



ISMS & 17799 REVISIONS BRIEFING

A number of significant changes to the range of information security management standards are planned over the course of the next few years. The first of these changes took place in June 2005.

This fourth free IT Governance ISMS Revisions Briefing provides its subscribers with an updates on planned changes, with information that enables subscribers to better manage their strategic standards-related activity. New versions are automatically sent to all subscribers to our regular newsletter, [24743](#).

FAQs

1 November 2005

1. What does 'ISMS' stand for?.....	2
2. What are the ISMS standards?	2
3. What is the difference between a 'specification' and a 'code of practice'? 2	
4. Can ISO/IEC 17799 be used as the basis for certification?	2
5. What changes are planned to these standards?	2
6. Were ISO/IEC 17799:2005 and BS 7799-2:2002 still aligned?	3
7. What will replace BS 7799-2:2002?	3
8. So, does that mean that the British version of the ISMS standard has now disappeared?.....	3
9. What differences are there between ISO/IEC 27001 and BS 7799-2:2002? ..	
10. What are those changes in detail?	3
11. What are the requirements around metrics?	4
12. How can I see what's in ISO/IEC 27001?	4
13. What is the relationship between ISO/IEC 27001 and ISO/IEC 17799? 4	
14. How will certification bodies handle transition from BS 7799-2:2002 to ISO/IEC 27001?	4
15. We are certified against BS7799-2:2002. What does the issue of ISO/IEC 27001 mean for us?	4
16. If my sector scheme or national standard hasn't yet updated, how do I use ISO/IEC 17799:2005 in my ISMS project?	5
17. Are there plans for other standards related to ISO 27001?.....	5
18. What has changed in ISO/IEC 17799:2005?	5
19. Where can I purchase a copy of ISO/IEC 17799:2005?	6
20. What are the changes to the chapter structure?	6
21. What do those changes look like in detail?	6
22. What are the changes to the controls?	7
23. How can I find out what the detailed changes to the controls are?.....	7
24. I have some more questions. How can I get answers?	8

FREQUENTLY ASKED QUESTIONS

1. What does 'ISMS' stand for?

'ISMS' is the acronym for 'Information Security Management System'

2. What are the ISMS standards?

In May 2005, there were two related standards:

- a. ISO/IEC 17799:2000, which was an international Code of Practice for Information Security Management and which carries national numbers (but is exactly the same standard) such as BS 7799-1:2000 or AS/NZS ISO/IEC 17799:2001
- b. BS 7799-2:2002, which is the specification for an ISMS, and which carries national numbers (but is exactly the same standard) elsewhere, such as AS/NZS 7799.2.2003

3. What is the difference between a 'specification' and a 'code of practice'?

- A specification contains the word 'shall' and specifies what is mandatory for a system if it is to comply with the standard. It sets out 'how' an ISMS should be designed, not what should be in. Accredited certification takes place against a requirements specification.
- A Code of Practice provides guidance and uses words like 'should' to indicate that compliance is not mandatory. It sets out what should be in an ISMS, rather than how it should be designed. Organizations can choose controls from this code of practice or anywhere else, provided the requirements of the specification are met.

4. Can ISO/IEC 17799 be used as the basis for certification?

No. As ISO/IEC 17799:2005 is a Code of Practice, not a specification, it cannot be used as the basis for certification of an ISMS. Any organization that wishes to have its ISMS externally certified should use ISO/IEC 27001:2005 in conjunction with ISO/IEC 17799:2005.

5. What changes are planned to these standards?

- a. On 15 June 2005, ISO/IEC 17799:2000 (and BS 7799-1:2000) was withdrawn and replaced by ISO/IEC 17799:2005 (BS 7799-1:2005). Copies of [ISO/IEC 17799:2005](http://www.itgovernance.co.uk/catalog/6) can be purchased from IT Governance (www.itgovernance.co.uk/catalog/6).
- b. BS 7799-2:2002 continued in force as the standard against which an ISMS was assessed until it was replaced in November 2005

6. Were ISO/IEC 17799:2005 and BS 7799-2:2002 still aligned?

No, they were not. Whereas the control numbering in Annex A of BS 7799-2:2002 was precisely aligned with the control numbering of ISO17799:2000, that was no longer the case with ISO/IEC 17799:2005. The controls in ISO/IEC 17799 have been substantially re-structured. It had been planned to issue an updated version of BS7799-2, in which Annex A would have been aligned with the new ISO/IEC 17799, but that project was shelved in favour of proceeding straight to a full scale replacement of BS 7799-2:2002. Many sector schemes are still aligned with BS7799-2, and the misalignment with ISO/IEC 17799:2005 will continue until every sector scheme is updated to ISO 27001

7. What will replace BS 7799-2:2002?

A new international standard, ISO/IEC 27001:2005 (BS 7799-2:2005), has replaced BS 7799-2:2002 with effect from October 2005. At this point, BS 7799-2:2002 is withdrawn. It is not yet clear that Australia's AS/NZS7799.2:2003 or other local versions of BS7799-2:2002 will be withdrawn and replaced at the same time.

