BS ISO/IEC 27036-2:2014

BSI Standards Publication

Information technology — Security techniques — Information security for supplier relationships

Part 2: Requirements

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 27036-2:2014

National foreword

This British Standard is the UK implementation of ISO/IEC 27036-2:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 76089 1

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2014.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27036-2:2014

INTERNATIONAL STANDARD

ISO/IEC 27036-2

First edition
2014-08-01

Information technology — Security techniques — Information security for supplier relationships —

Part 2: Requirements

Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur —

Partie 2: Exigences

Reference number
ISO/IEC 27036-2:2014(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2014

Full document details: BS ISO/IEC 27036-2:2014

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27036-2:2014

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols and abbreviated terms **1**

5 Structure of ISO/IEC 27036-2 ..... **2**

6 Information security in supplier relationship management **4**
- 6.1 Agreement processes 4
- 6.2 Organisational project-enabling processes 7
- 6.3 Project processes 10
- 6.4 Technical processes 14

7 Information security in a supplier relationship instance **15**
- 7.1 Supplier relationship planning process 15
- 7.2 Supplier selection process 17
- 7.3 Supplier relationship agreement process 21
- 7.4 Supplier relationship management process 24
- 7.5 Supplier relationship termination process 27

Annex A (informative) **Cross-references between ISO/IEC 15288 clauses and ISO/IEC 27036-2 clauses** **30**

Annex B (informative) **Cross-references between ISO/IEC 27036-2 clauses and ISO/IEC 27002 controls** **32**

Annex C (informative) **Objectives from Clauses 6 and 7** **34**

Bibliography **38**

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT 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 supply chain security*

The following part is under preparation:

— *Part 4: Guidelines for security of cloud services.*

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

Introduction

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

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

ISO/IEC 27036-2:

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

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

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

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

e) is not intended for certification purposes;

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

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

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

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

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 or recommendations where there is a certain freedom of choice.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27036-2:2014

INTERNATIONAL STANDARD ISO/IEC 27036-2:2014(E)

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 organizations, regardless of type, size and nature.

To meet these requirements, an organization 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, risk management, operational and human resources management, and information security.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 27036-1, *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 27036-1 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

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27036-2:2014

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 27036-2

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

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 information security risks resulting from supplier relationships.

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

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

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.

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

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

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

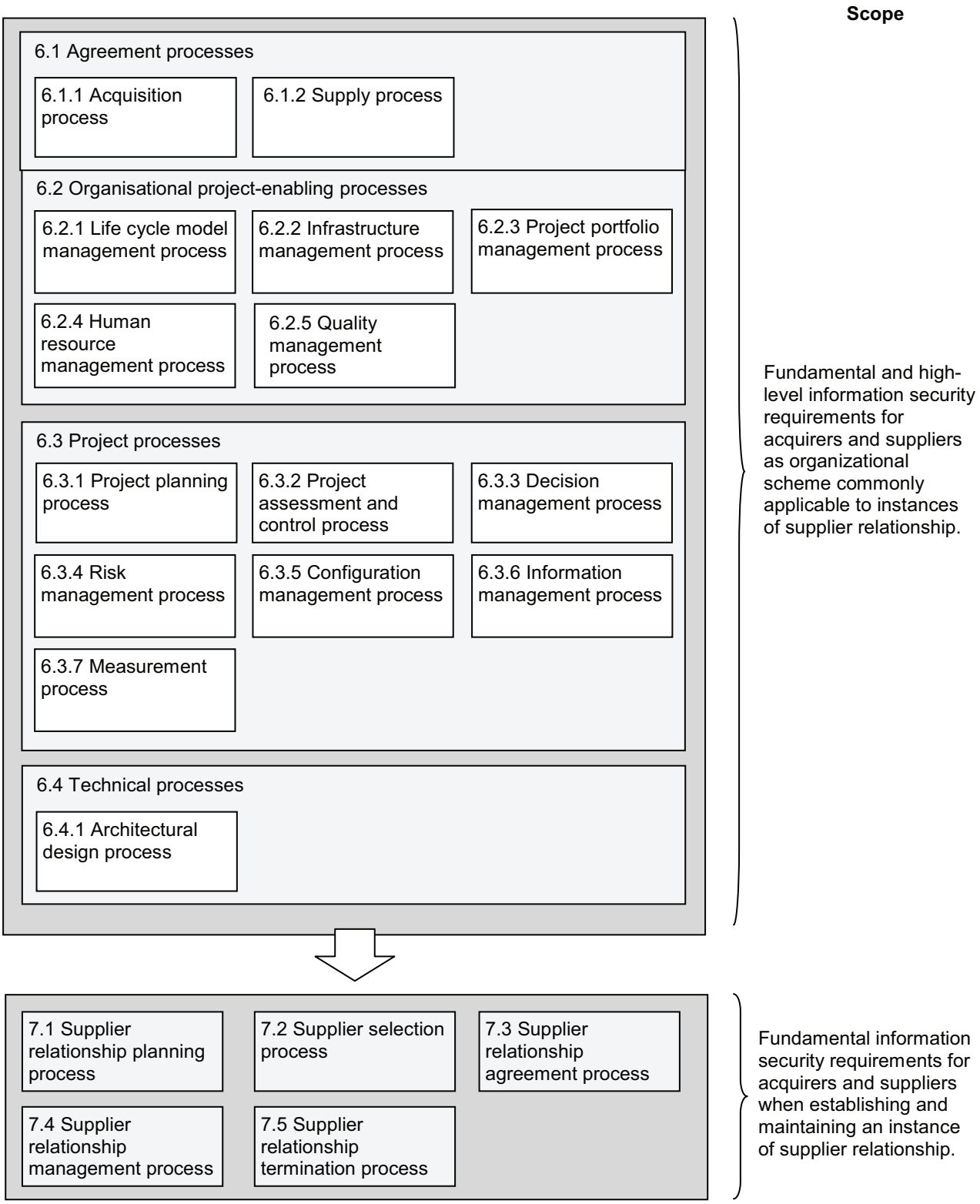

Figure 1 — Scope of fundamental information security requirements defined in Clauses 6 and 7

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

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:

Acquirer
Text specific to the acquirer.

