 2: If sudden termination is needed, acquirer's BCP should be activated pending on the importance of the product or service supply for which a 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 to 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: <ol style="list-style-type: none"> <li>1. Returned to the acquirer or forwarded to another supplier;</li> <li>2. Returned to the supplier; or</li> <li>3. Destroyed or retained by the acquirer or supplier.</li> </ol> g) Execute the termination of the product or service supply in accordance to 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; and i) Agree with the other party on the achievement of the supplied product or service termination.	

#### 7.5.4 Outputs

Following minimum outputs shall be produced by each of the following organisations when executing information security activities related to the supplier relationship termination process:

Acquirer	Supplier
— Communication plan related to the product or service supply termination; — Appointment of an individual responsible for the termination of product or service supply; — Up-to-date inventory of assets that are used within the product or service supply; — Termination plan execution report. If applicable: — Information security risk assessment and treatment plan associated with information security motivations given for terminating the product or service supply; — Transition plan execution report; — Assets destruction certificates;	

Acquirer	Supplier
—	Report on the logical and physical access rights removal execution.



## Annex A (informative)

### Information security requirements guidance

This annex provides implementation guidance for information security requirements defined in clauses 6 and 7.

Specifying information security requirements is critical to the acquirer and the supplier for ensuring that the delivery of product or service is executed in accordance to their environment and business, legal, regulatory, architectural, policy and contractual constraints.

Information security requirements should be defined at following supplier relationship documents level:

- a) Supplier relationship strategy;
- b) Acquirer relationship strategy;
- c) Acquirer's tender document;
- d) Supplier relationship plan;
- e) Supplier relationship agreement.

Information security requirements set out in these documents can contain technical, physical, environmental, human and continuity controls to be applied either to the acquirer or to the supplier or both.

Following table provide examples of information security requirements within the scope of supplier relationships:

Information security domains	Information security related categories	Information security requirements applied to the supplier
Governance, risk and compliance	Information security framework	Establish, maintain and monitor an information security governance framework.
	Information security policy	Develop and distribute a comprehensive, approved information security policy to all individuals with access to the organisation's information and systems.
	Operating procedures	Based on the Information security policy, establish a comprehensive set of standards and procedures aimed at privileged users (e.g. administrators, programmers) to ensure consistent implementation of information security controls.
	Awareness/education	Establish an information security awareness and behaviour change programme, supported by a range of education/training activities.
	Information risk management	Undertake information risk management for key aspects of the product or service, on a regular basis, in a rigorous and consistent manner, using a structured methodology.
	Identification and protection of information that is commercial, sensitive, regulated or personal in nature	Apply an approved method for identifying, maintaining and protecting information such as trade secrets, Intellectual Property, financial, defence-related, food and drug, or personally identifiable information.
	Accountability/ownership	Assign ownership and responsibility for all information, systems, other physical assets, services, and processes to designated individuals

Information security domains	Information security related categories	Information security requirements applied to the supplier
		who have the required skills, tools and authority.
System Management	Purchase of hardware and software	Acquire only secure, approved hardware and software (eg purchased from an approved list, subject to a security evaluation and recorded in an inventory).
	Robust resilient design	Design and operate robust, resilient systems that can cope with current and predicted levels of usage, are supported by alternative facilities and incorporate information security requirements.
	Separation of primary functions	Deploy servers that implement only one primary function (eg web server, transaction server or database servers should be implemented on separate servers).
	Separation of client databases/data sets	Separate, both physically and logically, data from one client from that of other clients.
	Configuration and security settings	Configure systems in a consistent, accurate manner and apply and monitor approved security settings.
	Input/process/output validation	Validate information entered into, processed by and output from business applications and verify that it has not been subject to unauthorised change.
	Control of portable storage devices	For approved devices, manage and control their use throughout the life cycle. For unapproved devices, restrict their use and disable the ability to copy information to them.
	Backup and restore	Regular backups of information and software shall be performed and stored away from live systems. Restore shall be tested regularly.
	Encryption of sensitive stored information	Apply approved, documented cryptographic solutions, supported by cryptographic key management.
Physical protection	Access to premises	Access to buildings and offices shall be controlled in order to protect the sensitivity of information and to prevent theft of documents or equipment.
	Sensitive areas	Further restrict access to areas with elevated confidentiality level for the acquirer, e.g. research, prototypes, intellectual property files.
	IT equipment and services protection	Protect IT facilities, equipment, media and services against malicious attack, accidental damage, natural hazards and unauthorised physical access.
Access management	Segregation of duties	Segregate duties and areas of responsibility to reduce the risk of accidental or deliberate system or application misuse.
	Identity and access management	Implement a consistent identity and access management approach that provides effective user administration, identification, authentication and authorisation mechanisms.
	Access control	Restrict access to designated information and systems to specified individuals or roles in external suppliers (eg customers, suppliers and business partners) who have been authorised and are subject to agreed security requirements in an approved contract.
	Privileged user management	Use strong authentication, force regular password changes and log, monitor and review the activities of privileged users (eg superusers, administrators, developers, programmers, DBAs, or people who have access to sensitive or critical information).
Security monitoring and response	Continuous monitoring of systems and networks	Perform continuous monitoring of designated systems and networks, employ intrusion detection systems and record security events.
	Malware protection	Deploy comprehensive, up-to-date malware protection software, supported by a user awareness campaign and a process for handling malware infections.

