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

bsi.

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

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.

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

4. Context of the organization
4.2 Understanding the needs and expectations of interested parties

Q1. Consider the following aspects relating to interested parties. Tick one box.

Aspect	YES	PARTIAL	NO
4.2.a Is there a process in place to enable the organization to determine interested parties that are relevant to the information security management system?			
4.2.b Is there a process in place to enable the organization to determine the requirements of these interested parties that are relevant to information security?			

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
4.2.a		
4.2.b		

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 details on actions taken.

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

4. Context of the organization
4.3 Determining the scope of the information security management system

Q1. Consider the following aspects relating to the scope of the ISMS. Tick one box.

Aspect	YES	PARTIAL	NO
4.3.a Has the organization determined the boundaries and applicability of the information security management system to establish its scope?			
4.3.b When determining the scope of its ISMS has the organization considered the external and internal issues referred to in 4.1?			
4.3.c When determining the scope of its ISMS has the organization considered the requirements referred to in 4.2?			
4.3.d When determining the scope of its ISMS has the organization considered the interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations?			
4.3.e Has the organization made the scope available as documented information?			

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
4.3.a		
4.3.b		
4.3.c		
4.3.d		
4.3.e		

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 details on actions taken.

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

4. Context of the organization
4.4 Information security management system

Q1. Consider the following aspects relating to the status of the ISMS. Tick one box.

Aspect	YES	PARTIAL	NO
4.4.a Has the organization established an information security management system, in accordance with the requirements of ISO/IEC 27001:2013?			
4.4.b Has the organization implemented an information security management system, in accordance with the requirements of ISO/IEC 27001:2013?			
4.4.c Has the organization processes in place for maintaining its information security management system, in accordance with the requirements of ISO/IEC 27001:2013?			
4.4.d Has the organization processes in place for continually improving an information security management system, in accordance with the requirements of ISO/IEC 27001:2013?			

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
4.4.a		
4.4.b		
4.4.c		
4.4.d		

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 details on actions taken.

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

5 Leadership
5.1 Leadership and commitment

Q1. Consider the following aspects relating to top management. Tick one box.

Aspect	YES	PARTIAL	NO
5.1.a Does top management demonstrate leadership and commitment with respect to the information security management system by ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization?			
5.1.b Does top management demonstrate leadership and commitment with respect to the information security management system by ensuring the integration of the information security management system requirements into the organization's processes?			
5.1.c Does top management demonstrate leadership and commitment with respect to the information security management system by ensuring that the resources needed for the information security management system are available?			
5.1.d Does top management demonstrate leadership and commitment with respect to the information security management system by communicating the importance of effective information security management and of conforming to the information security management system requirements?			
5.1.e Does top management demonstrate leadership and commitment with respect to the information security management system by ensuring that the information security management system achieves its intended outcome(s)?			
5.1.f Does top management demonstrate leadership and commitment with respect to the information security management system by directing and supporting persons to contribute to the effectiveness of the information security management system?			
5.1.g Does top management demonstrate leadership and commitment with respect to the information security management system by promoting continual improvement?			
5.1.h Does top management demonstrate leadership and commitment with respect to the information security management system by supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility?			

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
5.1.a		
5.1.b		
5.1.c		
5.1.d		
5.1.e		
5.1.f		
5.1.g		
5.1.h		

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 details on actions taken.

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

5 Leadership
5.2 Policy

Q1. Consider the following aspects relating to the information security policy. Tick one box.

Aspect	YES	PARTIAL	NO
5.2.a Has top management established an information security policy that is appropriate to the purpose of the organization?			
5.2.b Has top management established an information security policy that includes information security objectives (see 6.2) or provides the framework for setting information security objectives?			
5.2.c Has top management established an information security policy that includes a commitment to satisfy applicable requirements related to information security?			
5.2.d Has top management established an information security policy that includes a commitment to continual improvement of the information security management system?			
5.2.e Is the information security policy made available as documented information?			
5.2.f Is the information security policy communicated within the organization?			
5.2.g Is the information security policy made available to interested parties, as appropriate?			

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
5.2.a		
5.2.b		
5.2.c		
5.2.d		
5.2.e		
5.2.f		
5.2.g		

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 details on actions taken.

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

5 Leadership
5.3 Organizational roles, responsibilities and authorities

Q1. Consider the following aspects relating to roles, responsibilities and authorities. Tick one box.

Aspect	YES	PARTIAL	NO
5.3.a Does top management ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated?			
5.3.b Has top management assigned the responsibility and authority for ensuring that the information security management system conforms to the requirements of ISO/IEC 27001?			
5.3.c Has top management assigned the responsibility and authority for reporting on the performance of the information security management system to top management?			

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
5.3.a		
5.3.b		
5.3.c		

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 details on actions taken.

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

6 Planning
6.1 Actions to address risks and opportunities
6.1.1 General

Q1. Consider the following aspects relating to risk/opportunity identification and related actions. Tick one box.

