

AS ISO/IEC 27036.1:2023
ISO/IEC 27036-1:2021



STANDARDS
Australia



Cybersecurity — Supplier relationships

Part 1: Overview and concepts



AS ISO/IEC 27036.1:2023

This Australian Standard ® was prepared by IT-012, Information security, cybersecurity and privacy protection. It was approved on behalf of the Council of Standards Australia on 16 May 2023.

This Standard was published on 9 June 2023.

The following are represented on Committee IT-012:

- Australasian Society for Computers and Law
- Australian Industry Group
- Australian Information Industry Association
- Australian Information Security Association
- Australian Security Industry Association
- Business Continuity Institute Australasia
- Consumers Federation of Australia
- CSIRO Data61
- Cyber Security Cooperative Research Centre
- Department of Defence (Australian Government)
- Energy Networks Australia
- Engineers Australia
- ISACA Melbourne
- Joint Accreditation System of Australia & New Zealand
- Monash University
- Office of the Victorian Information Commissioner
- University of Wollongong

This Standard was issued in draft form for comment as DR AS ISO/IEC 27036.1:2023.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76139 213 9

Cybersecurity — Supplier relationships

Part 1: Overview and concepts

First published as AS ISO/IEC 27036.1:2023.

COPYRIGHT

© ISO/IEC 2023 — All rights reserved
© Standards Australia Limited 2023

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-012, Information security, cybersecurity and privacy protection.

After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this document as an Australian Standard rather than an Australian/New Zealand Standard.

The objective of this document is to provide an overview of guidance assisting organizations to secure information and information systems with regard to supplier relationships. It also introduces concepts described in detail in other parts of ISO/IEC 27036. This document addresses perspectives of both acquirers and suppliers.

This document is identical with, and has been reproduced from, ISO/IEC 27036-1:2021, *Cybersecurity — Supplier relationships, Part 1: Overview and concepts*.

As this document has been reproduced from an International document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
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	3
5.1 Motives for establishing supplier relationships	3
5.2 Types of supplier relationships	4
5.2.1 Supplier relationships for products	4
5.2.2 Supplier relationships for services	4
5.2.3 ICT supply chain	5
5.2.4 Cloud computing	5
5.3 Information security risks in supplier relationships and associated threats	6
5.4 Managing information security risks in supplier relationships	8
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 ISO/IEC 27036-1: Overview and concepts	10
6.3 Overview of ISO/IEC 27036-2: Requirements	10
6.4 Overview of ISO/IEC 27036-3: Guidelines for information and communication technology (ICT) supply chain security	11
6.5 Overview of ISO/IEC 27036-4: Guidelines for security of cloud services	11
Bibliography	12

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, *Information security, cybersecurity, and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27036-1:2014), of which this constitutes a minor revision.

The main changes compared to the previous edition are as follows:

- change of title;
- revision of [Clause 2](#);
- alignment with drafting rules;
- ISO/IEC 27036 (all parts) added in Bibliography.

A list of all parts in the ISO/IEC 27036 series can be found on the ISO website.

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 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 ISO/IEC 27001 and 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 document 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 document 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 should take responsibility for achieving the objectives in the supplier-acquirer relationship and adequately addressing the information security risks that can occur. It is expected that they implement the requirements and guidelines of this document. 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.