信息安全、网络安全和隐私保护 —信息安全管理体系—要求

ISO/IEC 27001:2022

(第三版　中文版)

2022 年 12 月

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 介绍

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体系的要求。本文件还包括针对组织需求量身定制的信息安全风险评估和处理要求。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。当组织声称符合本文件要求时，不接受排除第 4 条至第 10 条规定的任何要求。

2 规范性引用文件

以下文件在正文中的引用方式使其部分或全部内容构成本文件的要求。对于注明日期的引用文件，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-信息安全管理系统-概述和词汇

3 术语和定义

在本文件中，ISO/IEC 27000 中给出的术语和定义适用。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/ui

IEC 电子介质网址：https://www.electropedia.org/

4 组织背景

4.1 了解组织及其背景

组织应确定与其目的相关且影响其实现信息安全管理体系预期结果的能力的外部和内部问题。

注：确定这些问题是指建立在 ISO 31000:2018 第 5.4.1 条所述组织的外部和内部环境。

4.2 了解相关方的需求和期望

组织应确定：

a) 与信息安全管理体系相关的相关方；

b) 相关方的相关要求；

c) 其中哪些要求将通过信息安全管理体系解决。

注：相关方的要求可以包括法律法规要求和合同义务。

4.3 确定信息安全管理系统的范围

组织应确定信息安全管理体系的边界和适用性，以确定其范围。

在确定该范围时，组织应考虑：

a) 4.1 中提到的外部和内部问题；

b) 4.2 中提到的要求；

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**。