Aspect	YES	PARTIAL	NO
6.1.1.a When planning for the information security management system, does the organization consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to ensure the information security management system can achieve its intended outcome(s)?			
6.1.1.b When planning for the information security management system, does the organization consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to prevent, or reduce, undesired effects?			
6.1.1.c When planning for the information security management system, does the organization consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to achieve continual improvement?			
6.1.1.d Does the organization plan actions to address these risks and opportunities?			
6.1.1.e Does the organization plan how to 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions?			

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
6.1.1.a		
6.1.1.b		
6.1.1.c		
6.1.1.d		
6.1.1.e		

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 details on actions taken.

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

6 Planning
6.1 Actions to address risks and opportunities
6.1.2 Information security risk assessment

Q1. Consider the following aspects relating to the risk assessment process. Tick one box.

Aspect	YES	PARTIAL	NO
6.1.2.a Does the organization define and apply an information security risk assessment process that establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments?			
6.1.2.b Does the organization define and apply an information security risk assessment process that ensures that repeated information security risk assessments produce consistent, valid and comparable results?			
6.1.2.c Does the organization define and apply an information security risk assessment process that: 1) identifies risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identifies the risk owners?			
6.1.2.d Does the organization define and apply an information security risk assessment process that analyses the information security risks as follows: 1) assesses the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assesses the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determines the levels of risk?			
6.1.2.e Does the organization define and apply an information security risk assessment process that evaluates the information security risks as follows: 1) compares the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritizes the analysed risks for risk treatment?			
6.1.2.f Does the organization retain documented information about the information security risk assessment process?			

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
6.1.2.a		
6.1.2.b		
6.1.2.c		
6.1.2.d		
6.1.2.e		
6.1.2.f		

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 details on actions taken.

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

6 Planning
6.1 Actions to address risks and opportunities
6.1.3 Information security risk treatment

Q1. Consider the following aspects relating to the risk treatment process. Tick one box.

Aspect	YES	PARTIAL	NO
6.1.3.a Does the organization define and apply an information security risk treatment process to select appropriate information security risk treatment options, taking account of the risk assessment results?			
6.1.3.b Does the organization define and apply an information security risk treatment process to determine all controls that are necessary to implement the information security risk treatment option(s) chosen?			
6.1.3.c Does the organization define and apply an information security risk treatment process to compare the controls determined in 6.1.3.b above with those in Annex A and verify that no necessary controls have been omitted?			
6.1.3.d Does the organization define and apply an information security risk treatment process to 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?			
6.1.3.e Does the organization define and apply an information security risk treatment process to formulate an information security risk treatment plan?			
6.1.3.f Does the organization define and apply an information security risk treatment process to obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks?			
6.1.3.h Does the organization retain documented information about the information security risk treatment process?			

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
6.1.3.a		
6.1.3.b		
6.1.3.c		
6.1.3.d		
6.1.3.e		
6.1.3.f		
6.1.3.h		

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 details on actions taken.

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

6 Planning
6.2 Information security objectives and plans to achieve them

Q1. Consider the following aspects relating to information security objectives. Tick one box.

Aspect	YES	PARTIAL	NO
6.2.a Does the organization establish information security objectives at relevant functions and levels?			
6.2.b Are the information security objectives consistent with the information security policy?			
6.2.c Are the information security objectives measurable (if practicable)?			
6.2.d Do the information security objectives take into account applicable information security requirements, and risk assessment and risk treatment results?			
6.2.e Are the information security objectives communicated?			
6.2.f Are the information security objectives updated as appropriate?			
6.2.g Does the organization retain documented information about the information security objectives?			
6.2.h When planning how to achieve its information security objectives, does the organization determine what will be done?			
6.2.i When planning how to achieve its information security objectives, does the organization determine what resources will be required?			
6.2.j When planning how to achieve its information security objectives, does the organization determine who will be responsible?			
6.2.k When planning how to achieve its information security objectives, does the organization determine when it will be completed?			
6.2.l When planning how to achieve its information security objectives, does the organization determine how the results will be evaluated?			

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
6.2.a		
6.2.b		
6.2.c		
6.2.d		
6.2.e		
6.2.f		
6.2.h		
6.2.i		
6.2.j		
6.2.k		
6.2.l		

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 details on actions taken.

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

7 Support
7.1 Resources

Q1. Consider the following aspect relating to resources required Tick one box.

Aspect	YES	PARTIAL	NO
7.1. Is there a process in place and being used by the organization to determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system objectives determined in 6.2?			

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
7.1		

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 details on actions taken.

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

7. Support
7.2 Competence

Q1. Consider the following aspects relating to training and competence Tick one box.

Aspect	YES	PARTIAL	NO
7.2.a Is there a process in place and being used by the organization to determine the necessary competence of person(s) doing work under its control that affects its information security performance?			
7.2.b Is there a process in place and being used to ensure that these persons are competent on the basis of appropriate education, training, or experience?			
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?			
7.2.d Is appropriate documented information retained as evidence of competence?			

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
7.2.a		
7.2.b		
7.2.c		
7.2.d		

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 details on actions taken.

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

7. Support
7.3 Awareness

Q1. Consider the following aspects relating to awareness. Tick one box.

