

Information Security Management Systems (ISMS)

Overview

The standard effectively comes in two parts:

- ISO/IEC 17799:2000 (Part 1) is the standard code of practice and can be regarded as a comprehensive catalogue of good security things to do.
- BS7799-2:1999 (Part 2) is a standard specification for an Information Security Management Systems (ISMS). An ISMS is the means by which Senior Management monitor and control their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer and legal requirements.

Please note that certification is against BS7799-2:1999.

Part 1: The Code of Practice

ISO/IEC 17799:2000 defines 127 security controls structured under 10 major headings to enable readers to identify the particular safeguards that are appropriate to their particular business or specific area of responsibility. These security controls contain further detailed controls bringing the overall number somewhere in the region of 500+ controls and elements of best practice.

The standard stresses the importance of *risk management* and makes it clear that you do not have to implement every single guideline; only those that are relevant. The scope of the standard covers all forms of information, including voice and graphics, and media such as mobile phones and fax machines. The new standard recognizes new ways of doing business, such as e-commerce, the Internet, outsourcing, tele-working and mobile computing.

Part 2: The Management Standard

BS7799-2:1999 instructs you how to apply ISO/IEC 17799 and how to build an ISMS. It defines a six step process, see Figure 1.

Information Policy

It invites you to stand back and think about all of your information assets and their value to your organization. You ought then to devise a *policy* that identifies what information is important and why. From a practical point of view, it is only that information with some significant value that should be of concern.

Scope

Excluding low value information allows you to define the *scope* of your management concerns. You may discover that your concerns pervade your organization as a whole. In this case you will need to regard all of your information systems and their external interfaces -IT and electronic forms of communication, filing cabinets, telephone conversations, public relations and so on, as being in scope. Alternatively, your concerns may focus onto a particular customer-facing system. For example, an interesting extreme is the application of BS7799-2:1999 to the development, manufacture and delivery of a security product.

