

The essence of BS 7799 is that a sound Information Security Management System (ISMS) should be established within organisations. The purpose of this is to ensure that an organisation's information is secure and properly managed.

## CONTENTS

BENEFITS OF USING BS 7799  
UNDERSTANDING BS 7799 PART 1: 10 STEPS  
CERTIFICATION  
CHECKLIST  
FURTHER HELP AND ADVICE

## INTRODUCTION

BS 7799 is the most influential, globally recognised standard for information security management.

BS 7799 Part 1 became an international standard (ISO/IEC 17799) in December 2000. It has recently been revised in line with ISO procedures and the revised standard should be BS 7799 available during 2005. BS 7799 Part 2, although still a UK standard, has been published as a national standard in many countries and is now itself at an advanced stage of the process towards international status. It is expected that this process will be complete by late 2005.

The standard is currently divided into two parts:

- Part 1. Contains guidance and explanatory information
- Part 2. Provides a model that can be used by businesses to set up and run an effective Information Security Management System (ISMS)

The two parts are currently published as:

- ISO/IEC 17799 Code of Practice for Information Security
- BS 7799-2:2002 Specification for Information on Security Management

You may wish to visit <http://www.bsi-global.com/> or <http://www.iso.ch/> to purchase full versions of the standards.

This factsheet is for any business wanting to know more about BS 7799. It covers the benefits, the ten sections of the standard you need to consider and a checklist to help you implement BS 7799.

## BENEFITS OF USING BS 7799

The benefits of using ISO/IEC 17799 are straightforward.

Using it well will result in:

- Reduced operational risk
- Increased business efficiency
- Assurance that information security is being rationally applied

This is achieved by ensuring that:

- Security controls are justified
- Policies and procedures are appropriate
- Security awareness is good amongst staff and managers
- All security relevant information processing and supporting activities are auditable and are being audited
- Internal audit, incident reporting/management mechanisms are being treated appropriately
- Management actively focus on information security and its effectiveness

It is likely that a number of organisations, including Government, will require suppliers and other partners to be certified to BS 7799 before they can be given work. This could make

compliance (or certification) more of a necessity than a benefit.

Certification can also be used as part of a marketing initiative, providing assurance to business partners and other outsiders.

#### UNDERSTANDING BS 7799 PART 1: 10 STEPS

**1. Security Policy** - explains what an information security policy should cover and why each business should have one

**2. Organisational Security** explains how information security management is organised

**3. Asset Classification and Control** considers information and information processing equipment as valuable assets to be managed and accounted for

**4. Personnel Security** details any personnel issues such as training, responsibilities, vetting procedures, and how staff responded to security incidents

**5. Physical and Environmental Security** physical aspects of security including protection of equipment and information from physical harm, as well as physical control of access to information and equipment

**6. Communications and Operations Management** examines correct management and secure operation of information processing facilities during day-to-day activities

**7. Access Control** control of access to information and systems on the basis of business and security needs

**8. System Development and Maintenance** design and maintenance of systems so that they are secure and maintain information integrity

**9. Business Continuity Management** concerns the maintenance of essential business activities during adverse conditions, from coping with major disasters to minor, local issues

**10. Compliance** concerns business compliance with relevant national and international laws,

professional standards and any processes mandated by the Information Security Management System (ISMS).

#### BS 7799 IS DIVIDED INTO TEN MAIN SECTIONS:

##### BS 7799 PART 1 SECTION 1: SECURITY POLICY

The security policy normally describes:

- The organisation's requirements for information security
- The scope of the Information Security Management System (ISMS), including business functions, areas and sites covered
- The general philosophy towards information security

To be effective it should be clearly supported by senior management.

Specific policies and procedures within the Information Security Management System (ISMS) must be consistent with the security policy. If a person encounters a situation that is not specifically mentioned in detail, the security policy should be a good general guide for actions required.

##### BS 7799 PART 1 SECTION 2: ORGANISATIONAL SECURITY

The organisational security section should describe:

- How the organisation manages information security
- The responsibilities of each relevant person, committee or forum. Includes responsibilities for creating, revising and following procedures and policies.

Many companies will have a management structure that can support information security without major changes. In such companies, the only requirement may be that a few committees have 'information security report' as a standard agenda item.

An organisational security structure should be

detailed, indicating:

- Who staff can contact when they need help or advice
- Who staff should report to regarding security problems, difficulties or successes

At the top of the structure should be the Board (or equivalent), which has overall responsibility for the organisation. Those responsible for following the policies and procedures should be arranged in a hierarchy below this level.

Organisational security must include temporary staff, contractors and third parties with access to sites, equipment, people or information.

