



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 is taking place in June 2005.

This second 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

23 June 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	2
4. What changes are planned to these standards?	2
5. Are ISO/IEC 17799:2005 and BS 7799-2:2002 still aligned?.....	2
6. What will replace BS 7799-2:2002?	3
7. What differences will there be between ISO/IEC 27001 and BS 7799-2:2002?	3
8. How can I see what's in ISO/IEC 27001?	3
9. What will be the relationship between ISO/IEC 27001 and ISO/IEC 17799?.....	3
10. How will certification bodies handle transition from BS 7799-2:2002 to ISO/IEC 27001?	3
11. In the meantime, how do I use ISO/IEC 17799:2005 in my ISMS project?	3
12. Are there plans for other standards related to ISO 27001?.....	4
13. What has changed in ISO/IEC 17799:2005?	4
14. Where can I purchase a copy of ISO/IEC 17799:2005?	4
15. What are the changes to the chapter structure?	5
16. What do those changes look like in detail?	5
17. What are the changes to the controls?	5
18. How can I find out what the detailed changes to the controls are?.....	6
19. I have some more questions. How can I get answers?	6

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. 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 will continue in force as the standard against which an ISMS is assessed until it is replaced in November 2005

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

No, they are not. Whereas the control numbering in Annex A of BS 7799-2:2002 was precisely aligned with the control numbering of ISO17799:2000, that is no longer the case. 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 has been shelved in favour of proceeding straight to a full scale replacement of BS 7799-2:2002.

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

A new international standard, ISO/IEC 27001:2005 (BS 7799-2:2005), will replace BS 7799-2:2002 with effect from (about) November 2005. At that point, BS 7799-2:2002 will be withdrawn. It is not yet clear that Australia's AS/NZS7799.2:2003 will be withdrawn and replaced at the same time.

7. What differences will there be 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 ‘will not be challenging’. ‘Backwards compatibility, consistency and easy transition between the two standards have been kept in mind during the revision process’.

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

Purchase a copy of the FDIS (Final Draft International Standard) for ISO/IEC 27001 for delivery as soon as it's published at the end of June 2005. You can order copies of [FDIS ISO/IEC 27001](http://www.itgovernance.co.uk/catalog/6) from IT Governance Ltd (www.itgovernance.co.uk/catalog/6). When you purchase FDIS 27001, you get a *free upgrade* to the final published version of the standard when it is available in November 2005. A special [reduced price kit](#) containing both FDIS 27001 and ISO/IEC 17799:2005 will also be available at the end of June 2005.

9. What will be the relationship between ISO/IEC 27001 and ISO/IEC 17799?

ISO/IEC 27001 will contain an Annex A (in line with BS 7799-2:2002) which will reference the controls in ISO/IEC 17799:2005. In other words, ISO/IEC 17799:2005 will continue to be the essential underpinning standard for ISO/IEC 27001.

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

Once 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) will issue *Certification Transition Statements* that will set out the way in which the transition will be handled. It is expected that these statements will be issued prior to the issue of ISO/IEC 27001.

11. In the meantime, how do I use ISO/IEC 17799:2005 in my ISMS project?

If you are intending to achieve certification prior to publication of ISO/IEC 27001:2005 in November, 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 our documentation toolkit.

12. 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 will be 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.

13. 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.

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

You can order copies of [ISO/IEC 17799:2005](http://www.iso.org/iso/17799.html) from IT Governance Ltd (www.itgovernance.co.uk/catalog/6)

15. 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.

16. What do those changes look like in detail?

The chapter structure in ISO/IEC 17799:2005 is as set out in the comparative table below:

<u>ISO 17799:2000</u>	<u>ISO 17799:2005</u>
1. Scope	1. Scope
2. Terms and definitions	2. Terms and definitions
	3. Structure of the standard
3. Security policy	4. Risk assessment and treatment
4. Organizational security	5. Security policy
	6. Organizing information security
5. Asset classification and control	7. Asset management
6. Personnel security	8. Human resources security
7. Physical and environmental security	9. Physical and environmental security
8. Communications and operations management	10. Communications and operations management
9. Access control	11. Access control
10. Systems development and maintenance	12. Information systems acquisition, development and maintenance
	13. Information security incident management
11. Business continuity management	14. Business continuity management
12. Compliance	15. Compliance

17. 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

18. 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).

19. 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.