Supplier
Text specific to the supplier.

Acquirer	**Supplier**
Text specific to 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 cross-references between clauses of ISO/IEC 15288 that are relevant to supplier relationships and clauses of ISO/IEC 27036-2.

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

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

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 with respect to the supplier relationship.

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

a) Acquisition process;

b) Supply process.

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
a) Establish a supplier relationship strategy that: 1) Is based on the information security risk tolerance of the acquirer; 2) Defines the information security foundation to use when planning, preparing, managing and terminating the procurement of a product or service.

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

6.1.1.2 Activities

The following minimum activities shall be executed by the acquirer to meet the objective defined at Clause 6.1.1.1:

Acquirer
a) Define, implement, maintain and improve a supplier relationship strategy containing the following: 1) Management motives, needs and expectations from procuring products or services; NOTE These statements should be expressed from business, operational, legal and regulatory perspectives. 2) Management commitment to allocate necessary resources; 3) An information security risk management framework to use for assessing information security risks accompanying the procurement of a product or service; NOTE Clause 6.3.4 defines information security requirements for the establishment of an information security risk management framework. 4) A framework to use when defining information security requirements during the supplier relationship planning process; This framework shall be defined following information security guidelines and rules, such as information security policy and information classification, established by the acquirer. Information security requirements defined in this framework need to be customized to each supplier relationship instance, considering type and nature of the product or service that is procured. This framework shall also include the following: i) Methods for suppliers to provide evidence for adherence to the defined information security requirements; ii) Methods for the acquirer to validate suppliers' adherence to the defined information security requirements; iii) Processes for sharing information about information security changes, incidents and other relevant events among the acquirer and suppliers. 5) A supplier selection criteria framework to use when selecting a supplier and which includes the following: i) Methods for assessing the information security maturity required from a supplier; The following elements can be requested from the supplier to evaluate its information security maturity: 1. Past security-relevant performance; 2. Evidence of pro-active management of information security (e.g. holding an ISO/IEC 27001 certification relevant to the supply of the product or service); 3. Evidence of documented and tested business continuity and ICT continuity plans. ii) Methods to be used for assessing evidence provided by a supplier based on the defined information security requirements; iii) Methods for assessing supplier acceptance of the following: 1. Information security requirements defined in the supplier relationship plan; 2. Commitment to support the acquirer in its compliance monitoring and enforcement activities; 3. Transition of the product or service supply that may be procured when it has been previously manufactured or operated by the acquirer or by a different supplier;

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

4. Termination of the product or service supply.

iv) Supplier-specific requirements, to be defined in accordance to business, legal, regulatory, architectural, policy and contractual expectations from the acquirer, such as:

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

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

i) Transition plan to transfer a product or service procured to a different supplier;

ii) Information security change management procedure;

iii) Information security incident management procedure;

iv) Compliance monitoring and enforcement plan;

v) Termination plan to terminate the procurement of a product or service.

b) Appoint an individual responsible for handling the information security aspects of the supplier relationship strategy and ensure that this individual is appropriately and regularly trained.

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.

NOTE The supplier relationship strategy should also be reviewed when a product or service is procured that can significantly impact the acquirer.

6.1.2 Supply process

6.1.2.1 Objective

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

Supplier
a) Establish an acquirer relationship strategy that 1) Is based on the information security risk tolerance of the supplier; 2) Defines the information security foundation to use when planning, preparing, managing and terminating the supply of a product or service.

6.1.2.2 Activities

The following minimum activities shall be executed by the supplier to meet the objective defined at Clause 6.1.2.1:

Supplier
a) Define, implement, maintain and improve an acquirer relationship strategy containing the following: 1) Management motives, needs and expectations from supplying of products or services; NOTE These statements should be expressed from business, operational, and legal perspectives. 2) Management commitment to allocate necessary resources; 3) An information security risk management framework to use for assessing information security risks that accompany the supply of a product or a service; NOTE Clause 6.3.4 defines information security requirements for the establishment of an information security risk management framework.

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014

4) An information security management framework by:
   i) Defining, implementing, maintaining and improving an information security management within the organization;

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

   ii) Ensuring that 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.

   iii) Defining a process to accept, interpret, apply and measure acquirer information security requirements.
5) Methods for:
   i) Demonstrating supplier's capacity to supply a product or service of acceptable quality;
   ii) Providing evidence of adherence to information security requirements defined by acquirers.
6) High-level information security requirements to use when defining the following:
   i) Transition plan to support the transfer of a product or service supply when it has been previously manufactured or operated by an acquirer or by another supplier;
   ii) Information security change management procedure;
   iii) Information security incident management procedure;
   iv) Processes for sharing information about information security changes, incidents and other relevant events among the supplier and acquirers;
   v) Process for handling corrective actions;
   vi) Termination plan to terminate the supply of a product or service.

b) Appoint an individual responsible for handling the information security aspects of the acquirer relationship strategy and ensure that this individual is appropriately and regularly trained.

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

   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 organization'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) Project portfolio management process;

d) Human resource management process;

e) Quality management process.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-2:2014