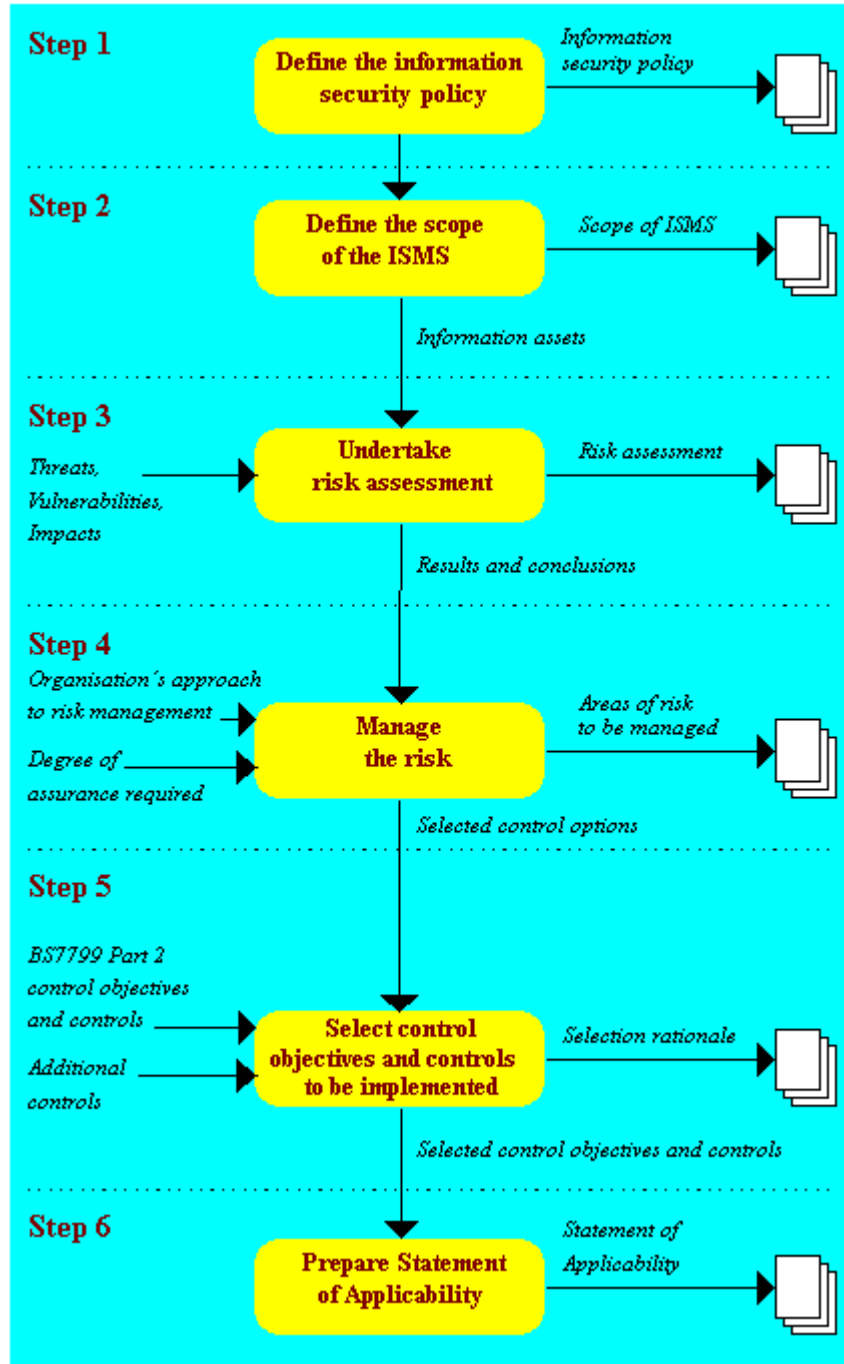


Figure 1 - The major steps towards BS7799-2 compliance

Risk assessment

Now you know what information is in scope and what its value is, your next move should be to determine the risk of losing that value.

Remember to consider everything. At one extreme you need to consider the complexities of technology; at the other you need to consider business forces in terms of advancing technology and enterprise, as well as the ugly side of industrial espionage and information warfare.

Risk management

You then need to decide how to manage that risk. Your forces certainly include technology, but don't forget people, administrative procedures and physical things like doors and locks and even CCTV. Don't forget insurance. If you can't prevent something from happening, maybe you can discover if it does happen and do something to contain it or otherwise reduce the danger. In the end, you will of course, need an effective continuity plan.

Choose your safeguards

You will then need to choose your "safeguards", i.e. the ways you have selected to manage the risk. BS7799-2:1999 lists a wide variety of such measures, but the list is not exhaustive and you are free to identify additional measures as you please. The list is drawn 1:1 from ISO/IEC 17799:2000.

Statement of applicability

You are required to identify all of your chosen security controls and justify why you feel they are appropriate, and show why those BS7799 controls that have not been chosen are not relevant. Clearly you could decline every BS7799 offering and invent your own. This is not a problem - it *is* allowed. However, you need to justify it - as much for your own benefit as anyone else's.

The Information Security Management System (ISMS)

The standard requires you to set up an Information Security Management System (ISMS) to make this happen. You should really, of course, set this up in the first place, but standards don't tell you how to do things, merely what you should achieve. [Click here](#) [offsite link] for our ideas.

Certification schemes

Certification schemes are being established in many parts of the world. It is therefore useful to reveal who the players are and what is going on. Have a look at Figure 2.

The European co-operation for Accreditation document EA7/03 provides guidance to National Accreditation Bodies for the accreditation of Certification Bodies wishing to assess ISMSs, e.g. against BS7799-2:1999. The various National Accreditation Bodies around the world operate a "mutual recognition" process that allows certificates awarded in one country to be accepted by the Accreditation Body of another.

