

# Information security management –

Part 2: Specification for information security  
management systems

## **BSI Private Circulation**

This draft is issued for a 3-month period of public comment. It is issued to all interested parties in both the UK and the 7799 International User Group Network (IUGNet). All comments will be given consideration after the public comment period prior to the publication of the new edition of the standard.

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within organizations participating in the public comment period or representative organisations of the IUGNet for briefing purposes.

Electronic circulation is limited to dissemination by e-mail within such an organizations or within representative organisations of the IUGNet.

## Editor Notes on the Revised Version

This revised version of the BS 7799 Part 2 standard has been developed primarily to:

- Harmonise it with other management system standards such as ISO 9001 and ISO 14001.
- Introduce and apply the PDCA (Plan, Do, Check and Act) process model as part of a management system approach to developing, implementing, and improving the effectiveness of an organisation's information security management system.

The following are specific highlights of this revised edition of Part 2:

1. **Sections 4 to 7** of this standard specify the ISMS based PDCA process. This is an amplification of the process that is contained in **Section 3** of the 1999 version of Part 2.
2. The control objectives and controls contained in **Section 4** of the 1999 version of Part 2 have now been included in the **normative Annex A**. This Annex contains the control objectives and controls from ISO/IEC 17799:2000.
3. An informative annex (**Annex B**) has been included to provide guidance on the use and interpretation of this revised version.
4. An informative annex (**Annex C**) has been included to show the correspondence between the clauses of BS 7799-2:2002, ISO 9001:2000 and ISO 14001:1996.
5. During the development of this revision majority opinion favoured removal of the definition of **Statement of Applicability (SoA)** from the main body of the text and to add the concept of a SoA in Annex B (see Annex B 1.4) together with the notion of a **Summary of Controls (SoC)**. In addition, text has been added to the Scope in keeping with other management system standards regarding the exclusions and claims of conformity to this standard.

BDD2 Panel 3 together with the BS 7799 International User Group (IUG) has developed this revised version in order to include requirements from an international perspective. This development is based on contributions and discussion and review of these contributions from experts and organizations from various countries.

## Foreword

This British Standard has been prepared by the BSI Committee BDD/2, which deals with Information security management. It supersedes BS 7799-2:1999, which is withdrawn.

This new edition has been produced to harmonise it with other management system standards such as ISO 9001 and ISO 14001. This new edition also introduces a Plan-Do-Check-Act process model as part of a management system approach to developing, implementing, and improving the effectiveness of an organisation's information security management system.

The control objectives and controls referred to in this edition are directly derived from and aligned with those listed in ISO/IEC 17799:2000 (the ISO/IEC version of BS 7799 Part 1:1999). The list of control objectives and controls of this British Standard are not exhaustive and an organisation may consider that additional control objectives and controls are necessary.

Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organisation.

In 1999 OECD issued a document entitled 'OECD principles of Corporate Governance' in response to the demands that organisations should be 'good corporate citizens'. This document is primarily written to address issues relating to publicly quoted companies however the principles, excluding references to shareholders, are equally applicable to other types of organisation.

These principles are being implemented around the world for example:

- The Bank of International Settlements has issued guidance to its members on this subject,
- The London Stock exchange has amended its listing requirements (Yellow Book) to include corporate governance requirements and the Institute of Chartered Accountants in England and Wales has issued guidance for directors on compliance with the combined code relating to Internal Control requirements - this is known as Turnbull.

Information security and any ISMS should form an integrated part of any Internal Control system created as part of the Corporate Governance procedures. Indeed, Turnbull requires (a) a business risk analysis (Plan); (b) internal controls to manage the applicable risks (Do); (c) a management review to verify effectiveness (Check) and (d) action as necessary (Act). Necessary internal controls encompass those suggested by IS 17799. The whole Turnbull approach fits together quite elegantly with that adopted by this document – BS 7799-2.

Annex A is normative and contains the control objectives and controls from ISO/IEC 17799:2000. Annex B is informative and provides guidance on the use and interpretation of this British Standard. Annex C is informative and shows the correspondence between the clauses of BS 7799-2:2002, ISO 9001:2000 and ISO 14001:1996.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

**Compliance with a British Standard does not of itself confer immunity from legal obligations.**

## Introduction

### 0.1 General

The adoption of an information security management system (ISMS) should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by security and business needs and objectives, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that simple situations require simple ISMS solutions.

This standard can be used by internal and external parties, including certification bodies, to assess the organization's ability to meet customer, the organization's own and regulatory requirements.

### 0.2 Process Approach

This standard promotes the adoption of a process approach for developing, implementing, and improving the effectiveness of an organisation's information security management system.

An organization must identify and manage many activities to function effectively. An activity using resources, and managed in order to enable the transformation of inputs into outputs, can be considered as a process. Often the output from one process directly forms the input to the next.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a process approach.

The process approach encourages its user emphasizes the importance of:

- a) understanding business information security requirements and the need to establish policy and objectives for information security,
- b) implementing and operating controls in the context of managing the organisation's overall business risk,
- c) monitoring and reviewing the performance and effectiveness of the ISMS, and
- d) continual improvement based on objective measurement.

The model adopted in this standard of a process based ISMS is illustrated in Figure 1. This illustrates the process linkages presented in Sections 3 to 7 of this document. The process model known as "Plan-Do-Check-Act" (PDCA) can be applied to all processes. The PDCA process model can be described briefly as follows:

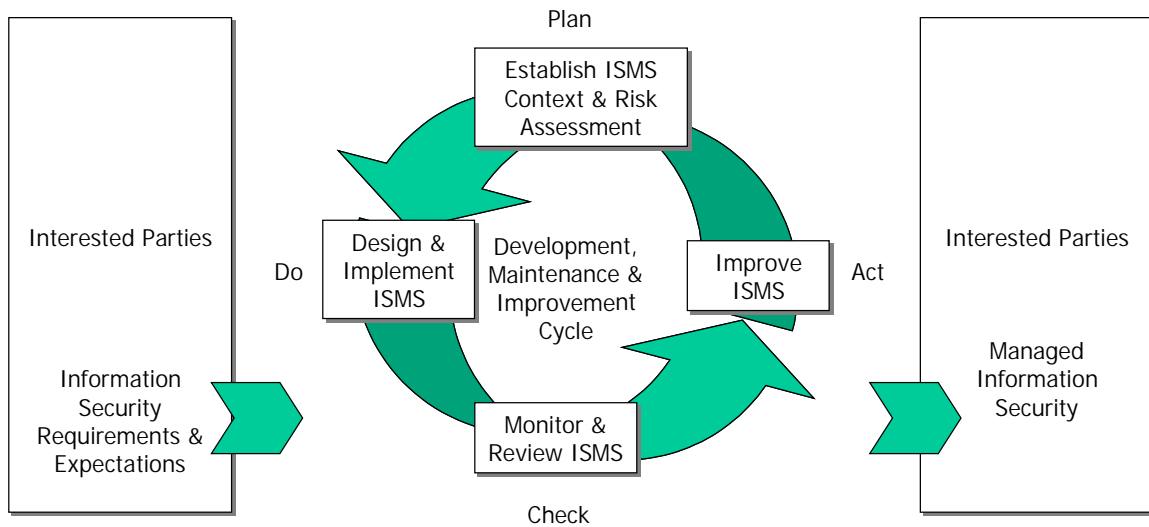


Figure 1 PDCA Process Model

**Plan (establish ISMS context)** Establish security policies, objectives, targets, processes and procedures relevant to controlling risk and improving information security to deliver results in accordance with the organisation's overall policies and objectives.

