ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 22081—2024/ISO/IEC 27002:2022
代替 GB/T 22081—2016

网络安全技术　信息安全控制

Cybersecurity technology—Information security controls

（ISO/IEC 27002:2022，Information security，cybersecurity and privacy protection—Information security controls，IDT）

2024-09-29 发布　　2025-04-01 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 …… Ⅴ
引言 …… Ⅵ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 5
4　文件结构 …… 6
4.1　章条设置 …… 6
4.2　主题和属性 …… 7
4.3　控制的设计 …… 7
5　组织控制 …… 8
5.1　信息安全策略 …… 8
5.2　信息安全角色和责任 …… 10
5.3　职责分离 …… 11
5.4　管理责任 …… 12
5.5　与职能机构的联系 …… 13
5.6　与特定相关方的联系 …… 13
5.7　威胁情报 …… 14
5.8　项目管理中的信息安全 …… 15
5.9　信息及其他相关资产的清单 …… 17
5.10　信息及其他相关资产的可接受使用 …… 18
5.11　资产归还 …… 19
5.12　信息分级 …… 20
5.13　信息标记 …… 21
5.14　信息传输 …… 23
5.15　访问控制 …… 25
5.16　身份管理 …… 26
5.17　鉴别信息 …… 27
5.18　访问权限 …… 29
5.19　供应商关系中的信息安全 …… 30
5.20　在供应商协议中强调信息安全 …… 32
5.21　管理信息通信技术供应链中的信息安全 …… 34

5.22 供应商服务的监视、评审和变更管理 …… 35
5.23 云服务使用的信息安全 …… 37
5.24 信息安全事件管理规划和准备 …… 38
5.25 信息安全事态的评估和决策 …… 40
5.26 信息安全事件的响应 …… 41
5.27 从信息安全事件中学习 …… 42
5.28 证据收集 …… 42
5.29 中断期间的信息安全 …… 43
5.30 业务连续性的信息通信技术就绪 …… 44
5.31 法律、法规、规章和合同要求 …… 46
5.32 知识产权 …… 47
5.33 记录的保护 …… 48
5.34 隐私和个人可识别信息保护 …… 49
5.35 信息安全的独立评审 …… 50
5.36 符合信息安全的策略、规则和标准 …… 51
5.37 文件化的操作规程 …… 52
6 人员控制 …… 53
6.1 审查 …… 53
6.2 任用条款和条件 …… 54
6.3 信息安全意识、教育和培训 …… 55
6.4 违规处理过程 …… 57
6.5 任用终止或变更后的责任 …… 58
6.6 保密或不泄露协议 …… 59
6.7 远程工作 …… 60
6.8 信息安全事态的报告 …… 61
7 物理控制 …… 62
7.1 物理安全边界 …… 62
7.2 物理入口 …… 63
7.3 办公室、房间和设施的安全保护 …… 64
7.4 物理安全监视 …… 65
7.5 物理和环境威胁防范 …… 66
7.6 在安全区域工作 …… 67
7.7 清理桌面和屏幕 …… 68
7.8 设备安置和保护 …… 69
7.9 组织场所外的资产安全 …… 70
7.10 存储媒体 …… 71
7.11 支持性设施 …… 72

7.12 布缆安全 …… 73
7.13 设备维护 …… 74
7.14 设备的安全处置或重复使用 …… 75
8 技术控制 …… 76
8.1 用户终端设备 …… 76
8.2 特许访问权限 …… 78
8.3 信息访问限制 …… 79
8.4 源代码的访问 …… 80
8.5 安全鉴别 …… 81
8.6 容量管理 …… 83
8.7 恶意软件防范 …… 84
8.8 技术脆弱性管理 …… 85
8.9 配置管理 …… 88
8.10 信息删除 …… 90
8.11 数据脱敏 …… 91
8.12 数据防泄露 …… 92
8.13 信息备份 …… 93
8.14 信息处理设施的冗余 …… 95
8.15 日志 …… 96
8.16 监视活动 …… 98
8.17 时钟同步 …… 100
8.18 特权实用程序的使用 …… 100
8.19 运行系统软件的安装 …… 101
8.20 网络安全 …… 102
8.21 网络服务的安全 …… 104
8.22 网络隔离 …… 105
8.23 网页过滤 …… 106
8.24 密码技术的使用 …… 106
8.25 安全开发生存周期 …… 108
8.26 应用程序安全要求 …… 109
8.27 系统安全架构和工程原则 …… 111
8.28 安全编码 …… 113
8.29 开发和验收中的安全测试 …… 115
8.30 开发外包 …… 116
8.31 开发、测试和生产环境的隔离 …… 117
8.32 变更管理 …… 118
8.33 测试信息 …… 119