Information security domains	Information security related categories	Information security requirements applied to the supplier
	Patch management	Have a documented and measured process for the deployment of system and software patches, including exceptions.
	Change management	Implement a comprehensive and approved change management process for information and systems that includes testing/accepting authorised changes and evaluating security implications.
	Incident management	Implement a comprehensive and approved incident management process for information and systems that includes identification, response, recovery and post-implementation review of information security incidents.
	e-discovery, e-forensic, audit and trail of evidence creation	Collect, store, archive and protect records, logs and other appropriate material.
Network connections	Network security	Design and operate robust, resilient networks that can cope with current and predicted levels of traffic, are supported by alternative facilities, incorporate firewalls and restrict network access to authorised individuals.
	Control of network access/ connectivity	Restrict connections to the Internet, to wireless networks, to customers and external suppliers and, where possible, separate those connections.
Electronic communications	Protection of electronic communications	Protect electronic communication systems (eg e-mail, instant messaging and VoIP) by setting policy for their use, configuring security settings, performing capacity planning and hardening the supporting infrastructure.
	Use of cryptographic solutions	Apply approved, documented cryptographic solutions, supported by effective cryptographic key management.
Business control	Sub-contractor management	Restrict access to designated information and systems to sub-contractors and business partners who have been authorised and are subject to agreed security requirements in an approved contract.
	Security audit and review	Conduct thorough, independent and regular security audits / reviews and publish the results both internally and for the acquirer.
	Business continuity	Have a business continuity plan that is supported by alternative processing facilities and tested regularly using simulations of the live environment.
	Human resources management	Ensure that staffs are reliable and qualified to handle information according to identified protection levels. Ensure the need-to-know principle and have appropriate disciplinary processes in place.
System Development	System Development Life Cycle methodology	Develop systems using a structured and approved system development methodology that ensures information security requirements are considered as part of the process, and consequently defined, documented and met.

## Annex B (informative)

### Cross-references between ISO/IEC 15288 clauses and ISO/IEC 27036 Part 2 clauses

ISO/IEC 15288 clauses	ISO/IEC 27036-2 clauses
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 Organisational 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	----
6.3 Project Processes	6.3 Project 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

ISO/IEC 15288 clauses	ISO/IEC 27036-2 clauses
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
6.4 Technical Processes	6.4 Technical processes
6.4.1 Stakeholder Requirements Definition Process	----
6.4.2 Requirements Analysis Process	----
6.4.3 Architectural Design Process	6.4.1 Architectural design process
6.4.4 Implementation Process	----
6.4.5 Integration Process	----
6.4.6 Verification Process	----
6.4.7 Transition Process	----
6.4.8 Validation Process	----
6.4.9 Operation Process	----
6.4.10 Maintenance Process	----
6.4.11 Disposal Process	----