**Do (design & implement)** Implement and operate the policies (processes and procedures).

**Check (monitor & review)** Measure and assess process performance against policies, objectives and practical experience and report the results to decision makers.

**Act (improve)** Take corrective and preventative actions to further improve the process performance.

### 0.3 Compatibility with other management systems

This standard is aligned with ISO 9001:2000 and ISO 14001:1996 in order to support consistent and integrated implementation and operation of management standards. The tables in Annex C illustrate the corresponding relationship between the respective clauses and sections of BS 7799-2, ISO 9001 and ISO 14001.

This standard enables an organization to align or integrate its information security management system with related management system requirements. It is possible for an organization to adapt its existing management system(s) in order to establish an information security management system that complies with the requirements of this standard.

## 1 Scope

### 1.1 General

This standard specifies requirements for establishing, implementing, and maintaining a documented ISMS within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof (see Annex B provides informative guidance on the use of the specification).

### 1.2 Application

The requirements set out in this standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature of business. Where any requirement(s) of this standard cannot be applied due to the nature of an organization and its business, this can be considered for exclusion.

Where exclusions are made, claims of conformity to this standard are not acceptable unless such exclusions do not affect the organization's ability, or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements. Any exclusions of the controls in Annex A need to be justified by the results of the risk assessment, proving that the particular control(s) excluded are not necessary to achieve and maintain information security in line with the security requirements of the ISMS considered (see also Annex B1.4 Summary of Controls). Excluding any of the elements of the PDCA process described in this standard is not acceptable.

## 2 Normative References

ISO 9001: 2000 Quality management systems - Requirements

ISO/IEC 17799:2000 Information technology - Code of practice for information security management.

## 3 Terms and definitions

For the purposes of this standard, the definitions for information security, risk assessment and risk management given in ISO/IEC 17799 apply.

## 4 Information security management system

### 4.1 General Requirements

The organisation shall develop, implement, maintain and continually improve a documented ISMS to establish policy and objectives for information security within the context of the organisation's overall business activities and risk. For the purposes of this standard the process used is based on the PDCA process model as illustrated in the Figure 2.

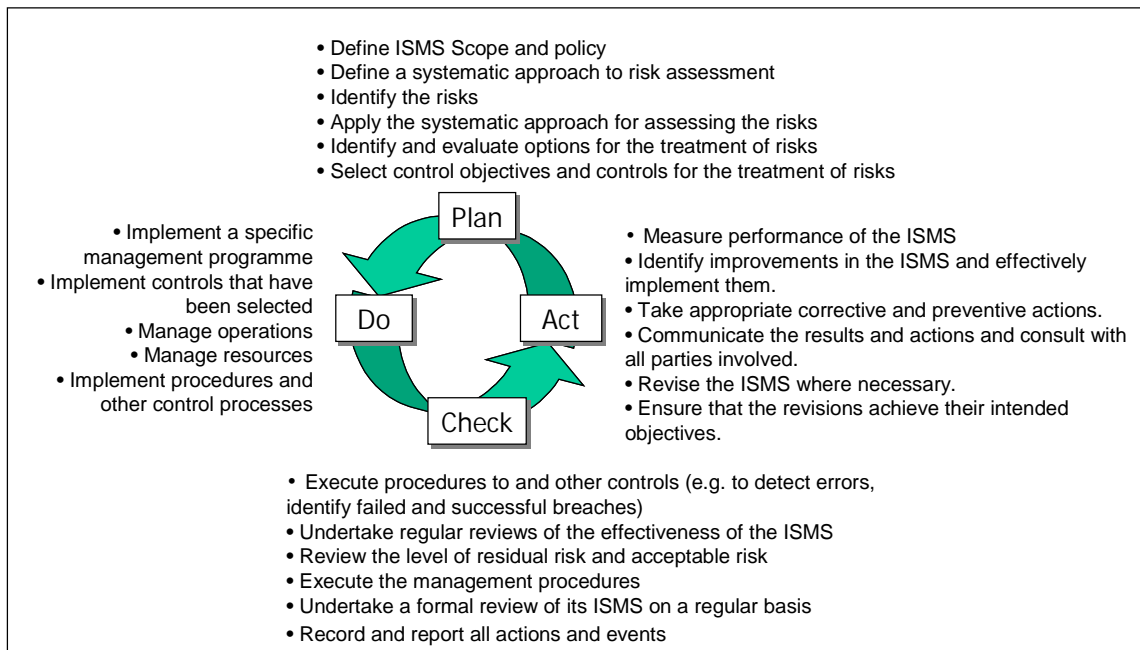


Figure 2 Process Elements

## 4.2 Process

### 4.2.1 Plan - Establishing ISMS Context & Risk Assessment

The organisation shall:

a) Define ISMS scope and policy:

The organisation and its management must define a business policy that includes a framework for setting its objectives and targets and establishes an overall sense of direction and principles for action in regard to information security. This policy must address legal or regulatory requirements and their context. It must establish the strategic, organisational and risk management context in which the rest of the process will take place. This shall be defined in terms of the characteristics of the business, the organization, its location, assets and technology. Criteria against which risk will be evaluated shall be established and the structure of the analysis defined.

b) Define a systematic approach to risk assessment:

Identify a method of risk assessment that is suitable to the ISMS being considered, and the identified business information security, legal and regulatory requirements. Set policy and objectives for the ISMS to reduce risks to acceptable levels. Determine criteria for accepting the risks.

c) Identify the risks:

- Identify the assets within the control of the ISMS;
- Identify the threats to those assets;
- Identify the vulnerabilities that might be exploited by the threats;

- Identify the impacts that potential losses of confidentiality, integrity and availability have on the assets.
- d) Apply the systematic approach defined in b) for assessing the risks:
- Assess the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the assets;
  - Assess the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.
  - Evaluate risks using the criteria established in b for determining the acceptable levels of risk.
- e) Identify and evaluate options for the treatment of risks;
- Possible actions include:
- Applying appropriate internal security controls;
  - Knowingly and objectively accepting risks, providing they clearly satisfy the organisation's policy and criteria on risk tolerance;
  - Avoiding risks;
  - Transferring risks to other parties e.g. Insurers, suppliers.
- f) Select control objectives and controls for the treatment of risks:
- Select and document the control objectives and physical, personal, administrative, procedural, legal and technical security measures and other controls to meet policy and objectives and to reduce the risks to an acceptable level. The control objectives and controls that can be selected are specified in Annex A and guidance on their implementation is given in ISO/IEC 17799.
- NOTE: Risk assessment may identify security risks requiring controls that are additional to the recommendations given in ISO/IEC 17799. These controls need to be justified on the basis of the conclusions of the risk assessment.
- g) Obtain management approval of the proposed residual risks and authorisation to implement and operate the ISMS.

