



# **ISO 27001:2005 vs. BS 7799-2:2002**

## **Comparison**



## Contrast

<b>BS 7799-2:2002</b>	<b>ISO 27001:2005</b>
4 ISMS requirements	4 Information security management system
4.1 General requirements	4.1 General requirements
4.2 Establishing and managing the ISMS	4.2 Establishing and managing the ISMS
4.2.1 Establish the ISMS	4.2.1 Establish the ISMS
4.2.2 Implement and operate the ISMS	4.2.2 Implement and operate the ISMS
4.2.3 Monitor and review the ISMS	4.2.3 Monitor and review the ISMS
4.2.4 Maintain and improve the ISMS	4.2.4 Maintain and improve the ISMS
4.3 Documentation requirements	4.3 Documentation requirements
4.3.1 General	4.3.1 General
4.3.2 Control of documents	4.3.2 Control of documents
4.3.3 Control of records	4.3.3 Control of records

BS 7799-2:2002	ISO 27001:2005
5 Management responsibility	5 Management responsibility
5.1 Management commitment	5.1 Management commitment
5.2 Resource management	5.2 Resource management
5.2.1 Provision of resources	5.2.1 Provision of resources
5.2.2 Training, awareness and competency	5.2.2 Training, awareness and competence
	6 Internal ISMS audits
6 Management review of the ISMS	7 Management review of the ISMS
6.1 General	7.1 General
6.2 Review input	7.2 Review input
6.3 Review output	7.3 Review output
6.4 Internal ISMS audits	



## Contrast

<b>BS 7799-2:2002</b>	<b>ISO 27001:2005</b>
7 ISMS improvement	8 ISMS improvement
7.1 Continual improvement	8.1 Continual improvement
7.2 Corrective action	8.2 Corrective action
7.3 Preventive action	8.3 Preventive action



# Contrast

BS 7799-2:2002 Annex A	ISO 27001:2005 Annex A
A.3 Security policy (1/2)	A.5 Security policy (1/2)
A.4 Organizational security (3/10)	A.6 Organization of information security (2/11) ↑
A.5 Asset classification and control (2/3)	A.7 Asset management (2/5) ↑
A.6 Information security (3/10)	A.8 Information resources security (3/9) ↓
A.7 Physical and environmental security (3/13)	A.9 Physical and environmental security (2/13) ↓
A.8 Communications and operations management (7/4)	A.10 Communications and operations management (7/4) ↑
A.9 Access control (8/31)	A.11 Access control (7/25) ↓
A.10 System development and maintenance (5/18)	A.12 Information systems acquisition, development and maintenance (6/16) ↓
A.11 Business continuity management (1/5)	A.13 Information security incident management (2/5)
A.12 Compliance (3/11)	A.14 Business continuity management (1/5)
	A.15 Compliance (3/10) ↓

**Total**

**36 control objectives**

**127 controls**

**Total**

**39 control objectives**

**133 controls**



## In figures

	<b>BS 7799-2:2002</b>	<b>ISO 27001:2005</b>
<b>Annex A. domains</b>	<b>10</b>	<b>11</b>
<b>Annex A. control objectives</b>	<b>36</b>	<b>39</b>
<b>Annex A. security controls</b>	<b>127</b>	<b>133</b>
<b>ISMS effectiveness</b>	<b>11</b>	<b>20</b>
<b>ISMS measurement</b>	<b>1</b>	<b>4</b>
<b>ISMS measure</b>	<b>0</b>	<b>6</b>
<b>Information security incident management</b>	<b>A.6.3.1~A.6.3.4 A.8.1.3 A.12.1.7</b>	<b>A.13.1.1~A.13.2.3</b>

## Information Security

<p><b>BS 7799-2:2002</b></p>	<p><b>Clause 3.3</b> security preservation of confidentiality, integrity and availability of information</p>
<p><b>ISO 27001:2005</b></p>	<p><b>Clause 3.4</b> preservation of confidentiality, integrity and availability of information; in addition, other properties such as <b>authenticity</b>, <b>accountability</b>, <b>non-repudiation</b> and <b>reliability</b> can also be involved</p>

## Owner

Page. 4 note 2  
Page 15 note 3

The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the **production, development, maintenance, use** and **security** of the assets.

The term 'owner' does not mean that the person actually has any property rights to the asset.

<p><b>BS 7799-2:2002</b></p>	<p><b>A.5.1 Accountability for assets</b></p> <p>To maintain appropriate protection of organizational assets.</p>
<p><b>ISO 27001:2005</b></p>	<p><b>A.7.1 Responsibility for assets</b></p> <p>To achieve and maintain appropriate protection of organizational assets.</p>

<p><b>BS 7799-2:2002</b></p>	<p><b>A.6.3.1 Reporting security incidents</b></p> <p><b>Security incidents</b> shall be reported through appropriate management channels as quickly as possible.</p>
<p><b>ISO 27001:2005</b></p>	<p><b>A.13.1.1 Reporting information security events</b></p> <p>Information <b>security events</b> shall be reported through appropriate management channels as quickly as possible.</p>