Preparing for BS 7799-2 Certification

Guidance
requirements
for certification

BSI
Business
Information

Whilst every care has been taken in developing and compiling this Published Document, BSI accepts no liability for any loss or damage caused, arising directly or indirectly, in connection with reliance on its contents except to the extent that such liability may not be excluded by law.

Information given on the supply of services is provided for the convenience of users of this Published Document and does not constitute an endorsement by BSI of the suppliers named

Preparing for BS 7799-2 certification

Guidance requirements for certification

This revision has been edited by:
Ted Humphreys (XiSEC Consultants Ltd)
Dr Angelika Plate (AEXIS Security Consulting)

Preparing for BS 7799 Certification

Guidance on requirements for certification

Contents

Foreword

Information is one of your organization's most valuable assets. Without suitable protection information can be:

- Given away, leaked or disclosed in an unauthorised way;
- Modified without your knowledge to become less valuable;
- Lost without trace or hope of recovery;
- Can be rendered unavailable when needed.

It should be the responsibility of all managers, information system owners or custodians and users in general to ensure that their information is properly protected from the multitude of threats faced by every organization. Information should be protected and properly managed like any other important business asset of the organization. Protected and properly managed in an ongoing, proactive manner.

The objectives above can be summarized as a need to protect the confidentiality, integrity and availability of information — the essence of information security. The code of practice, ISO/IEC 17799: 2000[1] *Information Security Management* was developed by a group of information security practitioners from industry and commerce for the benefit of all organizations, large, medium and small. It provides a statement of common practice that should be considered and implemented where appropriate.

BS 7799 Part 2: 2002 *Specification for information security management systems* was similarly developed so that organizations could properly prepare themselves for accredited certification against BS 7799.

This document, PD 3001, and the other guides in the PD3000 series are designed to provide users with assistance in establishing, implementing and maintaining their information security management system (ISMS) in a manner that should enable them to obtain certification.

Small print

A document such as this is provided with the best of intentions. It reflects common practice, which is derived by a consensus among those with a wide variety of skills, knowledge and

[1] This was previously BS 7799 Part 1:1999.

experience in the subject. This guidance makes no claim to be exhaustive or definitive and users of this guidance may need to seek further guidance in implementing the requirements of the BS 7799 Part 2:2002 standard. Furthermore, there will always be other aspects where additional guidance is required relevant to the organizational, operational, legal and environmental context of the business, including specific threats, controls, regulation and good practice.

It has been assumed in the drafting of this BSI guide that the execution of its advice is entrusted to appropriately qualified and experienced people.

1 General

1.1 Scope

This document provides guidance to users of BS 7799-2:2002 and the code of practice, ISO/IEC 17799:2000. It gives guidance for the establishment, implementation, monitoring and improvement of an ISMS, in other words the complete "life" cycle of activities required to have effective information security.

1.2 Field of application

This guide is intended to be used by those involved in:

- Designing, developing and implementing an ISMS.
- Preparing for ISMS audits.
- Carrying out an ISMS audit.

Types of ISMS audits include first party audits such as internal ISMS audits, second party audits such as those carried out by customer auditors and third party audits such as those carried out by independent certification bodies.

This PD provides detailed information on the implementation of the processes defined in BS 7799-2:2002 in readiness for third party audit to achieve accredited certification against BS 7799-2:2002. To claim compliance with the requirements in the Part 2 standard the organization needs to demonstrate that it has all the processes in place and provide evidence that they are being used. Of course, the processes themselves result in the organization implementing a system of controls to manage their risks. The organization should have implemented an effective system of controls as part of its ISMS and it should be able to demonstrate this by providing evidence to the ISMS auditor (whether it be a first, second or third party audit).

This guide can be used by those who may not have an immediate need for an audit but require a specification for establishing and implementing an ISMS based on industry accepted best practice processes. However, to claim compliance with BS 7799-2:2002 does require the organization to have at least an internal ISMS audit in place whether or not they go for a third party audit at a later stage. The organization may not have a business case for a third party audit but to be compliant with BS 7799-2:2002 the internal ISMS audit is mandatory.

1.3 PD 3000 Series Road Map

The following figure provides an indication of how the five parts of the PD 3000 series of guides relate together.

