BS ISO/IEC 27036-1:2014

BSI Standards Publication

Information technology — Security techniques — Information security for supplier relationships

Part 1: Overview and concepts

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 27036-1:2014

National foreword

This British Standard is the UK implementation of ISO/IEC 27036-1:2014.

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 75943 7

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 30 April 2014.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27036-1:2014

INTERNATIONAL STANDARD

ISO/IEC 27036-1

First edition
2014-04-01

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

Part 1: Overview and concepts

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

Partie 1: Aperçu général et concepts

Reference number
ISO/IEC 27036-1:2014(E)

Documents
Document Sharing Hub
© ISO/IEC 2014

Full document details: BS ISO/IEC 27036-1:2014

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 27036-1:2014

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **3**
5 Problem definition and key concepts **4**
5.1 Motives for establishing supplier relationships 4
5.2 Types of supplier relationships 4
5.3 Information security risks in supplier relationships and associated threats 6
5.4 Managing information security risks in supplier relationships 9
5.5 ICT supply chain considerations 9
6 Overall ISO/IEC 27036 structure and overview **10**
6.1 Purpose and Structure 10
6.2 Overview of Part 1: Overview and concepts 11
6.3 Overview of Part 2: Requirements 11
6.4 Overview of Part 3: Guidelines for Information and Communication Technology (ICT) supply chain security 11
6.5 Overview of Part 4: Guidelines for security of cloud services 11
Bibliography **13**

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-1:2014

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.

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 27036-1 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 supply chain security*

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

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-1:2014

Introduction

Most (if not all) organizations around the world, whatever their size or domains of activities, have relationships with suppliers of different kinds that deliver products or services.

Such suppliers can have either a direct or indirect access to the information and information systems of the acquirer, or will provide elements (software, hardware, processes, or human resources) that will be involved in information processing. Acquirers can also have physical and/or logical access to the information of the supplier when they control or monitor production and delivery processes of the supplier.

Thus, acquirers and suppliers can cause information security risks to each other. These risks need to be assessed and treated by both acquirer and supplier organizations through appropriate management of information security and the implementation of relevant controls. In many instances, organizations have adopted the International Standards of ISO/IEC 27001 and/or ISO/IEC 27002 for the management of their information security. Such International Standards should also be adopted in managing supplier relationships in order to effectively control the information security risks inherent in those relationships.

This International Standard provides further detailed implementation guidance on the controls dealing with supplier relationships that are described as general recommendations in ISO/IEC 27002.

Supplier relationships in the context of this International Standard include any supplier relationship that can have information security implications, e.g. information technology, healthcare services, janitorial services, consulting services, R&D partnerships, outsourced applications (ASPs), or cloud computing services (such as software, platform, or infrastructure as a service).

Both the supplier and acquirer have to take equal responsibility to achieve the objectives in the supplier-acquirer relationship and adequately address information security risks that can occur. It is expected that they implement the requirements and guidelines of this International Standard. Furthermore, fundamental processes should be implemented to support the supplier-acquirer relationship (e.g. governance, business management, and operational and human resources management). These processes will provide support in terms of information security as well as the accomplishment of business objectives.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27036-1:2014

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27036-1:2014