



ISO 27001:2005 - briefing note and transition requirements for IRCA ISMS auditors

Scope:

This document;

1. Explains the transition CPD requirements that you need to meet in order to maintain your IRCA Information Security Management auditor certification when conducting auditing to the new ISO/IEC 27001:2005 standard.
2. Outlines the broad implications of the ISO 27001:2005 standard for Information Security Management System auditors
3. Outlines a summary of the changes to be found in ISO 27001:2005 when compared with BS 7799-2:2002

Acknowledgements:

IRCA would like to thank Brian Henry, IRCA Information Security Management System Reviewing Officer who contributed to the development of this briefing note.

1. Transitioning your ISMS Auditor Certification

The publication of ISO 27001:2005 is an important milestone in the publication of requirements for an ISMS. We will require you (IRCA certificated ISMS auditors) to demonstrate that you have updated yourselves with the new standard and that you understand the implications of these changes in requirements in the context of your ISMS auditing activities.

The differences between the new standard ISO/IEC 27001:2005 and BS 7799-2:2002 are not challenging. Reverse compatibility and consistency with easy transition between the two standards has been kept in mind during the revision process. The differences between ISO/IEC 27001:2005 and BS 7799-2:2002 are mainly editorial and reformatting, and far less onerous than was the changes from the previous version BS 7799-2:1999.

It is however vital to keep in mind that it is virtually impossible to audit effectively against ISO/IEC 27001:2005 without a comprehensive knowledge and understanding of the corresponding ISO/IEC 17799:2005. This standard establishes guidelines and general principles and a code of practice for ISMS.

ISO/IEC 17799:2005 which was published in June 2005 has 17 additional sets of implementation advice and guidance on best practice, compared with the previous edition ISO/IEC 17799:2000. A small number of the old ones have been merged and/or deleted. In total there are now altogether 133 sets of implementation advice and guidance which correspond with the 39 control objectives and 133 controls specified in ISO 27001:2005 at Annex "A".

ISO/IEC 17799:2005 will not change its number in the short term. Arrangements are in hand to to allocate the number ISO/IEC 27002 in April 2007 but the text will remain unchanged.

Transition requirement for IRCA certificated ISMS auditors

All current IRCA certified ISMS auditors are required to complete at least **4 hours of continuing professional development (CPD) *before*** completing any acceptable audits to the new standard.

This is needed to enable ISMS auditors to be able to demonstrate their knowledge and understanding of the ISO/IEC 27001:2005 and ISO/IEC 17799:2005 standards (and referenced standards) in order to develop their auditing skills to audit against the requirements that are specified in ISO/IEC 17799:2005.

The evidence of CPD shall be submitted to IRCA on the CPD IRCA/173 verified logs together with IRCA/106 logs demonstrating audits conducted to the ISO/IEC 27001 standard.



ISO 27001:2005 - briefing note and transition requirements for IRCA ISMS auditors

The completed CPD form can normally be submitted with an application for re-grade or at renewal of certification.

When does this start?

We will accept transition CPD and audits to ISO/IEC 27001:2005 from 1 January 2006

What kind of CPD will IRCA accept?

We do not require ISMS auditors to complete a specific ISMS transition course as a means of CPD, and you may achieve this in a number of ways as is consistent with usual IRCA approach to CPD:

- Self-study, reading of the new standards and supporting documentation, publications.
- Reading (this briefing note and other relevant articles)
- On the job training
- In-house training and seminars with your company
- Attendance at relevant ISMS conferences, seminars and workshops
- Successful completion of an ISMS training course to the ISO/IEC 27001 standard.

IRCA will provide a list of ISO/IEC 27001:2005 events and seminars that are acceptable for CPD; this will not be an exhaustive list as other CPD is acceptable. These events are offered by IRCA approved training organizations and OEAs, but are not formally certified by IRCA and therefore do not fall under IRCA control even though we accept them for CPD along with other training events. You will find a list of such courses and events at our website www.irca.org as soon as they become available. Alternatively, IRCA can be contacted on Telephone No. + 44 (0) 0207 245 6833 for this information.