Aspect	YES	PARTIAL	NO
7.3.a Is there a process in place and being used by the organization to ensure persons doing work under the organization's control are aware of the information security policy?			
7.3.b Is there a process in place and being used by the organization to ensure persons doing work under the organization's control are aware of their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance?			
7.3.c Is there a process in place and being used by the organization to ensure persons doing work under the organization's control are aware of the implications of not conforming with the information security management system requirements?			

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
7.3.a		
7.3.b		
7.3.c		

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 details on actions taken.

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

7. Support
7.4 Communication

Q1. Consider the following aspects relating to training, awareness and competence Tick one box.

Aspect	YES	PARTIAL	NO
7.4.a Is there a process in place and being used by the organization to determine the need for internal and external communications relevant to the information security management system?			
7.4.b Has this process identified what to communicate?			
7.4.c Has this process identified when to communicate?			
7.4.d Has this process identified with whom to communicate?			
7.4.e Has this process identified who shall communicate?			
7.4.f Has this process identified the processes by which communication shall be effected?			

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
7.4.a		
7.4.b		
7.4.c		
7.4.d		
7.4.e		
7.4.f		

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 details on actions taken.

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

7. Support
7.5 Documented information
7.5.1 General

Q1. Consider the following aspects relating to the existence of ISMS documentation. Tick one box.

Aspect	YES	PARTIAL	NO
7.5.1.a Does the organization's information security management system include documented information required by ISO/IEC 27001:2013?			
7.5.1.b Does the organization's information security management system include documented information determined by the organization as being necessary for the effectiveness of the 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
7.5.1.a		
7.5.1.b		

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 details on actions taken.

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

7. Support
7.5 Documented information
7.5.2 Creating and updating

Q1. Consider the following aspects relating to creating and updating ISMS documentation. Tick one box.

Aspect	YES	PARTIAL	NO
7.5.2.a When creating and updating documented information, does the organization have in place a process to ensure appropriate identification and description (e.g. a title, date, author, or reference number)?			
7.5.2.b When creating and updating documented information, does the organization have in place a process to ensure appropriate format (e.g. language, software version, graphics) and media (e.g. paper, electronic)?			
7.5.2.c When creating and updating documented information, does the organization have in place a process to ensure appropriate review and approval for suitability and adequacy?			

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
7.5.2.a		
7.5.2.b		
7.5.2.c		

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 details on actions taken.

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

7 Support
7.5 Documented information
7.5.3 Control of documented information

Q1. Consider the following aspects relating to control of documented information. Tick one box.

Aspect	YES	PARTIAL	NO
7.5.3.a Does the organization have in place a process to control the documented information required by the information security management system and by ISO/IEC 27001:2013 to ensure it is available and suitable for use, where and when it is needed?			
7.5.3.b Does the organization have in place a process to control the documented information required by the information security management system and by ISO/IEC 27001:2013 to ensure it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)?			
7.5.3.c Does the organization have in place a process to control the documented information required by the information security management system and by ISO/IEC 27001:2013 to address, as applicable, its distribution, access, retrieval and use?			
7.5.3.d Does the organization have in place a process to control the documented information required by the information security management system and by ISO/IEC 27001:2013 to address, as applicable, its storage and preservation, including the preservation of legibility?			
7.5.3.e Does the organization have in place a process to control the documented information required by the information security management system and by ISO/IEC 27001:2013 to address, as applicable, the control of changes (e.g. version control)?			
7.5.3.f Does the organization have in place a process to control the documented information required by the information security management system and by ISO/IEC 27001:2013 to address, as applicable, its retention and disposition?			
7.5.3.g Does the organization have in place a process to identify as appropriate documented information of external origin that is determined by the organization to be necessary for the planning and operation of the information security management system?			
7.5.3.h Does the organization have in place a process to control documented information of external origin that is determined by the organization to be necessary for the			

Aspect	YES	PARTIAL	NO
planning and operation of the 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
7.5.3.a		
7.5.3.b		
7.5.3.c		
7.5.3.d		
7.5.3.e		
7.5.3.f		
7.5.3.g		
7.5.3.h		

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 details on actions taken.

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

8 Operations
8.1 Operational planning and control

Q1. Consider the following aspects relating to operational planning and control. Tick one box.

Aspect	YES	PARTIAL	NO
8.1.a Is there a process in place and being used by the organization to plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.			
8.1.b Has the organization implemented plans to achieve its information security objectives as determined in 6.2?			
8.1.c Does the organization keep documented information to the extent necessary to have confidence that the processes have been carried out as planned?			
8.1.d Does the organization control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary?			
8.1.e Does the organization ensure that outsourced processes are determined and controlled?			

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
8.1.a		
8.1.b		
8.1.c		
8.1.d		
8.1.e		

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 details on actions taken.

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

8 Operations
8.2 Information security risk management

Q1. Consider the following aspects relating to risk assessments. Tick one box.

Aspect	YES	PARTIAL	NO
8.2.a Is there a process in place and being used to perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a)?			
8.2.b Does the organization retain documented information of the results of the information security risk assessments?			

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
8.2.a		
8.2.b		

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 details on actions taken.

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

8. Operations
8.3 Information security risk treatment

Q1. Consider the following aspects relating to risk treatment. Tick one box.

Aspect	YES	PARTIAL	NO
8.3.a Is the organization implementing its information security risk treatment plan?			
8.3.b Does the organization retain documented information of the results of the information security risk treatment?			

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
8.3.a		
8.3.b		

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 details on actions taken.

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

9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation

Q1. Consider the following aspects relating to measurement of performance of the ISMS. Tick one box.

Aspect	YES	PARTIAL	NO
9.1.a Is there a process in place and being used to evaluate the information security performance and the effectiveness of the information security management system?			
9.1.b Does the process determine what needs to be monitored and measured, including information security processes and controls?			
9.1.c Does the process determine the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results?			
9.1.d Does the process determine when the monitoring and measuring shall be performed?			
9.1.e Does the process determine who shall monitor and measure?			
9.1.f Does the process determine when the results from monitoring and measurement shall be analysed and evaluated?			
9.1.g Does the process determine who shall analyse and evaluate these results?			
9.1.h Does the organization retain appropriate documented information as evidence of the monitoring and measurement results?			

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
9.1.a		
9.1.b		
9.1.c		
9.1.d		
9.1.e		
9.1.f		
9.1.g		
9.1.h		

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 details on actions taken.

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

9 Performance evaluation
9.2 Internal audit

Q1. Consider the following aspects relating to an internal ISMS audit function. Tick one box.

Aspect	YES	PARTIAL	NO
9.2.a Is there a process in place and being used to ensure that the organization conducts internal audits at planned intervals?			
9.2.b Do the internal audits provide information on whether the information security management system conforms to the organization's own requirements for its information security management system?			
9.2.c Do the internal audits provide information on whether the information security management system conforms to the requirements of ISO/IEC 27001:2013?			
9.2.d Do the internal audits provide information on whether the information security management system is effectively implemented and maintained?			
9.2.e Does the organization plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting?			
9.2.f Does the audit programme(s) take into consideration the importance of the processes concerned and the results of previous audits?			
9.2.g Does the organization define the audit criteria and scope for each audit?			
9.2.h Does the organization select auditors and conduct audits that ensure objectivity and the impartiality of the audit process?			
9.2.i Does the organization ensure that the results of the audits are reported to relevant management?			
9.2.j Does the organization retain documented information as evidence of the audit programme(s) and the audit results?			

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
9.2.a		
9.2.b		
9.2.c		
9.2.d		
9.2.e		
9.2.f		
9.2.g		
9.2.h		
9.2.i		
9.2.j		

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 details on actions taken.

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

9. Performance evaluation
9.3 Management review

Q1. Consider the following aspects relating to top management review of the ISMS. Tick one box.

Aspect	YES	PARTIAL	NO
9.3.a Is there a process in place and being used by top management to review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness?			
9.3.b Does the review include consideration of the status of actions from previous management reviews?			
9.3.c Does the review include consideration of changes in external and internal issues that are relevant to the information security management system?			
9.3.d Does the review include consideration of feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives?			
9.3.e Does the review include consideration of feedback from interested parties?			
9.3.f Does the review include consideration of results of risk assessment and status of risk treatment plan?			
9.3.g Do these reviews include consideration of opportunities for continual improvement?			
9.3.h Do the outputs of the management review include decisions related to continual improvement opportunities and any changes needed to the information security management system?			
9.3.i Does the organization retain documented information as evidence of the results of management reviews?			

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
9.3.a		
9.3.b		
9.3.c		
9.3.d		
9.3.e		
9.3.f		
9.3.g		
9.3.h		
9.3.i		

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 details on actions taken.

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

10 Improvement
10.1 Non-conformity and corrective action

Q1. Consider the following aspects relating to non-conformities and corrective action. Tick one box.

Aspect	YES	PARTIAL	NO
10.1.a Is there a process in place and being used by the organization to react to any nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences?			
10.1.b Is there a process in place and being used by the organization to evaluate the need for action to eliminate the causes of any nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur?			
10.1.c Is there a process in place and being used by the organization to implement any action needed?			
10.1.d Is there a process in place and being used by the organization to review the effectiveness of any corrective action taken?			
10.1.e Is there a process in place and being used by the organization to make changes to the information security management system, if necessary?			
10.1.f Is there a process in place and being used by the organization to ensure that corrective actions are appropriate to the effects of the nonconformities encountered?			
10.1.g Does the organization retain documented information as evidence of the nature of the nonconformities and any subsequent actions taken?			
10.1.h Does the organization retain documented information as evidence of the results of any corrective action?			

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
10.1.a		
10.1.b		
10.1.c		
10.1.d		
10.1.e		
10.1.f		
10.1.g		
10.1.h		

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

ISO/IEC 27001, *Information security management – Requirements*

10 Improvement
10.2 Continual improvement

Q1. Consider the following aspect relating to continual improvement. Tick one box.

Aspect	YES	PARTIAL	NO
10.2 Is there a process in place and being used to continually improve the suitability, adequacy and effectiveness of the 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
10.2		

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 details on actions taken.

5 Annex A Gap analysis workbook (assessment of ISMS controls)

The following questionnaires should be addressed to determine the extent to which the control requirements from Annex A of ISO/IEC 27001:2013 have been implemented within the ISMS. Guidance on completing the questionnaires can be found in Section 3.2 of this guide

Please note that exclusions to the following controls can only be made if these 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 exclusions of controls found to be necessary to satisfy the risk acceptance criteria need to be justified, and evidence needs to be provided to show that the associated risks have been accepted by those with sufficient management seniority within the organization who are accountable to the board, owner and shareholders for corporate decisions.

BIP 0073 (and ISO/IEC 27002: 2013) provides implementation guidance and further information regarding the control questions given in the tables below e.g. the control question for A.16.1.7 talks about evidence, and BIP 0073 and ISO/IEC 27002 provides some examples of this evidence.

NOTE The control guidance given in ISO/IEC 27002 is not mandatory, it is purely helpful guidance and so does not play any part in an ISO/IEC 27001: 2013 certification audit.

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

A.5 Information security policies
A.5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

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

Control requirement	YES	PARTIAL	NO
A.5.1.1 Is the information security policy document set defined, approved by management, published and communicated to all employees and relevant external parties?			
A.5.1.2 Are the information security policies reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.5.1.1		
A.5.1.2		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.6 Organization of information security
A.6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

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

Control requirement	YES	PARTIAL	NO
A.6.1.1 Are all information security responsibilities defined and allocated?			
A.6.1.2 Are areas of conflicting duties and areas of responsibility segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets?			
A.6.1.3 Are appropriate contacts with relevant authorities maintained?			
A.6.1.4 Are appropriate contacts with special interest groups or other specialist security forums and professional associations maintained?			
A.6.1.5 Is information security addressed in project management, regardless of the type of the project?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.6.1.1		
A.6.1.2		
A.6.1.3		
A.6.1.4		
A.6.1.5		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.6 Organization of information security
A.6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

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

Control requirement	YES	PARTIAL	NO
A.6.2.1 Have a policy and supporting security measures been adopted to manage the risks introduced by using mobile devices?			
A.6.2.2 Have a policy and supporting security measures been implemented to protect information accessed, processed or stored at teleworking sites?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.6.2.1		
A.6.2.2		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.7 Human resource security
A.7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

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

Control requirement	YES	PARTIAL	NO
A.7.1.1. Have background verification checks on all candidates for employment been carried out in accordance with relevant laws, regulations and ethics and are they proportional to the business requirements, the classification of the information to be accessed and the perceived risks?			
A.7.1.2. Do the contractual agreements with employees and contractors state their and the organization's responsibilities for information security?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.7.1.1		
A.7.1.2		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.7 Human resource security
A.7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

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

Control requirement	YES	PARTIAL	NO
A.7.2.1 Does management require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization?			
A.7.2.2 Do all employees of the organization and, where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function?			
A.7.2.3 Is there a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.7.2.1		
A.7.2.2		
A.7.2.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.7 Human resource security
A.7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

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

Control requirement	YES	PARTIAL	NO
A.7.3.1 Have information security responsibilities and duties that remain valid after termination or change of employment been defined, communicated to the employee or contractor and enforced?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.7.3.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.8 Asset management
A.8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

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

Control requirement	YES	PARTIAL	NO
A.8.1.1 Have assets associated with information and information processing facilities been identified, has an inventory of these assets been drawn up, and is it being maintained?			
A.8.1.2 Are all assets maintained in the inventory assigned owners?			
A.8.1.3 Have rules for the acceptable use of information and of assets associated with information and information processing facilities been identified, documented and implemented?			
A.8.1.4 Do all employees and external party users return all of the organizational assets in their possession upon termination of their employment, contract or agreement?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.8.1.1		
A.8.1.2		
A.8.1.3		
A.8.1.4		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.8 Asset management
A.8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

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

Control requirement	YES	PARTIAL	NO
A.8.2.1 Is information classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification?			
A.8.2.2 Has an appropriate set of procedures for information labelling been developed and implemented in accordance with the information classification scheme adopted by the organization?			
A.8.2.3 Are procedures for handling assets developed and implemented in accordance with the information classification scheme adopted by the organization?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.8.2.1		
A.8.2.2		
A.8.2.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.8 Asset management
A.8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media

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

Control requirement	YES	PARTIAL	NO
A.8.3.1 Have procedures been implemented for the management of removable media in accordance with the classification scheme adopted by the organization?			
A.8.3.2 Is media disposed of securely when no longer required, using formal procedures?			
A.8.3.3 Is media containing information protected against unauthorized access, misuse or corruption during transportation?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.8.3.1		
A.8.3.2		
A.8.3.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.9 Access control
A.9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

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

Control requirement	YES	PARTIAL	NO
A.9.1.1 Has an access control policy been established, documented and reviewed based on business and information security requirements?			
A.9.1.2 Have users only been provided with access to the network and network services that they have been specifically authorized to use?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.9.1.1		
A.9.1.2		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.9 Access control
A.9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

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

Control requirement	YES	PARTIAL	NO
A.9.2.1 Has a formal user registration and de-registration process been implemented to enable assignment of access rights?			
A.9.2.2 Has a formal user access provisioning process been implemented to assign or revoke access rights for all user types to all systems and services?			
A.9.2.3 Is the allocation and use of privileged access rights being restricted and controlled?			
A.9.2.4 Is the allocation of secret authentication information being controlled through a formal management process?			
A.9.2.5 Do asset owners review users' access rights at regular intervals?			
A.9.2.6 Are the access rights of all employees and external party users to information and information processing facilities being removed upon termination of their employment, contract or agreement, or adjusted upon change?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.9.2.1		
A.9.2.2		
A.9.2.3		
A.9.2.4		
A.9.2.5		
A.9.2.6		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.9 Access control
A.9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

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

Control requirement	YES	PARTIAL	NO
A.9.3.1 Are users required to follow the organization's practices in the use of secret authentication information?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.9.3.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.9 Access control
A.9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

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

Control requirement	YES	PARTIAL	NO
A.9.4.1 Is access to information and application system functions restricted in accordance with the access control policy?			
A.9.4.2 Where required by the access control policy, is access to systems and applications being controlled by a secure log-on procedure?			
A.9.4.3 Are password management systems interactive and do they ensure quality passwords?			
A.9.4.4 Is the use of utility programs that might be capable of overriding system and application controls restricted and tightly controlled?			
A.9.4.5.Is access to program source code restricted?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.9.4.1		
A.9.4.2		
A.9.4.3		
A.9.4.4		
A.9.4.5		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.10 Cryptography
A.10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

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

Control requirement	YES	PARTIAL	NO
A.10.1.1 Has a policy on the use of cryptographic controls for protection of information been developed and implemented?			
A.10.1.2 Has a policy on the use, protection and lifetime of cryptographic keys been developed and is it implemented through their whole life cycle?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.10.1.1		
A.10.1.2		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.11 Physical and environmental security
A.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

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

Control requirement	YES	PARTIAL	NO
A.11.1.1 Are security perimeters defined and used to protect areas that contain either sensitive or critical information and information processing facilities?			
A.11.1.2 Are secure areas protected by appropriate entry controls to ensure that only authorized personnel are allowed access?			
A.11.1.3 Has physical security for offices, rooms and facilities been designed and is it being applied?			
A.11.1.4 Has physical protection against natural disasters, malicious attack or accidents been designed and is it being applied?			
A.11.1.5 Have procedures for working in secure areas been designed and are they being applied?			
A.11.1.6 Are access points such as delivery and loading areas and other points where unauthorized persons could enter the premises controlled and, if possible, isolated from information processing facilities to avoid unauthorized access?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.11.1.1.		
A.11.1.2.		
A.11.1.3.		
A.11.1.4.		
A.11.1.5.		
A.11.1.6.		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.11 Physical and environmental security
A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

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

Control requirement	YES	PARTIAL	NO
A.11.2.1 Is equipment sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access?			
A.11.2.2 Is equipment being protected from power failures and other disruptions caused by failures in supporting utilities?			
A.11.2.3 Are power and telecommunications cabling carrying data or supporting information services being protected from interception, interference or damage?			
A.11.2.4 Is equipment being correctly maintained to ensure its continued availability and integrity?			
A.11.2.5 Is equipment, information or software not being taken off-site without prior authorization?			
A.11.2.6 Is security applied to off-site assets, taking into account the different risks of working outside the organization's premises?			
A.11.2.7 Are all items of equipment containing storage media being verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use?			
A.11.2.8 Do users ensure that unattended equipment has appropriate protection?			
A.11.2.9 Has a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities been adopted?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.11.2.1		
A.11.2.2		
A.11.2.3		
A.11.2.4		
A.11.2.5		
A.11.2.6		
A.11.2.7		
A.11.2.8		
A.11.2.9		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.12 Operations security
A.12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

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

Control requirement	YES	PARTIAL	NO
A.12.1.1 Are operating procedures documented and made available to all users who need them?			
A.12.1.2 Are changes to the organization, business processes, information processing facilities and systems that affect information security being controlled?			
A.12.1.3 Is the use of resources being monitored, tuned and are projections made of future capacity requirements to ensure the required system performance?			
A.12.1.4 Are development, testing, and operational environments separated to reduce the risks of unauthorized access or changes to the operational environment?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.12.1.1		
A.12.1.2		
A.12.1.3		
A.12.1.4		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.12 Operations security
A.12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

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

Control requirement	YES	PARTIAL	NO
A.12.2.1 Are detection, prevention and recovery controls to protect against malware implemented, combined with appropriate user awareness?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.12.2.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.12 Operations security
A.12.3 Backup

Objective: To protect against loss of data

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

Control requirement	YES	PARTIAL	NO
A.12.3.1 Are backup copies of information, software and system images being taken and tested regularly in accordance with an agreed backup policy?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.12.3.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.12 Operations security
A.12.4 Logging and monitoring

Objective: To record events and generate evidence

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

Control requirement	YES	PARTIAL	NO
A.12.4.1 Are event logs recording user activities, exceptions, faults and information security events being produced, kept and regularly reviewed?			
A.12.4.2 Are logging facilities and log information being protected against tampering and unauthorized access?			
A.12.4.3 Are system administrator and system operator activities being logged and the logs protected and regularly reviewed?			
A.12.4.4 Are the clocks of all relevant information processing systems within an organization or security domain being synchronized to a single reference time source?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.12.4.1		
A.12.4.2		
A.12.4.3		
A.12.4.4		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.12 Operations security
A.12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

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

Control requirement	YES	PARTIAL	NO
A.12.5.1 Are procedures implemented to control the installation of software on operational systems?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.12.5.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.12 Operations security
A.12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

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

Control requirement	YES	PARTIAL	NO
A.12.6.1 Is information about technical vulnerabilities of information systems being used being obtained in a timely fashion, is the organization's exposure to such vulnerabilities evaluated and are appropriate measures taken to address the associated risk?			
A.12.6.2 Are rules governing the installation of software by users established and implemented?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.12.6.1		
A.12.6.2		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.12 Operations security
A.12.7 Information systems audit considerations

Objective: To minimize the impact of audit activities on operational systems.

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

Control requirement	YES	PARTIAL	NO
A.12.7.1 Are audit requirements and activities involving verification of operational systems being carefully planned and agreed to minimize disruptions to business processes?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.12.7.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.13 Communications security
A.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

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

Control requirement	YES	PARTIAL	NO
A.13.1.1 Are networks being managed and controlled to protect information in systems and applications?			
A.13.1.2 Are security mechanisms, service levels and management requirements of all network services identified and included in network services agreements, whether these services are provided in-house or outsourced?			
A.13.1.3 Are groups of information services, users and information systems segregated on networks?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.13.1.1		
A.13.1.2		
A.13.1.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.13 Communications security
A.13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

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

Control requirement	YES	PARTIAL	NO
A.13.2.1 Are formal transfer policies, procedures and controls in place to protect the transfer of information through the use of all types of communication facilities?			
A.13.2.2 Are agreements in place to address the secure transfer of business information between the organization and external parties?			
A.13.2.3 Is information involved in electronic messaging being appropriately protected?			
A.13.2.4 Are requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information being identified, regularly reviewed and have they been documented?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.13.2.1		
A.13.2.2		
A.13.2.3		
A.13.2.4		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.14 System acquisition, development and maintenance
A.14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire life cycle This also includes the requirements for information systems, which provide services over public networks.

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

Control requirement	YES	PARTIAL	NO
A.14.1.1 Are information security related requirements included in the requirements for new information systems or enhancements to existing information? systems?			
A.14.1.2 Is information involved in application services passing over public networks being protected from fraudulent activity, contract dispute and unauthorized disclosure and modification?			
A.14.1.3 Is information involved in application service transactions being protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.14.1.1		
A.14.1.2		
A.14.1.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.14 System acquisition, development and maintenance
A.14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development life cycle of information systems.

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

Control requirement	YES	PARTIAL	NO
A.14.2.1 Are rules for the development of software and systems established and are they being applied to developments within the organization?			
A.14.2.2 Are changes to systems within the development life cycle being controlled by the use of formal change control procedures?			
A.14.2.3 When operating platforms are changed, are business critical applications reviewed and tested to ensure there is no adverse impact on organizational operations or security?			
A.14.2.4 Are modifications to software packages discouraged, limited to necessary changes and are all changes strictly controlled?			
A.14.2.5 Are principles for engineering secure systems being established, documented, maintained and applied to any information system implementation efforts?			
A.14.2.6 Does the organization establish and appropriately protect secure development environments for system development and integration efforts. Do these secure development environments cover the entire system development life cycle?			
A.14.2.7 Does the organization supervise and monitor the activity of outsourced system development?			
A.14.2.8 Is testing of security functionality being carried out during development?			
A.14.2.9 Are acceptance testing programs and related criteria being established for new information systems, upgrades and new versions?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.14.2.1		
A.14.2.2		
A.14.2.3		
A.14.2.4		
A.14.2.5		
A.14.2.6		
A.14.2.7		
A.14.2.8		
A.14.2.9		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.14 System acquisition, development and maintenance
A.14.3 Test data

Objective: To ensure the protection of data used for testing

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

Control requirement	YES	PARTIAL	NO
A.14.3.1 Is test data being selected carefully, protected and controlled?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.14.3.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.15 Supplier relationships
A.15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

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

Control requirement	YES	PARTIAL	NO
A.15.1.1 Have information security requirements for mitigating the risks associated with each supplier's access to the organization's assets been agreed with the supplier and documented?			
A.15.1.2 Have all relevant information security requirements been established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information?			
A.15.1.3 Do agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.15.1.1		
A.15.1.2		
A.15.1.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.15 Supplier relationships
A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

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

Control requirement	YES	PARTIAL	NO
A.15.2.1 Does the organization regularly monitor, review and audit supplier service delivery?			
A.15.2.2 Are changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, being managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.15.2.1		
A.15.2.2		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.16 Information security incident management
A.16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

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

Control requirement	YES	PARTIAL	NO
A.16.1.1 Have management responsibilities and procedures been established to ensure a quick, effective and orderly response to information security incidents?			
A.16.1.2 Are information security events being reported through appropriate management channels as quickly as possible?			
A.16.1.3 Are employees and contractors using the organization's information systems and services required to note and report any observed or suspected information security weaknesses in systems or services?			
A.16.1.4 Are information security events being assessed and is it being decided if they are to be classified as information security incidents?			
A.16.1.5 Are information security incidents being responded to in accordance with the documented procedures?			
A.16.1.6 Is the knowledge gained from analysing and resolving information security incidents being used to reduce the likelihood or impact of future incidents?			
A.16.1.7 Does the organization define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.16.1.1		
A.16.1.2		
A.16.1.3		
A.16.1.4		
A.16.1.5		
A.16.1.6		
A.16.1.7		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.17 Information security aspects of business continuity management
A.17.1 Information security continuity

Objective: Information security continuity shall be embedded in the organization's business continuity management systems.