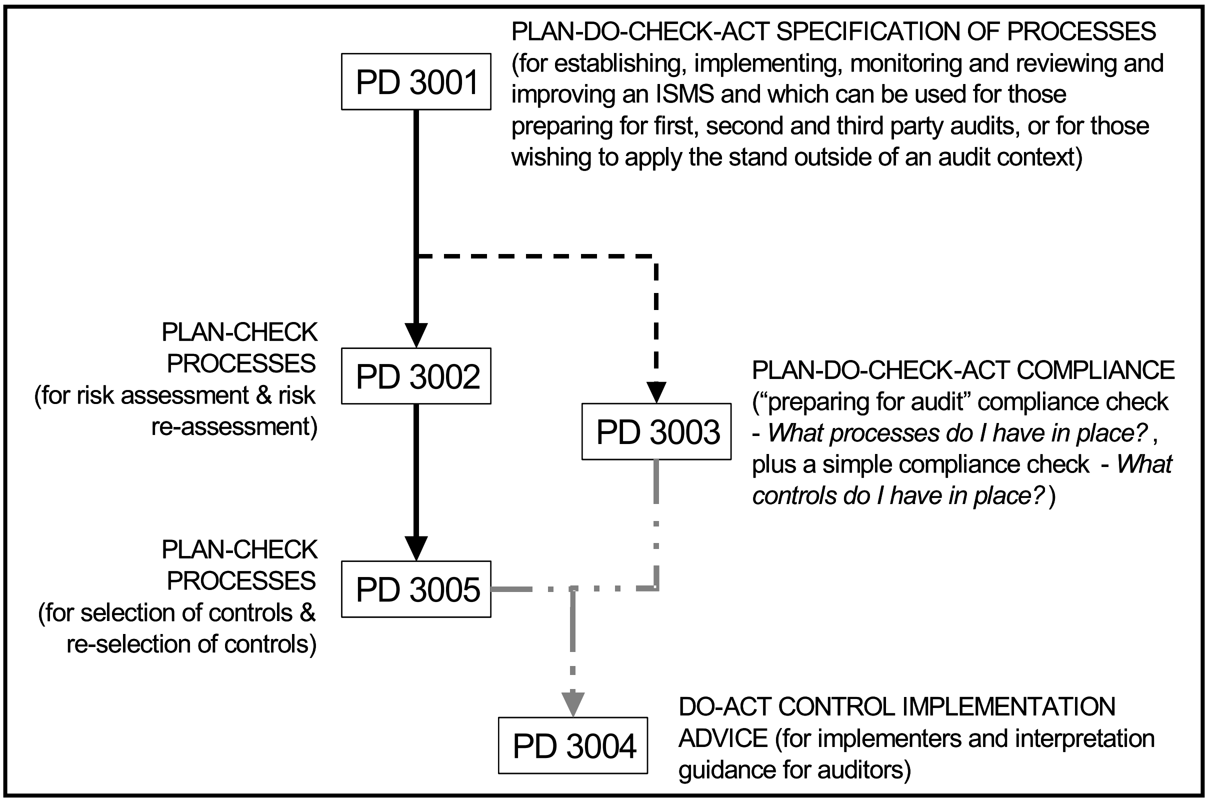
PD 3001
PLAN-DO-CHECK-ACT SPECIFICATION OF PROCESSES (for establishing, implementing, monitoring and reviewing and improving an ISMS and which can be used for those preparing for first, second and third party audits, or for those wishing to apply the stand outside of an audit context)
PLAN-CHECK PROCESSES (for risk assessment & risk re-assessment)
PD 3002
PD 3003
PLAN-DO-CHECK-ACT COMPLIANCE ("preparing for audit" compliance check - What processes do I have in place?, plus a simple compliance check - What controls do I have in place?)
PLAN-CHECK PROCESSES (for selection of controls & re-selection of controls)
PD 3005
PD 3004
DO-ACT CONTROL IMPLEMENTATION ADVICE (for implementers and interpretation guidance for auditors)

Figure 1 – PD 3000 series road map

1.4 Definitions

For the purposes of this guide the definitions listed in ISO/IEC 17799:2000, BS 7799 Part 2:2002 and ISO/IEC Guide 73:2002 apply.

1.5 Related documents

This guide makes reference to the following standards and guidelines:

a) ISO/IEC 17799:2000 (previously BS 7799-1:1999) - a code of practice that identifies control objectives and controls and provides common practice advice for the implementation of these controls.

b) BS 7799-2:2002 - is the specification for an information security management system. This standard is used as the basis for accredited certification.

c) ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards

d) EA 7/03: EA Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems

e) ISO/IEC Guide 62: 1996, General requirements for bodies operating assessment and certification/ registration of quality systems.

f) The Newly Revised Part 2 of BS 7799 (version 6.0, October 2002), www.xisec.com/ISMS.htm

Note Users should always ensure that the correct version of these standards is used.

This document is one of a set of five guides published by BSI DISC to support the use and application of ISO/IEC 17799:2000 and BS 7799-2:2002. The reader may find it of benefit to have copies of the other four guides:

- *Guide to BS 7799 Risk Assessment (PD 3002) - Guidance aimed at those responsible for carrying out risk assessment*
- *Are you ready for a BS 7799 Audit? (PD 3003) - A compliance assessment workbook*
- *Guide to the implementation and auditing of BS 7799 controls (PD 3004)*
- *Guide on the selection of BS 7799 controls (PD 3005)*

2 The essence of information security

2.1 Confidentiality

The protection of information, in any form, while in storage, processing or transport, from being available to any organization or person that is not authorized by its owner to have it.

Many forms of access control are basically about protecting confidentiality. Encryption is another example of a control, which can provide for the confidentiality of information. Controls may be applied at every level of an information security management system, the physical level (e.g. locks on doors, filing cabinets, safes etc), and the logical level individual data fields in a database, data in applications and in hardcopy form such as paper documents. In every case the threats and vulnerabilities should be identified, the associated risks assessed, and a system of controls selected, implemented and applied to protect against these risks.

2.2 Integrity

Ensuring that information is accurate and complete in storage and transport; that it is correctly processed and that it has not been modified in any unauthorised way. We also wish to establish the integrity of the networks and systems that we connect to, to ensure that they are who we intend them to be.

Many data handling devices contain automatic integrity checking facilities to ensure that they, including disk drives and other media, and telecommunications systems, do not corrupt data. Integrity controls are essential in operating systems, software and application programs in order to prevent intentional or unintentional corruption of programs and data during processing. Integrity controls need to be included at the procedural level to reduce the risks of human error, theft or fraud, e.g. controls for input/output data validation, user training and other operational type controls.

2.3 Availability

Ensuring that information is available to those who are authorized to have it, when and where they should have it.

In practice the availability of information requires a system of controls: for example information back-ups, capacity planning, procedures and criteria for system acceptance, incident management procedures, management of removable computer media, information handling procedures, equipment maintenance and testing, procedures for monitoring system use, and business continuity procedures. Monitoring, reviewing and checking security incidents, service levels, and system performance in a timely and on-going manner can be a preventative control to ensure availability.

