Are you ready for an ISMS audit

based on ISO/IEC 27001?

Second edition

Edward Humphreys and Bridget Kenyon

Are you ready for an ISMS audit based on ISO/IEC 27001?

Are you ready for an ISMS audit based on ISO/IEC 27001?

Second edition

Edward (Ted) Humphreys and Bridget Kenyon

First published in the UK in 1999
Second edition 2002
Third edition 2005
Reprinted 2008
Fourth edition 2014
by
BSI Standards Limited
389 Chiswick High Road
London W4 4AL

Whilst every care has been taken in developing and compiling this publication, BSI accepts no liability for any loss or damage caused, arising directly or indirectly in connection with reliance on its contents except to the extent that such liability may not be excluded in law.

BSI has made every reasonable effort to locate, contact and acknowledge copyright owners of material included in this book. Anyone who believes that they have a claim of copyright in any of the content of this book should contact BSI at the above address.

BSI has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this book, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Typeset in Great Britain by Letterpart Limited - letterpart.com
Printed in Great Britain by Berforts, www.berforts.co.uk

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 978 0 580 82913 0

Contents

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:

- **BIP 0071, *Guidelines on requirements and preparation for ISMS certification based on ISO/IEC 27001*;**
- **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*;**
- **BIP 0076, *Information security risk management — Handbook for ISO/IEC 27001*.**

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 managing and protecting their important business assets whilst minimizing 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 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

The 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 0072, as with the other guides in the BIP 0070 series, is designed to provide users with assistance in checking the processes and controls in place in their ISMS against the requirements laid out in ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

Note: *The information provided in this document 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 more specific to the business context of the organization implementing the requirements of ISO/IEC 27001:2013. Furthermore, there will always be other aspects where additional guidance is required relevant.*

1 Introduction

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. Other guides include:

- BIP 0071, *Guidelines on requirements and preparation for ISMS certification 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 implementation based on ISO/IEC 27001;*
- BIP 0076, *Information security risk management. Handbook for ISO/IEC 27001*.

This guide is intended primarily for use by organizations wishing to carry out internal assessment of their ISMS against the requirements in ISO/IEC 27001:2013 either as a precursor to an internal ISMS audit (see Clause 9 of ISO/IEC 27001:2013) or in preparation for a formal third-party ISMS certification audit (see BIP 0071). It is recommended that the assessments specified in this guide be carried out by those persons responsible for information security management in the organization or by internal audit staff ISMS developers and implementers may also find this guide a useful reference document when considering the security aspects of new systems. This assessment guide is intended as an aid to satisfying the requirements for a formal compliance audit and is not a replacement for a compliance audit.

1.1 Scope of this guide

This guide provides a means to help organizations assess their ISMS with respect to the requirements specified in ISO/IEC 27001:2013 using the following workbooks.

- *ISMS processes workbook* – a gap analysis to check whether the organization has a set of systems and processes in place to satisfy the requirements specified in Clauses 4 to 10 of ISO/IEC 27001:2013.
- *Annex A Gap analysis workbook* – this workbook lists the controls that are defined in Annex A of ISO/IEC 27001:2013. This workbook can be used either as part of the risk treatment process as defined in ISO/IEC 27001:2013, 6.1.3 or as a stand-alone gap analysis tool to check the implementation of Annex A controls. After determining the controls needed (6.1.3.b)), organizations are directed to Annex A to do a comparison check to ensure that no necessary controls are overlooked (6.1.3 c). This workbook can be used to check and document whether Annex A controls are implemented or not, and to record the justification for any exclusions. The reasons and justification why a particular control has or has not been implemented are subsequently used to satisfy the mandatory requirement for production of a Statement of Applicability (SoA) (6.1.3.d).

Note: For accredited certification, this type of gap analysis has no formal status and should not be taken as a replacement for the SoA.

