INTERNATIONAL STANDARD

ISO/IEC 27036-2

Second edition
2022-06

Cybersecurity — Supplier relationships —

Part 2: Requirements

Partie 2: Exigences

Reference number
ISO/IEC 27036-2:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document 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 27036-2:2014), which has been technically revised.

The main changes are as follows:

— the structure and content have been aligned with the most recent version of ISO/IEC 15288.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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.

This document:

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 an overview and concepts associated with information security in supplier relationships.

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

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

Cybersecurity — Supplier relationships —

Part 2: Requirements

1 Scope

This document 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.

This document is applicable to all organizations, regardless of type, size and nature.

To meet the requirements, it is expected that an organization has internally implemented a number of foundational processes or is actively planning to do so. These processes include, but are not limited to: business management, risk management, operational and human resources management, and information security.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27036-1, *Cybersecurity — 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.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Abbreviated terms

ASP	application service provider
BCP	business continuity plan
ICT	information and communication technology
ISMS	information security management system

国际标准

ISO/IEC 27036-2

第二版
2022-06

网络安全 - 供应商关系

第二部分。
要求

第2部分：要求

参考号 ISO/IEC 27036-2:2022(E)

内容

前言

ISO（国际标准化组织）和IEC（国际电工委员会）构成了全世界标准化的专门体系。作为ISO或IEC成员的国家机构通过各自组织建立的技术委员会参与国际标准的制定，以处理特定的技术活动领域。ISO和IEC技术委员会在共同感兴趣的领域进行合作。其他国际组织，政府和非政府组织，与ISO和IEC联络，也参加了工作。

用于制定本文件的程序和打算进一步维护本文件的程序在ISO/IEC指令第1部分中有所描述。特别要注意的是，不同类型的文件需要不同的批准标准。本文件是根据ISO/IEC指令第2部分的编辑规则起草的（见www.iso.org/directives 或 www.iec.ch/members_experts/refdocs）。

请注意，本文件中的某些内容可能是专利权的对象。ISO和IEC不负责识别任何或所有此类专利权。在文件制定过程中发现的任何专利权的细节将在导言中和/或在ISO收到的专利声明清单中（见www.iso.org/patents）或IEC收到的专利声明清单中（见https://patents.iec.ch）。

本文件中使用的任何商品名称是为方便用户而提供的信息，并不意味着
构成认可。

关于标准的自愿性质的解释，与合格评定有关的ISO特定术语和表达方式的含义，以及关于ISO在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，见www.iso.org/iso/foreword.html。在IEC中，见www.iec.ch/understanding-standards。

本文件由联合技术委员会ISO/IEC JTC 1，*信息技术*，小组委员会SC 27，*信息安全、网络安全和隐私保护*编写。

该第二版取消并取代了第一版（ISO/IEC 27036-2:2014），该版本已进行了技术修订。

主要变化如下。

- 其结构和内容已与ISO/IEC 15288的最新版本相一致。ISO/IEC 27036系列的所有部分的清单

可以在ISO和IEC的网站上找到。

对本文件的任何反馈或问题应直接向用户的国家标准机构提出。这些机构的完整名单可在www.iso.org/members.html 和 www.iec.ch/national-committees 上找到。

简介

世界各地的组织与供应商合作以获得产品和服务。许多组织建立了几个供应商关系，以涵盖各种业务需求，如运营或制造。反之，供应商向几个收购方提供产品和服务。

收购方和供应商之间为获取各种产品和服务而建立的关系可能会给收购方和供应商带来信息安全风险。这些风险是由相互接触对方的资产，如信息和信息系统，以及业务目标和信息安全方法的差异造成的。收购方和供应商都应管理这些风险。

这份文件。

a) 规定了定义、实施、操作、监控、审查、维护和改进供应商和收购方关系的基本信息安全要求。

b) 有助于相互了解对方的信息安全方法和对信息安全风险的容忍度。

c) 反映了管理可能对供应商和收购方关系产生信息安全影响的风险的复杂性。

d) 本手册旨在供任何愿意评估供应商或收购方关系中的信息安全的组织使用。

e) 并非用于认证目的。

f) 其目的是用来设定一些适用于供应商和收购方关系的明确的信息安全目标，作为保证的基础。

ISO/IEC 27036-1提供了与供应商的信息安全相关的概述和概念。
关系。

ISO/IEC 27036-3为收购方和供应商提供了管理ICT产品和服务供应链特有的信息安全风险的准则。

ISO/IEC 27036-4为收购方和供应商提供了管理云服务特有的信息安全风险的指南。

网络安全 - 供应商关系

第二部分。
要求

1 范围

本文件规定了定义、实施、操作、监控、审查、维护和改进供应商和收购方关系的基本信息安全要求。

这些要求涵盖了任何产品和服务的采购和供应，如制造或装配、业务流程采购、软件和硬件组件、知识流程采购、建设-运营-转让和云计算服务。

本文件适用于所有组织，无论其类型、规模和性质如何。

为了满足这些要求，预计一个组织已经在内部实施了一些基本的流程，或者正在积极计划这样做。这些流程包括但不限于：业务管理、风险管理、运营和人力资源管理、以及信息安全。

2 规范性参考资料

以下文件在文中被提及，其部分或全部内容构成本文件的要求。对于注明日期的参考文件，仅适用于所引用的版本。对于未注明日期的参考文件，适用于所参考文件的最新版本（包括任何修正案）。

ISO/IEC 27000，*信息技术-安全技术-信息安全管理系统-概述和词汇*

ISO/IEC 27036-1，*网络安全 - 供应商关系 - 第1部分。概述和概念*

3 术语和定义

在本文件中，适用ISO/IEC 27000和ISO/IEC 27036-1中的术语和定义。

ISO和IEC在以下地址维护用于标准化的术语数据库。

— ISO在线浏览平台：可在https://www.iso.org/obp

— IEC Electropedia：可在https://www.electropedia.org/

4 缩略语

ASP应用服务提供者

BCP业务连续性计划

ICT信息和通信技术

ISMS信息安全管理系统

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。