2.4 Sensitive or critical information

ISO/IEC 17799:2000 defines a number of controls, which are applicable to both sensitive and critical information. What is sensitive or critical information and how do we recognize it? For every organization the definition will be different. Some means should be found to assess the value or utility of information in the context of the individual organization in order to be able to label information as sensitive or critical when needed and the rest as non-sensitive or non-critical.

There is also a time element: an organization's financial information will be very sensitive in the days before reporting to the stock market, but have no sensitivity at all once reported. Sensitivity will also be reflected in the level of classification given to the data.

Part of the risk assessment process (see PD 3002) involves the valuation of information assets in order to calculate the risks and the level of security required to protect these assets using an appropriate system of controls.

3 Information security management system (ISMS)

3.1 Introduction

Fundamental to BS 7799 Part 2:2002 is the concept of an information security management system (ISMS). The information security management system (ISMS) is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, maintain and improve information security. The management system includes organization, structure, and policies, planning activities, responsibilities, practices, procedures, processes and resources. For the management of information security its scope, administration and resources will depend on the size of the organization and information resources in question.

The ISMS should be effective if it is to be useful to the organization. Information security should be an integral part of the organization's operating and business culture. Information security is primarily a management issue, rather than a technical issue, although one should not ignore the technical problems especially given the widespread dependence on the use of IT. Information security management is not a once off exercise, but should be seen as an ongoing activity of continual improvement. Well-managed information security is a business enabler. No organization can operate successfully in today's world without information security. A well chosen management system of controls for information security properly implemented and used will make a positive contribution to the success of the organization, not just a cost against the bottom line.

3.2 Compliance with BS 7799 Part 2

As a code of practice ISO/IEC 17799:2000 takes the form of guidance and recommendations which means it should not be quoted as a specification and care needs to be taken to ensure that claims of compliance are not misleading.

As a specification for an ISMS BS 7799 Part 2 takes the form of a set of requirements using the prescriptive **"shall"** statements, to which a completed, installed ISMS shall conform if compliance by an organisation is to be claimed. In the case of Part 2 this covers all the requirements associated with the process approach given in the standard (clauses 1-7). Further details on this aspect of compliance can be found in 1.3 f).

The term **“shall”** indicates those provisions, which reflecting the requirements of BS 7799 Part 2, are mandatory. The term “should” is also used to indicate those provisions, which, although they constitute guidance for the application of the requirements, are expected to be adopted but are not mandatory.

3.3 PDCA Model

The model, known as the “Plan-Do-Check-Act model” (PDCA Model), is used in the BS 7799 Part 2:2002 standard (see Figure 2). This model is used as the basis for establishing, implementing, monitoring, reviewing, maintaining and reviewing an ISMS.

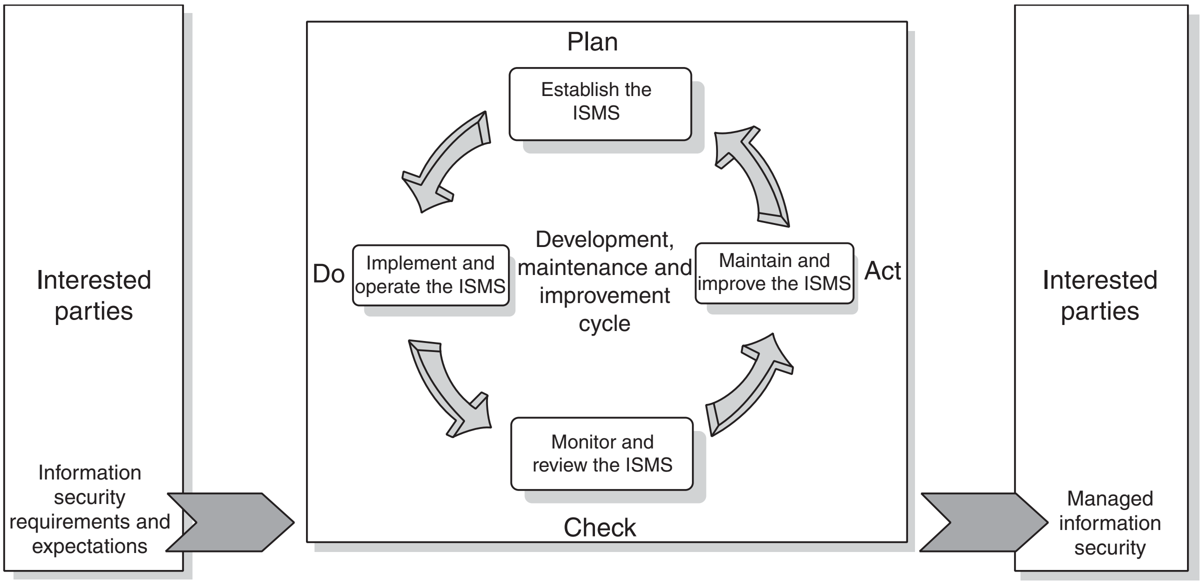
Interested parties
Information security requirements and expectations
Plan
Establish the ISMS
Do
Implement and operate the ISMS
Development, maintenance and improvement cycle
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested parties
Managed information security

Figure 2 - PDCA model applied to ISMS processes

Plan (establish the ISMS)	Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the security policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.