### 4.2.2 Do - Implement and Operate the ISMS

The organisation shall:

- a) Implement selected controls:
- Identify the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks, including:
- Implement a specific management programme to achieve the identified security objectives, which includes consideration of funding and allocation of roles and responsibilities.
  - Implement controls that have been selected
  - Manage operations
  - Manage resources
  - Implement procedures and other controls capable of prompt detection of and response to security incidents

## 4.2.3 Check - Monitoring and Reviewing the ISMS

The organisation shall:

- a) Execute procedures to and other controls to:
  - Promptly detect errors in the results of processing;
  - Promptly identify failed and successful breaches in the security system;
  - Enable management to determine that the security activities delegated to people or automated have performed as expected;
  - Determine the actions taken to resolve a breach of security in the light of the business priorities;
  - Apply the lessons learnt from security experiences of other organisations as well as from within the organisation itself;
- b) Undertake regular reviews of the effectiveness of the ISMS taking into account results of security audits, incidents, suggestions and feedback from all stakeholders and other interested parties;
- c) Review the level of residual risk and acceptable risk taking into account changes to organisation, technology, business objectives and processes and external events including identified threats, and changes in social climate;
- d) Execute the management procedures to determine if the specified security procedures are in place, are in conformance with this standard and are working as intended;
- e) Undertake a formal review of its ISMS on a regular basis (at least an annual review cycle) to ensure that the scope remains adequate and improvements in the ISMS process are identified and implemented;
- f) Record and report all actions and events that could have an impact on the effectiveness or performance of the ISMS.

## 4.2.4 Act - Improve the ISMS

The organisation shall on an ongoing basis:

- a) Measure performance of the ISMS in meeting security policy and objectives.
- b) Identify improvements in the ISMS and effectively implement them.
- c) Take appropriate corrective and preventive actions.
- d) Communicate the results and actions and consult with all parties involved.
- e) Revise the ISMS where necessary.
- f) Ensure that the revisions achieve their intended objectives.

## 4.3 Documentation requirements

### 4.3.1 General

The information security management system documentation shall include:

- a) Documented statements of the security policy and security objectives,
- b) An ISMS manual (see 4.3.2),
- c) Risk Assessment Report,
- d) Risk Treatment Plan,

- e) Documents needed by the organization to ensure the effective planning, operation and control of its information security processes, and
- f) Records required by this standard (see 4.3.4).
- g) A summary of the controls implemented including details of and justification for any exclusions (see Annex B 1.4 Summary of Controls).

NOTE: The extent of the ISMS documentation can differ from one organization to another due to

- a) The size of organization and type of activities,
- b) The scope and complexity of the security requirements and the system being managed.

All documentation shall be readily available to members of staff who are required to use it in accordance with the ISMS policy.

### 4.3.2 ISMS manual

The organization shall establish and maintain an ISMS manual that includes

- a) The scope of the ISMS (see 4.2.1),
- b) Processes in support of the ISMS
- c) The documented procedures established for the ISMS, or reference to them.

### 4.3.3 Control of documents

Documents required by the ISMS shall be protected and controlled. Records are a special type of document and shall be controlled according to the requirements given in 4.3.4. A documented procedure shall be established to define the controls needed to:

- a) Approve documents for adequacy prior to issue,
- b) Review and update as necessary and re-approve documents,
- c) Ensure that changes and the current revision status of documents are identified,
- d) Ensure that relevant versions of applicable documents are available at points of use,
- e) Ensure that documents remain legible and readily identifiable,
- f) Ensure that documents of external origin are identified,
- g) Ensure that the distribution of documents is appropriately controlled,
- h) Prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

### 4.3.4 Control of Records

Records established and maintained to provide evidence of conformity to requirements and of the effective operation of the ISMS shall be controlled. Legal requirements in each country need to be considered. Records shall remain legible, readily identifiable and retrievable. A documented procedure shall be established to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of records.

Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of security incidents related to the ISMS.

The need for and extent of records shall be determined by a management process, which records key decisions and takes into account the use to which the records will be put and the risks associated with the lack of records.

NOTE: Records support the check activities in the PDCA process model for the benefit of management, as well as allowing a third party (such as an auditor) to determine conformance.

## 5 Management responsibility

### 5.1 Management commitment

Management shall provide evidence of its commitment to the development and improvement of the ISMS by:

- a) Communicating to the organisation the importance of meeting information security objectives as well as legal and regulatory requirements and the need for continual improvement;
- b) Establishing security policy, objectives and plans;
- c) Conducting management reviews of the ISMS;
- d) Deciding the level of acceptable risk.

### 5.2 Resource management

#### 5.2.1 Provision of resources

The organisation shall determine and provide the necessary resources to

- a) Set up and maintain an ISMS;
- b) Implement the ISMS;
- c) Ensure security procedures support the business requirements;
- d) Identify and address legal and regulatory requirements and contractual security obligations;
- e) Maintain adequate security by correct application of all implemented controls;
- f) Carry out reviews when necessary, and to react appropriately to the results of these reviews;
- g) Where required, improve the processes of the ISMS.

#### 5.2.2 Training, awareness and competency

All personnel who are assigned responsibilities defined in the ISMS shall be competent to perform the required tasks. Competence can be achieved by various means including the following:

- a) Provide competent training to satisfy these needs;
- b) Evaluate the effectiveness of the training provided;
- c) Ensure that its employees are aware of the relevance and importance of their activities and how they contribute to the achievement of the security objectives.

It is necessary to maintain appropriate records of education, experience and qualifications (see 4.3.4).

## **6 Management Review of the ISMS**

### **6.1 General**

The ISMS shall include documented procedures to

- a) Identify vulnerabilities or threats not adequately addressed in the previous risk assessment;
- b) Identify techniques, products or procedures, which could be used in the organisation to improve the ISMS, its performance or effectiveness;
- c) Identify relevant changes to organisational environment which require review of ISMS
- d) Management shall conduct periodic reviews of the ISMS. The reviews shall be clearly documented.
- e) The procedures to effect information security shall be modified, as necessary, to respond to those internal or external events that may impact on the ISMS, including changes to
  - Business requirements;
  - Business processes to effect the existing business requirements;
  - Regulatory or legal environment;
  - Levels of risk and/or levels of risk acceptance.

### **6.2 Audits**

Management shall ensure periodic audits are conducted at least annually.

## **7 ISMS Improvement**

### **7.1 Continual improvement**

The organization shall seek to continually improve the effectiveness of the ISMS through the use of the security policy, security objectives, results of security reviews and audits, corrective and preventive actions and management review.

### **7.2 Corrective action**

The organisation shall determine action to eliminate the cause of nonconformities of the implementation, operation and use of the ISMS in order to prevent recurrence. The documented procedures within the ISMS for corrective action shall define requirements for:

- a) Identifying nonconformities of the ISMS, its implementation or its operation;
- b) Determining the causes of nonconformity;
- c) Evaluating the need for actions to ensure that nonconformities do not recur;
- d) Determining and implementing the corrective action needed;
- e) Recording results of action taken;
- f) Reviewing of corrective action taken, e.g. the effectiveness.

## 7.3 Preventive action

The organisation shall determine action to eliminate the causes of potential nonconformities in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

- a) Identifying potential nonconformities and their causes;
- b) Determining and ensuring the implementation of preventive action needed;
- c) Recording results of action taken;
- d) Reviewing of preventive action taken;
- e) Identifying changed risks and ensuring that attention is focused on significantly changed risks.

