

---

---

**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*

**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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
Foreword .....	iv
Introduction .....	v
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>1</b>
<b>4 Symbols and abbreviated terms .....</b>	<b>1</b>
<b>5 Structure of ISO/IEC 27036-2 .....</b>	<b>2</b>
<b>6 Information security in supplier relationship management .....</b>	<b>4</b>
6.1 Agreement processes .....	4
6.2 Organisational project-enabling processes .....	7
6.3 Project processes .....	10
6.4 Technical processes .....	14
<b>7 Information security in a supplier relationship instance .....</b>	<b>15</b>
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
<b>Annex A (informative) Cross-references between ISO/IEC 15288 clauses and ISO/IEC 27036-2 clauses .....</b>	<b>30</b>
<b>Annex B (informative) Cross-references between ISO/IEC 27036-2 clauses and ISO/IEC 27002 controls .....</b>	<b>32</b>
<b>Annex C (informative) Objectives from Clauses 6 and 7 .....</b>	<b>34</b>
<b>Bibliography .....</b>	<b>38</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.

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](http://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](http://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.*

## 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.

# 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*