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

安全与韧性 — 安全管理体系 — 要求

查阅全文请联系北京海德国际认证有限公司
联系电话：010-84905056, 010-65817800
邮箱地址：common@hicchina.com.cn





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

目录

前言	5
引言	6
1 范围	8
2 规范性引用文件	8
3 术语和定义	8
4 组织环境	11
4.1 理解组织及其环境	11
4.2 理解相关方的需求和期望	11
4.2.1 总则	11
4.2.2 法律、法规和其他要求	11
4.2.3 原则	11
4.3 确定安全管理体系的范围	13
4.4 安全管理体系	13
5 领导力	13
5.1 领导力与承诺	13
5.2 安全方针	14
5.2.1 建立安全方针	14
5.2.2 安全方针要求	14
5.3 职责、权限和授权	15
6 策划	15
6.1 应对风险和机遇的措施	15
6.1.1 总则	15
6.1.2 确定安全相关风险并识别机遇	15
6.1.3 应对安全相关风险并利用机遇	16
6.2 安全目标及实现策划	16
6.2.1 建立安全目标	16
6.2.2 确定安全目标	16
6.3 变更策划	17
7 支持	17
7.1 资源	17
7.2 能力	17
7.3 意识	17
7.4 沟通	18
7.5 成文信息	18
7.5.1 总则	18
7.5.2 成文信息的创建和更新	18

7.5.3 成文信息的控制	18
8 运行	19
8.1 运行策划和控制	19
8.2 过程和活动的识别	19
8.3 风险评估和处置	19
8.4 控制措施	20
8.5 安全策略、程序、过程和处置	20
8.5.1 策略和处置的识别与选择	20
8.5.2 资源要求	21
8.5.3 处置的实施	21
8.6 安全计划	21
8.6.1 总则	21
8.6.2 响应架构	21
8.6.3 预警和沟通	22
8.6.4 安全计划的内容	22
8.6.5 恢复	23
9 绩效评价	23
9.1 监视、测量、分析和评价	23
9.2 内部审核	23
9.2.1 总则	23
9.2.2 内部审核方案	23
9.3 管理评审	24
9.3.1 总则	24
9.3.2 管理评审输入	24
9.3.3 管理评审输出	25
10 改进	25
10.1 持续改进	25
10.2 不合规和纠正措施	25
参考文献	27