8. So, does that mean that the British version of the ISMS standard has now disappeared?

Not at all. In the United Kingdom, ISO/IEC 27001:2005 has the alternative numbering of BS7799-2:2005 and it will continue to be dual numbered for the foreseeable future.

9. What are the differences between ISO/IEC 27001 and BS 7799-2:2002?

According to ISO/IEC JTC1/SC27 – the standards committee at the International Standards Organization that deals with information security – the differences ‘are not challenging’. ‘Backwards compatibility, consistency and easy transition between the two standards have been kept in mind during the revision process.’

10. What are those changes in detail?

FDIS ISO/IEC 27001:2005 had a table at the front of the document that set out the exact changes between the FDIS and BS7799-2:2002. With the publication of the final version of ISO/IEC 27001, the FDIS has been withdrawn and, consequently, the only option today for identifying in detail the changes between the two standards is to use a tool such as the ISMS converter (available online from www.itgovernance.co.uk/products/153). There are changes in every section of the standard, ranging from changes in numbering (of which there are only a few) to more detailed changes in the wording of clauses. These include further clarification of requirements around risk assessment, around management commitment, measurement, and around continuous improvement. Every organization with a current BS7799-2:2002 ISMS, or that has an ISMS

project underway, now needs to purchase and review a copy of ISO/IEC 27001 itself and ensure that the project is in line with the new standard.

The biggest change between BS7799-2:2002 and ISO/IEC 27001:2005 is, of course, in the controls annex. The new Annex A is precisely aligned with ISO/IEC 17799:2005 and, therefore, every organization that currently has a certified (or conforming) ISMS will need to make major revisions to its Statement of Applicability in order to bring it into line with the new requirements.

11. What are the requirements around metrics?

BS7799-2 has always expected organizations to use measurement as part of its mechanism for continuous improvement, borrowing from the world of capability maturity models the notion that measurement of the effectiveness of what has been implemented enables one to plan and execute specific, measurable improvements. While this ambition is strongly within ISO/IEC 27001, measurement and metrics for use within an ISMS are still in their infancy and every organization will have to develop an appropriate solution that meets its own requirements.

12. How can I see what's in ISO/IEC 27001?

Purchase a copy of ISO/IEC 27001. You can order copies of [ISO/IEC 27001](#) from IT Governance Ltd (www.itgovernance.co.uk/catalog/6). If you previously purchased FDIS 27001, you get a **free upgrade** to the final published version of the standard, and this is sent out automatically. A special [reduced price kit](#) containing both ISO/IEC 27001 and ISO/IEC 17799:2005 is also available.

13. What is the relationship between ISO/IEC 27001 and ISO/IEC 17799?

ISO/IEC 27001 contains an Annex A (as did BS 7799-2:2002) which references the controls in ISO/IEC 17799:2005. In other words, ISO/IEC 17799:2005 continues to be the essential underpinning standard for ISO/IEC 27001, and clause 2 of ISO/IEC 27001 says that ISO/IEC 17799:2005 is “indispensable for the application of” ISO/IEC 27001.

14. How will certification bodies handle transition from BS 7799-2:2002 to ISO/IEC 27001?

Now that ISO/IEC 27001 has replaced BS 7799-2:2002, all future accreditations and re-certifications will be against ISO/IEC 27001. National accreditation bodies (eg UKAS) issue *Certification Transition Statements* that set out the way in which the transition is handled. .

15. We are certified against BS7799-2:2002. What does the issue of ISO/IEC 27001 mean for us?

It means that, over a period of time (18 months is a typical example) you will have to bring your ISMS into line with the requirements of ISO/IEC 27001. Your national accreditation body's *Certification Transition Statement* should describe the transitional arrangements for already-certified organizations. Practically, you should treat your transition plan as part of the continuous improvement component of your ISMS.

16. If my sector scheme or national standard hasn't yet updated, how do I use ISO/IEC 17799:2005 in my ISMS project?

If you are intending to achieve certification to a sector or national version of BS7799-2:2002 that hasn't yet transitioned to ISO/IEC 27001:2005, your Statement of Applicability will still have to meet the requirements of Annex A of BS 7799-2:2002. Each of the controls, as set out in the Annex, must be applied, partially applied or not applied at all. You cannot look to ISO/IEC 17799:2000 for guidance on these controls, because this standard has been withdrawn. Therefore, you look to the new standard, ISO/IEC 17799:2005 for guidance on how to apply each of the controls that you have selected in your Statement of Applicability.

Remember that you are not limited, by BS 7799-2:2002 to ONLY applying the controls in Annex A; you are expected to apply the controls that your organization identifies, through a risk assessment, as being required. You can, therefore, include some of the new controls that are in ISO/IEC 17799:2005 (eg vulnerability management) in your Statement of Applicability.