## Annex A Control Objectives and Controls

(Normative Annex)

### A.1 Introduction

The control objectives and controls listed in the tables A.3 to A.12 below are directly derived from and aligned with those listed in ISO/IEC 17799 clauses 3 to 12. The lists in these tables are not exhaustive and an organisation may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables are selected as part of the PDCA process specified in clause 4.2.1 of this standard.

### A.2 Guidance on best practice

ISO/IEC 17799 provides guidance on best practice in support of the requirements listed in the Tables A.3 to A.12. Clauses 3 to 12.

### A.3 Security policy

			ISO/IEC 17799 numbering
<b>A.3.1 Information security policy</b>			3.1
<i>Control objective:</i> To provide management direction and support for information security.			
<b>Controls</b>			
A3.1.1	Information security policy document	A policy document shall be approved by management, published and communicated, as appropriate, to all employees.	3.1.1
A3.1.2	Review and evaluation	The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate,	3.1.2

**A.4 Security organisation**

			ISO/IEC 17799 numbering
<p><b>A.4.1 Information security infrastructure</b>  <i>Control objective: To manage information security within the organisation.</i></p>			4.1
<b>Controls</b>			
A.4.1.1	Management information security forum	A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place.	4.1.1
A.4.1.2	Information security co-ordination	In large organizations, a cross functional forum of management representatives from relevant parts of the organization shall be used to co-ordinate the implementation of information security controls.	4.1.2
A.4.1.3	Allocation of information security responsibilities	Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.	4.1.3
A.4.1.4	Authorisation process for information processing facilities	A management authorization process for new information processing facilities shall be established.	4.1.4
A.4.1.5	Specialist information security advice	Advice on information security provided by in-house or specialists advisors shall be sought and co-ordinated throughout the organization.	4.1.5
A.4.1.6	Co-operation between organisations	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.	
A.4.1.7	Independent review of information security	The implementation of the information security policy shall be reviewed independently.	4.1.6
<p><b>A.4.2 Security of third party access</b>  <i>Control objective: To maintain the security of organisational information processing facilities and information assets accessed by third parties.</i></p>			4.2
<b>Controls</b>			
A.4.2.1	Identification of risks from third party access	The risks associated with access to organizational information processing facilities by third parties shall be assessed and appropriate security controls implemented.	4.2.1
A.4.2.2	Security requirements in third party contracts	Arrangements involving third party access to organizational information processing facilities shall be based on a formal contract containing all necessary security requirements.	4.2.2

<b>A.4.3 Outsourcing</b> <i>Control objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.</i>			4.3
<b>Controls</b>			
A.4.3.1	Security requirements in outsourcing contracts	The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks and/or desk top environments shall be addressed in a contract agreed between the parties.	4.3.1

**A.5 Asset classification and control**

			ISO/IEC 17799 numbering
<b>A.5.1 Accountability for assets</b> <i>Control objective: To maintain appropriate protection of organisational assets.</i>			5.1
<b>Controls</b>			
A.5.1.1	Inventory of assets	An inventory of all important assets shall be drawn up and maintained.	
<b>A.5.2 Information classification</b> <i>Control objective: To ensure that information assets receive an appropriate level of protection.</i>			5.2
<b>Controls</b>			
A.5.2.1	Classification guidelines	Classifications and associated protective controls for information shall take account of business needs for sharing or restricting information, and the business impacts associated with such needs.	5.2.1
A.5.2.2	Information labelling and handling	An appropriate set of procedures shall be defined for information labelling and handling in accordance with the classification scheme adopted by the organization.	5.2.2

**A.6 Personnel security**

			ISO/IEC 17799 numbering
<p><b>A.6.1 Security in job definition and resourcing</b>  <i>Control objective: To ensure the risks of human error, theft, fraud or misuse of facilities.</i></p>			6.1
<b>Controls</b>			
A.6.1.1	Including security in job responsibilities	Security roles and responsibilities, as laid down in the organisation's information security policy shall be documented in job definitions where appropriate.	6.1.1
A.6.1.2	Personnel screening and policy	Verification checks on permanent staff shall be carried out at the time of job applications.	6.1.2
A.6.1.3	Confidentiality agreements	Employees shall sign a confidentiality agreement as part of their initial terms and conditions of employment.	6.1.3
A.6.1.4	Terms and conditions of employment	The terms and conditions of employment shall state the employee's responsibility for information security.	6.1.4
<p><b>A.6.2 User training</b>  <i>Control objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.</i></p>			6.2
<b>Controls</b>			
A.6.2.1	Information security education and training	All employees of the organization and, where relevant, third party users, shall receive appropriate training and regular updates in organizational policies and procedures.	
<p><b>A.6.3 Responding to security incidents and malfunctions</b>  <i>Control objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.</i></p>			6.3
<b>Controls</b>			
A.6.3.1	Reporting security incidents	Security incidents shall be reported through appropriate management channels as quickly as possible.	6.3.1
A.6.3.2	Reporting security weaknesses	Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services.	6.3.2
A.6.3.3	Reporting software malfunctions	Procedures shall be established for reporting software malfunctions.	6.3.3
A.6.3.4	Learning from incidents	Mechanisms shall be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.	6.3.4

A.6.3.5	Disciplinary process	The violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process.	6.3.5
---------	----------------------	--	-------

**A.7 Physical and environmental security**

			ISO/IEC 17799 numbering
<b>A.7.1 Secure areas</b>			7.1
<i>Control objective: To prevent unauthorised access, damage and interference to business premises and information.</i>			
<b>Controls</b>			
A.7.1.1	Physical security perimeter	Organizations shall use security perimeters to protect areas which contain information processing facilities.	7.1.1
A.7.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	7.1.2
A.7.1.3	Securing offices, rooms and facilities	Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.	7.1.3
A.7.1.4	Working in secure areas	Additional controls and guidelines for working in secure areas shall be used to enhance the security of the secure area.	7.1.4
A.7.1.5	Isolated delivery and loading areas	Delivery and loading areas shall be controlled, and if possible, isolated from information processing facilities to avoid unauthorized access.	7.1.5
<b>A.7.2 Equipment security</b>			7.2
<i>Control objective: To prevent loss, damage or compromise of assets and interruption to business activities.</i>			
<b>Controls</b>			
A.7.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	7.2.1
A.7.2.2	Power supplies	Equipment shall be protected from power failures and other electrical anomalies.	7.2.2
A.7.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	7.2.3
A.7.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	7.2.4

A.7.2.5	Security of equipment off-premises	Security procedures and controls shall be used to secure equipment used outside an organization's premises.	7.2.5
A.7.2.6	Secure disposal or re-use of equipment	Information shall be erased from equipment prior to disposal or re-use.	7.2.6
<b>A.7.3 General controls</b> <i>Control objective: To prevent compromise or theft of information and information processing facilities.</i>			7.3
<b>Controls</b>			
A.7.3.1	Clear desk and clear screen policy	Organizations shall have a clear desk and a clear screen policy in order to reduce the risks of unauthorized access, loss of, and damage to information.	7.3.1
A.7.3.2	Removal of property	Equipment, information or software belonging to the organization shall not be removed without authorization.	7.3.2

