

# ISO/IEC 27001:2013-10 (E)

## Information technology - Security techniques - Information security management systems - Requirements

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
<b>0</b>	<b>Introduction .....</b>	<b>v</b>
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>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 .....	1
4.4	Information security management system .....	2
<b>5</b>	<b>Leadership .....</b>	<b>2</b>
5.1	Leadership and commitment .....	2
5.2	Policy .....	2
5.3	Organizational roles, responsibilities and authorities .....	3
<b>6</b>	<b>Planning .....</b>	<b>3</b>
6.1	Actions to address risks and opportunities .....	3
6.2	Information security objectives and planning to achieve them .....	5
<b>7</b>	<b>Support .....</b>	<b>5</b>
7.1	Resources .....	5
7.2	Competence .....	5
7.3	Awareness .....	5
7.4	Communication .....	6
7.5	Documented information .....	6
<b>8</b>	<b>Operation .....</b>	<b>7</b>
8.1	Operational planning and control .....	7
8.2	Information security risk assessment .....	7
8.3	Information security risk treatment .....	7
<b>9</b>	<b>Performance evaluation .....</b>	<b>7</b>
9.1	Monitoring, measurement, analysis and evaluation .....	7
9.2	Internal audit .....	8
9.3	Management review .....	8
<b>10</b>	<b>Improvement .....</b>	<b>9</b>
10.1	Nonconformity and corrective action .....	9
10.2	Continual improvement .....	9
<b>Annex A (normative) Reference control objectives and controls .....</b>		<b>10</b>
<b>Bibliography .....</b>		<b>23</b>