3.4 Establish the ISMS

The **shall** statements defined in BS 7799 Part 2 clause 4.2.1 for the **Plan phase** are as follows:

a) **Define the scope of the ISMS** in terms of the characteristics of the business, the organization, its location, assets and technology. The scope of the ISMS may be a limited part of the organization and independently defined, or the scope may be defined to be the whole organization. The ISMS scope needs to be well defined and complete. The scope needs to take account an interfaces with other systems, organizations, third party suppliers, and it also needs to take account any dependencies, e.g. security requirements that need to be satisfied by the ISMS.

b) **Define a ISMS policy** in terms of the characteristics of the business, the organization, its location, assets, technology and taking account any legal and regulatory requirements, and contractual or third party obligations or dependencies. Management shall approve the ISMS policy. This policy shall include a framework for setting objectives, giving management direction and action, establishing the risk management context and criteria against which risk will be evaluated.

c) **Define a systematic approach to risk assessment** – this should be an approach that is best suited to the ISMS. The organization needs to include its criteria for accepting risks and the identification of acceptable levels of risk. The method of risk assessment that an organization adopts is entirely the decision of the organization.

It is important to note that whatever method is used it needs to deal with management systems covering all the control areas of the BS 7799 Part 2; this method needs to cover the risks related to organizational aspects, personnel controls, business processes, operational and maintenance processes and procedures, legal, regulatory and contractual matters, and information processing facilities. PD3002 provides information on risk assessment appropriate to this step and also to d) and e) below.

Risk assessment is a mandatory requirement but this does not require the use of any automated software tools though in many situations there are benefits in the use of such tools especially when risks need to be re-assessed and risk related information such as the threats, vulnerabilities and assets need to be updated. The complexity of the risk assessment method and approach will depend on the complexity of the ISMS under review. The techniques employed should be consistent with the complexity and the levels of assurance required by the organization.

d) **Identify the risks** to the assets taking account the threats and vulnerabilities associated with these assets and the impacts that the losses of confidentiality, integrity and availability may have on the assets. Again the risks need to relate to all the control areas as indicated in c) above (see PD3002 provides more information on risk assessment).

e) **Assess the risks** based on the information processed in d) above, taking care to include all the control areas such as organizational, personnel, business processes, operational and maintenance, legal, regulatory and contractual matters, and information processing facilities (see PD3002 which provides more information on risk assessment). This will involve the organization assessing the harm to its business as result from a security failure and the likelihood of such a failure happening. The organization needs also to estimate the level of risk and to determine whether the risks are acceptable or requirement treatment within its own business context.

f) **Identify and evaluate options for the treatment of risks** – Once the organization has identified, assessed and understood the impact the risks might have on its business it can take various actions to manage and treat these risks appropriately within its business context. The actions the organization could consider include applying appropriate controls to reduce the risks, avoiding the risks through non-engagement of a risk related activity, transferring the risk (wholly or partly) to another party such as an insurer, or knowingly and objectively accepting the risk.

g) **Select control objectives and controls for the treatment of risks –** If the organization decides to apply controls to manage and treat the risk then it first needs to select a system of controls that are suitable for this purpose (see PD3005 which provides information on selection of controls). The controls an organization can select from are contained in Annex A of BS 7799 Part 2:2002. The organization may also need to select additional controls not included in Annex A.

As discussed in PD 3005 the selection of controls should be cost effective, i.e. the cost of their implementation should not exceed the financial impact of the risks they are intended to reduce. Of course, some impacts will be non-financial. Account should also be taken of those impacts related to safety, personal information, legal and regulatory obligations, image and reputation.

h) **Prepare a Statement of Applicability** – The SoA (Statement of Applicability) is a mandatory requirement for those organizations that are seeking certification to BS 7799 Part 2. The SoA is a document, which presents the control objectives, and controls that have been selected, and this selection shall be linked to the results of the risk assessment and risk treatment processes. This linkage should indicate the justification and rationale for the selection of control objectives and controls. A listing of the control objectives and controls **does not alone** constitute a valid SoA.

3.5 Implement and operate the ISMS

The **shall** statements defined in BS 7799 Part 2 clause 4.2.2 for the **Do phase** are designed to ensure that the organization has an appropriate set of processes in place to implement and use the ISMS they have establish in the **Plan phase**. This includes producing a risk treatment plan for managing the information security risks the organization has identified and assessed. This plan should outline what management actions need to be invoked, the responsibilities of those involved in the process of managing the information security risks and those involved in any security relevant user/manager activity related to the ISMS.

The organization should have a set of processes in place for implementation of the risk treatment plan and the system of selected controls, taking account the funding for the ISMS, allocation of roles and responsibilities, the roll out of an appropriate awareness and training programme, management of resources and operations, and deployment and use of procedures for managing information security incidents. The guide PD3004 provides information on the implementation of the system of controls.

Effectiveness is the by-word when implementing the selected controls. Controls should be effective in their management of the security risk(s) for which they have been selected. Their cost effectiveness should also be considered — there may be many degrees of implementation for a given control. The degree (for instance, how much training, recording or reporting) of implementation should be finely judged to avoid wasted resource. Over implementation can lead to frustration among staff affected by the control, often resulting in a reduction in the effectiveness of overall control. Security and control will always impinge on the lives and working practices of people but it should never become a burden.

It is also important to remember that security is not there to prevent staff from doing what they are employed to do — rather; it should enable them to do it with managed and effective control. It should enable them to demonstrate their fulfilled accountabilities; establish their trustworthiness without leaving a trail of doubts. Staff will soon see well-implemented security as a benefit, rather than as an inconvenience.