## A.8 Communications and operations management

			ISO/IEC 17799 numbering
<b>A.8.1 Operational procedures and responsibilities</b> <i>Control objective: To ensure the correct and secure operation of information processing facilities</i>			8.1
<b>Controls</b>			
A.8.1.1	Document operating procedures	The operating procedures identified in the security policy shall be documented and maintained.	8.1.1
A.8.1.2	Operational change control	Changes to information processing facilities and systems shall be controlled.	8.1.2
A.8.1.3	Incident management procedures	Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents.	8.1.3
A.8.1.4	Segregation of duties	Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.	8.1.4
A.8.1.5	Separation of development and operational facilities	Development and testing facilities shall be separated from operational facilities.	8.1.5
A.8.1.6	External facilities management	Prior to using external facilities management services, the risks shall be identified and appropriate controls agreed with the contractor, and incorporated into the contract.	8.1.6
<b>A.8.2 System planning and acceptance</b> <i>Control objective: To minimise the risk of systems failure</i>			8.2

<b>Controls</b>			
A.8.2.1	Capacity planning	Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.	8.2.1
A.8.2.2	System acceptance	Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.	8.2.2
<b>A.8.3 Protection against malicious software</b> <i>Control objective: To protect the integrity of software and information</i>			8.3
<b>Controls</b>			
A.8.3.1	Controls against malicious software	Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.	8.3.1
<b>A.8.4 Housekeeping</b> <i>Control objective: To maintain the integrity and availability of information processing and communication services</i>			8.4
<b>Controls</b>			
A.8.4.1	Information back-up	Back-up copies of essential business information and software shall be taken regularly.	8.4.1
A.8.4.2	Operator logs	Operational staff shall maintain a log of their activities.	8.4.2
A.8.4.3	Fault logging	Faults shall be reported and corrective action taken.	8.4.3
<b>A.8.5 Network management</b> <i>Control objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure</i>			8.5
<b>Controls</b>			
A.8.5.1	Network controls	A range of controls shall be implemented to achieve and maintain security in networks.	8.5.1
<b>A.8.6 Media handling and security</b> <i>Control objective: To prevent damage to assets and interruptions to business activities.</i>			8.6
<b>Controls</b>			
A.8.6.1	Management of removable computer media	The management of removable computer media, such as tapes, disks, cassettes and printed reports shall be controlled.	8.6.1

A.8.6.2	Disposal of media	Media shall be disposed of securely and safely when no longer required.	8.6.2
A.8.6.3	Information handling procedures	Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse.	8.6.3
A.8.6.4	Security of system documentation	System documentation shall be protected from unauthorized access.	8.6.4
<b>A.8.7 Exchanges of information and software</b>			8.7
<i>Control objective: To prevent loss, modification or misuse of information exchanged between organizations.</i>			
<b>Controls</b>			
A.8.7.1	Information and software exchange agreements	Agreements, some of which may be formal, shall be established for the exchange of information and software (whether electronic or manual) between organizations.	8.7.1
A.8.7.2	Security of media in transit	Media being transported shall be protected from unauthorized access, misuse or corruption.	8.7.2
A.8.7.3	Electronic commerce security	Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.	8.7.3
A.8.7.4	Security of electronic mail	A policy for the use of electronic mail shall be developed and controls put in place to reduce security risks created by electronic mail.	8.7.4
A.8.7.5	Security of electronic office systems	Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.	8.7.5
A.8.7.6	Publicly available systems	There shall be a formal authorization process before information is made publicly available and the integrity of such information shall be protected to prevent unauthorized modification.	8.7.6
A.8.7.7	Other forms of information exchange	Procedures and controls shall be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.	8.7.7

**A.9 Access control**

			ISO/IEC 17799 numbering
<b>A.9.1 Business requirement for access control</b>			9.1
<i>Control objective: To control access to information.</i>			
<b>Controls</b>			
A.9.1.1	Access control policy	Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.	9.1.1

<b>A.9.2 User access management</b> <i>Control objective: To prevent unauthorized access to information systems.</i>			9.2
<b>Controls</b>			
A.9.2.1	User registration	There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.	9.2.1
A.9.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	9.2.2
A.9.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	9.2.3
A.9.2.4	Review of user access rights	Management shall conduct a formal process at regular intervals to review users' access rights.	9.2.4
<b>A.9.3 User responsibilities</b> <i>Control objective: To prevent unauthorized user access.</i>			9.3
<b>Controls</b>			
A.9.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	9.3.1
A.9.3.2	Unattended user equipment	Users shall be required to ensure that unattended equipment has appropriate protection.	9.3.2
<b>A.9.4 Network access control</b> <i>Control objective: Protection of networked services.</i>			9.4
<b>Controls</b>			
A.9.4.1	Policy on use of network services	Users shall only have direct access to the services that they have been specifically authorized to use.	9.4.1
A.9.4.2	Enforced path	The path from the user terminal to the computer service shall be controlled.	9.4.2
A.9.4.3	User authentication for external connections	Access by remote users shall be subject to authentication.	9.4.3
A.9.4.4	Node authentication	Connections to remote computer systems shall be authenticated.	9.4.4
A.9.4.5	Remote diagnostic port protection	Access to diagnostic ports shall be securely controlled.	9.4.5
A.9.4.6	Segregation in networks	Controls shall be introduced in networks to segregate groups of information services, users and information systems.	9.4.6
A.9.4.7	Network connection control	The connection capability of users shall be restricted in shared networks, in accordance with the access control policy.	9.4.7
A.9.4.8	Network routing control	Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.	9.4.8

A.9.4.9	Security of network services	A clear description of the security attributes of all network services used by the organisation shall be provided.	9.4.9
<b>A.9.5 Operating system access control</b> <i>Control objective: To prevent unauthorized computer access.</i>			9.5
<b>Controls</b>			
A.9.5.1	Automatic terminal identification	Automatic terminal identification shall be considered to authenticate connections to specific locations and to portable equipment.	9.5.1
A.9.5.2	Terminal log-on procedures	Access to information services shall use a secure logon process.	9.5.2
A.9.5.3	User identification and authentication	All users shall have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.	9.5.3
A.9.5.4	Password management system	Password management systems shall provide an effective, interactive facility which ensures quality passwords.	9.5.4
A.9.5.5	Use of system utilities	Use of system utility programs shall be restricted and tightly controlled.	9.5.5
A.9.5.6	Duress alarm to safeguard users	Duress alarms shall be provided for users who might be the target of coercion.	9.5.6
A.9.5.7	Terminal time-out	Inactive terminals in high risk locations or serving high risk systems shall shut down after a defined period of inactivity to prevent access by unauthorized persons.	9.5.7
A.9.5.8	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.	9.5.8
<b>A.9.6 Application access control</b> <i>Control objective: To prevent unauthorized access to information held in information systems.</i>			9.6
<b>Controls</b>			
A.9.6.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	9.6.1
A.9.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.	9.6.2
<b>A.9.7 Monitoring system access and use</b> <i>Control objective: To detect unauthorized activities.</i>			9.7
<b>Controls</b>			
A.9.7.1	Event logging	Audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	9.7.1

