Guidelines on Requirements and Preparation for ISMS Certification based on ISO/IEC 27001
# Contents

Information Security Management Systems Guidance series vii  
Acknowledgements viii  
Foreword ix  

## 1 General 1  
1.1 Scope of this guide 1  
1.2 Field of application 1  
1.3 Definitions 2  
1.4 Related documents 2  

## 2 Essence of information security 5  
2.1 Confidentiality 5  
2.2 Integrity 5  
2.3 Availability 6  
2.4 Sensitive, critical or personally identifiable information 6  

## 3 Information security management system (ISMS) 7  
3.1 Introduction 7  
3.2 Compatibility with other management system standards (MSS) 11  
3.3 ‘Shall’ statements 11  

## 4 ISMS requirements 12  
4.1 Context of the organization (Clause 4) 12  
4.2 Leadership (Clause 5) 15  
4.3 Planning (Clause 6) 20  
4.4 Support (Clause 7) 30  
4.5 Operation (Clause 8) 39  
4.6 Performance evaluation (Clause 9) 41  
4.7 Improvement (Clause 10) 45  

## 5 ISMS certification 48  
5.1 Overview 48  
5.2 Certification audit process 54  
5.3 Initial audit and certification 64  
5.4 Surveillance activities 71  
5.5 Recertification 74  
5.6 Special audits 75  
5.7 Suspending, withdrawing or reducing the scope of certification 76  
5.8 Appeals 77
5.9 Complaints 77
5.10 Records of applicants and clients 78
5.11 Other related topics 78
Information Security Management Systems
Guidance series

The Information Security Management Systems (ISMS) series of books is designed to provide users with assistance on establishing, implementing, maintaining, checking and auditing 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);
Acknowledgements

Special thanks go to Dr Angelika Plate (one of the co-editors of the 2013 edition of ISO/IEC 27001) for her expert opinion and her attentive and detailed review of this guide. Thanks also go to those SC27 ISMS experts who have been consulted during the development of this guide, and to the founder/director and experts of the ISMS International User Group who supplied some of the appropriate background intellectual property.
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 basic 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;
- personally identifiable information being compromised;
- 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 the information they are processing is properly managed and protected from a variety of risks and threats faced by every organization. The two standards, ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements and ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls, together provide a basis for organizations to develop an effective information security management framework for protecting their important business assets, whilst managing their risks, helping to maximize the organization’s investments and business opportunities, and ensuring their information systems continue to be available and operational.

ISO/IEC 27001:2013 is the requirements standard that can be used for accredited third-party information security management system (ISMS) certifications. 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 section 5 of this guide) to ensure that they have appropriate management processes and systems in place that conform to the requirements specified in the ISO/IEC 27001 ISMS standard.
ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls* provides a comprehensive set of best practice controls for information security and implementation guidance. Organizations can adopt these controls as part of the risk treatment process specified in ISO/IEC 27001:2013 in order to manage the risks they face to their information assets.

This guide, BIP 0071, as with the other guides in the BIP 0070 series, is designed to provide users with assistance in establishing, implementing and maintaining their ISMS to help them in preparing for ISMS certification. This is the fourth edition of this guide and it has been produced to reflect the publication of the new editions of ISO/IEC 27001 and ISO/IEC 27002.

Note: A document such as this is provided with the best of intentions. It reflects common practice that is derived by a consensus among those with a wide variety of skills, knowledge and experience in the subject. This guide makes no claim to be exhaustive or definitive and users of this guide may need to seek further guidance in implementing the requirements of ISO/IEC 27001:2013 or in using the guidance found in ISO/IEC 27002:2013. 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. BSI or the author of this guide cannot be held liable by organizations, users or third parties for any loss or damage, arising directly or indirectly in connection with reliance on the contents of this guide, or in the execution or implementation of this information. It has been assumed in the drafting of the information and advice given in this guide that the execution of this information by organizations and users is entrusted to appropriately qualified and experienced people.
1 General

1.1 Scope of this guide
This document provides guidance and commentary on the requirements specified in the information security management system (ISMS) standard ISO/IEC 27001:2013. It gives guidance on the complete ‘life cycle’ of ISMS activities required to establish, implement, monitor and continually improve a set of management controls and processes to achieve effective information security.

1.2 Field of application

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

- designing, implementing and maintaining an ISMS;
- preparing for ISMS audits and assessments;
- undertaking ISMS audits and assessments.¹

The different types of ISMS audits include first-party audits, such as internal ISMS audits, second-party audits, such as those carried out by customer auditors, and third-party audits, such as those carried out by accredited certification bodies.

This guide provides commentary on the implementation of the processes defined in ISO/IEC 27001:2013 to help understand and prepare for third-party ISMS audits to achieve accredited certification against ISO/IEC 27001:2013. It is also useful for those carrying out internal audits on a regular basis or those doing a pre-audit assessment prior to a formal third-party audit.

¹ 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 27001:2013, the organization needs to demonstrate that it has all the processes in place and needs to provide appropriate objective evidence to support such claims. 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 who have the executive responsibility for making such decisions and who are accountable for making such decisions.

Excluding any of the requirements specified in Clauses 4 to 10 of ISO/IEC 27001:2013 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 its 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 or audit team (whether it be a first, second or third-party audit).

This guide can be used by those who may not have an immediate need for an external ISMS audit but who require an understanding for establishing and implementing ISMS-based or industry-accepted best practice processes. However, claiming compliance with ISO/IEC 27001:2013 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 27001:2013, 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 Definitions


1.4 Related documents

This guide makes reference to the following standards and guidelines:

- BIP 0074, Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001;
- BIP 0076, Information security risk management — Handbook for ISO/IEC 27001;
1 General

- BS 7799-3:2006, Information security management systems — Guidelines for information security risk management;
- ISO 9001, Quality management systems — Requirements;
- ISO 19011:2011, Guidelines for auditing management systems;
- ISO 31000:2009, Risk management — Principles and guidelines;
- ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles;
- ISO/IEC 17021:2011, Conformity assessment — Requirements for bodies providing audit and certification of management systems;
- ISO/IEC 27006:2011, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems;
- ISO/IEC JTC1/SC27 will be publishing the following standard: ISO/IEC JTC 1/SC27/WG1 SD3 – ISO/IEC 27001 and ISO/IEC 27002 ‘old to new’ transition maps. Extracts of this are included in Annex A of this guide;
- ISO/IEC Directives, Part 1 — Consolidated ISO Supplement — Procedures specific to ISO.

Note: Users should always ensure that the correct version of these standards is used. The list above indicates the date of publication of the current editions of these standards at the time of the publication of this guide. However, all standards are reviewed from time to time to check their currency and validity, and this can result in a revised edition being published.

This document is one of a set of five guides published by BSI to support the use and application of ISO/IEC 27001:2013 and ISO/IEC 27002:2013. The reader may find it of benefit to have copies of these other guides:
1 General

- BIP 0072, Are you ready for an ISMS audit based on ISO/IEC 27001?
- BIP 0073, Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001;
- BIP 0074, Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001 (also listed above);
- BIP 0076, Information security risk management — Handbook for ISO/IEC 27001 (also listed above).