## Annex C (informative)

### Cross-references between ISO/IEC 27036 Part 2 clauses and ISO/IEC 27002 controls

ISO/IEC 27036-2 clauses	ISO/IEC 27002 controls
6.1 Agreement processes	Controls listed in following clauses:  5 Security policies  6 Organisation of information security  15.1 Security in supplier relationships  18 Compliance
6.1.1 Acquisition process	Please refer to the mapping specific to the clause 6.1 Agreement processes.
6.1.2 Supply process	Please refer to the mapping specific to the clause 6.1 Agreement processes.
6.2 Organisational project-enabling processes	---
6.2.1 Life cycle model management process	---
6.2.2 Infrastructure management process	Controls listed in following clauses:  8 Asset management  9 Access control  10 Cryptography  11 Physical and environmental security  12 Operations security  13 Communications security  14 System acquisition, development and maintenance  16 Information security incident management  17 Information security aspects of business continuity management
6.2.3 Project portfolio management process	---
6.2.4 Human resource management process	Controls listed in the following clause:

ISO/IEC 27036-2 clauses	ISO/IEC 27002 controls
	7 Human resources security
6.3 Project 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	Controls listed in the following clause: 12.1.2 Change management
6.3.6 Information management process	Controls listed in following clauses: 12.1.1 Documented operating procedures 13.2 Information transfer 18 Compliance
6.3.7 Measurement process	---
6.4 Technical processes	---
6.4.1 Architectural design process	---
7.1 Supplier relationship planning process	Controls listed in the following clause: 15.1 Security in supplier relationships
7.2 Supplier selection process	---
7.3 Supplier relationship agreement process	Controls listed in the following clause: 15.1 Security in supplier relationships
7.4 Supplier relationship management process	Controls listed in the following clause: 15.2 Supplier service delivery management
7.5 Supplier relationship termination process	---

## Bibliography

- [1] ISO/IEC 15288, *Systems and software engineering -- System life cycle processes*
- [2] ISO/IEC 27002, *Information technology -- Security techniques -- Information security management systems -- Code of practice for information security management*
- [3] ISO/IEC 27031, *Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity*
- [4] ISO 22313, *Societal security -- Business continuity management systems – Guidance*
- [5] ISO 22301, *Societal security -- Business continuity management systems – Requirements*
- [6] ISO/IEC 27005, *Information technology -- Security techniques -- Information security risk management*
- [7] ISO 31000, *Risk management – Principles and guidelines*
- [8] ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems – Requirements*
- [9] ISO/IEC 27004, *Information technology -- Security techniques -- Information security management – Measurement*
- [10] ISO/IEC 27035, *Information technology -- Security techniques – Information security incident management*




**EXPLANATORY REPORT  
RAPPORT EXPLICATIF**
**ISO/IEC DIS 27036-2**
**ISO/IEC JTC 1/SC 27**

 Secretariat **DIN**

This form should be sent to the ISO Central Secretariat, together with the English and French versions of the committee draft, by the secretariat of the technical committee or subcommittee concerned.

Ce formulaire doit être envoyé au Secrétariat central de l'ISO en même temps que les versions anglaise et française du projet de comité, par le secrétariat du comité technique ou du sous-comité concerné.

The accompanying document is submitted for circulation to member body vote as a DIS, following consensus obtained from the P-members of the committee.

Le document ci-joint est soumis, pour diffusion comme DIS, au vote comité membre, suite au consensus des membres (P) du comité obtenu.

 on **2012-10-26**

☒ at the meeting of **JTC 1/SC 27/WG 4**  
à la réunion du

see resolution No. **35** in document **N11941**  
voir résolution n° dans le

☐ by postal ballot initiated on  
par un vote par correspondance démarré le

P-members in favour: Membres (P) approuvant le projet:	Number <b>19</b>	Countries <b>Belgium, Brazil, Czech Republic, Denmark, India, Ireland, Kazakhstan, Korea, Republic of, Malaysia, Mexico, Netherlands, Norway, Romania, Russian Federation, Singapore, Slovenia, Sweden, Thailand, Ukraine</b>
P-members voting against: Membres (P) désapprouvant:	<b>3</b>	<b>France*, Japan, United States*</b>
P-members abstaining: Membres (P) s'abstenant:	<b>16</b>	<b>Australia, Canada**, Cyprus, Finland**, Germany**, Israel, Italy**, Luxembourg, Morocco, New Zealand, Peru, Poland, South Africa**, Spain, Switzerland, United Kingdom**</b>
P-members who did not vote: Membres (P) n'ayant pas voté:	<b>11</b>	<b>Algeria, Austria, Côte d'Ivoire, Cyprus, Estonia, France, Mauritius, Singapore, Slovakia, Sri Lanka, United Arab Emirates</b>

## Remarks/Remarques

The 1st CD document was circulated as SC 27 N11014. The summary of voting is presented in SC 27 N11526. JTC 1/SC 7 liaison comments were circulated as SC 27 N11605. The disposition of comments is shown in SC 27 N11994. The text for a 3-month DIS balloting is contained in N11995.

