
**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*



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

由于涉及版权保护问题，如需文件完整内容，请联系中国标准出版社
(<https://www.spc.net.cn/>) 购买正版标准。