8.34 在审计测试中保护信息系统 …… 120
附录 A（资料性） 属性的使用 …… 122
A.1 概述 …… 122
A.2 组织视图 …… 132
附录 B（资料性） 本文件与 GB/T 22081—2016 的对应关系 …… 133
参考文献 …… 143

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 22081—2016《信息技术　安全技术　信息安全控制实践指南》,与GB/T 22081—2016相比,除结构调整和编辑性改动外,主要技术变化如下:

——对控制进行了合并、删除,同时也增加了新的控制,与GB/T 22081—2016对应关系见附录B。

本文件等同采用ISO/IEC 27002:2022《信息安全、网络安全和隐私保护　信息安全控制》。

本文件做了下列最小限度的编辑性改动:

——为与现有网络安全国家标准协调一致,标准名称调整为《网络安全技术　信息安全控制》。

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:北京赛西科技发展有限责任公司、中国合格评定国家认可中心、中电长城网际系统应用有限公司、中国网络安全审查技术与认证中心、北京赛西认证有限责任公司、北京时代新威信息技术有限公司、北京江南天安科技有限公司、山东省标准化研究院、四川大学、杭州安恒信息技术股份有限公司、黑龙江省网络空间研究中心、上海浦东发展银行股份有限公司信用卡中心、北京百度网讯科技有限公司、亚信科技(成都)有限公司、工业互联网创新中心(上海)有限公司、阿里云计算有限公司、联想(北京)有限公司、深信服科技股份有限公司、启明星辰信息技术集团股份有限公司、麒麟软件有限公司、易航科技股份有限公司、华夏认证中心有限公司、北京数安行科技有限公司、上海观安信息技术股份有限公司、网安联信息技术有限公司、北京天融信网络安全技术有限公司、国家信息技术安全研究中心、北京蓝象标准咨询服务有限公司、厦门美柚股份有限公司、长扬科技(北京)股份有限公司、浪潮电子信息产业股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、陕西省网络与信息安全测评中心、美的集团股份有限公司、中能融合智慧科技有限公司、北京神州绿盟科技有限公司、华为技术有限公司、北京时代亿信科技股份有限公司、北京源堡科技有限公司、国网新疆电力有限公司电力科学研究院、北京快手科技有限公司。

本文件主要起草人:上官晓丽、王姣、王秉政、甘俊杰、付志高、闵京华、尤其、赵丽华、许玉娜、王连强、陈冠直、朱雪峰、公伟、林阳荟晨、胡勇、赵玉洁、陈星、李锐、王寒生、铁锦程、李文清、郭建领、廖双晓、秦峰、黄正艳、施辰琛、刘晨、杨天识、杨诏钧、赵翔、夏芳、刘玉红、谢江、阮懿宗、谢琴、朱松、肖婷婷、张德保、黄鹏华、张亚京、高丽琴、胡建勋、杨帆、张亮亮、刘长川、程潞样、张喆、易天舒、俞晓昕、顾俊、邹振婉、刘海军、袁莹颖、王昕。

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 22081—2008,2016年第一次修订;

——本次为第二次修订。

引　言

0.1　背景

本文件适用于所有类型和规模的组织。组织在实施基于GB/T 22080信息安全管理体系的信息安全风险处置时，本文件作为其确定和实施所需控制的参考；本文件还作为组织在确定和实施普遍接受的信息安全控制时的指导文件。此外，本文件还能用于针对行业或组织的具体信息安全风险环境编制其信息安全管理指南。除本文件包含的控制外，能通过风险评估来确定特定于组织或环境所需要的控制。

所有类型和规模的组织（包括公共和私营部门、商业和非营利性组织）都会以多种形式创建、收集、处理、存储、传输和处置信息，包括电子的、物理的和口头的（如对话/会话和演示）。

信息的价值超出了文字、数字和图像的本身：如知识、概念、观点和品牌都是无形信息。在互联的世界中，信息和相关资产都值得或需要保护，以防范各种风险源，无论该风险是源自自然界，还是意外或故意破坏。

信息安全是通过实施一组适宜的控制来实现的，包括策略、规则、过程、规程、组织结构和软硬件功能。组织宜在必要时定义、实施、监视、评审和改进这些控制，以满足其特定的安全和业务目标。GB/T 22080中规定的信息安全管理体系（ISMS）从整体、协调的视角审视组织的信息安全风险，在协调一致的管理体系总框架内确定和实施一套全面的信息安全控制。

对照GB/T 22080所规定的ISMS和本文件，许多信息系统，包括其管理和运营，尚未被设计为安全的。在进行风险处置时，需要仔细规划、注意细节，来确定实施哪些控制。

成功的ISMS需要得到组织内所有人员的支持，还可能需要股东或供应商等其他相关方的参与，同时也可能需要业内专家的建议。

一个适宜、充分和有效的信息安全管理体系，为组织的管理层及其他相关方提供以下保证：它们的信息及其他相关资产处于合理的安全状态并免受威胁和损害，从而使组织能够实现既定的业务目标。

