



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 发布
国家标准化管理委员会

目 次

| | |
|------------------------|-----|
| 前言 | III |
| 引言 | IV |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语和定义 | 1 |
| 4 组织环境 | 1 |
| 4.1 理解组织及其环境 | 1 |
| 4.2 理解相关方的需求和期望 | 1 |
| 4.3 确定信息安全管理体系范围 | 2 |
| 4.4 信息安全管理体系 | 2 |
| 5 领导 | 2 |
| 5.1 领导和承诺 | 2 |
| 5.2 方针 | 2 |
| 5.3 组织的角色、责任和权限 | 2 |
| 6 规划 | 3 |
| 6.1 应对风险和机会的措施 | 3 |
| 6.2 信息安全目标及其实现规划 | 4 |
| 6.3 针对变更的规划 | 4 |
| 7 支持 | 4 |
| 7.1 资源 | 4 |
| 7.2 能力 | 4 |
| 7.3 意识 | 5 |
| 7.4 沟通 | 5 |
| 7.5 文件化信息 | 5 |
| 8 运行 | 6 |
| 8.1 运行规划和控制 | 6 |
| 8.2 信息安全风险评估 | 6 |
| 8.3 信息安全风险处置 | 6 |
| 9 绩效评价 | 6 |
| 9.1 监视、测量、分析和评价 | 6 |
| 9.2 内部审核 | 6 |
| 9.3 管理评审 | 7 |
| 10 改进 | 7 |

| | |
|---------------------------|----|
| 10.1 持续改进 | 7 |
| 10.2 不符合与纠正措施 | 7 |
| 附录 A (规范性) 信息安全控制参考 | 9 |
| 参考文献 | 16 |

注：本文件内容受到版权保护，未经恰当的授权禁止复制。本公司客户及相关单位，如需获取文件完整内容，请联系市场部门获取，电话：010-84724911。