

---

---

**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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>iv</b>
<b>Introduction</b>	<b>v</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Context of the organization</b>	<b>1</b>
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
<b>5 Leadership</b>	<b>2</b>
5.1 Leadership and commitment	2
5.2 Policy	3
5.3 Organizational roles, responsibilities and authorities	3
<b>6 Planning</b>	<b>3</b>
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
<b>7 Support</b>	<b>6</b>
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
<b>8 Operation</b>	<b>7</b>
8.1 Operational planning and control	7
8.2 Information security risk assessment	8
8.3 Information security risk treatment	8
<b>9 Performance evaluation</b>	<b>8</b>
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
<b>10 Improvement</b>	<b>10</b>
10.1 Continual improvement	10
10.2 Nonconformity and corrective action	10
<b>Annex A (normative) Information security controls reference</b>	<b>11</b>
<b>Bibliography</b>	<b>19</b>