This is what we have done in the model Statement of Applicability included in the BS7799-2:2002 versions of our unique [7799 Documentation Toolkits](#).

17. Are there plans for other standards related to ISO 27001?

The International Standards Organization is launching a series of information security standards, modelled on the ISO 9000 series concept.

- a. ISO/IEC 27001 is titled 'Information Security Management System – Requirements'
- b. ISO/IEC 27002, which is planned for April 2007, will replace ISO/IEC 17799:2005
- c. ISO/IEC 27004, for which there is not yet a launch date, has the provisional title 'Information Security Metrics and Measurement'.
- d. Other proposals are under consideration, including the possibility of an 'ISMS Implementation Guidance' standard.

18. What has changed in ISO/IEC 17799:2005?

There have been a number of significant changes to ISO/IEC 17799.

- a. There are 17 new controls, and a number of other controls have been deleted or merged, with the result that the total number of controls has increased to 134.

- b. The chapter structure has changed. Three new chapters have been introduced.
- c. There have been significant changes to the layout of controls and to wording throughout the standard.

19. Where can I purchase a copy of ISO/IEC 17799:2005?

You can order copies of [ISO/IEC 17799:2005](#) from IT Governance Ltd (www.itgovernance.co.uk/catalog/6). A special [reduced price kit](#) containing both ISO/IEC 27001:2005 and ISO/IEC 17799:2005 is also available.

20. What are the changes to the chapter structure?

- a. One new chapter explains the structure of the standard, and has no real impact on deployment of the ISMS.
- b. ‘Assessing security risks’ is taken from the Introduction to the ISO/IEC 17799:2000 and becomes the second of the three new chapters in ISO/IEC 17799:2005. This is important because the ISO/IEC 17799:2005 expressly requires that selection of control objectives and controls be made in the light of (a) risk assessment(s)
- c. All the clauses around information security incident management are now consolidated into the third of the new chapters.

21. What do those changes look like in detail?

The chapter structure in ISO/IEC 17799:2005 is as set out in the comparative table (drawn from our [ISMS Conversion Tool](#)) set out on the next page:

<u>ISO 17799:2000</u>	<u>ISO 17799:2005</u>
<ol style="list-style-type: none"> 1. Scope 2. Terms and definitions 3. Security policy 4. Organizational security 5. Asset classification and control 6. Personnel security 7. Physical and environmental security 8. Communications and operations management 9. Access control 10. Systems development and maintenance 11. Business continuity management 12. Compliance 	<ol style="list-style-type: none"> 1. Scope 2. Terms and definitions 3. Structure of the standard 4. Risk assessment and treatment 5. Security policy 6. Organizing information security 7. Asset management 8. Human resources security 9. Physical and environmental security 10. Communications and operations management 11. Access control 12. Information systems acquisition, development and maintenance 13. Information security incident management 14. Business continuity management 15. Compliance

22. What are the changes to the controls?

- a. The way in which controls are laid out has been changed; each control now consists of:
 - i. A control statement, which describes (in the context of the control objective) what the control is for;
 - ii. Implementation guidance, which is detailed guidance which may (or may not) help individual organizations implement the control;
 - iii. Other information that needs to be considered.
- b. 36 Control areas and controls have been either deleted or re-structured and moved to somewhere else in the standard.
- c. 46 New control areas and controls added, which includes those that were deleted from elsewhere in the standard, re-structured and re-inserted.
- d. There has been a net increase in the total number of controls of seven, from 127 in ISO/IEC 17799:2000 to 134 in ISO/IEC 17799:2005

23. How can I find out what the detailed changes to the controls are?

The best way to do this is to purchase a copy of ISO/IEC 17799:2005. It is also essential to refer to the standard if you have an existing ISMS project.

An alternative approach, which also provides a detailed side by side comparison of new and old controls, is to purchase an **[ISMS conversion tool](#)**, such as the one available from IT Governance Ltd (www.itgovernance.co.uk/catalog/1).

24. I have some more questions. How can I get answers?

E-Mail servicecentre@itgovernance.co.uk and we will answer any further questions you have, and we will update these FAQs as and when appropriate.

Subscription details:

Readers can subscribe to **24743**, our regular newsletter service – which brings regular updates on ISMS and 17799 changes – on the IT Governance Ltd website at www.itgovernance.co.uk/page/bs7799

IT Governance Ltd is an official international BSI distributor. Copies of all information security management standards and related documents and tools can be purchased from www.itgovernance.co.uk. It is also an official distributor for The Stationery Office (TSO), and a full range of ITIL, PRINCE2 and other Office of Government Commerce publications can also be purchased from the website.

IT Governance also publishes a wide range of books and tools for IT governance and information security. In the context of implementing an ISMS to ISO/IEC 27001, the three books most worth referring to are:

[IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799](#)

[The Case for ISO 27001](#)

[Nine Steps to Success: an ISO 27001 Implementation Overview](#)