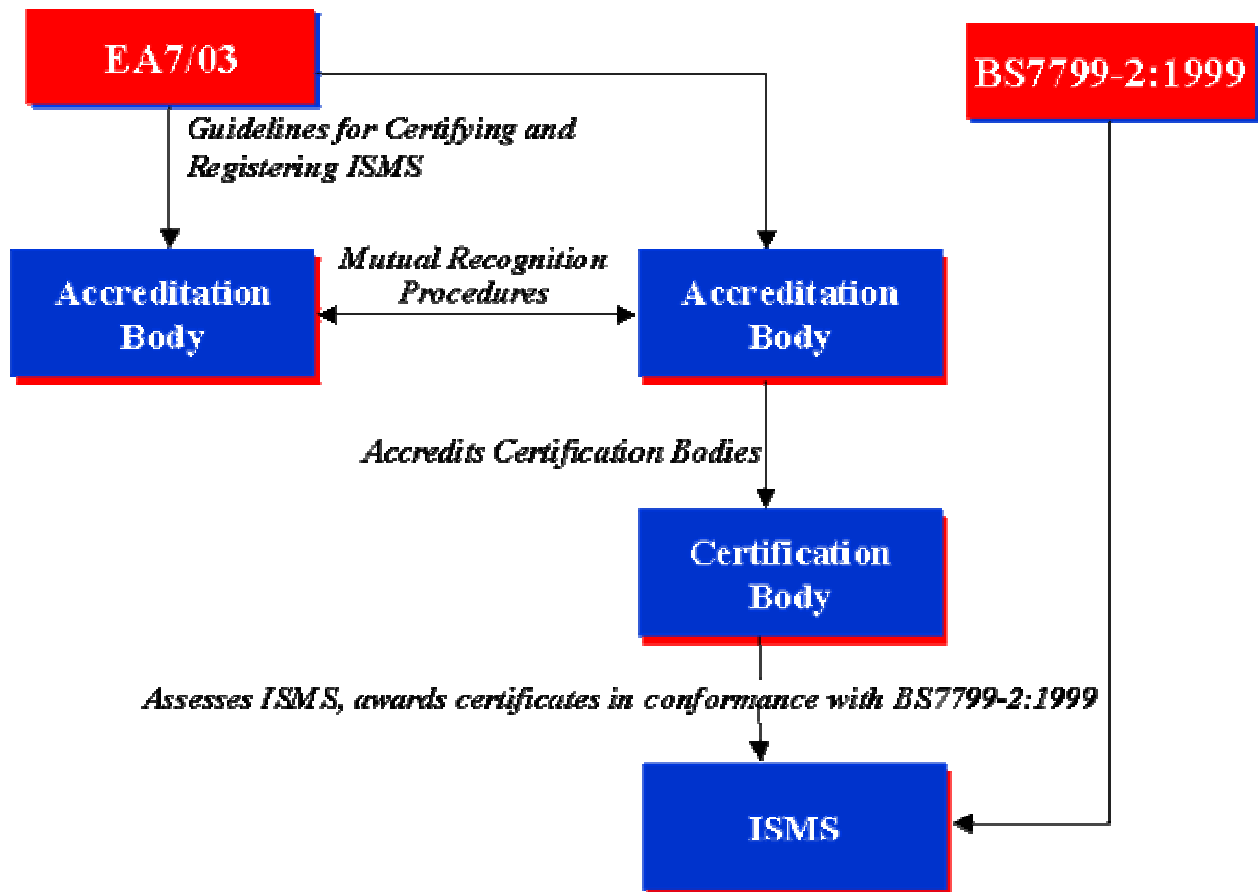


Figure 2: Relationship between scheme players

In order to be awarded a certificate, your ISMS will be audited by a BS7799 *assessor*. The assessor cannot also be a consultant. There are very strict rules about this. The assessor will work for a *Certification Body* (such as BSI Assessment Services Limited and Det Norske Veritas).

The Certification Body will award you the certificate. The certificate will document the *scope* of your ISMS and other relevant details, such as the *statement of applicability*. Only Certification Bodies that have been duly accredited by a National Accreditation Body can issue certificates.

The assessor will return periodically to check that your ISMS is working as intended.

Other Useful Documentation

BSI has published a useful set of supporting documentation to help apply ISO/IEC 17799:2000 and BS7799-2:1999. They are:

- Information Security Management: An Introduction (PD3000)
- Preparing for BS7799 Certification (PD3001)
- Guide to BS7799 Risk Assessment and Risk Management (PD3002)
- Are you ready for a BS7799 Audit? (PD3003)
- Guide to BS7799 Auditing (PD3004).
- Selecting BS7799 Controls (PD3005).

PD3000 provides an overview of the scheme for accredited certification and forms a useful a preface to other guidance documents in the scheme.

PD3001 provides guidance to users of BS7799 and gives detailed information in readiness for assessment against the Accredited Certification Scheme. It offers industry accepted best practice methods for providing and demonstrating the evidence required by an assessment auditor.

The guide to BS7799 Risk Assessment and Risk Management (PD3002) describes the underlying concepts behind BS7799 risk assessment and risk management, including the terminology and the overall process of assessing and managing risks. It is based on the ISO/IEC Guidelines for the Management of IT Security (GMITS).

Are you ready for a BS7799 Audit? (PD3003) is a pre-certification assessment workbook for organizations to assess and record the extent of their compliance with the control requirements in BS7799: Part 2 and to aid in their preparations for a certification audit.

This is a useful starting point for anyone considering BS7799 for the first time. Merely complete the workbook, answering “Yes”, “No” or “Partly”, and explain why. The completed workbook can also serve as your Statement of Applicability.

The guide to BS7799 Auditing (PD3004) provides general information and guidance on auditing ISMSs. It was effectively the BS7799 "audit methodology" for BS7799:1995. Although recently updated for BS7799:1999 Part 1, it probably has the wrong focus now, as it should perhaps concentrate on the management of the ISMS which it does not.