\* Negative votes of the National Bodies indicated have been satisfactorily resolved and changed to APPROVAL.

\*\* National Bodies indicated changed their votes to APPROVAL.

I hereby confirm that this draft meets the requirements of part 2 of the ISO/IEC Directives  
Je confirme que ce projet satisfait aux prescriptions de la partie 2 des Directives ISO/CEI

Date

 Name and signature of the secretary  
Nom et signature du secrétaire

**2012-11-14**
**Krystyna Passia**

## Result of voting

### Ballot Information

<b>Ballot reference</b>	ISO/IEC CD 27036-2 - ISO-IECJTC1-SC27_N11014
<b>Ballot type</b>	CD
<b>Ballot title</b>	Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Common requirements
<b>Opening date</b>	2012-07-12
<b>Closing date</b>	2012-10-12
<b>Note</b>	1st CD Registration and Consideration  In accordance with resolution 4 (see SC 27 N11330) of the 24th SC 27 Plenary meeting held in Stockholm, Sweden (14th and 15th May 2012) the attached document has been registered with the ISO Central Secretariat (ITTF) as a 1st Committee Draft (CD) and is hereby circulated for a 1st CD letter ballot closing by  2012-10-12

### Member responses:

<b>Votes cast (38)</b>	Australia (SA) Belgium (NBN) Brazil (ABNT) Canada (SCC) Cyprus (CYS) Czech Republic (UNMZ) Denmark (DS) Finland (SFS) France (AFNOR) Germany (DIN) India (BIS) Ireland (NSAI) Israel (SII) Italy (UNI) Japan (JISC) Kazakhstan (KAZMEMST) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Mexico (DGN)
------------------------	---

	Morocco (IMANOR) Netherlands (NEN) New Zealand (SNZ) Norway (SN) Peru (INDECOPI) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Singapore (SPRING SG) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Thailand (TISI) Ukraine (DSSU) United Kingdom (BSI) United States (ANSI)
<b>Comments submitted (0)</b>	
<b>Votes not cast (11)</b>	Algeria (IANOR) Austria (ASI) China (SAC) Côte d'Ivoire (CODINORM) Estonia (EVS) Kenya (KEBS) Mauritius (MSB) Slovakia (SUTN) Sri Lanka (SLSI) United Arab Emirates (ESMA) Uruguay (UNIT)

Questions:	
<b>Q.1</b>	"Do you agree with approval of the CD text?"
<b>Q.2</b>	"If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"
<b>Q.3</b>	"If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

Votes by members	Q.1	Q.2	Q.3
<b>Australia (SA)</b>	Abstention	Ignore	Ignore
<b>Belgium (NBN)</b>	Approval as presented	Ignore	Ignore
<b>Brazil (ABNT)</b>	Approval as presented	Ignore	Ignore
<b>Canada (SCC)</b>	Abstention	Ignore	Ignore
<b>Cyprus (CYS)</b>	Abstention	Ignore	Ignore
<b>Czech Republic (UNMZ)</b>	Approval as presented	Ignore	Ignore
<b>Denmark (DS)</b>	Approval as	Ignore	Ignore

