
**Information security, cybersecurity
and privacy protection — Information
security management systems —
Requirements**

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Systèmes de management de la sécurité de l'information —
Exigences*





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	1
4.1 Understanding the organization and its context	1
4.2 Understanding the needs and expectations of interested parties	1
4.3 Determining the scope of the information security management system	2
4.4 Information security management system	2
5 Leadership	2
5.1 Leadership and commitment	2
5.2 Policy	3
5.3 Organizational roles, responsibilities and authorities	3
6 Planning	3
6.1 Actions to address risks and opportunities	3
6.1.1 General	3
6.1.2 Information security risk assessment	4
6.1.3 Information security risk treatment	4
6.2 Information security objectives and planning to achieve them	5
7 Support	6
7.1 Resources	6
7.2 Competence	6
7.3 Awareness	6
7.4 Communication	6
7.5 Documented information	6
7.5.1 General	6
7.5.2 Creating and updating	7
7.5.3 Control of documented information	7
8 Operation	7
8.1 Operational planning and control	7
8.2 Information security risk assessment	8
8.3 Information security risk treatment	8
9 Performance evaluation	8
9.1 Monitoring, measurement, analysis and evaluation	8
9.2 Internal audit	8
9.2.1 General	8
9.2.2 Internal audit programme	9
9.3 Management review	9
9.3.1 General	9
9.3.2 Management review inputs	9
9.3.3 Management review results	9
10 Improvement	10
10.1 Continual improvement	10
10.2 Nonconformity and corrective action	10
Annex A (normative) Information security controls reference	11
Bibliography	19

信息安全、网络安全和隐私保护 信息安全管理体系 要求

(ISO/IEC 27001:2022)

目录

0 引言	1
0.1 总则	1
0.2 与其他管理体系标准的兼容性	1
1 范围	2
2 规范性引用文件	2
3 术语和定义	2
4 组织环境	2
4.1 理解组织及其环境	2
4.2 理解相关方的需求和期望	2
4.3 确定信息安全管理体的范围	3
4.4 信息安全管理体系	3
5 领导力	3
5.1 领导力和承诺	3
5.2 方针	3
5.3 组织角色、职责和权限	4
6 策划	4
6.1 应对风险和机遇的措施	4
6.1.1 总则	4
6.1.2 信息安全风险评估	5
6.1.3 信息安全风险处置	5
6.2 信息安全目标及其实现的策划	6
6.3 变更的策划	6
7 支持	7
7.1 资源	7
7.2 能力	7
7.3 意识	7
7.4 沟通	7
7.5 文件化信息	7
7.5.1 总则	7
7.5.2 创建和更新	8
7.5.3 文件化信息的控制	8

8	运行.....	8
8.1	运行策划和控制.....	8
8.2	信息安全风险评估.....	9
8.3	信息安全风险处置.....	9
9	绩效评价.....	9
9.1	视、测量、分析和评价.....	9
9.2	内部审核.....	9
9.2.1	总则.....	9
9.2.2	内部审核方案.....	10
9.3	管理评审.....	10
9.3.1	总则.....	10
9.3.2	管理评审输入.....	10
9.3.3	管理评审输出.....	11
10	改进.....	11
10.1	持续改进.....	11
10.2	不符合和纠正措施.....	11
	附录 A.....	12
	参考文献.....	18



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： zjyh2015@sina.com