国际标准

ISO/IEC 27001

第三版
2022-10

信息安全、网络安全和隐私保护 - 信息安全管理系统 - 要求

信息安全、网络安全和生命保护
私人 - 信息安全管理系统 - 要求

参考号 ISO/IEC
27001:2022(E)

受版权保护的文件

ISO版权局
CP 401 - Ch. de Blandonnet 8
CH-1214 Vernier, Geneva 电
话。+41 22 749 01 11
电子邮件：copyright@iso.org
网站：www.iso.org
发表于瑞士

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。在本文件编写过程中发现的任何专利权的细节将出现在导言中和/或ISO收到的专利声明清单（见www.iso.org/patents）或IEC收到的专利声明清单（见https://patents.iec.ch）上。

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，不构成对其的认可。

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。

第三版取消并取代了第二版（ISO/IEC 27001:2013），并对其进行了技术修订。它还纳入了技术更正ISO/IEC 27001:2013/Cor 1:2014和ISO/IEC 27001:2013/Cor 2:2015。

主要变化如下。

- 该文本已与管理体系标准的统一结构和ISO/IEC 27002:2022保持一致。

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。

简介

0.1 一般

编写本文件是为了提供建立、实施、维护和持续改进信息安全管理系统的要求。采用信息安全管理系统是一个组织的战略决策。一个组织的信息安全管理系统的建立和实施受到该组织的需求和目标、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会随着时间的推移而改变。

信息安全管理系统通过应用风险管理过程来维护信息的保密性、完整性和可用性，并使有关各方相信风险得到了充分的管理。

重要的是，信息安全管理系统是组织流程和整体管理结构的一部分，并与之相结合，在流程、信息系统和控制的设计中考虑到信息安全。预计信息安全管理系统的实施将根据组织的需要进行扩展。

本文件可供内部和外部人士使用，以评估组织满足其自身信息安全要求的能力。

本文件中要求的顺序并不反映它们的重要性，也不意味着它们被实施的顺序。列表中的项目仅用于参考目的。

ISO/IEC 27000描述了信息安全管理系统的概述和词汇，参考了信息安全管理系统系列标准（包括ISO/IEC 27003[2]、ISO/IEC 27004[3]和ISO/IEC 27005[4]），并附有相关术语和定义。

0.2 与其他管理系统标准的兼容性

本文件采用了ISO/IEC指令第1部分ISO综合补编附件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，因此与采用附件SL的其他管理体系标准保持兼容。

附件SL中定义的这种通用方法对于那些选择运行一个符合两个或更多管理体系标准要求的单一管理体系的组织来说将是非常有用的。

信息安全、网络安全和隐私保护 - 信息安全管理系统 - 要求

1 范围

本文件规定了在组织范围内建立、实施、维护和持续改进信息安全管理系统的要求。本文件还包括根据组织的需要对信息安全风险进行评估和处理的要求。本文件中规定的要求是通用的，旨在适用于所有组织，无论其类型、规模或性质如何。当一个组织声称符合本文件时，不包括第4至10条规定的任何要求是不可接受的。

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献，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*

3 术语和定义

在本文件中，适用ISO/IEC 27000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 组织的背景

4.1 了解组织和其背景

组织应确定与其目的相关的、影响其实现信息安全管理系统预期结果能力的外部和内部问题。

注意 确定这些问题是指建立ISO 31000:2018[5]第5.4.1条中考虑的组织的外部和内部环境。

4.2 了解有关各方的需求和期望

该组织应确定：

a) 与信息安全管理系统有关的有关各方。

b) 这些相关方的相关要求。

c) 这些要求中的哪些将通过信息安全管理系统来解决。