BRITISH STANDARDS PUBLISHING LIMITED (BSPL)

GENERAL TERMS AND CONDITIONS
17799 ELECTRONIC SHOP

Customers are asked to note that the following terms apply to the standards they order.

1. INTERPRETATION

1.1 In these Conditions: 'Buyer' means the person whose online order for the Publications is accepted by the Seller. 'Publications' means British Standards which the Seller is to supply in accordance with these Conditions. 'British Standard' means a standard published under the authority of the Seller. 'Electronic' means the digital form of a 'Publication'. 'Online' means BSPL's 17799 Electronic Shop found at www.bspsl.com/17799. 'Seller' means British Standards Publishing Sales Limited (BSPSL). 'Conditions' means the standard terms and conditions of sale set out in this document and (unless the context otherwise requires) includes any special terms and conditions agreed in writing between the Buyer and Seller. 'Writing' includes facsimile transmission and comparable means of communication.

1.2 Any reference in these Conditions to any provision of a statute shall be constructed as a reference to that provision as amended, re-enacted or extended at the relevant time.

1.3 The headings in these Conditions are for convenience only and shall not affect their interpretation.

2. BASIS OF THE SALE

2.1 The Seller shall sell and the Buyer shall purchase the Publications in accordance with these Terms and Conditions.

2.2 No variation to these Conditions shall be binding unless agreed in writing between the authorised representatives of the Buyer and the Seller.

2.3 The Buyer will be responsible for the selection of the Publications and any advice or recommendation given by the Seller or its employees or agents to the Buyer or its employees or agents as to the suitability, fitness for any purpose, application or use of the Publications is intended for guidance only and is followed or acted upon entirely at the Buyer's own risk. Accordingly the Seller shall not be liable for any such advice or recommendations.

2.4 BSI will normally accept returns which have been incorrectly supplied or are in some way deficient. BSI is not obliged, however, to accept the return of goods correctly supplied. Guidelines for the return of goods supplied are available on request.

3. ORDERS

3.1 Orders for Publications can be placed Online through www .bspsl.com/17799.

3.2 The Buyer shall be responsible to the Seller for ensuring the accuracy of the terms of any order submitted by the Buyer.

3.3 The quantity and description of the Publications shall be as ordered by the Buyer via the Web site. The Publications shall be inclusive of any amendments issued by the Seller to date of order.

3.4 No order which has been accepted by the Seller may be cancelled by the Buyer except with the agreement in writing of the Seller.

3.5 Unless otherwise specified all Publications supplied will be to the current issue at date of order.

4. PRICE OF THE PUBLICATIONS

4.1 The price of the Publications is as displayed on the Web site at the time of purchase.

4.2 The Seller reserves the right to increase the price of the Publications.

4.3 The price is inclusive of value added tax.

5. TERMS OF PAYMENT

5.1 Payment can only be made via credit card.

6. DELIVERY

6.1 Returns will not be accepted without previous authorisation by the Seller. Where the Seller has authorised and accepted a correctly supplied Publication as a return, the Seller reserves the right to charge a handling fee for the return.

7. RISK AND PROPERTY

7.1 Notwithstanding delivery and the passing of risk in the Publications, or any other provision of these Conditions the property in the Publications shall not pass to the Buyer until the Seller has received cleared funds payment in full of the price of the Publications.

8. RESTRICTION ON USE

8.1 The Buyer acknowledges that:

8.1.1 in calculating the price for the Publications the Seller has assumed that there will be no resale market.

8.1.2 to maintain state of the art in the Publications it is essential that users receive the current version of the Publications.

8.1.3 to provide adequate protection against copying by third parties it is reasonable to prevent alienation of the Publications. Accordingly it is a condition of the sale that the Buyer will not without the prior consent in writing of the Seller resell, loan or part with possession of the Publications or any part of them.

8.2 Copyright subsists in the Publications. No part of a Publication may be reproduced in any form without the prior permission in writing of the Seller (refer to the Copyright Terms & Conditions).

8.3 The restriction contained in Condition 8.2 does not preclude the Buyer in applying a Publication from making free use of necessary details such as symbols and size type or grade designations including without limitation use by incorporating the same into computer programs but the Buyer is precluded from selling, licensing or in any way parting with possession of any resulting product including without limitation, computer programs without the consent in writing of the Seller which if granted will be on terms including royalty.