2. Introduction – implications of ISO 27001:2005 for auditors

The long awaited publication of ISO 27001:2005 which is based on BS 7799-2:2002 represents a major step forward in the international recognition and development of ISMS certification. The new standard was published on 15 October 2005 and as a consequence BS 7799-2:2002 has now been withdrawn and superseded.

The emergence of ISO 27001:2005 is expected to cause an explosion of interest by organizations looking to implement an ISMS and have this certified against the requirements of the new standard. This is expected to happen outside of the United Kingdom and Japan, which up until now has traditionally been the main areas of activity for ISMS, accredited certification.

At the present time there are almost 2000 ISMS certificates issued against BS 7799-2:2002 around the world and accreditation bodies are currently developing transition arrangements for conformity assessment bodies to convert these within a set time period to ISO 27001:2005. At the present time it looks like the deadline for this will be 31 October 2007.

For existing BS 7799-2:2002 certified organizations it looks like the assessment to ISO 27001:2005 will be handled through normal routine surveillance audits. New clients are currently being audited against ISO 27001:2005

Auditors should be aware that the publication of ISO 27001:2005 is only the first in the ISO/IEC 27000 series of standards. Many others are expected to be developed or are currently under way as follows:

ISO/IEC 27000 ISMS Principles and vocabulary



ISO 27001:2005 - briefing note and transition requirements for IRCA ISMS auditors

ISO/IEC 27002 ISMS Security techniques – code of practice (ISO/IEC 17799:2005)

ISO/IEC 27003 ISMS Implementation Guidelines

ISO/IEC 27004 ISMS Metrics and Measurements

ISO/IEC 27005 ISMS Risk Management

ISO/IEC 27006 ISMS Business Continuity & Disaster Recovery Services

It would seem that ISMS is going to develop into big business on a global scale over a wide range of businesses and industrial/commercial sectors. ISMS auditors will undoubtedly be faced in the immediate future with new opportunities and challenges and as a consequence will need to be suitably prepared to handle them.

3. ISO 27001:2005 requirements – General overview of the main changes

Below you will see the main requirements by clauses where changes have taken place together with any specific implications for auditors.

Forward and Introduction

No significant changes. ISO 27001:2005 still has the comprehensive introduction that was found in BS 7799-2:2002. Reference to the process approach is still maintained but with greater elaboration.

Still retains the important caveat that this standard is aligned with ISO 9001:2000 and ISO 14001:2004 and that this standard is designed to enable any organization to align or integrate its ISMS with related management system requirements.

Scope – Clause 1

Clarifies that this standard is applicable to all organizations. Addresses under Application the mandatory requirements in clauses 4-8 which cannot be excluded when claiming conformity to this standard

Normative references – Clause 2

Shows that ISO 27001:2005 is directly linked with ISO/IEC 17799:2005 for its application.

Terms and Definitions – Clause 3

Some definitions have been added and others modified or replaced to align with other standards such as ISO/IEC 13335-1:2004 and ISO/IEC TR 18044:2004. In addition some of the definitions have been modified and clarified to avoid misunderstanding.

General requirements – clause 4.1

The requirement has been clarified to include the activities of operate, monitor and review the documented ISMS.

Establishing and Monitoring the ISMS – clause 4.2

4.2.1 Establish the ISMS

- a) Define the scope - this requirement has been modified to ensure that the scope statement defines not only the scope but also the boundaries of the ISMS. The need for boundaries was always previously implied, but now it is clearly expressed and must include details and justification for any exclusions.



ISO 27001:2005 - briefing note and transition requirements for IRCA ISMS auditors

- b) Define the ISMS policy – very slight editorial changes in words - now modified to ensure that it “aligns with the organization’s strategic risk management context” making it clearer.
New “NOTE” added indicating that the ISMS policy is a subset of the Information Security Policy.

- c) Define the risk assessment approach of the organization - text has been restructured to provide an itemized list. Additional text makes it clear that the risk assessment selected shall produce comparable and reproducible results.
New “Note” added making reference to examples of risk assessment methodologies found in ISO/IEC TR 13335-3

- d) Identify the risks – text unchanged but footnote added clarifying the term “owner of assets.

- e) Analyse and evaluate the risks – was previously “assess the risks” - slight editorial changes with terms such as “business harm” now replaced with “business impact on the organization”.

