

INTERNATIONAL
STANDARD

ISO/IEC
27001

Third edition

2022-10

Information security,cybersecurity
And privacy protection-Information
Security management systems-
Requirements

信息安全 网络安全 隐私保护
安全管理体系 要求

Reference number

ISO/IEC 27001:2022 (E)

目 录

前 言.....3

引 言.....4

1 范围.....5

2 规范性引用文件5

3 术语和定义.....5

4 组织环境.....5

 4.1 理解组织及其环境.....5

 4.2 理解相关方的需求和期望5

 4.3 确定信息安全管理范围5

 4.4 信息安全管理6

5 领导作用.....6

 5.1 领导作用和承诺.....6

 5.2 方针.....6

 5.3 组织的角色、责任和权限.....6

6 规划.....7

 6.1 应对风险和机遇的措施.....7

 6.2 信息安全目标及其实现的策划8

 6.3 变更策划.....8

7 支持.....8

 7.1 资源.....8

 7.2 能力.....8

 7.3 意识.....9

 7.4 沟通.....9

 7.5 文件化信息.....9

8 运行.....10

 8.1 运行策划与控制.....10

 8.2 信息安全风险评估.....10

 8.3 信息安全风险处置.....10

9 绩效评价.....10

 9.1 监视、测量、分析和评价10

 9.2 内部审核.....11

 9.3 管理评审.....11

10 改进.....12

 10.1 持续改进.....12

 10.2 不符合和纠正措施.....12