These workbooks can be useful to those organizations preparing for a formal third-party accredited certification, as well as for those preparing for post-certification activities such as surveillance audits and for recertification. They provide a means of checking how many activities have been carried out and what activities still need to be undertaken. Assessments using both these workbooks should not be taken as a definitive quality check on the completeness of these activities, or the correctness and effectiveness of the results and the implementation of these processes and activities. These workbooks only provide a high level 'health check' on the state of ISMS progress.

Please note that the use of these workbooks and this guide does not constitute a replacement for a formal compliance audit with ISO/IEC 27001:2013.

1.2 Use of the standards

This guide makes reference to the following standards:

- ISO/IEC 27001:2013 — *Information technology — Security techniques — Information security management systems — Requirements*. This standard is used as the basis for accredited certification.
- ISO/IEC 27002:2013 – *Information technology – Security techniques – Code of practice for information security controls.*

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

1.3 Companion guides

Additional guides are available that provide a more detailed interpretation of ISO/IEC 27001:2013 and practical development advice, e.g. BIP 0071 on preparing for ISMS certification and BIP 0073 on the implementation and auditing of ISMS controls.

2 ISMS scope

It is important both for the organization whose ISMS is being assessed, and for the auditors' understanding of the ISMS, that the scope of the ISMS is well defined and unambiguous. Given the complexity of many business applications and processes, as well as the growth of information systems, IT and networking, there are many possible ways to define the ISMS boundaries. Similarly, the size of organization and its geographical spread will influence the view of what is a suitable scope It is very rare that business systems and processes work in isolation or are self-contained, as they will have interfaces with other systems. Therefore, in defining the scope of the ISMS, any interfaces with other systems and processes outside the ISMS boundaries need to be taken into consideration.

Guidance on the identification and definition of the ISMS scope is given in BIP 0071, which expands on the requirement that the organization shall determine the boundaries and applicability of the ISMS to establish its scope as given in ISO/IEC 27001:2013. It is important that when determining this scope, the organization shall consider: a) the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS; b) the requirements of these interested parties relevant to information security; and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

3 How to use this guide

The aim of the guide is to allow organizations to assess the extent of their ISMS processes and controls in place against the requirements specified in ISO/IEC 27001:2013. This Section tells you how to prepare for, and complete, these workbook assessments; the major component of the workbooks is carried out using questionnaires. The form and content of these questionnaires is described below and a sample of a completed questionnaire is shown in Section 3.3. The workbooks are contained in sections 4 and 5 of this guide

3.1 ISMS process requirements

Introduction

The ISMS process requirements workbook deals with the set of requirements defined in ISO/IEC 27001:2013. It covers an ongoing life cycle of activities aimed at establishing effective information security management, providing a programme of ISMS continual improvement.

The ISMS requirements defined in ISO/IEC 27001:2013 require the implementation of a systematic information security risk management process and the implementation of a set of processes used to establish, implement, monitor and maintain an ISMS (see clauses of ISO/IEC 27001:2013 for details):

- Context of the organization (Clause 4);
- Leadership (Clause 5);
- Planning (Clause 6);
- Support (Clause 7);
- Operation (Clause 8);
- Performance evaluation (Clause 9);
- Improvement (Clause 10).

This includes having an appropriate system of documented information in place that is kept up to date, accurate and available for inspection and reference with appropriate documented information in accordance with the requirements of ISO/IEC 27001:2013, 7.5.

The third-party certification or internal ISMS audit will need to check, based on appropriate evidence being provided, that the organization has a set of ISMS processes in place, as well as an ISMS system of controls (based on Annex A of ISO/IEC 27001:2013) to cover the requirements of Clauses 4 to 10 of ISO/IEC 27001:2013.

Workbook checklist

Section 4 of this guide considers the workbook checklists for the ISMS process requirements. The two basic questions, which may be addressed to each of the process requirements, are as follows.

Q1. Is a relevant process in place to satisfy the mandatory prescriptive 'shall' requirements specified in Clauses 4 to 10 of ISO/IEC 27001:2013?

Three answers are possible:

- **YES** – This indicates that there is a process in place that completely fulfils the requirement. Some explanation should be given justifying and providing evidence to support this answer.
- **PARTIAL** – This indicates that a process is in place but not sufficiently developed or implemented to allow an answer of 'yes' for this requirement. Further action is needed to meet the requirements specified in ISO/IEC 27001.
- **NO** – This indicates that there is no process in place to address the requirement and action is needed to meet the requirements specified in ISO/IEC 27001.

Q2. If the requirement has been either not implemented or only partially implemented, why is this the case?

It will be important to provide an explanation to understand the reasons and justification for partial implementation or non-implementation and to provide appropriate evidence to support this. Also, an indication needs to be given as to what action shall be taken to address this gap in meeting the requirements of ISO/IEC 27001. An explanation justifying and providing evidence for the answer that a requirement of ISO/IEC 27001 has been completely addressed is also helpful.

3.2 Annex A Reference control objectives and controls

3.2.1 Introduction

Annex A of ISO/IEC 27001:2013 contains the control objectives and controls that are to be used in context with the risk treatment process in 6.1.3. These are directly derived from and aligned with those listed in ISO/IEC 27002:2013 Clauses 5 to 18. This guide presents each of the control requirements in question form and should be used in conjunction with the ISMS processes workbook to support as appropriate the implementation of the risk treatment processes (see ISO/IEC 27001:2013, 6.1.3 and 8.3).

The risk treatment process defined in ISO/IEC 27001:2013, 6.1.3 states the following:

> ### 6.1.3 Information security risk treatment
>
> The organization shall define and apply an information security risk treatment process to:
>
> a) Select appropriate information security risk treatment options, taking account of the risk assessment results;
> b) Determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
>
> NOTE: Organizations can design controls as required, or identify them from any source
>
> c) Compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;
>
> NOTE: Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked
>
> NOTE: Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed
>
> d) Produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A.

Section 5 of this guide enables organizations to indicate whether the control:

- has been implemented, and justification and evidence can be given to support this answer;
- only partially been implemented, and the reason(s) and justification for this;
- has not been implemented at all and the reason(s) and justification for this. For example, the control may not have been determined as necessary as part of the risk management process (see ISO/IEC 27001:2013, 6.1.3 and 8.3), or it may have been determined but has not yet been implemented

It should be understood that external or internal auditors, whose task it is to assess the ISMS against the requirements of ISO/IEC 27001, may not regard the reasons given for non-implementation as sufficient justification and may require additional reasons to be given during the audit. Please note that any exclusion from the controls in Annex A of ISO/IEC 27001:2013 is to be justified, based on the results of the risk assessment and the risk treatment decisions made

Organizations may wish to further refine the process defined in this guide with more detailed questions regarding the control requirements within each general category. This might be necessary to completely assess all details of a specific control implementation in place in an organization. Due to the number of controls, this might be an extensive task, but will lead to more detailed information and a more accurate account of the status of the ISMS implementation.

Workbook checklist

The two basic questions that may be addressed to each of the control requirements are as follows.

Q1. Has this control requirement been implemented? Three answers are possible:

- **YES** – This indicates that there is a control in place that completely fulfils the control requirements. An explanation with reference to supporting evidence should be given justifying this answer – see 'Comments'.
- **PARTIAL** – This indicates that some measures are in place that address the control requirements but not sufficiently to allow an answer of 'yes' to be given. An explanation with reference to supporting evidence should be given justifying this answer – see 'Comments'.
- **NO** – This indicates that no measures have been taken to address the control requirements. This is also the correct answer if the control is not relevant to the system under review as determined by the risk assessment and risk treatment processes (see ISO/IEC 27001:2013, 6.1.2 to 6.1.3). A 'no' response may also be given if a control requirement is relevant but is not yet implemented or the requirement has been satisfied by deploying another control.

Q2. If the control requirement has not been fully implemented then why is this the case?

It will be important to understand the reasons and justification for either partial or non-implementation. Supporting evidence for an answer stating that the control requirement, has been completely addressed would also be helpful.

The ISMS implementation is based on a risk management process. A third-party certification or internal ISMS audit will check and require evidence that the ISMS has been developed and implemented based on a risk management process. One important audit requirement is that any implemented ISMS system of controls can be traced back to the risk assessment and risk treatment processes. Consequently, if this workbook check is carried out just prior to the certification, e.g. as a pre-certification assessment, then the absence or non-applicability of controls should be documented and justified with supporting evidence based on the results of the risk assessment. One example of such a justification is that the implementation of a particular control could not be justified by the levels of risk exposure, or that the risk treatment decision was different from reducing the risk.

COMMENTS: In all cases some further comment should be given to expand on the particular control implementation, or reasons for partial or non-implementation. Such comments could include:

- where there are controls deemed to be in place, it may be useful to describe evidence and justifications for their implementation, and the way in which they have been implemented This in itself may lead to identification and recognition that further action and work still needs to be done in that area, or to support the activities described in the 'Performance evaluation' stage (Clause 9). Alternatively, setting out the implemented controls in this way may indicate that more is being done than necessary and that savings can be made by reducing some controls;
- where control requirements have not or have only been partially met, an indication should be given of what steps are to be taken and over what time period to mitigate the (partial) absence of the control requirement, and justification for this status should be given;
- where a decision has been made to take no further action to implement controls in a given area, in effect, a decision has been taken to accept this as a potential risk. Such a decision should be clearly documented and justified to be fully understood and explained.

3.3 A sample of a completed questionnaire

To help those completing this guide, an example page from one of the questionnaire sections follows.

ISO/IEC 27001, *Information security management systems — Requirements*

7. Support
7.2.c.Competence

Requirement: The organization shall where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

Q1. Implementation status. Tick one box for each control requirement..

Control requirement	YES	PARTIAL	NO
7.2.c Is there a process in place and being used, where applicable, to take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken?			

Q2. If you have ticked either of the boxes marked **PARTIAL** or **NO** you should indicate the reason in the following table

Aspect	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.6.2.1	There is a process in place but it is not fully operational. Although actions have been taken to acquire the necessary competence, the evaluation of the effectiveness of these actions has yet to be carried out. The reason for this that those tasked with carrying the work were employed on other tasks.	Management needs to take action to ensure that this evaluation activity gets done: by reassessing the resources needed, and to reassign the work if necessary, and to properly schedule and prioritise the work to ensure the resource is available to do the work within a given time frame

4 ISMS processes workbook (assessment of ISMS process requirements)

It is important to lay a firm foundation for the ISMS process within which a system of controls is implemented Clauses 4 to 10 of ISO/IEC 27001:2013 provide requirements for establishing, implementing, maintaining and continually improving an ISMS. The user guide BIP 0071 expands on the issues involved By referring to these two documents as necessary, you should review and follow the compliance checks addressed in this Clause in the following tables.

Guidance on completing the questionnaires can be found in Section 3.1 of this guide

Please note that the question given in the tables below are based on requirements that are mandatory for any organization claiming compliance with ISO/IEC 27001:2013, and should be addressed by any organization that aims for accredited ISO/IEC 27001:2013 certification.

ISO/IEC 27001*, Information security management systems — Requirements*

4. Context of the organization
4.1 Understanding the organization and its context

Q1. Consider the following aspect relating to the organizational context of the ISMS. Tick one box.

Aspect	YES	PARTIAL	NO
4.1 Is there a process in place to enable the organization to determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system?			

Q2. If you have ticked either of the boxes marked **PARTIAL** or **NO** you should indicate the reasons and justification in the following boxes.

Aspect	Reasons and justification (with reference to supporting evidence)	Action to be taken
4.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate Where aspects are already addressed it may be helpful to provide detail on actions taken.