
安全性和弹性——安全管理系统要求
**Security and resilience — Security management
systems Requirements**





受版权保护的文件

© ISO 2022

保留所有权利。除非另有规定，或在实施过程中需要，未经事先书面许可，不得以任何形式或任何手段，包括电子或机械，复制或利用本出版物的任何部分，或在互联网或内部网上发布。可以通过以下地址向国际标准化组织或请求者所在国家的国际标准化组织的成员机构申请许可。

国际标准化组织版权办公室
CP 401 莱色de Blandonnet
8 CH-1214 Vernier, 日内瓦
电话:+41 22 749 01 11
copyright@iso.org
www.iso.org

在瑞士出版

内容页

前言 v

简介 vi

1	范围 1
2	规范性参考文献 1
3	术语和定义 1
4	本组织的背景 4
4.1	了解组织及其背景 4
4.2	了解相关方的需求和期望 4
4.2.1	一般情况 4
4.2.2	法律、法规和其他要求 4
4.2.3	原则 5
4.3	确定安全管理系统的范围 6
4.4	安全系统 6
5	领导力 7
5.1	领导和承诺 7
5.2	安全政策 7
5.2.1	确立安全政策 7
5.2.2	安全政策要求 8
5.3	角色、责任和权限 8
6	规划 8
6.1	应对风险和机遇的行动 8
6.1.1	一般 8
6.1.2	确定与安全相关的风险并确定机会 9
6.1.3	应对安全相关风险和利用机会 9
6.2	安全目标 9
6.2.1	确立安全目标 9
6.2.2	确定安全目标 10
6.3	变更的规划 10
7	支持 10
7.1	资源 10
7.2	能力 10
7.3	认知 11
7.4	沟通 11
7.5	记载的信息 11
7.5.1	一般情况 11
7.5.2	创建和更新文件化的信息 11
7.5.3	对文件信息的控制 12
8	操作 12
8.1	业务规划和控制 12
8.2	流程和活动的识别 12
8.3	风险评估和处理 13
8.4	控制措施 13
8.5	安全战略、程序、过程和处理方法 14
8.5.1	识别和选择战略和处理方法 14
8.5.2	资源要求 14
8.5.3	治疗方法的实施 14
8.6	安全计划 14
8.6.1	一般情况 14
8.6.2	响应结构 14
8.6.3	警告和沟通 15

9 绩效评估 16

9.1 监测、测量、分析和评价 16

9.2 内部审计 17

9.2.1 一般 17

9.2.2 内部审计方案 17

9.3 管理审查 17

9.3.1 一般 17

9.3.2 管理审查的投入 18

9.3.3 管理评审结果 18

10 改进 18

10.1 持续改进 18

10.2 不合格品和纠正措施 19

参考文献 20

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。