3.6 Monitor and review the ISMS

The **shall** statements defined in BS 7799 Part 2 clause 4.2.3 for the **Check phase** are designed to ensure that the organization has an appropriate set of processes in place to monitor and review the ISMS they have implemented in the **Do phase**. For the ISMS to be effective in managing the information security risks it is important to monitor and keep track of any changes that might effect the ISMS. This might be changes to the threats, vulnerabilities or impacts due to changes in:

- The business environment or context: new business partners, new or different supply chains, new, different or modified customer base, expansion into different markets, market conditions, third party arrangements, outsourcing arrangements, home working;
- Business policy or objectives;
- The organizational structure, workforce, operational environment;
- The use and deployment of technology: new systems and applications, upgrades, expanding networks, greater diversity of system platforms, greater use of remote working, greater third party access, more outsourcing arrangements;
- The legal and regulatory environment.

These examples of changes can all have an effect on the risks and impact to an organization's business. A re-assessment of the risks, level of residual risk and level of acceptable risk is necessary to ensure the ISMS remain effective.

During the **Check Phase** the organization needs to undertake reviews and re-assessments of its ISMS: is the scope still valid, is the system of controls still valid and effective, are the procedures still valid and being used correctly in the current business context, are the allocated roles and responsibilities still valid and are the assigned security activities being performed as expected, is the security incident handling processes still appropriate, have the results of the security incident handling processes been dealt with correctly and is the business continuity plan still appropriate.

During the **Check Phase** the results of management reviews, security audits, system tests, security incident reports, feedback and suggestions from information system owners, managers and users should all be taken in account to ensure that the ISMS is still appropriate for the business and is still managing the information security risks to the level of acceptable risk.

3.7 Maintain and improve the ISMS

The **shall** statements defined in BS 7799 Part 2 clause 4.2.4 for the **Act phase** are designed to ensure that the organization has an appropriate set of processes in place to maintain and improve the ISMS following the processes implemented in the **Check phase**. The monitoring and review processes in the **Check phase** may have identified changes that require improvements to the ISMS to ensure that the information security risks are being properly managed.

Risk is constantly changing, being influenced by internal and external conditions. It is therefore necessary to manage it proactively with reviews being made in response to changes identified in the **Check phase**. Incidents demonstrate risks realised and may require escalation procedures to ensure they are responded to promptly and effectively. Risk should be monitored with regular reviews of threats, the system of controls in place and their effectiveness, and audits.

In clause 7.1 of BS 7799 Part 2 there is a requirement that the organization shall have a set of processes in place to be able to continually improve the effectiveness of the ISMS. This will involve the use of information security policy, security objectives, results from audits and reviews, analysis of monitoring activities, and corrective and preventive actions.

The **Act phase** will need to have process in place to implement any identified ISMS improvements and to take corrective and preventive actions with clauses 7.2 and 7.3 of the BS 7799 Part 2 standard. The organization shall identify non-conformities of the implementation and operation of the ISMS, determine the causes of these non-conformities, evaluate the need for actions to eliminate the causes of the non-conformities and take corrective actions to prevent their recurrence. In addition, the organization shall identify any potential non-conformities and their causes, and determine preventive actions needed.

An important aspect is making sure that all actions, corrective and preventive are recorded and that appropriate communication channels are in place to convey the results of the ISMS improvements to the right people in the organization and that implementation of actions actually takes place as a result of this communication. The organization shall ensure that the implemented improvements meet the desired requirements and achieve their intended objectives. This includes reviewing the corrective and preventive actions that taken place.

3.8 System of documentation

3.8.1 Requirements

It is important that the ISMS is a documented management system complying with the requirements of clause 4.3 of BS 7799 Part 2:2002. The ISMS documentation shall include:

- Statements of security policy in accordance with the mandatory requirement in 4.2.1 a) of BS 7799 Part 2;
- The ISMS scope in accordance with the mandatory requirement in 4.2.1 b) of BS 7799 Part 2;
- Procedures and controls to support the ISMS;
- A risk assessment report in accordance with the mandatory requirements given in 4.2.1 c)-g) of BS 7799 Part 2;
- A risk treatment plan in accordance with the mandatory requirement in 4.2.2 b) of BS 7799 Part 2;
- Procedures needed to ensure the effective planning, operational and control of the information security processes in accordance with the mandatory requirement in 6.1 of BS 7799 Part 2;

- Records providing evidence of conformity to requirements and effective operation of the ISMS;
- Statement of Applicability in accordance with the mandatory certification requirement in 4.2.1 h) of BS 7799 Part 2.

3.8.2 Control of documentation and records

Clauses 4.3.2 and 4.3.3 in BS 7799:2002 define a set of mandatory requirements for the control of documents and records to ensure that the ISMS documents are adequately protected and controlled. These requirements shall be satisfied by an appropriate set of procedures and processes to ensure the documents and records are protected and controlled. This is an important part of the risk management process alongside the other controls for information security.

Records play an especially important part in the world of information security management. When an information security incident occurs it is important that the incident is dealt with to degree of timeliness and priority commensurate with its severity. In most cases evidence is required to be able to deal with the incident in the most appropriate manner: where and when did it happen, what were the circumstances, who/what did it, what was the outcome and so on. Good, accurate record keeping can provide this evidence. Of course, there are legal requirements for the collection and presentation of evidence in the case of a criminal incident. Therefore it is not only important to keep records, but also that these records are protected and their integrity, availability and confidentiality are ensured.

In the 2002 edition of the BS 7799 Part 2 the control requirements for documentation and records have been harmonised with the requirements specified in other management system standards, e.g. ISO 9001. This offers several benefits to an organization, including the opportunity to have combined/integrated audits, economise on the resources needed to manage and maintain the system of documentation and records, it can provide better control of the business assets and smoother, more integrated management.

3.9 Management responsibility

It is important that the management shall provide evidence of its commitment processes and activities that are involved in the establishment, implementation, operation, monitoring and review, maintenance and improvement of the ISMS in accordance with clause 5 of the BS

7799 Part 2:2002 standard. From establishing information security policy, setting objectives, allocating roles and responsibilities, communication of the importance of information security management to the business, provision of resources for the ISMS, deciding upon the acceptable level of risk through to conducting management reviews there needs to positive, visible, real support and commitment from management.

The organization shall ensure that it provides adequate resources to implement the requirements and processes identified in the BS 7799 Part 2:2002 standard, this includes all that is defined in clauses 4 through 7 inclusive. It also shall ensure that these resources are managed appropriately according to clause 5.2 of the Part 2 standard. Users, staff, managers, and where necessary contractors, should be given training commensurate with their job role and function and their specific information security responsibilities. The organization shall ensure that they provide appropriate awareness to all users, staff, managers to ensure that the ISMS is effective and that information security is marketed as an important day to day aspect of business. The organization should as part of its general training and awareness programme include information security management, and it needs to ensure it has allocated the right roles and responsibilities to those that have been trained, and that those are competent in dealing with information security management issues. This can range from a simple level of understanding and competency that all staff should have, e.g. handling passwords, basics of physical security, proper use of email, virus protection and so on, through to more involved levels which not all staff would be expected to be competent in, e.g. configuring a firewall, managing the information security incident handing process.

3.10 Management review of the ISMS

It is important that the management shall review the organization's ISMS according an established plan and review programme in accordance with clause 6 of the BS 7799 Part 2:2002 standard. Review of the ISMS enables the organization to judge and assess whether improvements and changes are needed to the ISMS. The **Check Phase** (see 2.5 of this guide) stresses the importance of monitoring and reviewing changes to the business and operational environment of the ISMS to identify and evaluate whether the ISMS is still valid and provides effective information security. After reviewing the situation it may mean that some policies and procedures need to be added/changed/improved, some technical controls need to be added/changed/improved and so on. Without reviewing and auditing the ISMS on a regular basis the ISMS can become out of date, ineffective and inefficient in managing the risks the organization faces, and so eventually the organization is investing in an ISMS that is no longer useful or relevant.

There are various types of audit and review that an organization may need to consider: a first party audit and review (e.g. an internal ISMS audit), a second party audit and review (e.g. as might be a requirement of a customer requirement or contractual arrangement) or a third party audit and review (e.g. a BS 7799 certification carried out by an independent third party certification body).

Clauses 6.2 and 6.3 of BS 7799 Part 2 define specific requirements for the input and output of management reviews. It is important that organizations make sure that sufficient and accurate information is input into the review proves to enable the right decisions can be made and appropriate actions can be taken. If organizations are to go to the effort of having management reviews then it is important that sufficient information is available to make these right decisions to avoid wasting time and resource.

It is important that the organization carries out an internal ISMS audit in accordance with the mandatory requirement given in clause 6.4 of the BS 7799 Part 2 standard. On the other hand, whether or not the organization goes for third party certification is a management decision but is not mandatory. However all the requirements specified in clauses 1 to 7 of the Part 2 standard are mandatory for certification.

4 Certification Audits

4.1 General

Certification of an organization’s information security management system (ISMS) is an accepted way of providing assurance that the organization has implemented a management system of information security which meets the requirements specified in the BS 7799 Part 2 standard.

The guidelines and criteria EA 7/03[2] (entitled EA Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems) is a publication issued by the European cooperation for Accreditation (EA). The members of the EA are the national accreditation bodies in Europe, so for example it includes UKAS for the UK, RvA for the Netherlands, Swedac for Sweden and so on. EA 7/03 specifies requirements that certification bodies need to comply with to ensure they operate third party certification systems in a consistent and reliable manner, thereby facilitating their acceptance on a national and international basis. Thereby EA 7/03 serves as a basis for the recognition of national systems in the interests of international trade. Therefore certification body wishing to offer certification services to achieve such recognition and acceptance under the sector scheme for BS 7799 Part 2 needs to be accredited by a national accreditation in accordance with EA 7/03.

Accredited BS 7799 Part 2 certification involves the assessment of an organization’s ISMS. ISMS certification ensures that the organization has undertaken a risk assessment and has identified and implemented a system of management controls appropriate to the information security needs of the business. Evidence that an organization is conforming to the BS 7799 Part 2 standard, and any supplementary documentation, will be presented in the form of a certification document or certificate. It should be noted that this does not imply that the

[2] The text of EA 7/03 is drawn from three main sources: original text of ISO/IEC Guide 62:1996 (to which EN 45012:1998 is identical), original text of IAF Guidance to ISO/IEC Guide 62, and specific text giving additional guidance on the application of EN 45012 to bodies involved in ISMS certification/ registration.

organization has achieved specific levels of information security related to its products and services. Evidence may be presented to the certification auditors that such levels have been meet via separate security evaluation of its products but such evaluation is not part of the certification process.

Certification to the BS 7799 Part 2 sector scheme is entirely voluntary. Organizations which successfully complete the BS 7799 certification process can have greater confidence in their ability to manage information security and this in turn will help them assure trading partners, customers and shareholders with whom they do business. The accredited BS 7799 Part 2 certificate is a public statement of its ISMS capability whilst allowing the organization to keep the specific details of its information security controls secret and confidential.

4.2 Assessment

4.2.1 ISMS Scope of certification

As stated in 2.3.a) of this guide organizations shall define the scope of their ISMS. It is the role of the certification body to confirm this scope in order to ensure that organizations do not exclude from the scope of their ISMS elements of their operation or business, which they should have properly be included under it.

Certification bodies shall need to ensure itself that the organization's information security risk assessment properly reflects its business activities and extends to the boundaries and interfaces of its activities as defined in the BS 7799 Part 2 standard. Certification bodies should confirm that this is reflected in the organization's risk treatment plan and its Statement of Applicability in accordance with 2.3 h) of this guide and the Part 2 standard.

Interfaces with services or activities that are not completely within the scope of the ISMS should be addressed within the ISMS subject to certification and should be included in the organization's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. computers, telecommunication systems, etc.) with others.

As specified in clause 1.2 of the BS 7799 Part 2 standard:
"Where exclusions are made, claims of conformity to this standard are not acceptable unless such exclusions do not effect the organization's ability, and/or responsibility, to provide

information security that meets the security requirements determined by risk assessment and applicable regulatory requirements. Any exclusions of controls found to be necessary to satisfy the risk acceptance criteria need to be justified and evidence needs to be provided that the associated risks have been properly accepted by accountable people. Excluding any of the requirements specified in clauses 4, 5, 6 and 7 is not acceptable."

4.2.2 ISMS Scope covering multiple sites

Where multiple sites are covered by a single ISMS, a certificate may be issued by the certification body to cover all such sites provided that:

- All sites are operated under the same ISMS control, which is centrally administered, managed and audited and subject to central management review.
- All sites have been audited in accordance with the organization's internal security review procedures.

When defining an ISMS that covers more than one site (multiple sites) then special care needs to be taken to ensure the interfaces and dependencies are suitably specified and taken account of in the risk assessment and that the results of this assessment are properly reflected in the system of controls that have been implemented.

If the certification body adopts a sample based approach to multiple site audits then it is expected that the sample shall be partly selective based on a number of site differences and partly non-selective and is expected to result in a range of different sites being selected, without excluding the random element of site selection. The differences that might apply between each of the site covered by a single ISMS include the following:

- Variations in the size of the sites.
- Variations in the business carried out on these sites.
- Complexity of the information systems at the different sites.
- Variations in working practices and operational activities undertaken at the different sites.
- Variations in types of information processed (critical/non-critical, sensitive/non-sensitive) at different sites.
- Variants in legal and regulatory requirements applicable for different sites.

Every site included in the ISMS which is subject to significant threats to assets, vulnerabilities or impacts is expected to be audited by the certification body.

The follow on surveillance audit (see 3.2.6) programmes are expected to cover, within a reasonable time, all sites of the organization or within the scope of the ISMS certification as specified in the Statement of Applicability.

Where a nonconformity has been raised either at the head office (main site) or at a single site included in the ISMS, the corrective action procedure should apply to the head office and all sites covered by the certificate.

4.2.3 Audit methodology

The guidance in EA 7/03 states that the certification body should perform its audit of an organization's ISMS in at least two stages at the organization's site(s), unless it can justify an alternative approach, e.g. this might be the case with the adaptation of the certification process to the needs of very small organizations. EA 7/03 defines two stages of audit: **Stage 1 Audit** and **Stage 2 Audit**.

4.2.3.1 Stage 1 Audit

One objective of the Stage 1 Audit is to enable the certification body to gain an understanding of the ISMS in the context of the organization's security policy and objectives, approach to risk management. The audit stage also provides a focus for planning out the Stage 2 Audit and is an opportunity to check how prepared the organization is for the audit.

The Stage 1 Audit includes a document review, which needs to be completed prior to the commencement of Stage 2 Audit. The certification body is expected to review documents relevant to the design and implementation of the ISMS covering at least the organization's risk assessment report, risk treatment plan and the Statement of Applicability, and other core elements of the ISMS (see 2.8.1 of this guide).

A written report will be produced giving the results of the Stage 1 Audit. The findings given in this report are used to decide whether the time is right to precede with the Stage 2 Audit. The findings of the report are also used for selecting Stage 2 Audit team members with the necessary competence to deal with the specific nature of the ISMS. In preceding to the next stage the certification body will inform the organization what additional documents, other types of information and records that may be required for detailed inspection during the Stage 2 Audit.

4.2.3.2 Stage 2 Audit

The Stage 2 Audit) is based on the findings given in the Stage 1 Audit report. The certification body produces an audit plan for the carrying out the Stage 2 Audit based on these findings. The Stage 2 Audit) takes place at the site(s) of the organization where the ISMS is located.

The Stage 2 Audit should cover:

a) Confirmation that the organization is acting in accordance with its own policies, objectives, and procedures;

b) Confirmation that the ISMS conforms with all the requirements of the BS 7799 Part 2 standard and is achieving the organization's policy objectives (includes checking that the organization has a system of processes in place to cover the requirements given in Clauses 4 to 7 inclusive of the BS 7799 Part 2 standard);

Specifically the Stage 2 Audit should focus on how the organization is dealing with:

c) Assessment of information security related risks and the resulting design of its ISMS;

   - The approach to risk assessment (BS 7799 Part 2; Clause 4.2.1 c))
   - Identification of the risks (BS 7799 Part 2; Clause 4.2.1 d))
   - Assessment of the risks (BS 7799 Part 2; Clause 4.2.1 e))
   - Treatment of risks (BS 7799 Part 2; Clause 4.2.1 f))
   - Select control objectives and controls for the treatment of risks (BS 7799 Part 2; Clause 4.2.1 g))
   - Prepare a Statement of Applicability (BS 7799 Part 2; Clause 4.2.1 h))

d) Checking objectives and targets derived from this process;

e) Performance monitoring, measuring, reporting and reviewing against the objectives and targets. This should include checking that processes are in place and are being used for at least the following;