0.2　信息安全要求

组织确定其信息安全要求是必要的。信息安全要求有三个主要来源。

a）　考虑组织的整体业务战略与目标来对组织风险进行评估。这能通过特定于信息安全的风险评估来给予帮助或支持。这宜得出对必要控制的确定，以确保组织面临的残余风险符合其风险接受准则。

b）　组织及其相关方（贸易伙伴、服务提供者等）必须遵守的法律、法规、规章和合同要求及其社会文化环境。

c）　组织为支持其运行而为信息生存周期的所有步骤所建立的一整套原则、目标和业务要求。

0.3　控制

控制的定义是改变或维持风险的措施。本文件中的某些控制是修改风险，而其他控制则是维持风险。例如，信息安全方针只能维持风险，而遵守信息安全方针则能改变风险。此外，某些控制描述了不同风险环境下相同的通用措施。本文件提供了源于国际公认最佳实践的一系列组织、人员、物理和技术信息安全控制。

0.4 控制的确定

控制的确定取决于组织在风险评估后做出的决策，并有一个明确定义的范围。与已识别风险相关的决策宜基于风险接受准则、风险处置选项和组织所采用的风险管理方法。控制的确定还宜考虑所有相关的国家和国际法律法规。控制的确定还取决于不同控制的协同，以实现纵深防御。

组织能根据需要来设计控制，或从任何来源识别控制。在制定此类控制时，组织宜考虑实施和运行一项控制所需的资源和投资与该控制所能实现的业务价值之间的比较。请参见 ISO/IEC TR 27016，其提供了在资源需求竞争的情况下做出 ISMS 投资决策以及这些决策的经济后果的指南。

在为实施控制而部署的资源与因缺乏这些控制而发生安全事件所导致的潜在业务影响之间宜取得平衡。风险评估的结果宜有助于指导和确定适当的管理措施、管理信息安全风险的优先顺序，以及实施为防范这些风险而确定的必要控制。

本文件中的某些控制能被视为信息安全管理的指导原则，适用于大多数组织。有关确定控制和其他风险处置选项的更多信息参见 ISO/IEC 27005。

0.5 编制特定于组织的指南

本文件能被视为制定特定于组织的指南的出发点。本文件中并非所有的控制和指南都适用所有组织。组织还可能需要本文件中未包含的额外控制和指南，以满足其具体需求和解决已识别到的风险。在编制包含额外的指南或控制的文件时，给出与本文件条款间的交叉引用，有助于日后参考。

0.6 生存周期的考虑

信息具有从创建到销毁的生存周期。在其整个生存周期中，信息的价值和其面临的风险可能会变化（例如，未经授权披露或窃取公司财务账户在公布后并不重要，但完整性仍然至关重要），因此，在所有阶段信息安全都很重要。

与信息安全相关的信息系统和其他资产具有生存周期，包括构思、规范、设计、开发、测试、实施、使用、维护并最终退役和销毁。每个阶段均宜考虑信息安全。新的系统开发项目和对现有系统的变更，能考虑组织面临的风险和从安全事件中吸取的经验教训，从而为改进安全控制提供了机会。

0.7 相关标准化文件

本文件为普遍应用于各类组织的广泛的信息安全控制提供了指导。

一些适用于特定行业的标准化文件给出了针对特定领域的额外控制（例如，针对云服务的 ISO/IEC 27017、针对隐私保护的 ISO/IEC 27701、针对能源的 ISO/IEC 27019、针对电信组织的 ISO/IEC 27011 和针对健康的 ISO 27799）。这些标准化文件收录在参考文献中，第 5 章～第 8 章的“指南”和“其他信息”条目中引用了其中的一些标准化文件。

网络安全技术　信息安全控制

1　范围

本文件提供了一套通用信息安全控制参考集，包括实施指南。

本文件适用于：

a）　组织 ISO/IEC 27001 实施信息安全管理体系（ISMS）；

b）　组织基于国际公认最佳实践实施信息安全控制；

c）　组织编制其自身的信息安全管理指南。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语、定义和缩略语

3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1

访问控制　access control

确保对资产（3.1.2）的物理和逻辑访问是基于业务和信息安全要求进行授权和限制的手段。

3.1.2

资产　asset

对组织有价值的任何事物。

注：在信息安全的语境下，分为两类资产。

——主要资产：

- 信息；
- 业务过程（3.1.27）和活动。

——所有类型的支撑性资产（主要资产所依赖的资产），例如：

- 硬件；
- 软件；
- 网络；
- 人员（3.1.20）；
- 场所；
- 组织结构。

3.1.3

攻击　attack

未经授权企图销毁、更改、禁用、访问资产（3.1.2）的行为（无论成功或失败），或者企图泄露、窃取或未经授权使用资产的任何行为。