	presented		
<b>Finland (SFS)</b>	Abstention	Ignore	Ignore
<b>France (AFNOR)</b>	Disapproval of the draft	All	Ignore
<b>Germany (DIN)</b>	Abstention	Ignore	Ignore
<b>India (BIS)</b>	Approval with comments	All	Ignore
<b>Ireland (NSAI)</b>	Approval as presented	Ignore	Ignore
<b>Israel (SH)</b>	Abstention	Ignore	Ignore
<b>Italy (UNI)</b>	Abstention	Ignore	Ignore
<b>Japan (JISC)</b>	Disapproval of the draft	Ignore	No
<b>Kazakhstan (KAZMEMST)</b>	Approval as presented	Ignore	Ignore
<b>Korea, Republic of (KATS)</b>	Approval as presented	Ignore	Ignore
<b>Luxembourg (ILNAS)</b>	Approval as presented	Ignore	Ignore
<b>Malaysia (DSM)</b>	Approval as presented	Ignore	Ignore
<b>Mexico (DGN)</b>	Approval as presented	Ignore	Ignore
<b>Morocco (IMANOR)</b>	Abstention	Ignore	Ignore
<b>Netherlands (NEN)</b>	Approval with comments	All	Ignore
<b>New Zealand (SNZ)</b>	Abstention	Ignore	Ignore
<b>Norway (SN)</b>	Approval as presented	Ignore	Ignore
<b>Peru (INDECOPI)</b>	Abstention	Ignore	Ignore
<b>Poland (PKN)</b>	Abstention	Ignore	Ignore
<b>Romania (ASRO)</b>	Approval as presented	Ignore	Ignore
<b>Russian Federation (GOST R)</b>	Approval as presented	Ignore	Ignore
<b>Singapore (SPRING SG)</b>	Approval as presented	Ignore	Ignore
<b>Slovenia (SIST)</b>	Approval as presented	Ignore	Ignore
<b>South Africa (SABS)</b>	Abstention	Ignore	Ignore
<b>Spain (AENOR)</b>	Abstention	Ignore	Ignore
<b>Sweden (SIS)</b>	Approval with comments	All	Ignore
<b>Switzerland (SNV)</b>	Abstention	Ignore	Ignore

<b>Thailand (TISI)</b>	Approval as presented	Ignore	Ignore
<b>Ukraine (DSSU)</b>	Approval as presented	Ignore	Ignore
<b>United Kingdom (BSI)</b>	Abstention	Ignore	Ignore
<b>United States (ANSI)</b>	Disapproval of the draft	Ignore	Yes

#### Answers to Q.1: "Do you agree with approval of the CD text?"

<b>17 x</b>	<b>Approval as presented</b>	<b>Belgium (NBN)</b> <b>Brazil (ABNT)</b> <b>Czech Republic (UNMZ)</b> <b>Denmark (DS)</b> <b>Ireland (NSAI)</b> <b>Kazakhstan (KAZMEMST)</b> <b>Korea, Republic of (KATS)</b> <b>Luxembourg (ILNAS)</b> <b>Malaysia (DSM)</b> <b>Mexico (DGN)</b> <b>Norway (SN)</b> <b>Romania (ASRO)</b> <b>Russian Federation (GOST R)</b> <b>Singapore (SPRING SG)</b> <b>Slovenia (SIST)</b> <b>Thailand (TISI)</b> <b>Ukraine (DSSU)</b>
<b>3 x</b>	<b>Approval with comments</b>	<b>India (BIS)</b> <b>Netherlands (NEN)</b> <b>Sweden (SIS)</b>
<b>3 x</b>	<b>Disapproval of the draft</b>	<b>France (AFNOR)</b> <b>Japan (JISC)</b> <b>United States (ANSI)</b>
<b>15 x</b>	<b>Abstention</b>	<b>Australia (SA)</b> <b>Canada (SCC)</b> <b>Cyprus (CYS)</b> <b>Finland (SFS)</b> <b>Germany (DIN)</b> <b>Israel (SII)</b> <b>Italy (UNI)</b> <b>Morocco (IMANOR)</b> <b>New Zealand (SNZ)</b> <b>Peru (INDECOPI)</b> <b>Poland (PKN)</b> <b>South Africa (SABS)</b> <b>Spain (AENOR)</b> <b>Switzerland (SNV)</b> <b>United Kingdom (BSI)</b>