#### BS 7799 PART 1 SECTION 3: ASSET CLASSIFICATION & CONTROL

Organisations are used to completing inventories of physical assets for example, computers, printers, machinery, vehicles etc. But information is also recognised as a vital asset for every organisation. The value of specific information will depend on factors such as:

- How much it cost to obtain
- How much it would cost to replace
- The extent of damage done to the organisation if it was disclosed to the public or a competitor

#### INFORMATION SECURITY: UNDERSTANDING BS 7799

An Information Asset Register (IAR) should be created, detailing every information asset within the organisation. For example:

- Databases
- Personnel records
- Scale models
- Prototypes
- Test samples
- Contracts
- Software licences
- Publicity material

The Information Asset Register (IAR) should also describe:

- Who is responsible for each information asset
- Any special requirements for confidentiality, integrity or availability

The value of each asset can then be determined to ensure appropriate security is in place.

#### BS 7799 PART 1 SECTION 4: PERSONNEL SECURITY

This covers aspects of job definitions and resourcing, to reduce the risk of human error and ensure that staff understand what their rights and responsibilities are concerning information security.

Most organisations require staff to keep client information confidential. They also ask staff to report security incidents and perceived weaknesses. Appropriate personnel security ensures that:

- Employment contracts and staff handbooks have agreed, clear wording
  - Ancillary workers, temporary staff, contractors and third parties are covered
  - Anyone else with legitimate access to business information or systems is covered
- It must deal with rights as well as responsibilities, for example:
- Access to personal files under the Data Protection Act
  - Proper use of equipment as covered by the Computer Misuse Act

Staff training is an important feature of personnel security to ensure the Information Security Management System (ISMS) continues to be effective. Periodically, refreshers on less frequently used parts of the Information Security Management System (ISMS), such as its role in disaster recovery plans, can make a major difference when there is a need to put the theory into practice.

**BS 7799 PART 1 SECTION 5: PHYSICAL AND ENVIRONMENTAL SECURITY**

This section details any physical aspects of access control to information and information systems. Ensuring that there is a proper environment for systems, records and staff is essential for maintaining confidentiality, integrity and availability of information.

**INFORMATION SECURITY: UNDERSTANDING BS 7799**

The following aspects should be considered:

**Protection**

- of information and information systems from the elements is as important as protecting them from unauthorised people.
- of physical access, which should be restricted to authorised personnel. IT equipment is tempting to thieves, and can be damaged by accidents or sabotage.

**Maintenance**

- of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading.
- of supporting equipment such as air conditioning plant or mains services. Physical controls can be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

**BS 7799 PART 1 SECTION 6: COMMUNICATIONS AND OPERATIONS MANAGEMENT**

The day-to-day operation of IT systems is fundamental to most organisations, and as such, security is vital. Keeping IT and communications systems secure is covered in this, the largest section of BS 7799. Everything from acceptance criteria for new or updated systems to virus

defence software and incident management procedures is described. Many of the issues covered apply to every IT system, irrespective of size, purpose, internal or external operation.

Subsections include:

- Networks
- Handling computer media
- Electronic commerce
- E-mail
- Publicly available systems (such as websites)

This is a rapidly changing area of security. New viruses and hacking opportunities are the most publicised issues. However, many incidents are caused by poor system design and management as well as accidents or unauthorised access for 'playing' rather than malicious actions. Good security practice in communications and operations management ensures efficient and effective business systems.

**BS 7799 PART 1 SECTION 7: ACCESS CONTROL**

Access control is about managing direct access to:

- Information
- Computer applications
- Operating system facilities

Effective control ensures that staff have appropriate access to information and applications, and do not abuse it.

**INFORMATION SECURITY: UNDERSTANDING BS 7799**

Management issues, such as periodic reviews of user accounts, can apply as much to IT systems as to physical access control systems.

Confidentiality of information is best achieved by ensuring that people only have access to the information they actually need.

If access rules are too detailed, managing them will be very difficult. If they are too general, people will have access to information

or applications that they will never need. A balance must be struck depending on:

- Needs of the business
- Security features provided by the systems
- Trust in staff

Consideration of security issues during system design, development and procurement will greatly enhance effectiveness. Look for:

- Strong password enforcement
- Management of access rights to read, amend, process or delete information
- Analysis of what users require to do their job
- Analysis of the security features each system can provide

#### BS 7799 PART 1 SECTION 8: SYSTEM DEVELOPMENT AND MAINTENANCE

Designing a new system with security in mind is more likely to result in effective and workable security features, than if you attempt to impose security on an existing (but insecure) system.

This area includes:

- Security requirements analysis and specification
- Application security
- Use of cryptography
- Security of system files

If you develop your own systems, or have them developed for you, good practice in this area is essential to ensure that they work and information remains secure.

