

# ISO/IEC 27006:2011-12 (E)

## Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<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>Principles .....</b>	<b>2</b>
<b>5</b>	<b>General requirements .....</b>	<b>2</b>
5.1	Legal and contractual matter .....	2
5.2	Management of impartiality .....	2
5.3	Liability and financing .....	3
<b>6</b>	<b>Structural requirements .....</b>	<b>3</b>
6.1	Organizational structure and top management .....	3
6.2	Committee for safeguarding impartiality .....	3
<b>7</b>	<b>Resource requirements .....</b>	<b>3</b>
7.1	Competence of management and personnel .....	3
7.2	Personnel involved in the certification activities .....	4
7.3	Use of individual external auditors and external technical experts .....	6
7.4	Personnel records .....	6
7.5	Outsourcing .....	6
<b>8</b>	<b>Information requirements .....</b>	<b>6</b>
8.1	Publicly accessible information .....	6
8.2	Certification documents .....	7
8.3	Directory of certified clients .....	7
8.4	Reference to certification and use of marks .....	7
8.5	Confidentiality .....	7
8.6	Information exchange between a certification body and its clients .....	7
<b>9</b>	<b>Process requirements .....</b>	<b>8</b>
9.1	General requirements .....	8
9.2	Initial audit and certification .....	11
9.3	Surveillance activities .....	15
9.4	Recertification .....	16
9.5	Special audits .....	16
9.6	Suspending, withdrawing or reducing scope of certification .....	16
9.7	Appeals .....	17
9.8	Complaints .....	17
9.9	Records of applicants and clients .....	17
<b>10</b>	<b>Management system requirements for certification bodies .....</b>	<b>17</b>
10.1	Options .....	17
10.2	Option 1 - Management system requirements in accordance with ISO 9001 .....	17
10.3	Option 2 - General management system requirements .....	17

<b>Annex A (informative) Analysis of a client organization's complexity and sector-specific aspects ...</b>	<b>19</b>
<b>Annex B (informative) Example areas of auditor competence .....</b>	<b>22</b>
<b>Annex C (informative) Audit time .....</b>	<b>24</b>