
**Security and resilience —
Security management systems —
Requirements**





COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester:

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	4
4.1 Understanding the organization and its context	4
4.2 Understanding the needs and expectations of interested parties	4
4.2.1 General	4
4.2.2 Legal, regulatory and other requirements	4
4.2.3 Principles	5
4.3 Determining the scope of the security management system	6
4.4 Security management system	6
5 Leadership	7
5.1 Leadership and commitment	7
5.2 Security policy	7
5.2.1 Establishing the security policy	7
5.2.2 Security policy requirements	8
5.3 Roles, responsibilities and authorities	8
6 Planning	8
6.1 Actions to address risks and opportunities	8
6.1.1 General	8
6.1.2 Determining security-related risks and identifying opportunities	9
6.1.3 Addressing security-related risks and exploiting opportunities	9
6.2 Security objectives and planning to achieve them	9
6.2.1 Establishing security objectives	9
6.2.2 Determining security objectives	10
6.3 Planning of changes	10
7 Support	10
7.1 Resources	10
7.2 Competence	10
7.3 Awareness	11
7.4 Communication	11
7.5 Documented information	11
7.5.1 General	11
7.5.2 Creating and updating documented information	11
7.5.3 Control of documented information	12
8 Operation	12
8.1 Operational planning and control	12
8.2 Identification of processes and activities	12
8.3 Risk assessment and treatment	13
8.4 Controls	13
8.5 Security strategies, procedures, processes and treatments	14
8.5.1 Identification and selection of strategies and treatments	14
8.5.2 Resource requirements	14
8.5.3 Implementation of treatments	14
8.6 Security plans	14
8.6.1 General	14
8.6.2 Response structure	14
8.6.3 Warning and communication	15
8.6.4 Content of the security plans	15

安全和复原力 - 安全管理系统 - 要求





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。

ISO版权局

CP 401 - Ch. de Blandornet 8

CH-1214 Vernier, Geneva 电

话: +41 22 749 01 11

电子邮件: copyright@iso.org

网站: www.iso.org

发表于瑞士

内容

前言 简介

- 1 范围
- 2 规范性参考资料
- 3 术语和定义
- 4 组织的背景
 - 4.1 了解组织和其背景
 - 4.2 了解有关各方的需求和期望
 - 4.2.1 一般
 - 4.2.2 法律、监管和其他要求
 - 4.2.3 原则
 - 4.3 确定安全管理体系的范围
 - 4.4 安全管理制度
- 5 领导人
 - 5.1 领导和承诺
 - 5.2 安全政策
 - 5.2.1 建立安全政策
 - 5.2.2 安全政策要求
 - 5.3 角色、责任和权力
- 6 规划
 - 6.1 应对风险和机遇的行动
 - 6.1.1 一般
 - 6.1.2 确定与安全有关的风险并确定机会
 - 6.1.3 应对与安全有关的风险和利用机会
 - 6.2 安全目标和实现这些目标的规划
 - 6.2.1 确立安全目标
 - 6.2.2 确定安全目标
 - 6.3 变化的规划
- 7 支持
 - 7.1 资源
 - 7.2 能力
 - 7.3 认识
 - 7.4 沟通
 - 7.5 记录的信息
 - 7.5.1 一般
 - 7.5.2 创建和更新文件化的信息
 - 7.5.3 对文件资料的控制
- 8 运作
 - 8.1 业务规划和控制
 - 8.2 确定过程和活动
 - 8.3 风险评估和治疗
 - 8.4 控制措施
 - 8.5 安全战略、程序、过程和处理
 - 8.5.1 确定和选择战略和治疗方法
 - 8.5.2 所需资源
 - 8.5.3 实施治疗
 - 8.6 安全计划
 - 8.6.1 一般
 - 8.6.2 响应结构
 - 8.6.3 警告和沟通
 - 8.6.4 安全计划的内容

	8.6.5	恢复
9		业绩评估
	9.1	监测、测量、分析和评价
	9.2	内部审计
	9.2.1	一般
	9.2.2	内部审计方案
	9.3	管理审查
	9.3.1	一般
	9.3.2	管理审查投入
	9.3.3	管理审查结果
10		改进
	10.1	持续改进
	10.2	不合格品和纠正措施



北京中交远航认证有限公司
BEIJING ZHONGJIAOYUANHANG CERTIFICATION LIMITED

如需查阅全文，可联系公司获取

联系电话:010-63260528

邮 箱:isoooffer0211@sina.com