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

Control requirement	YES	PARTIAL	NO
A.17.1.1 Has the organization determined its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster?			
A.17.1.2 Has the organization established, documented and implemented, and does it maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation?			
A.17.1.3 Does the organization verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.17.1.1		
A.17.1.2		
A.17.1.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.17 Information security aspects of business continuity management
A.17.2 Redundancies

Objective: To ensure availability of information processing facilities.

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

Control requirement	YES	PARTIAL	NO
A.17.2.1 Have information processing facilities been implemented with redundancy sufficient to meet availability requirements?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.17.2.1		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.18 Compliance
A.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

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

Control requirement	YES	PARTIAL	NO
A.18.1.1 Are all relevant legislative statutory, regulatory and contractual requirements and the organization's approach to meet these requirements, explicitly identified, documented and kept up to date for each information system and the organization?			
A.18.1.2 Are appropriate procedures implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products?			
A.18.1.3 Are records protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements?			
A.18.1.4 Is the privacy and protection of personally identifiable information ensured as required in relevant legislation and regulation where applicable?			
A.18.1.5 Are cryptographic controls used in compliance with all relevant agreements, legislation and regulations?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.18.1.1		
A.18.1.2		
A.18.1.3		
A.18.1.4		
A.18.1.5		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

A.18 Compliance
A.18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

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

Control requirement	YES	PARTIAL	NO
A.18.2.1 Is the organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) reviewed independently at planned intervals or when significant changes occur?			
A.18.2.2 Do managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements?			
A.18.2.3 Are information systems regularly reviewed for compliance with the organization's information security policies and standards?			

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

Control	Reasons and justification (with reference to supporting evidence)	Action to be taken
A.18.2.1		
A.18.2.2		
A.18.2.3		

COMMENTS: Enter a more detailed explanation of the reason(s) indicated above as appropriate. Where control measures are in place it may be helpful to provide details on actions taken. See Section 3.2 for details. Use additional sheets if necessary.

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

Second edition

This guide is based on the 2013 edition of the Information Security Management System standard, ISO/IEC 27001. It provides a means to help organizations assess their information security management system (ISMS) with respect to the requirements specified in ISO/IEC 27001 using the following gap analysis workbooks:

- An ISMS Process Workbook, which helps assess the current status of the organization's compliance with the requirements of ISO/IEC 27001;
- A Controls Workbook, which helps assess the current status of the organization's implementation of controls in comparison with the controls given in Annex A of ISO/IEC 27001.

It is intended primarily for use by organizations wishing to carry out an internal assessment of their ISMS against the requirements in the 2013 edition of ISO/IEC 27001 either as a precursor to an internal ISMS audit (which is required by ISO/IEC 27001) or in preparation for a formal third-party ISMS certification audit (see BIP 0071 for guidance).

It will help those organizations involved in certification audits that need to make the transition from the 2005 to the 2013 edition of ISO/IEC 27001 whether it be preparing for a formal third-party accredited certification, or for post-certification activities such as surveillance audits and for recertification.

It is essential reading for those organizations that already have a certified ISMS against the 2005 edition of ISO/IEC 27001 and will need to upgrade to the 2013 edition or those organizations that are about to embark on the process of certification.

About the authors

Edward Humphreys (Chartered Fellow of the BCS - FBCS CITP, CISM) is Director of XiSEC, a UK company providing Information Security Management consultancy services around the world. He has been an expert in the field of information security and risk management for just over 39 years. During this time he has worked for major international organizations as well as the European Commission and the OECD. He is convenor of the ISO/IEC working group responsible for the development and maintenance of the family of ISO/IEC 27001 ISMS standards. He was the editor of several of the earlier versions of the ISMS standards. He is the founder of the ISMS International User Group and in 2002 he was honoured with the Secure Computing Lifetime Achievement award for his achievements on the internationalization of the ISMS standards and ISMS certification. He teaches as a visiting professor at various universities around the world.

Bridget Kenyon (CISSP) is Head of Information Security for University College London. Her experience in information security started in 2000 with a role in network vulnerabilities at DERA, following which she has been a Qualified Security Assessor against PCI DSS, the Information Security Officer for Warwick University, and has held a variety of roles in consultancy and academia. She has been involved with ISO/IEC 27001 and its fellows since 2006, when she first joined BSI Panel 1, coordinating development of information security management system standards. She is editor for ISO/IEC 27013, and now chairs BSI Panel 1. She also chairs the Janet IG Working Group, which aims to provide higher educational input into the NHS's Information Governance Toolkit.

BSI order ref: BIP 0072

ISBN 978-0-580-82913-0

9 780580 829130

bsi.

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL
www.bsigroup.com