#### Answers to Q.2: "If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"

<b>0 x</b>	<b>General</b>
------------	----------------

<b>0 x</b>	<b>Technical</b>	
<b>0 x</b>	<b>Editorial</b>	
<b>4 x</b>	<b>All</b>	<b>France (AFNOR)</b> <b>India (BIS)</b> <b>Netherlands (NEN)</b> <b>Sweden (SIS)</b>
<b>34 x</b>	<b>Ignore</b>	<b>Australia (SA)</b> <b>Belgium (NBN)</b> <b>Brazil (ABNT)</b> <b>Canada (SCC)</b> <b>Cyprus (CYS)</b> <b>Czech Republic (UNMZ)</b> <b>Denmark (DS)</b> <b>Finland (SFS)</b> <b>Germany (DIN)</b> <b>Ireland (NSAI)</b> <b>Israel (SII)</b> <b>Italy (UNI)</b> <b>Japan (JISC)</b> <b>Kazakhstan (KAZMEMST)</b> <b>Korea, Republic of (KATS)</b> <b>Luxembourg (ILNAS)</b> <b>Malaysia (DSM)</b> <b>Mexico (DGN)</b> <b>Morocco (IMANOR)</b> <b>New Zealand (SNZ)</b> <b>Norway (SN)</b> <b>Peru (INDECOPI)</b> <b>Poland (PKN)</b> <b>Romania (ASRO)</b> <b>Russian Federation (GOST R)</b> <b>Singapore (SPRING SG)</b> <b>Slovenia (SIST)</b> <b>South Africa (SABS)</b> <b>Spain (AENOR)</b> <b>Switzerland (SNV)</b> <b>Thailand (TISI)</b> <b>Ukraine (DSSU)</b> <b>United Kingdom (BSI)</b> <b>United States (ANSI)</b>

Answers to Q.3: "If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

<b>1 x</b>	<b>Yes</b>	<b>United States (ANSI)</b>
<b>1 x</b>	<b>No</b>	<b>Japan (JISC)</b>
<b>36 x</b>	<b>Ignore</b>	<b>Australia (SA)</b> <b>Belgium (NBN)</b> <b>Brazil (ABNT)</b> <b>Canada (SCC)</b> <b>Cyprus (CYS)</b> <b>Czech Republic (UNMZ)</b> <b>Denmark (DS)</b> <b>Finland (SFS)</b> <b>France (AFNOR)</b>

<p> Germany (DIN)  India (BIS)  Ireland (NSAI)  Israel (SII)  Italy (UNI)  Kazakhstan (KAZMEMST)  Korea, Republic of (KATS)  Luxembourg (ILNAS)  Malaysia (DSM)  Mexico (DGN)  Morocco (IMANOR)  Netherlands (NEN)  New Zealand (SNZ)  Norway (SN)  Peru (INDECOPI)  Poland (PKN)  Romania (ASRO)  Russian Federation (GOST R)  Singapore (SPRING SG)  Slovenia (SIST)  South Africa (SABS)  Spain (AENOR)  Sweden (SIS)  Switzerland (SNV)  Thailand (TISI)  Ukraine (DSSU)  United Kingdom (BSI) </p>
---

Comments from Voters		
Member:	Comment:	Date:
<b>France</b> (AFNOR)	<i>Comment File</i>	2012-10-12 11:33:44
<a href="#">CommentFiles/ISO_IEC_CD_27036-2_-_ISO-IECJTC1-SC27_N11014_AFNOR.doc</a>		
<b>India</b> (BIS)	<i>Comment File</i>	2012-10-11 07:35:33
<a href="#">CommentFiles/ISO_IEC_CD_27036-2_-_ISO-IECJTC1-SC27_N11014_BIS.doc</a>		
<b>Japan</b> (JISC)	<i>Comment File</i>	2012-10-03 07:42:41
<a href="#">CommentFiles/ISO_IEC_CD_27036-2_-_ISO-IECJTC1-SC27_N11014_JISC.doc</a>		
<b>Netherlands</b> (NEN)	<i>Comment File</i>	2012-10-05 13:41:15
<a href="#">CommentFiles/ISO_IEC_CD_27036-2_-_ISO-IECJTC1-SC27_N11014_NEN.doc</a>		
<b>Sweden</b> (SIS)	<i>Comment File</i>	2012-09-25 09:28:39
<a href="#">CommentFiles/ISO_IEC_CD_27036-2_-_ISO-IECJTC1-SC27_N11014_SIS.doc</a>		
<b>United States</b> (ANSI)	<i>Comment File</i>	2012-10-10 20:37:45
<a href="#">CommentFiles/ISO_IEC_CD_27036-2_-_ISO-IECJTC1-SC27_N11014_ANSI.doc</a>		

Comments from Commenters		
Member:	Comment:	Date: