Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001
Information Security Management Systems Guidance series

The Information Security Management Systems (ISMS) series of books are designed to provide users with assistance on establishing, implementing, maintaining, checking and auditing of their ISMS in order to prepare for certification. Titles in this Information Security Management Systems Guidance Series include:

- Guidelines on requirements and preparation for ISMS certification based on ISO/IEC 27001 (ref.: BIP 0071)
- Are you ready for an ISMS audit based on ISO/IEC 27001? (ref.: BIP 0072)
- Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001 (ref.: BIP 0073)
- Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001 (ref.: BIP 0074)
Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001

Ted Humphreys and Angelika Plate

This is a sample chapter from Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001. To read more and buy, visit http://shop.bsigroup.com/bip0073

© BSI British Standards Institution
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>ix</td>
</tr>
<tr>
<td>1 General</td>
<td></td>
</tr>
<tr>
<td>1.1 Scope of this guide</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Field of application</td>
<td>1</td>
</tr>
<tr>
<td>1.2.1 Usage</td>
<td>1</td>
</tr>
<tr>
<td>1.2.2 Compliance</td>
<td>2</td>
</tr>
<tr>
<td>1.3 Meeting ISO/IEC 27001 requirements</td>
<td>2</td>
</tr>
<tr>
<td>2 Implementing and auditing ISMS control objectives and controls</td>
<td></td>
</tr>
<tr>
<td>2.1.1 Information security policy (ISO/IEC 27001:2005, A.5.1)</td>
<td>5</td>
</tr>
<tr>
<td>2.2 Organization of information security (ISO/IEC 27001:2005, clause A.6)</td>
<td>7</td>
</tr>
<tr>
<td>2.2.1 Internal organization (ISO/IEC 27001:2005, A.6.1)</td>
<td>7</td>
</tr>
<tr>
<td>2.2.2 Security of third-party access (ISO/IEC 27001:2005, A.6.2)</td>
<td>13</td>
</tr>
<tr>
<td>2.3 Asset management (ISO/IEC 27001:2005, clause A.7)</td>
<td>16</td>
</tr>
<tr>
<td>2.3.1 Responsibility for assets (ISO/IEC 27001:2005, A.7.1)</td>
<td>16</td>
</tr>
<tr>
<td>2.3.2 Information classification (ISO/IEC 27001:2005, A.7.2)</td>
<td>19</td>
</tr>
<tr>
<td>2.4 Human resources security (ISO/IEC 27001:2005, clause A.8)</td>
<td>21</td>
</tr>
<tr>
<td>2.4.1 Prior to employment (ISO/IEC 27001:2005, A.8.1)</td>
<td>21</td>
</tr>
<tr>
<td>2.4.2 During employment (ISO/IEC 27001:2005, A.8.2)</td>
<td>24</td>
</tr>
<tr>
<td>2.4.3 Termination or change of employment (ISO/IEC 27001:2005, A.8.3)</td>
<td>27</td>
</tr>
<tr>
<td>2.5 Physical and environmental security (ISO/IEC 27001:2005, clause A.9)</td>
<td>30</td>
</tr>
<tr>
<td>2.5.1 Secure areas (ISO/IEC 27001:2005, A.9.1)</td>
<td>30</td>
</tr>
<tr>
<td>2.5.2 Equipment security (ISO/IEC 27001:2005, A.9.2)</td>
<td>35</td>
</tr>
<tr>
<td>2.6 Communications and operations management (ISO/IEC 27001:2005, clause A.10)</td>
<td>41</td>
</tr>
<tr>
<td>2.6.1 Operational procedures and responsibilities (ISO/IEC 27001:2005, A.10.1)</td>
<td>41</td>
</tr>
<tr>
<td>2.6.2 Third-party service delivery management (ISO/IEC 27001:2005, A.10.2)</td>
<td>45</td>
</tr>
<tr>
<td>2.6.3 System planning and acceptance (ISO/IEC 27100:2005, A.10.3)</td>
<td>48</td>
</tr>
<tr>
<td>2.6.4 Protection against malicious and mobile code (ISO/IEC 27001:2005, A.10.4)</td>
<td>50</td>
</tr>
</tbody>
</table>
Guide to the implementation and auditing of ISMS controls

2.6.5 Back-up (ISO/IEC 27001:2005, A.10.5) 52
2.6.6 Network security management (ISO/IEC 27001:2005, A.10.6) 53
2.6.7 Media handling (ISO/IEC 27001:2005, A.10.7) 55
2.6.8 Exchange of information (ISO/IEC 27001:2005, A.10.8) 58
2.6.9 Electronic commerce services (ISO/IEC 27001:2005, A.10.9) 62
2.6.10 Monitoring (ISO/IEC 27001:2005, A.10.10) 65

2.7 Access control (ISO/IEC 27001:2005, clause A.11) 69
2.7.1 Business requirement for system access (ISO/IEC 27001:2005, A.11.1) 69
2.7.2 User access management (ISO/IEC 27001:2005, A.11.2) 71
2.7.3 User responsibilities (ISO/IEC 27001:2005, A.11.3) 74
2.7.4 Network access control (ISO/IEC 27001:2005, A.11.4) 77
2.7.5 Operating system access control (ISO/IEC 27001:2005, A.11.5) 82
2.7.6 Application and information access control (ISO/IEC 27001:2005, A.11.6) 86
2.7.7 Mobile computing and teleworking (ISO/IEC 27001:2005, A.11.7) 87

2.8 Information systems acquisition, development and maintenance (ISO/IEC 27001:2005, clause A.12) 89
2.8.1 Security requirements of information systems (ISO/IEC 27001:2005, A.12.1) 89
2.8.2 Correct processing in applications (ISO/IEC 27001:2005, A.12.2) 90
2.8.3 Cryptographic controls (ISO/IEC 27001:2005, A.12.3) 93
2.8.4 Security of system files (ISO/IEC 27001:2005, A.12.4) 95
2.8.5 Security in development and support processes (ISO/IEC 27001:2005, A.12.5) 97
2.8.6 Technical vulnerability management (ISO/IEC 27001:2005, A.12.6) 101

2.9 Information security incident management (ISO/IEC 27001:2005, clause A.13) 103
2.9.1 Reporting information security events and weaknesses (ISO/IEC 27001:2005, A.13.1) 103
2.9.2 Management of information security incidents and improvements (ISO/IEC 27001:2005, A.13.2) 105

2.11 Compliance (ISO/IEC 27001:2005, clause A.15)  
   2.11.1 Compliance with legal requirements  
   (ISO/IEC 27001:2005, A.15.1)  
   2.11.2 Compliance with security policies and standards, and  
   technical compliance (ISO/IEC 27001:2005, A.15.2)  
   2.11.3 Information systems audit considerations  
   (ISO/IEC 27001:2005, A.15.3)
Foreword

Information is one of your organization’s most valuable assets. The objectives of information security are to protect the confidentiality, integrity and availability of information. These basics elements of information security help to ensure that an organization can protect against:

- sensitive or confidential information being given away, leaked or disclosed both accidentally or in an unauthorized way;
- critical information being accidentally or intentionally modified without your knowledge;
- any important business information being lost without trace or hope of recovery;
- any important business information being rendered unavailable when needed.

It should be the responsibility of all managers, information system owners or custodians, and users in general to ensure that their information is properly managed and protected from a variety of risks and threats faced by every organization. The two standards ISO/IEC 17799:2005,¹ Code of practice for information security management, and ISO/IEC 27001:2005 (revised version of BS 7799-2:2002),² Information security management systems — Requirements, together provide a basis for organizations to develop an effective information security management framework for managing and protecting their important business assets whilst minimizing their risks, maximizing the investments and business opportunities of the organization and ensuring their information systems continue to be available and operational.

The standard ISO/IEC 17799:2005, Code of practice for information security management, provides a comprehensive set of best practice for information security, which organizations can adopt and implement to address the risks they face using the risk management approach specified in the standard ISO/IEC 27001:2005, Information security management systems — Requirements (the ISO revised version of BS 7799-2:2002). In addition, ISO/IEC 27001:2005 (the revised version of BS 7799-2:2002) is the base requirements standard for accredited third-party ISMS (information security management system) certification³ based on this risk management approach. Organizations going through the accredited certification route to obtain an ISMS certificate would need their ISMS to be audited and assessed by an accredited certification body (see 1.2.2 of this guide) to ensure that they have appropriate management processes and systems in place that conform to the requirements specified in the ISMS standard.

¹ This is the revised version of ISO/IEC 17799:2000, which previously was BS 7799-1:1999.
² With the publication of ISO/IEC 27001:2005 the current version of BS 7799-2 will be withdrawn and Part 2 will no longer be a valid standard for third-party accredited certification. Any such certification work will be carried out against the requirements specified in ISO/IEC 27001:2005. Accreditation bodies are responsible for issuing a “transition statement” (see 1.2.2 of this guide) which provides details of the time period during which organization’s and certification bodies (see 1.2.2 of this guide) involved in the ISMS certification process need to make the transition from BS 7799-2:2002 to ISO/IEC 27001:2005.
³ The accredited certification process also employs the accreditation and certification guides and standards ISO Guide 62/EN 45012 and EA 7/03.
This guide, BIP 0073, and the other guides in the BIP 0070 series are designed to provide users with assistance for the implementation and auditing of the ISMS controls that are listed in ISO/IEC 27001:2005, Annex A, and with more implementation guidance in ISO/IEC 17799:2005.

**Note:** A document such as this is provided with the best of intentions. It reflects common practice, which is derived by a consensus among those with a wide variety of skills, knowledge and experience in the subject. This guidance makes no claim to be exhaustive or definitive and users of this guidance may need to seek further guidance in implementing the requirements of the ISO/IEC 27001:2005 standard. Furthermore, there will always be other aspects where additional guidance is required relevant to the organizational, operational, legal and environmental context of the business, including specific threats, controls, regulatory compliance, governance and good practice.

*It has been assumed in the drafting of this BSI guide that the execution of its advice is entrusted to appropriately qualified and experienced people.*
1 General

1.1 Scope of this guide

This document provides guidance on the implementation of ISMS control requirements for auditing existing control implementations to help organizations preparing for certification in accordance with ISO/IEC 27001:2005, Information security management systems — Requirements.

The contents of this guide include the ISMS control requirements that should be addressed by organizations considering certification according to ISO/IEC 27001:2005. Clause 2 of this guide discusses each of the controls in Annex A of ISO/IEC 27001:2005 in two different viewpoints:

• implementation guidance – describing what needs to be considered to fulfil the control requirements when implementing the controls from ISO/IEC 27001:2005, Annex A. This guidance is aligned with ISO/IEC 17799:2005, which gives advice on the implementation of the controls;
• auditing guidance – describing what should be checked when examining the implementation of ISO/IEC 27001:2005 controls to ensure that the implementation covers the essential ISMS control requirements.

It is important to emphasize that this guide does not cover the implementation or auditing of the ISMS process requirements that are covered in BIP 0071. This is also discussed in more detail in 1.3, “Meeting ISO/IEC 27001 requirements”.

1.2 Field of application

1.2.1 Usage

This guide is intended to be used by those involved in:

• designing, implementing and/or maintaining an ISMS;
• preparing for ISMS audits and assessments;
• undertaking both internal and third-party ISMS audits and assessments.4

This guide makes reference to the following standards:

• ISO/IEC 17799:2005 (previously ISO/IEC 17799:2000) – a code of practice that identifies control objectives and controls for information security and provides common practice advice for the implementation of these controls;
• ISO/IEC 27001:2005 – the requirements specification for an information security management system. This standard is used as the basis for accredited certification.

This guide will be updated following any changes to these standards. Organizations should therefore ensure that the correct version is being used for compliance checks related to pre-certification, certification and post-certification purposes.

4 Auditors deployed by the organization to carry out an internal ISMS audit, auditors from certification bodies and assessors from accreditation bodies engaged in assessing certification bodies.
1.2.2 Compliance

To claim compliance with the requirements in ISO/IEC 27001:2005, the organization needs to demonstrate that it has all the processes in place and provides appropriate evidence to support such claims. Where exclusions are made, claims of compliance with ISO/IEC 27001:2005 are not acceptable unless such exclusions do not affect the organization’s ability and/or responsibility to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements. Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been knowingly and objectively accepted by those in management that have the executive responsibility for making such decisions and who are accountable for making such decisions.

Excluding any of the requirements specified in ISO/IEC 27001:2005, Clauses 4, 5, 6, 7 and 8 is not acceptable.

The implementation of a set of ISMS processes results in the organization deploying a system of controls based on a risk management approach to manage their risks. The organization should have implemented an effective system of management controls and processes as part of its ISMS, and it should be able to demonstrate this by providing evidence to the ISMS auditor (whether it be a first-, second- or third-party audit).

This guide can be used by those who might not have an immediate need for an audit but require a specification for establishing and implementing an ISMS based on industry accepted best practice processes. However, claiming compliance with ISO/IEC 27001:2005 does require the organization to have at least an internal ISMS audit in place whether or not it goes for a third-party audit at a later stage. The organization may not have a business case for a third-party audit, but to be compliant with ISO/IEC 27001:2005 the internal ISMS audit is mandatory. This guide can of course also be used by those preparing for a second- and third-party audit.

1.3 Meeting ISO/IEC 27001 requirements

There are two different types of requirements stated in BS 7799-2:2002:

- the requirements contained in the ISMS process that are described in ISO/IEC 27001:2005, clauses 4 to 8;
- the ISMS control requirements, contained in ISO/IEC 27001:2005, Annex A.

The ISMS process requirements address how an organization should establish and maintain its ISMS, based on the Plan–Do–Check–Act (PDCA) model. An organization that wants to achieve ISO/IEC 27001 certification needs to comply with all these requirements – exclusions are not acceptable. The guide BIP 0071, Guidelines on requirements and preparation for ISMS Certification based on ISO/IEC 27001, provides guidance on the PDCA model and the ISMS process requirements, certification process and preparing for certification. An organization can also check whether it has implemented all of the ISMS process requirements by using the checklists provided by the guide BIP 0072, Are you ready for an ISMS audits based on ISO/IEC 27001?

---

The ISMS control requirements stated in ISO/IEC 27001:2005, Annex A are applicable for an organization unless the risk assessment and the risk acceptance criteria prove that this is not the case. This is stated in ISO/IEC 27001: “Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons.”