INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

信息安全 网络安全 隐私保护 信息安全管理体系 要求

Reference number
ISO/IEC 27001:2022(E)

目录

前言 i
引言 ii
0.1 总则 ii
0.2 与其他管理体系标准的兼容性 ii
0.3 交流探讨 ii
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 2
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 领导作用 2
5.1 领导作用和承诺 2
5.2 方针 3
5.3 组织角色、职责和权限 3
6 策划 3
6.1 应对风险和机遇的措施 3
6.1.1 总则 3
6.1.2 信息安全风险评估 4
6.1.3 信息安全风险处置 4
6.2 信息安全目标及其实现的策划 5
6.3 变更策划 5
7 支持 5
7.1 资源 5
7.2 能力 6
7.3 意识 6
7.4 沟通 6
7.5 文件化信息 6
7.5.1 总则 6
7.5.2 创建和更新 6
7.5.3 文件化信息的控制 7
8 运行 7
8.1 运行策划与控制 7
8.2 信息安全风险评估 7
8.3 信息安全风险处置 7
9 绩效评价 8
9.1 监视、测量、分析和评价 8
9.2 内部审核 8

9.2.1 总则 8
9.2.2 内部审核方案 8
9.3 管理评审 9
9.3.1 总则 9
9.3.2 管理评审输入 9
9.3.3 管理评审结果 9
10 改进 9
10.1 持续改进 9
10.2 不符合和纠正措施 9
附录 A（规范性附录） 信息安全控制参考 11
参考文献 18