- g) Select control objectives – text expanded to clarify that the selection and implementation of control objectives and controls is to meet the identified requirements that were identified by the risk assessment and risk treatment process. Further sentence requires that the selection will take account of the criteria for accepting risks as well as legal, regulatory and contractual requirements.
Extended requirements for selection of control objectives and controls and a revised “NOTE” added explaining the content and purpose of Annex A.

- h & i) Obtain management approval and authorization to implement and operate the ISMS – existing text restructured.

- j) Prepare a Statement of Applicability - existing text extended and reformatted into an itemized list to clarify that the Statement of Applicability shall include the existing control objectives and controls.
New “NOTE” added distinguishing that the Statement of Applicability provides a summary of decisions concerning risk treatment and justifying exclusions provides a cross check that no controls have been inadvertently omitted.

4.2.2 Implement and operate the ISMS

- a) Formulate a risk treatment plan – “resources” added to the list of appropriate management action.
- d) Define how to measure – additional to the requirements to implement and utilize the ISMS. Now required to define how to measure the effectiveness of controls or groups of controls and also how these measurements are to be used to assess control of effectiveness to produce comparable and reproducible results. New “NOTE” added that provides clarification that measuring the effectiveness of controls enables it to be determined how well controls achieve planned control objectives.
- f) Manage operations – ISMS added to provide useful clarification on which operations are to be managed
- g) Manage resources – ISMS added to provide useful clarification on which resources are to be managed



4.2.3 Monitor and Review the ISMS

- a) Execute monitoring procedures – Requires that the execution is extended from just monitoring but also now includes reviewing procedures. In subclause a) 2 the word “failed” as been replaced by “attempted” so as to ensure that all breaches and incidents are included.

Sub clause a) 4 was added to include the detection of security events and thereby prevent security incidents by the use of indicators. Subclause 5 is modified existing text to ensure that it shall be determined whether the actions taken to resolve a breach of security were effective.
- b) Undertake regular reviews – this requirement has been modified to include the results of effectiveness measurements in the regular reviews. Also the previous “security policy” now becomes “ISMS policy” as this impacts on the review of the ISMS.
- c) Measure the effectiveness of controls – this is in addition to the existing requirement to monitor and review the ISMS. Need now to measure the effectiveness of controls to verify that the security requirements have been met.
- d) Review risk assessments – text modified to include the review of risk assessment at planned intervals. Subclause d) 5 is an addition to the existing requirement to include the effectiveness of the implemented controls in the review. In subclause d) 6 the words “changed contractual obligations” was added.
- e) Conduct internal ISMS audits – no change to the text but reference given to the revamped title of Section 6. New “NOTE” added explaining what internal audits are and who conducts them.
- f) Undertake a Management Review – deleted reference to the frequency of at least once a year.
- g) Update security plans - new requirement

4.2.4 Maintain and Improve the ISMS

- c) Communicate the actions and improvements – text has been modified to move away from communicating results and extended to ensure that there is a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

Documentation requirements - clause 4.3

4.3.1 General

New introductory paragraphs give detailed explanation of what is expected and to include records of management decisions, and to ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible. Makes clear the importance of being able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

- a) Documented statements – revised to address the “ISMS policy and objectives” in place of the “security policy and control objectives”.
- b) The scope of the ISMS – deletes reference to “procedures and controls in support of the ISMS.”
- c) Inserts reference to “procedures and controls in support of the ISMS”.



ISO 27001:2005 - briefing note and transition requirements for IRCA ISMS auditors

- d) Description of the risk assessment methodology – provides clarification to ensure that a description of the risk assessment methodology is included within the documentation.
- g) Documented procedures – text expanded and clarified to take account of the requirement to describe how to measure the effectiveness of controls.

4.3.2 Control of Documents

- d) Ensure that relevant versions – changed from “most recent versions of relevant documents” to “relevant versions of applicable documents”.
- f) Ensure that documents are available – clarification to ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification

4.3.3 Control of Records

In the first paragraph the second sentence was changed into “They shall be protected and controlled”. The third sentence was expanded to also cover “regulatory requirements and contractual obligations”. The fifth sentence has been extended to require that controls shall be “documented and implemented”. The last sentence of this requirement in BS 7799-2:2002 has been deleted.

