Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001
Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001

Bridget Kenyon and Edward (Ted) Humphreys
Contents

1 General
1.1 Scope of this guide 1
1.2 Field of application 1
1.3 Meeting ISO/IEC 27001 requirements 3
1.4 General 3

2 Implementing and auditing ISMS control objectives and controls
2.1 Information security policies (ISO/IEC 27001:2013, Clause A.5) 4
2.2 Organization of information security (ISO/IEC 27001:2013, Clause A.6) 7
2.3 Human resource security (ISO/IEC 27001:2013, Clause A.7) 15
2.4 Asset management (ISO/IEC 27001:2013, Clause A.8) 22
2.5 Access control (ISO/IEC 27001:2013, Clause A.9) 34
2.6 Cryptography (ISO/IEC 27001:2013, Clause A.10) 49
2.7 Physical and environmental security (ISO/IEC 27001:2013, Clause A.11) 52
2.8 Operations security (ISO/IEC 27001:2013, Clause A.12) 69
2.9 Communications security (ISO/IEC 27001:2013, Clause A.13) 85
2.10 System acquisition, development and maintenance (ISO/IEC 27001:2013, Clause A.14) 94
2.11 Supplier relationships (ISO/IEC 27001:2013, Clause A.15) 107
2.12 Information security incident management (ISO/IEC 27001:2013, Clause A.16) 113
2.14 Compliance (ISO/IEC 27001:2013, Clause A.18) 123
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);
- Information security risk management — Handbook for ISO/IEC 27001
  (ref.: BIP 0076).
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 their information is properly managed and protected from the 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 managing and protecting their important business assets, whilst minimizing their risks, maximizing the investments and business opportunities of their organizations, 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 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.

Foreword

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 0073, 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 publicly available common best practice that is derived by a consensus among international experts 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 authors of this guide cannot be held liable by organizations, users or third parties for 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 on the implementation of information security management system (ISMS) control requirements and on auditing existing control implementations to help organizations preparing for certification in accordance with ISO/IEC 27001:2013.

The contents of this guide include the ISMS control requirements that should be addressed by organizations considering certification. Section 2 of this guide discusses each of the controls in Annex A of ISO/IEC 27001:2013 from two different viewpoints:

1. implementation guidance – describing what needs to be considered to fulfil the control requirements when implementing the controls from ISO/IEC 27001:2013, Annex A. This guidance is aligned with ISO/IEC 27002:2013, which gives advice on the implementation of the controls;
2. auditing guidance – describing what should be checked when examining the implementation of ISO/IEC 27001:2013 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; these are covered in BIP 0071. These are 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;

To read more and buy, visit http://shop.bsigroup.com/BIP0073
© The British Standards Institution 2013
1 General

- undertaking both internal and third-party ISMS audits and assessments.\(^1\)

This guide makes reference to the following standards:

- ISO/IEC 27001:2013 – the requirements specification for an ISMS. This standard is used as the basis for accredited certification;
- ISO/IEC 27002:2013 – a reference for selecting controls as part of the implementation of an ISMS, and a guidance document for organizations implementing commonly accepted security controls.

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.

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 ISO/IEC 27001:2013, Clauses 4 to 10 is not acceptable.\(^2\)

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 (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 audit, but who require a specification for establishing and implementing an ISMS based on 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

\(^1\) 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.

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 Meeting ISO/IEC 27001 requirements

There are two different types of requirements stated in ISO/IEC 27001:2013:

1. the requirements contained in the ISMS process that are described in ISO/IEC 27001:2013, Clauses 4 to 10;
2. the ISMS controls contained in ISO/IEC 27001:2013, Annex A.

The ISMS process requirements address how an organization should establish and maintain its ISMS. An organization that wants to achieve ISO/IEC 27001:2013 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 ISMS process requirements and 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 audit based on ISO/IEC 27001?*

1.4 General

The ISMS control requirements stated in ISO/IEC 27001:2013, 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: ‘The organization shall…produce a Statement of Applicability that contains the necessary controls…and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A’ (ISO/IEC 27001, 6.1.3).