- BS 7799 Part 2 Clause 4.2.2 Monitor and review the ISMS;
- BS 7799 Part 2 Clause 6 Management review of the ISMS;
- BS 7799 Part 2 Clause 7 ISMS improvement

f) Security and management reviews. This should include checking that processes are in place and are being used for at least the following;

- BS 7799 Part 2 Clause 4.2.2 Monitor and review the ISMS;
- BS 7799 Part 2 Clause 6 Management review of the ISMS.

g) Management responsibility for the information security policy. This should include checking that processes are in place and are being used for at least the following;

- BS 7799 Part 2 Clause 4.2.2 Monitor and review the ISMS;
- BS 7799 Part 2 Clause 5 Management responsibility;
- BS 7799 Part 2 Clause 6 Management review of the ISMS),

h) Links between policy, the results of information security risk assessments, objectives and targets, responsibilities, programmes, procedures, performance data, and security reviews (should include showing the links between the various activities, processes and results specified in BS 7799 Part 2; Clauses 4 to 7 inclusive).

4.2.4 Audit report

The certification body is expected to adopt various reporting methods and procedures to convey to the organization the results of the audit. This includes a written or oral reports provided during the audit meetings on the organizations premises as well formal reports at the end of the audit. These reports indicate the conformity of the organization's ISMS to the BS 7799 Part 2 requirements.

Reports given during the audit provide an opportunity for the organization to ask questions about the auditor’s findings and the basis for the findings. It is expected that the certification body will deliver reports to the organization in a timely manner as there may be non-conformities to be dealt with and discharged in order to comply with all of the certification requirements.

The organization is invited to comment on the audit reports and to describe the specific corrective actions it has taken, or it plans to take to remedy any nonconformity identified during the audit. The certification body will inform the organization if there is a need for full or partial reassessment or whether a written declaration to be confirmed during surveillance will be considered adequate to check whether the corrective actions have been cleared.

4.2.5 Certification decision

The decision whether to grant certification to an organization is be taken by the certification body. This decision is based of the information and evidence gathered during the audit process and any other relevant information. Those who make the certification decision are not those that have participated in the audit.

An organization that has been granted certification is provide a BS 7799 Part 2 certificate from the certification body. This BS 7799 certificate includes information such as the scope of the certification, the effective date of certification, and reference to the specific version of the statement of applicability, applicable certification body and accreditation body logos or marks.

4.2.6 Surveillance and reassessment procedures

The certification body is expected to carry out periodic surveillance audits on the organization's ISMS. The frequency of these follow-up audits is the responsibility of the certification body but typically an organization might be visited for such an audit every six months. The purpose of these surveillance audits is to verify that the organization who's ISMS has been certified continues to comply with the certification requirements and the BS 7799 Part 2 standard.

Reassessment of the organization's ISMS normally takes place every three years i.e. the maximum lifetime of a BS 7799 certificate is normally three years after which the ISMS needs to be re-certified. The purpose of this reassessment is to:

- Verify overall continuing conformity of the organization's ISMS to the requirements of the BS 7799 Part 2;
- Review of past implementation and continuing maintenance of the system over the

period of certification including:

- Checking that the ISMS has been properly implemented, maintained and improved in accordance with the requirements of BS 7799 Part 2;
- Reviewing the ISMS documents and the results of regular ISMS audits including internal audits and surveillance audits);
- Checking the effective interaction between all elements of the ISMS;
- Checking the overall effectiveness of the ISMS in its entirety taking account changes in the organization's business and operations;
- Verifying a demonstrated commitment to maintain the effectiveness of the ISMS.

_Annex A Example policy statement

The following is an example of an Information Security Policy Statement.

OBJECTIVE

The objective of information security is to ensure business continuity and minimize business damage by preventing and minimising the impact of security incidents.

POLICY

- The purpose of the Policy is to **protect the organization's information assets**[3] from **all** threats, whether internal or external, deliberate or accidental.
- The Chief Executive has approved the Information Security Policy.
- It is the Policy of the organization to ensure that:
  - ◊ Information will be **protected against unauthorized access**;
  - ◊ **Confidentiality** of information will be assured[4];
  - ◊ **Integrity** of information will be maintained[5];
  - ◊ **Availability** of information is ensured as required by the business processes;
  - ◊ **Regulatory** and **legislative** requirements will be met[6];
  - ◊ **Business Continuity plans** will be produced, maintained and tested[7];
  - ◊ **Information security training** will be available to **all** staff;
  - ◊ **All breaches of information security**, actual or suspected, will be reported to, and investigated by the **Information Security Manager** [8].
- Procedures exist to support the policy. These include virus control, passwords and business continuity.

[3] Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone.

[4] The protection of valuable or sensitive information from unauthorized disclosure or intelligible interruption.

[5] Safeguarding the accuracy and completeness of information by protecting against unauthorized modification.

[6] This applies to record keeping and most controls will already be in place; it includes the requirements of legislation such as the Companies Act and the Data Protection Act.

[7] This will ensure that information and vital services are available to users when and where they need them.

[8] This may be a full or part time role for the allocated person.

- Business requirements for the availability of information and information systems will be met.
- The Information Security Manager has direct responsibility for maintaining the Policy and providing advice and guidance on its implementation.
- All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the Policy.

Signed: ………………………………………………

Title: …………………………………………………… Date: ………………

(The Policy will be reviewed by the Information Security Manager, usually 1 year on from the date signed.)