

# DIN ISO/IEC 27001:2008-09 (E)

## Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2005)

---

<b>Contents</b>		<b>Page</b>
National foreword .....		6
National Annex NA (informative) Bibliography .....		6
<b>0</b>	<b>Introduction .....</b>	<b>4</b>
<b>0.1</b>	<b>General .....</b>	<b>4</b>
<b>0.2</b>	<b>Process approach .....</b>	<b>4</b>
<b>0.3</b>	<b>Compatibility with other management systems .....</b>	<b>5</b>
<b>1</b>	<b>Scope .....</b>	<b>6</b>
<b>1.1</b>	<b>General .....</b>	<b>6</b>
<b>1.2</b>	<b>Application .....</b>	<b>6</b>
<b>2</b>	<b>Normative references .....</b>	<b>6</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>7</b>
<b>4</b>	<b>Information security management system .....</b>	<b>8</b>
<b>4.1</b>	<b>General requirements .....</b>	<b>8</b>
<b>4.2</b>	<b>Establishing and managing the ISMS .....</b>	<b>9</b>
<b>4.2.1</b>	<b>Establish the ISMS .....</b>	<b>9</b>
<b>4.2.2</b>	<b>Implement and operate the ISMS .....</b>	<b>11</b>
<b>4.2.3</b>	<b>Monitor and review the ISMS .....</b>	<b>11</b>
<b>4.2.4</b>	<b>Maintain and improve the ISMS .....</b>	<b>12</b>
<b>4.3</b>	<b>Documentation requirements .....</b>	<b>12</b>
<b>4.3.1</b>	<b>General .....</b>	<b>12</b>
<b>4.3.2</b>	<b>Control of documents .....</b>	<b>13</b>
<b>4.3.3</b>	<b>Control of records .....</b>	<b>13</b>
<b>5</b>	<b>Management responsibility .....</b>	<b>14</b>
<b>5.1</b>	<b>Management commitment .....</b>	<b>14</b>
<b>5.2</b>	<b>Resource management .....</b>	<b>14</b>
<b>5.2.1</b>	<b>Provision of resources .....</b>	<b>14</b>
<b>5.2.2</b>	<b>Training, awareness and competence .....</b>	<b>14</b>
<b>6</b>	<b>Internal ISMS audits .....</b>	<b>15</b>
<b>7</b>	<b>Management review of the ISMS .....</b>	<b>15</b>
<b>7.1</b>	<b>General .....</b>	<b>15</b>
<b>7.2</b>	<b>Review input .....</b>	<b>15</b>
<b>7.3</b>	<b>Review output .....</b>	<b>16</b>
<b>8</b>	<b>ISMS improvement .....</b>	<b>16</b>
<b>8.1</b>	<b>Continual improvement .....</b>	<b>16</b>
<b>8.2</b>	<b>Corrective action .....</b>	<b>16</b>
<b>8.3</b>	<b>Preventive action .....</b>	<b>17</b>
<b>Annex A (normative) Control objectives and controls .....</b>		<b>18</b>
<b>Annex B (informative) OECD principles and this International Standard .....</b>		<b>35</b>

<b>Annex C (informative) Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard .....</b>	<b>36</b>
<b>Bibliography .....</b>	<b>39</b>