ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 22080—2025/ISO/IEC 27001:2022
代替 GB/T 22080—2016

网络安全技术　信息安全管理体系　要求

Cybersecurity technology—Information security management systems—Requirements

（ISO/IEC 27001:2022，Information security，cybersecurity and privacy protection—Information security management systems—Requirements，IDT）

2025-06-30 发布　　2026-01-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 22080—2016《信息技术　安全技术　信息安全管理体系　要求》,与 GB/T 22080—2016 相比,除编辑性改动外,主要技术变化如下:

a) 增加了“组织应确定气候变化是否是一个相关事项”(见 4.1);

b) 增加了“组织应确定哪些要求将通过信息安全管理体系来解决”[见 4.2c)];

c) 更改了“信息安全风险处置”中适用性声明相关要求[见 6.1.3d),2016 年版的 6.1.3d)];

d) 增加了“针对变更的规划”要求(见 6.3);

e) 更改了信息安全控制参考,包括对部分原有的控制进行合并、增加新的控制和调整控制的展示方式(见附录 A,2016 年版的附录 A)。

本文件等同采用 ISO/IEC 27001:2022《信息安全、网络安全和隐私保护信息安全管理体系　要求》。

本文件做了下列最小限度的编辑性改动:

——为与我国技术标准体系协调,标准名称改为《网络安全技术　信息安全管理体系　要求》;

——纳入 ISO/IEC 27001:2022/Amd 1:2024《信息安全、网络安全和隐私保护　信息安全管理体系　要求》修正案 1:与气候行动相关的变化,并用双垂线在对应有变化的条款外侧标示。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国电子技术标准化研究院、中国合格评定国家认可中心、中国网络安全审查认证和市场监管大数据中心、北京安信天行科技有限公司、中国信息安全测评中心、黑龙江省网络空间研究中心、中电长城网际系统应用有限公司、山东省标准化研究院、亚信科技(成都)有限公司、深圳市腾讯计算机系统有限公司、南方电网数字电网集团信息通信科技有限公司、中国烟草总公司湖北省公司、北京天融信网络安全技术有限公司、唯品会(中国)有限公司、杭州安恒信息技术股份有限公司、广州赛宝认证中心服务有限公司、中国船级社质量认证有限公司、北京赛西认证有限责任公司、启明星辰信息技术集团股份有限公司、北京中金云网科技有限公司、浙江网商银行股份有限公司、北京时代新威信息技术有限公司、中国石油天然气股份有限公司西北销售分公司。

本文件主要起草人:许玉娜、付志高、王秉政、林阳荟晨、尤其、魏立茹、翟亚红、陈青民、陆丽、杨婧婧、王琰、曲家兴、方舟、白瑞、杨霄璇、闵京华、白旭东、王姣、朱雪峰、公伟、廖双晓、刘震宇、王琼、杨斯可、寇增杰、周禹、王拓、鲁立、孙毅、赵丽华、杨天识、程燕、史艳语、王连强、谢建林、刘杰、于慧超。

本文件及其所代替文件的历次版本发布情况为:

——2008 年首次发布为 GB/T 22080—2008,2016 年第一次修订;

——本次为第二次修订。

引　言

0.1　概述

本文件提供了建立、实现、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组织的一项战略性决策。组织信息安全管理体系的建立和实现受组织的需求和目标、安全要求、组织所采用的过程、规模和结构的影响。所有这些影响因素可能随时间发生变化。

信息安全管理体系通过应用风险管理过程来保持信息的保密性、完整性和可用性，并为相关方树立风险得到充分管理的信心。

对组织而言，重要的是要将信息安全管理体系整合到组织的过程和整体管理结构中，使之成为后者的一部分，并在组织的过程、信息系统和控制的设计中要考虑信息安全。信息安全管理体系的实现程度是要与组织的需求相符合。

本文件能被内部和外部各方用于评估组织的能力是否满足自身的信息安全要求。

本文件表述要求的顺序并不反映各要求的重要性，也不意味着实现这些要求时的顺序。条款编号仅是为了方便引用。

ISO/IEC 27000 描述了信息安全管理体系的概述和词汇，引用了信息安全管理体系标准族（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

本文件应用 ISO/IEC Directives，Part1 附录 SL 定义的高层结构、相同条款标题、相同文本、通用术语和核心定义，因此维护了与其他采用附录 SL 的管理体系标准的兼容性。

附录 SL 中定义的通用途径对于选择运行单一管理体系来满足多个管理体系标准要求的组织是有用的。

网络安全技术　信息安全管理体系　要求

1　范围

本文件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。本文件还规定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。本文件规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织声称符合本文件时，不接受排除第4章到第10章中规定的任何要求。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

注：GB/T 29246—2023　信息安全技术信息安全管理体系概述和词汇(ISO/IEC 27000:2018，IDT)

3　术语和定义

ISO/IEC 27000界定的术语和定义适用于本文件。

ISO和IEC维护的用于标准化的术语数据库网址如下：

——ISO在线浏览平台：https://www.iso.org/obp；

——IEC电子百科：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，且影响其达到信息安全管理体系预期结果能力的外部和内部事项。

组织应确定气候变化[1)]是否是一个相关事项。

注：对这些事项的确定，见GB/T 24353—2022中5.4.1建立外部和内部环境。

4.2　理解相关方的需求和期望

组织应确定：

a)　信息安全管理体系的相关方；

b)　这些相关方的有关要求；

c)　哪些要求将通过信息安全管理体系予以解决。

注1：相关方的要求包括法律、法规和合同义务。

注2：相关方可能提出与气候变化相关的要求。

1)　有关气候变化的更多信息，见ISO和国际认可论坛(IAF)关于管理体系标准中增加气候变化因素的联合公报。