A.9.7.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.	9.7.2
A.9.7.3	Clock synchronization	Computer clocks shall be synchronized for accurate recording.	9.7.3
<b>A.9.8 Mobile computing and teleworking</b> <i>Control objective: To ensure information security when using mobile computing and teleworking facilities.</i>			9.8
<b>Controls</b>			
A.9.8.1	Mobile computing	A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.	9.8.1
A.9.8.2	Teleworking	Policies, procedures and standards shall be developed to authorize and control teleworking activities.	9.8.2

## A.10 System development and maintenance

			ISO/IEC 17799 numbering
<b>A.10.1 Security requirements of systems</b> <i>Control objective: To ensure that security is built into information systems.</i>			10.1
<b>Controls</b>			
A.10.1.1	Security requirements analysis and specification	Business requirements for new systems, or enhancements to existing systems shall specify the requirements for controls.	10.1.1
<b>A.10.2 Security in application systems</b> <i>Control objective: To prevent loss, modification or misuse of user data in application systems.</i>			10.2
<b>Controls</b>			
A.10.2.1	Input data validation	Data input to application systems shall be validated to ensure that it is correct and appropriate.	10.2.1
A.10.2.2	Control of internal processing	Validation checks shall be incorporated into systems to detect corruption of the data processed.	10.2.2
A.10.2.3	Message authentication	Message authentication shall be used for applications where there is a security requirement to protect the integrity of the message content.	10.2.3

A.10.2.4	Output data validation	Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	10.2.4
<b>A.10.3 Cryptographic controls</b> <i>Control objective: To protect the confidentiality, authenticity or integrity of information.</i>			10.3
<b>Controls</b>			
A.10.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for the protection of information shall be developed.	10.3.1
A.10.3.2	Encryption	Encryption shall be applied to protect the confidentiality of sensitive or critical information.	10.3.2
A.10.3.3	Digital signatures	Digital signatures shall be applied to protect the authenticity and integrity of electronic information.	10.3.3
A.10.3.4	Non-repudiation services	Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action.	10.3.4
A.10.3.5	Key management	A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques.	10.3.5
<b>A.10.4 Security of system files</b> <i>Control objective: To ensure that IT projects and support activities are conducted in a secure manner.</i>			10.4
<b>Controls</b>			
A.10.4.1	Control of operational software	Control shall be applied to the implementation of software on operational systems.	10.4.1
A.10.4.2	Protection of system test data	Test data shall be protected and controlled.	10.4.2
A.10.4.3	Access control to program source library	Strict control shall be maintained over access to program source libraries.	10.4.3
<b>A.10.5 Security in development and support processes</b> <i>Control objective: To maintain the security of application system software and information.</i>			10.5
<b>Controls</b>			
A.10.5.1	Change control procedures	The implementation of changes shall be strictly controlled by the use of formal change control procedures to minimize the corruption of information systems.	10.5.1
A.10.5.2	Technical review of operating system changes	Application systems shall be reviewed and tested when changes occur.	10.5.2
A.10.5.3	Restrictions on changes to software packages	Modifications to software packages shall be discouraged and essential changes strictly controlled.	10.5.3

A.10.5.4	Covert channels and Trojan code	The purchase, use and modification of software shall be controlled and checked to protect against possible covert channels and Trojan code.	10.5.4
A.10.5.5	Outsourced software development	Controls shall be applied to secure outsourced software development.	10.5.5

### A.11 Business continuity management

			ISO/IEC 17799 numbering
<b>A.11.1 Aspects of business continuity management</b> <i>Control objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.</i>			11.1
<b>Controls</b>			
A.11.1.1	Business continuity management process	There shall be a managed process in place for developing and maintaining business continuity throughout the organization.	11.1.1
A.11.1.2	Business continuity and impact analysis	A strategy plan, based on appropriate risk assessment, shall be developed for the overall approach to business continuity.	11.1.2
A.11.1.3	Writing and implementing continuity plans	Plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.	11.1.3
A.11.1.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.	11.1.4
A.11.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans shall be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.	11.1.5

### A.12 Compliance

			ISO/IEC 17799 numbering
<b>A.12.1 Compliance with legal requirements</b> <i>Control objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.</i>			12.1

<b>Controls</b>			
A.12.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements shall be explicitly defined and documented for each information system.	12.1.1
A.12.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.	12.1.2
A.12.1.3	Safeguarding of organizational records	Important records of an organization shall be protected from loss, destruction and falsification.	12.1.3
A.12.1.4	Data protection and privacy of personal information	Controls shall be applied to protect personal information in accordance with relevant legislation.	12.1.4
A.12.1.5	Prevention of misuse of information processing facilities	Management shall authorize the use of information processing facilities and controls shall be applied to prevent the misuse of such facilities.	12.1.5
A.12.1.6	Regulation of cryptographic controls	Controls shall be in place to ensure compliance with national agreements, laws regulations or other instruments to control the access to or use of cryptographic controls.	12.1.6
A.12.1.7	Collection of evidence	Where action against a person or organisation involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. This shall include compliance with any published standard or code of practice for the production of admissible evidence.	12.1.7
<b>A.12.2 Reviews of security policy and technical compliance</b> <i>Control objective: To ensure compliance of systems with organizational security policies and standards.</i>			12.2
<b>Controls</b>			
A.12.2.1	Compliance with security policy	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly and all areas within the organization shall be subject to regular review to ensure compliance with security policies and standards.	12.2.1
A.12.2.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.	12.2.2
<b>A.12.3 System audit considerations</b> <i>Control objective: To maximize the effectiveness of and to minimize interference to/from the system audit process.</i>			12.3
<b>Controls</b>			
A.12.3.1	System audit controls	Audits of operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.	12.3.1
A.12.3.2	Protection of system audit tools	Access to system audit tools shall be protected to prevent any possible misuse or compromise.	12.3.2

## **Annex B Guidance Notes on Use of the Standard**

### **(Informative Annex)**

## **B 1 Overview**

### **B 1.1 PDCA Model**

Setting up and managing an Information Security Management System (ISMS) requires the same approach(es) as for any other management system. The process model described here follows a continuous cycle of activities: Plan, Do, Check, and Act. This can be described as a virtuous cycle because its purpose is to ensure that the best practices of your organization are documented, reinforced and improved with time.

### **B 1.2 Plan and Do**

A process of continual improvement often requires an initial investment: documenting practices, formalising the approach to risk management, determining methods of review and allocating resources. These activities are used to 'kick start' the cycle. They do not need to be completed before the review phases can become active. The Plan phase is used to ensure that the context and scope for the ISMS have been correctly established, that the information security risks are assessed and that a plan for the appropriate treatment of these risks is developed. The Do phase is used to implement the decisions made and solutions identified in the Plan phase.

### **B 1.3 Check and Act**

The Check and Act review phases are then used to reinforce, amend and improve the security solutions identified and implemented so far. The reviews can take place at any time and frequency, depending on what is most appropriate for the situation considered. In some systems they may have to be built into computerised processes to operate and respond immediately. Other processes will be needed to respond only when there is a security failure, where changes or additions are made to the information assets being protected, and when changes to threats and vulnerabilities occur. Finally, annual or other periodic reviews are needed to ensure that the whole management system is achieving its objectives.