#### BS 7799 PART 1 SECTION 9: BUSINESS CONTINUITY MANAGEMENT

Each organisation's business relies on its own staff, systems and, to some extent, other organisations. Anything from a burst water main to a terrorist attack on a foreign country can have a major effect on an organisation. As such, there must be a process for:

- Managing business continuity plans

- Business impact analysis
- Implementation and testing

Business continuity management considers the risks within an organisation and ensures that core processes keep running during adverse events. Tests do not have to be carried out 'for real', but could be 'paper exercises'.

#### INFORMATION SECURITY: UNDERSTANDING BS 7799

A review procedure to ensure that the plans are workable, and are sufficiently general to cover the most likely occurrences, is also necessary.

#### BS 7799 PART 1 SECTION 10: COMPLIANCE

Every organisation within the United Kingdom is required to comply with UK and EU law. Within the scope of the Information Security Management System (ISMS), each organisation should list the main laws that affect its activities. Within the UK, these include:

- Health and Safety legislation
- The Data Protection Act
- The Computer Misuse Act
- The Designs, Copyrights and Patents Act
- The Human Rights Act

Compliance with these is a legal requirement, and implementing BS 7799 is a good way of ensuring that your business does comply.

#### CERTIFICATION

Certification to BS 7799 is a formal acknowledgement that your Information Security Management System (ISMS) reflects your organisation's information security needs.

#### HOW IS CERTIFICATION OBTAINED?

Organisations can be formally certified for BS 7799 by a UK Accreditation Service (UKAS) accredited body.

A professional auditor completes an

independent formal review of the Information Security Management System (ISMS). The aim of the review is to confirm that the ISMS is both effective and appropriate.

The auditor will check for:

**1. Completeness.** Have all parts of BS 7799 been covered?

**2. Relevance.** Is the interpretation of BS 7799 relevant for the organisation?

**3. Implementation.** Is the Information Security Management System (ISMS) being followed? The auditor will require a Statement of Applicability (SOA). This is a document that lists all requirements in BS 7799 Part 2, with:

- An explanation of how the organisation complies with them
- An explanation and justification of any deviations from them

The BSI (<http://www.bsi-global.com/>) has several publications that are specifically designed to help organisations achieve certification to BS 7799.

## INFORMATION SECURITY: UNDERSTANDING BS 7799

### WHAT ARE THE ORGANISATION'S ONGOING REQUIREMENTS FOR BS 7799?

#### 1. Self audits

Each organisation must have a schedule of audits for the whole Information Security Management System (ISMS) over a reasonable period of time. This involves checking that staff are actually following the ISMS, and can prove it with appropriate records. The audits are internal, usually involve completing a standard checklist, and are conducted by the organisation's own staff, who are not required to have UKAS accreditation. Where a failure to follow the ISMS, or a security breach is detected, a report should go through the normal management structure. The importance of self-monitoring is that the

organisation can react quickly to problems in its own procedures - sometimes the procedures must be improved to take account of reality.

#### 2. Accredited Audits

After the initial audit, the certification body makes a review every six months.

#### 3. Statement of Applicability (SOA)

This is a living document and must be kept up to date. It should always reflect the current status of the organisation's Information Security Management System (ISMS).

### WHAT GETS CERTIFIED?

There are many options for certification. A small scope that addresses core business functions could be formally certified, but equally, the organisation as a whole could comply with the policies and procedures. Only the formally certified scope of the Information Security Management System (ISMS) would be subject to six monthly reviews.

## INFORMATION SECURITY: UNDERSTANDING BS 7799

### BS 7799 Checklist

Consider the following points for BS 7799:

- Security Policy ensure that your organisation has an Information Security Policy which includes the organisation's requirements for information security and its general philosophy towards it
- Organisational Security outline roles and responsibilities for relevant people and include an organisational security structure - Asset Classification and Control - consider information and information processing equipment as valuable assets to be managed and accounted for
- Personnel Security - detail any personnel

issues such as training, responsibilities, vetting procedures, and how staff responded to security incidents

- Physical and Environmental Security consider the protection of information in the same way that you would for physical assets.
- Communications and Operations Management examine correct management and secure operation of information processing facilities during day-to-day activities
- Access Control manage direct access to information, including computer systems and operations.
- System Development and Maintenance if you are developing or installing new systems, consider security issues from the outset.
- Business Continuity Management develop plans and procedures for the maintenance of essential business activities during adverse conditions, from coping with major disasters to minor, local issues
- Compliance ensure that your business is compliant with relevant national and international laws, professional standards, and any processes mandated by the Information Security Management System (ISMS)

#### GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business contact your local Business Link advisor by visiting the website at <http://www.businesslink.gov.uk> or calling 0845 600 9 006.

Published by the Department of Trade and Industry. <http://www.dti.gov.uk> © Crown Copyright