

INTERNATIONAL
STANDARD

ISO
28000

Second edition
2022-03

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



Reference number
ISO 28000:2022(E)

© ISO 2022



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

8.6.5	Recovery	16
9	Performance evaluation	16
9.1	Monitoring, measurement, analysis and evaluation.....	16
9.2	Internal audit.....	17
9.2.1	General	17
9.2.2	Internal audit programme.....	17
9.3	Management review	17
9.3.1	General	17
9.3.2	Management review inputs	18
9.3.3	Management review results.....	18
10	Improvement.....	18
10.1	Continual improvement.....	18
10.2	Nonconformity and corrective action.....	19
	Bibliography.....	20

国际标准

ISO
28000

第二版
2022-03

安全与韧性-安全管理体系-要求



参考编号 ISO
28000:2022(E)

© ISO 2022



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 Blandonnet 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

目次

前言

引言

1 范围

2 规范性引用文件

3 术语和定义

4 组织环境

4.1 理解组织及其环境

4.2 理解相关方的需求和期望

4.2.1 总则

4.2.2 合规义务

4.2.3 原则

4.3 确定安全管理体系的范围

4.4 安全管理体系

5 领导作用

5.1 领导作用和承诺

5.2 安全方针

5.2.1 建立安全方针

5.2.2 安全方针要求

5.3 岗位、职责和权限

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

6.1.2 确定与安全有关的风险并识别机遇

6.1.3 应对与安全有关的风险和机遇

6.2 安全目标及其实现的策划

6.2.1 建立安全目标

6.2.2 确定安全目标

6.3 变更的策划

7 支持

7.1 资源

7.2 能力

7.3 意识

7.4 沟通

7.5 成文信息

7.5.1 总则

7.5.2 创建和更新

7.5.3 成文信息的控制

8 运行

8.1 运行的策划和控制

8.2 确定过程和活动

8.3 风险评估和应对

8.4 控制

8.5 安全策略、程序、过程和应对方法

8.5.1 确定和选择策略、应对方法

8.5.2 资源要求

8.5.3 应对的实施

8.6 安全计划

8.6.1 总则

8.6.2 响应架构

8.6.3 警告和沟通

8.6.4 安全计划的内容

8.6.5 恢复

9 绩效评价

9.1 监视、测量、分析和评价

9.2 内部审核

9.2.1 总则

9.2.2 内部审核方案

9.3 管理评审

9.3.1 总则

9.3.2 管理评审输入

9.3.3 管理评审输出

10 改进

10.1 持续改进

10.2 不符合和纠正措施

参考文献

如有需要，请通过如下方式联系本
机构索取相关认证依据（标准）全
文。

电话：0571-85067843

邮箱：wangxin@gac.org.cn