### **B 1.4 Summary of controls**

The organisation may find it beneficial to make available a Summary of Controls (SoC) that is relevant and applicable to the organisation's ISMS. This can facilitate business relationships such as electronic outsourcing by providing a summary of the controls in place.

Note: "Statement of Applicability" (SoA) is a term introduced in BS 7799 Part 2: 1999 that is used for certification purposes as defined in EA-7/03 (The European Co-operation for Accreditation (EA) Guidelines for the Accreditation of Bodies Operating Certification/ Registration of Information Security Management Systems). The SoA requirements for certification as defined in EA-7/03 can be satisfied by making available to the certification audit team a summary of the risk assessment results together with the SoC (referred to above) reflecting these results.

## **B 2 Plan Phase**

### **B 2.1 Introduction**

The Plan activity of the Plan, Do, Check and Act cycle is designed to ensure that the context and scope for the ISMS have been correctly established, that all information security risks are identified and assessed, and that a plan for the appropriate treatment of these risks is developed. It is important that all stages of the Plan activity are documented for traceability and for the management of change.

### **B 2.2 Scope of the ISMS**

The ISMS may cover all or part of an organization. Dependencies, interfaces and assumptions about the boundary with the environment need to be clearly identified. This is particularly relevant if only part of an organization is within the scope of the ISMS. The scope may be divided in some way, for example into domains that will make subsequent risk management tasks simpler. The ISMS scope documentation should cover:

- a) The processes used to establish the scope and context of the information security management system;
- b) The strategic and organizational context(s);
- c) The organization's approach to information security risk management;
- d) Criteria for information security risk evaluation and the degree of assurance required;
- e) Identification of the information assets within the scope of the ISMS.

The ISMS may fall within the scope of control of a Quality Management System or another ISMS (of the same or a third party organisation). In such cases, only those controls the ISMS has management control over can be considered as being within scope of the ISMS. There are two possibilities for the management of the controls:

- a) The subordinate ISMS does not make use of the superior Management System control: in this case, that control is not subject to the PDCA activities of the subordinate ISMS.
- b) The subordinate ISMS does make use of the superior Management System control: in this case, that control is identified as an "external control" in the Plan activity of the subordinate ISMS. However, such external controls are not the subject of the Do, Check and Act activities of the subordinate ISMS, but it is still the responsibility of this subordinate ISMS to ensure that this external control provides sufficient protection.

### **B 2.3 Risk identification and assessment**

Risk assessment documentation should explain which risk assessment approach has been chosen, and why this approach is appropriate to the security requirements and the business environment. The approach adopted should aim to focus security effort and resources in a cost effective and efficient way. The documentation should also cover the tools and techniques that have been chosen, and why they are suitable for the chosen scope and risks and used correctly used to produce valid results.

The following risk assessment details should be documented:

- a) The valuation of the assets within the ISMS, including information about the valuation scale used;
- b) Identification of threats and vulnerabilities;
- c) Assessment of threats exploiting vulnerabilities, and of the impacts caused by such incidents might ;
- d) Calculation of the risks based on the results of the assessment, and identification of residual risks.

## **B 2.4 Risk treatment plan**

Organisations should create a detailed schedule, or risk treatment plan, showing for each identified risk:

- a) The method selected for treating the risk
- b) What controls are in place
- c) What additional controls are proposed
- d) The time frame over which the proposed controls are to be implemented.

The risk treatment plan is a coordination document defining the actions to reduce unacceptable risks and implement the required controls to protect information. An acceptable level of residual risk needs to be identified, and for each of these risks the appropriate action needs to be identified:

- a) Accept the residual risks;
- b) Transfer the risks; or
- c) Reduce the risks to an acceptable level.

It might not always be possible to reduce risks to an acceptable level within an acceptable cost, and then a decision needs to be made whether to add more controls, or accept the higher risks. When setting the acceptable level of risk the strength and cost of control should be compared to the potential cost of an incident.

Annex A provides specifications of many commonly relevant controls. ISO/IEC 17799:2000 provides additional information relevant to implementing these controls. Additional controls may need to be designed and implemented where the identified risks exceed the level that can be managed with those controls. The controls selected may be summarised as a SOC. This may be used to communicate your security approaches to business partners, senior management and staff.

Controls detecting security violations (in accordance with the ISMS) are very important means in the implementation of the PDCA model and should be put in place early enough to be effective, as well as controls providing prevention, deterrence, limitation and recovery.

The plan should include a schedule and priorities, a detailed work plan and responsibilities for the implementation of controls.

## **B 3 Do Phase**

### **B 3.1 Introduction**

The Do activity within the PDCA cycle is to implement selected controls and appropriate action to manage the information security risks in line with the decisions that have been taken in the Plan phase.

### **B 3.2 Resources, training and awareness**

Appropriate resources (people, time and money) need to be allocated to operate the ISMS and all security controls. This includes the documentation of all controls that have been implemented, and the active maintenance of the ISMS documentation. In addition, security awareness and training programmes should be put in place, in parallel with implementing the security controls.

The aim of the awareness programme is to generate an appropriate risk and security culture.

The success of the awareness programme should be monitored to ensure its continual effectiveness and topicality. Specific security training should be applied wherever necessary to support the awareness programme, and to enable all interested parties to fulfil their security tasks as required.

### **B 3.3 Risk treatment**

For those risks that have been assessed as acceptable, no further action is needed.

If the decision has been made to transfer risks, the necessary actions should be taken, e.g. using contracts, insurance arrangements and organisational structures such as partnership and joint ventures. In such cases, it should be ensured that the organisation(s) to which the risks are transferred, understand the nature of those risks and are able to manage the risks effectively.

Wherever the decision has been made to reduce the risks, the controls that have been selected need to be implemented. This should take place in line with the risk treatment plan prepared in the Plan activity. The successful implementation of the plan requires an effective management system, which specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria.

After unacceptable risks have been reduced or transferred, there may be residual risks that are retained. Controls should ensure that undesirable impacts or breaches are promptly identified and appropriately managed.

## **B 4 Check Phase**

### **B 4.1 Introduction**

The purpose of the Check activity is to ensure that the controls are working effectively and as intended. If they are found inadequate then the necessary corrective action needs to be determined. The execution of such actions is the subject of the Act phase of the PDCA cycle. It is important to realise that corrective action is only necessary:

- a) To maintain internal consistency of the ISMS documentation, and
- b) If the effect of not making the change would result in exposing the organization to an unacceptable risk.

The nature of the Check activity depends on the character of the PDCA cycle concerned, for example:

- a) The automatic actions of intrusion detection technology: a network intrusion detector checks whether the security of other components has been penetrated.
- b) The actions resulting from a security incident: Procedures for taking action in the event of a security incident may well disclose where controls have failed or where additional controls are required.

Other examples are detailed in the following subsections and are: routine checking, self-policing procedures, learning from others, audit and management review.

## **B 4.2 Routine checking**

These procedures are performed on a regular basis as part of the normal business process and are designed to detect errors in the results of processing. The procedures would include: reconciliation of bank accounts, inventory counts, resolving customer complaints etc. Clearly checks of this type need to be designed into systems to be performed often enough to limit any damage (and consequent liability) from any errors that occur.