In the second paragraph the word “significant” was added in front of security incidents”.

Examples of what constitutes a record are now provided.

Management Responsibility – Clause 5

5.1 Management Commitment

- a) Establishing an ISMS – the expression “information security policy” was replaced by “ISMS policy” as the main focus here is the ISMS.
- b) Ensuring that ISMS – the expression “information security objectives” have been replaced with “ISMS objectives” as the main focus here is the ISMS
- e) Providing sufficient resources- the description of the ISMS activities has been aligned with the definition of the ISMS.
- f) Deciding the criteria – This requirement has been expanded to cover the decision on “criteria for accepting risks and for acceptable risk levels”.
- g) Ensuring that internal audits – This is a clarification and addition to the management commitment to ensure that internal ISMS audits are conducted. Includes a reference to the new Clause 6.



5.2 Resource Management

5.2.1 Provision of Resources

- a) Establish, implement, operate – extended to cover the whole range of activities related to an ISMS.

5.2.2 Training awareness and competence

- b) Providing training – text has been changed to take account of the possibility to take other actions e.g. employing competent personnel) this change was made to align with ISO 9001:2000.
- c) Evaluating the effectiveness – this has been reduced into “evaluating the effectiveness of the actions taken.”

Internal ISMS Audits – Clause 6

The previous subclause 6.4 in BS 7799-2:2002 was made a prime clause in ISO 27001:2005 and the text was moved across unchanged except where identified below:

Fourth paragraph – in the second sentence the expression “improvement activities” have been replaced with “follow-up activities”

A new NOTE has been added to refer to ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing.

Management Review of the ISMS – Clause 7

The clause numbering has been adjusted to take account of the insertion of the new Clause 6.

- 7.1 General – change of numbering – First paragraph – in the first sentence “at least once a year has been added after “intervals” (moved from clause 4.2.3 of BS 7799-2:2002).

Also the text modified where “security policy and security objectives” has been replaced with “information security policy and information security objectives” in order to clarify what is to be included in the review.

- 7.2 Review Input – change of numbering – sentence shortened to “The input to a management review shall include”

- 7.3 Review Output – change of numbering

- b) Update of the risk - clarification and expansion of text to update the risk assessment and risk treatment plan.
- c) Modifications of procedures – text extended to include “modifications of procedures and controls”
- c) 5 contractual obligations - clarification
- c) 6 levels of risk – text extended to include “levels of risk and/or risk acceptance criteria
- e) Improvements to how – clarification of text



ISO 27001:2005 - briefing note and transition requirements for IRCA ISMS auditors

ISMS Improvement – Clause 8

Clause numbering adjusted due to the introduction of the new Clause 6

8.1 Continual Improvement

First paragraph – “information” placed in front of “security objectives”.

8.2 Corrective Action

Clause numbering adjusted – text related to “associated with the implementation and operation of the ISMS” replaced with “with the ISMS requirements”

- a) identifying nonconformities – text shortened.

8.3 Preventive Action

First paragraph - clause numbering adjusted – text adjusted – “guard against future nonconformities” was replaced by “with the ISMS requirements”

- b) evaluating the need – new text

Second paragraph – new paragraph using the last bullet point from the previous list requiring that the organization shall identify changed risks and that the organization shall also identify preventive action requirements focusing attention on significantly changed risks

ANNEX A

Has been updated – control objectives and controls correspond with the guidance in ISO/IEC 17799: 2005

ANNEX B

The text of the Annex B in BS7799-2: 2002 has not been included and is intended to be used in the development of ISO/IEC 27003 ISMS Implementation Guidelines. The old table B.1 forms the ANNEX B in ISO/IEC 27001:2005. ISO/IEC 27003 ISMS Implementation Guidelines

ANNEX C

This has been updated to take account of the re-structuring and correspondence with ISO 9001:2000 and of course the re-structuring that was needed with ISO 14001:2004

ANNEX D

This Annex has been removed

Bibliography

This has been updated to reflect the latest standards and other publications

If you have any questions, please contact us as registration@irca.org.

For more information on IRCA ISMS Auditor certification, visit www.irca.org.

**Subscribe to our free auditing magazine, *IRCA INform*,
by email at registration@irca.org or at www.irca.org.**