INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2022(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 third edition cancels and replaces the second edition (ISO/IEC 27001:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001:2013/Cor 1:2014 and ISO/IEC 27001:2013/Cor 2:2015.

The main changes are as follows:

— the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

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

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

信息安全、网络安全和隐私保护

—信息安全管理体系—要求

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

(第三版 中文版)

翻译本

2022 年 12 月

目录

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专门体系。作为 ISO 或 IEC 成员的国家机构通过各自组织为处理特定技术活动领域而设立的技术委员会参与国际标准的制定。ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。与 ISO 和 IEC 保持联系的其他国际组织，包括政府组织和非政府组织也参与了这项工作。

ISO/IEC 指令第 1 部分描述了用于编制本文件的程序及其进一步维护的程序。特别是，应注意不同类型文件所需的不同批准标准。本文件根据 ISO/IEC 指令第 2 部分的编辑规则起草（见 www.ISO.org/Directives 或 https://www.iec.ch/members_experts/refdocs）。

请注意，本文件的某些要素可能是专利权的主题。ISO 和 IEC 不对识别任何或所有此类专利权负责。文件开发过程中确定的任何专利权的详细信息将在引言和/或收到的 ISO 专利声明列表（见 www.ISO.org/patents）或 IEC 专利声明列表中（见 https://patents.iec.ch/)。

本文件中使用的任何商品名称都是为方便用户而提供的信息，不构成背书。

有关标准自愿性质的解释、与合格评定相关的 ISO 特定术语和表达的含义，以及 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，请参见 www.ISO.org/ISO/foreword.html。在 IEC 中，请参阅 https://www.iec.ch/understanding-standards.

本文件由 ISO/IEC JTC1 信息技术联合技术委员会 SC27 信息安全、网络安全和隐私保护小组委员会编写。

第三版取消并取代了第二版（ISO/IEC 27001:2013），该版本已进行了技术修订。它还包含了技术勘误表 ISO/IEC 27001:2013/Cor 1:2014 和 ISO/IEC 27001:2013/Cor 2:2015。

主要变化如下：

文本已与管理体系标准和 ISO/IEC 27002:2022 的协调结构保持一致。

关于本文件的任何反馈或问题都应提交给用户的国家标准机构。这些机构的完整清单可在 www.iso.org/members.html 和 https://www.iec.ch/national-committees 上找到。

0 引言

0.1 概述

本文件旨在提供建立、实施、维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是一个组织的战略决策。组织信息安全管理体系的建立和实施受组织的需求和目标、安全要求、使用的组织流程以及组织的规模和结构的影响。所有这些影响因素都将随着时间的推移而改变。

信息安全管理体系通过应用风险管理流程来保护信息的机密性、完整性和可用性，并向相关方提供充分管理风险的信心。

重要的是，信息安全管理体系是组织过程和总体管理结构的一部分并与之集成，并且在过程、信息系统和控制的设计中考虑信息安全。预计将根据本组织的需要扩大信息安全管理体系的实施规模。

内部和外部各方可使用本文件来评估组织满足自身信息安全要求的能力。

本文件中提出要求的顺序并不反映其重要性或暗示其实施顺序。列举列表项仅供参考。

ISO/IEC 27000 描述了信息安全管理系统的概述和词汇，参考了信息安全安全管理体系系列标准（包括 ISO/IEC 27003、ISO/IEC 27004 和 ISO/IEC 27005）以及相关术语和定义。

0.2 与其他管理体系标准的兼容性

本文件采用 ISO/IEC 指令第 1 部分《综合 ISO 增补件》附录 SL 中定义的高层结构、相同的子条款标题、相同的文本、通用术语和核心定义，因此与采用附录 SL 的其他管理体系标准保持兼容性。

附录 SL 中定义的这种通用方法对于那些选择运行满足两个或多个管理系统标准要求的单一管理系统的组织来说是有用的。

1 范围

本标准规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求。本标准还包括了根据组织需求所剪裁的信息安全风险评估和处置的要求。本标准规定的要求是通用的，适用于各种类型、规模或性质的组织。

当一个组织声称符合本标准时，不能排除第 4 章到第 10 章中所规定的任何要求。

2 规范性引用文件

以下文件在文本中被引用，其部分或全部内容构成本标准的要求。对于注明日期的参考文献，仅引用的版本适用。对于未注明日期的引用文件，引用文件的最新版本(包括任何修订)适用。ISO/IEC 27000，信息技术—安全技术—信息安全管理体系—概述和词汇。

3 术语和定义

就本标准而言，以下术语和定义适用。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：https://www.iso.org/obp
— IEC 电子词典：https://www.electropedia.org/

4 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现信息安全管理体系预期结果能力的外部和内部事项。

注：对这些事项的确定，参见 ISO 31000:2018 中 5.4.1 建立外部和内部环境的内容。

4.2 理解相关方的需求和期望

组织应确定：

a) 信息安全管理体系相关方；

b) 这些相关方与信息安全相关的要求。

c) 这些要求中，哪些将通过信息安全管理体系来达成。

注：相关方的要求可包括法律、法规要求和合同义务。

如需要获取全文

请联系北京三星九千认证中心有限公司技术部

联系电话:010-64429578-612

邮箱:duqq@sanxing9000.com