In today's systems this type of check might be extended to include:

- a) Checks that there are no unintended and unauthorised changes to parameters governing the actions of software, that there are no unintended and unauthorised changes to data displayed on websites etc.
- b) Confirmation of completeness and accuracy of transfers of data between parties in 'virtual' companies in cyberspace.

## **B 4.3 Self-policing procedures**

A self-policing procedure is a control that has been constructed in such a manner that any error, or failure perpetrated during execution is capable of prompt detection. An example would be a device that monitors a network (e.g. such as equipment failures, errors) and raises an alarm. The alarm alerts the responsible people about the problem, who then have the task of diagnosing the cause of the problem and fixing it. However if the problem is not corrected within a defined period of time additional alarms are raised to more senior management, thus escalating the problem automatically.

## **B 4.4 Learning from others**

One way to identify where the organisation's procedures are sub-optimal is to identify where other organisations deal with problems more effectively. This learning applies both to the technical software and to the management activities. There are many sources, that identify vulnerabilities in technology and software. Organisations should refer to these frequently and make the necessary updates to their software.

Information on management techniques is exchanged and discussed in many forums, professional societies, and user groups and there are many articles in the technical and management press and conferences etc where organisations may learn how other tackle similar problems.

## **B 4.5 Audit**

The overall objective is to check over a specified regular audit period (which should last no more than one year) that all aspects of the ISMS are functioning as intended. A sufficient number of audits should be planned so that the audit task is spread uniformly over the chosen period. Management should ensure that there is evidence that confirms that:

- a) The information security policy is still an accurate reflection of the business requirements.
- b) The documented procedures are being followed (i.e. within scope of the ISMS), and are meeting their desired objectives.
- c) Technical controls (e.g. firewalls, physical access controls) are in place, are correctly configured and working as intended.
- d) The residual risks have been assessed correctly and are still acceptable to the management of the organization.
- e) The agreed actions from previous audits and reviews have been implemented.
- f) The ISMS is compliant with this standard.

The audits will involve sample documents and records, and interviewing management and staff.

## **B 4.6 Management review**

The overall objective is to check, at least once per year, that the ISMS is effective, to identify where improvements can be made and to take action.

# **B 5 Act Phase**

## **B 5.1 Introduction**

In order for the ISMS to remain effective it should be regularly reviewed and improved.

This should also include a description of procedures for the management and operation of the controls in the ISMS and processes for ongoing review of risks and their treatment in the light of changing technology, threats, or functions.

Whilst it may be determined that the current state of security is satisfactory, attention should be paid to changing technology and business requirements and the onset of new threats and vulnerabilities to anticipate future changes to the ISMS to ensure its continued effectiveness in the future.

The information collected during the Check phase provides a valuable source of data that can be used to determine and measure the effectiveness of the ISMS in meeting the documented security policy and

objectives of the organization. It should also be used as a source to identify inefficient and ineffective processes and procedures.

### **B 5.2 Non-conformities**

A non-conformity is:

- The absence of, or the failure to implement, maintain and improve, one or more required management system elements, or
- A situation which would, on the basis of objective evidence, raise significant doubt as to the capability of the ISMS to comply with the security policy and achieve the security objectives of the organisation.

It is important that where reviews during the Check phase highlight areas of non-conformance, further investigations are conducted to identify the root cause of the event and actions are identified not only to resolve the issue but also to minimise and prevent reoccurrence. Corrective action should be consistent with the severity of the nonconformity and the risk to the assurance of the ISMS to meet specified requirements.

### **B 5.3 Corrective actions**

What may appear as a single isolated event may in fact have an impact across the entire organization if not addressed and must be considered when identifying and implementing the agreed corrective actions. In addition to the immediate corrective actions identified, it is important to consider the medium to long term view ensuring the remedial work not only addresses the issue under consideration but also prevents or reduces the likelihood of a similar event reoccurring.

### **B 5.4 Trend Analysis**

Trend analysis undertaken on a regular basis will help organisations identify those areas where improvement is indicated and should form an essential part of the continuous improvement cycle.

### **B 5.5 Changes**

It is vital that all interested parties are advised regularly of any changes of the ISMS and additional training should be required where required.

## Annex C Correspondence between ISO 9001:2000, ISO 14001:1996 and BS 7799 Part 2: 2002

(Informative Annex)

Correspondence between the clauses of BS 7799-2, ISO 9001:2000 and ISO 14001:1996

<b>BS 7799-2: 2002</b>		<b>ISO 9001: 2000</b>		<b>ISO 14001: 1996</b>	
<b>Introduction</b>	<b>0</b>	<b>Introduction</b>	<b>0</b>	-	<b>Introduction</b>
General	0.1	General	0.1		
Process approach	0.2	Process model	0.2		
Compatibility with other management systems	0.3	Compatibility with other management system disciplines	0.3		
<b>Scope</b>	<b>1</b>	<b>Scope</b>	<b>1</b>	<b>1</b>	<b>Scope</b>
General	1.1	General	1.1		
Application	1.2	Application	1.2		
<b>Normative reference</b>	<b>2</b>	<b>Normative reference</b>	<b>2</b>	<b>2</b>	<b>Normative references</b>
<b>Terms and definitions</b>	<b>3</b>	<b>Terms and definitions</b>	<b>3</b>	<b>3</b>	<b>Definitions</b>
<b>Information security management system</b>	<b>4</b>	<b>Quality management system requirements</b>	<b>4</b>	<b>4</b>	<b>Environmental management system requirements</b>
General requirements	4.1	General requirements	4.1	4.1	General requirements
Process	4.2	Process model	0.2	-	
Documentation requirements	4.3	Quality management system		-	
General	4.3.1	General requirements	4.2.1	4.1	General requirements
ISMS manual	4.3.2	Quality manual	4.2.2	4.4.4	Environmental management system documentation
Control of documentation	4.3.3	Control of documents	4.2.3	4.4.5	Document control
Control of records	4.3.4	Control of records	4.2.4	4.5.3	Records
<b>Management responsibility</b>	<b>5</b>	<b>Management responsibility</b>	<b>5</b>	-	-
Management commitment	5.1	General requirements	5.1	-	-
		Internal communication	5.5.3	4.4.3	Communication
<b>Resource management</b>	<b>5.2</b>	<b>Resource management</b>	<b>6</b>	4.4.1	Structure and responsibility
Provision of resources	5.2.1	Assignment of personnel	6.2.1	4.4.1	Structure and responsibility
		General requirements	6.1	4.4.1	Structure and responsibility
		Human resources	6.2	4.4.1	Structure and responsibility
Training, awareness and competency	5.2.2	Competence, training, qualification and awareness	6.2.2	4.4.2	Training, awareness and competence
		Information	6.3	4.4.4	Environmental management system documentation
<b>Management review of ISMS</b>	<b>6</b>	<b>Management review</b>	<b>5.6</b>	<b>4.6</b>	<b>Management review</b>

BS 7799-2: 2002		ISO 9001: 2000		ISO 14001: 1996	
<b>Improvement</b>	7	<b>Improvement</b>	8.5	-	-
Continual improvement	7.1	General requirements	8.5.1	4.2	Environmental policy
Corrective action	7.2	Corrective action	8.5.2	4.5.2	Nonconformance and corrective and preventive action
Preventive action	7.3	Preventive action	8.5.3	4.5.2	Nonconformance and corrective and preventive action