9. WARRANTIES AND LIABILITY

9.1 The Seller accepts liability in respect of death or personal injury caused by the Seller's negligence.

9.2 British Standards are prepared under the direction of policy committees upon which bodies with substantial relevant expert knowledge or interest are represented. The Seller acts as secretary to these committees. All British Standards are made available for public comment before publication. British Standards are periodically reviewed with the intention of keeping the content up to date. If the Buyer encounters an inaccuracy or ambiguity in a Publication, the Buyer will notify the Seller without delay in order that the matter may be investigated and any necessary amendment made to the Publication. Free supply of any such amendment shall constitute the full extent of the Buyer's rights and the Seller's liability for any such inaccuracy or ambiguity. Whilst all reasonable care is taken in the preparation and review of British Standards, the Seller does not warrant that the content of the Publications is accurate or up to date or that the Publications are suitable for the Buyer's purposes. Subject as expressly provided in these Conditions and to the fullest extent permitted by law all warranties conditions or other Terms and duties implied by statute or common law are excluded.

9.3 The Buyer is responsible for ensuring:

9.3.1 that it obtains and uses the latest amendments or additions to Publications.

9.3.2 where a Publication is incorporated into or referred to in a contract between the Buyer and a third party that the Publication is correctly applied under that contract

9.4 The Buyer acknowledges that a Publication does not purport to include all necessary provisions of a contract with a third party and that compliance with a Publication does not of itself confer immunity from legal obligations.

9.5 The Seller shall have no liability with regard to the content or use of any Publication which is not published under the authority of the Seller. The Seller will assign to the Buyer the benefit of any warranty given by the publisher to the Seller.

10. GENERAL

10.1 Any notice required or permitted to be given by either party to the other under these Conditions shall be in writing addressed to that other party at its registered office or principal place of business or such other address as may at the relevant time have been notified pursuant to this provision to the party giving the notice.

10.2 No waiver by the Seller or any breach of the Contract by the Buyer shall be considered as a waiver of any subsequent breach of the same or any other provision.

10.3 If any provision of these Conditions is held by any competent authority to be invalid or unenforceable in whole or in part the validity of the other provisions of these Conditions and the remainder of the provision in question shall not be affected thereby.

10.4 The Contract shall be governed by the laws of England and the parties submit to exclusive jurisdiction of the courts of England.

BRITISH STANDARD

BS ISO/IEC 17799:2000
BS 7799-1:2000

Information technology — Code of practice for information security management

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 17799:2000 and implements it as the UK national standard. It supersedes BS 7799-1:1999 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques, which has the responsibility to:

- — aid enquirers to understand the text;
- — present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- — monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

BS 7799-1:1999 was submitted as the proposed text for an international standard on Information Security Management using the ISO/IEC JTC 1 fast-track procedure. During the resolution of comments phase of the development, it was agreed that the international standard would be considered as a single part standard until such time that further submissions/developments are produced. For the purposes of implementation in the UK the British Standard has been dual numbered as:

BS ISO/IEC 17799:2000	UK implementation of the international standard
BS 7799-1:2000	Retention of the original British Standard identifier

As part of the implementation in the UK national annex NA (informative) has been included to enable users of the existing British Standard BS 7799-1:1999 to quickly identify the changes between it and BS ISO/IEC 17799:2000.

BS ISO/IEC 17799 provides a comprehensive set of controls comprising best practices in information security. It is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce, and to be used by large, medium and small organizations. The term organization is used throughout this standard to mean both profit and non-profit making organizations such as public sector organizations.

Not all of the controls described in this document will be relevant to every situation. It cannot take account of local system, environmental or technological constraints. It may not be in a form that suits every potential user in an organization. Consequently the document may need to be supplemented by further guidance. It can be used as a basis from which, for example, a corporate policy or an inter-company trading agreement can be developed.

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification, and particular care should be taken to ensure that claims of compliance are not misleading.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on
15 February 2001

Amendments issued since publication

Amd. No.	Date	Comments

ISBN 0 580 36958 7

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

Cross-references

The British Standards which implement international publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled "International Standards Correspondence Index", or by using the "Find" facility of the BSI Standards Electronic Catalogue.

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.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO/IEC title page, pages ii to xi, a blank page, pages 1 to 77, and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

blank

INTERNATIONAL STANDARD

ISO/IEC 17799

First edition
2000-12-01

Information technology — Code of practice for information security management

Technologies de l'information — Code de pratique pour la gestion de sécurité d'information

Reference number
ISO/IEC 17799:2000(E)

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 17799 was prepared by the British Standards Institution (as BS 7799) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

What is information security?

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized here as the preservation of:

a) confidentiality: ensuring that information is accessible only to those authorized to have access;

b) integrity: safeguarding the accuracy and completeness of information and processing methods;

c) availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Why information security is needed

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image.

Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organizations may also be needed.

Information security controls are considerably cheaper and more effective if incorporated at the requirements specification and design stage.

How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources.

The first source is derived from assessing risks to the organization. Through risk assessment threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

The second source is the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy.

The third source is the particular set of principles, objectives and requirements for information processing that an organization has developed to support its operations.

Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques can be applied to the whole organization, or only parts of it, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful.

Risk assessment is systematic consideration of:

a) 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 information and other assets;

b) the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

The results of this assessment will help guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

It is important to carry out periodic reviews of security risks and implemented controls to:

a) take account of changes to business requirements and priorities;

b) consider new threats and vulnerabilities;

c) confirm that controls remain effective and appropriate.

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that management is prepared to accept. Risk assessments are often carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

Selecting controls

Once security requirements have been identified, controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this document or from other control sets, or new controls can be designed to meet specific needs as appropriate. There are many different ways of managing risks and this document provides examples of common approaches. However, it is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practicable for all organizations. As an example, 8.1.4 describes how duties may be segregated to prevent fraud and error. It may not be possible for smaller organizations to segregate all duties and other ways of achieving the same control objective may be necessary. As another example, 9.7 and 12.1 describe how system use can be monitored and evidence collected. The described controls e.g. event logging might conflict with applicable legislation, such as privacy protection for customers or in the workplace.

Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors such as loss of reputation should also be taken into account.

Some of the controls in this document can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading “Information security starting point”.

Information security starting point

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security.

Controls considered to be essential to an organization from a legislative point of view include:

a) data protection and privacy of personal information (see 12.1.4).

b) safeguarding of organizational records (see 12.1.3);

c) intellectual property rights (see 12.1.2);

Controls considered to be common best practice for information security include:

a) information security policy document (see 3.1);

b) allocation of information security responsibilities (see 4.1.3);

c) information security education and training (see 6.2.1);

d) reporting security incidents (see 6.3.1);

e) business continuity management (see 11.1).

These controls apply to most organizations and in most environments. It should be noted that although all controls in this document are important, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

a) security policy, objectives and activities that reflect business objectives;

b) an approach to implementing security that is consistent with the organizational culture;

c) visible support and commitment from management;

d) a good understanding of the security requirements, risk assessment and risk management;

e) effective marketing of security to all managers and employees;

f) distribution of guidance on information security policy and standards to all employees and contractors;

g) providing appropriate training and education;

h) a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidance. Not all of the guidance and controls in this code of practice may be applicable. Furthermore, additional controls not included in this document may be required. When this happens it may be useful to retain cross-references which will facilitate compliance checking by auditors and business partners.

blank

Information technology — Code of practice for information security management

1 Scope

This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations.

2 Terms and definitions

For the purposes of this document, the following definitions apply.

2.1 Information security

Preservation of confidentiality, integrity and availability of information.

- **Confidentiality**
  Ensuring that information is accessible only to those authorized to have access.

- **Integrity**
  Safeguarding the accuracy and completeness of information and processing methods.

- **Availability**
  Ensuring that authorized users have access to information and associated assets when required.

2.2 Risk assessment

Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

2.3 Risk management

Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.

3 Security policy

3.1 Information security policy

Objective: To provide management direction and support for information security.

Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

3.1.1 Information security policy document

A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization’s approach to managing information security. As a minimum, the following guidance should be included:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) a statement of management intent, supporting the goals and principles of information security;

c) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, for example:

   1) compliance with legislative and contractual requirements;
   2) security education requirements;
   3) prevention and detection of viruses and other malicious software;
   4) business continuity management;
   5) consequences of security policy violations;

d) a definition of general and specific responsibilities for information security management, including reporting security incidents;

e) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

3.1.2 Review and evaluation

The policy should have an owner who is responsible for its maintenance and review according to a defined review process. That process should ensure that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure. There should also be scheduled, periodic reviews of the following:

a) the policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents;

b) cost and impact of controls on business efficiency;

c) effects of changes to technology.

4 Organizational security

4.1 Information security infrastructure

Objective: To manage information security within the organization.

A management framework should be established to initiate and control the implementation of information security within the organization.
Suitable management fora with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management.

4.1.1 Management information security forum

Information security is a business responsibility shared by all members of the management team. A management forum to ensure that there is clear direction and visible management support for security initiatives should therefore be considered. That forum should promote security within the organization through appropriate commitment and adequate resourcing. The forum may be part of an existing management body. Typically, such a forum undertakes the following:

a) reviewing and approving information security policy and overall responsibilities;

b) monitoring significant changes in the exposure of information assets to major threats;

c) reviewing and monitoring information security incidents;

d) approving major initiatives to enhance information security.

One manager should be responsible for all security related activities.

4.1.2 Information security co-ordination

In a large organization a cross-functional forum of management representatives from relevant parts of the organization may be necessary to co-ordinate the implementation of information security controls. Typically, such a forum:

a) agrees specific roles and responsibilities for information security across the organization;

b) agrees specific methodologies and processes for information security, e.g. risk assessment, security classification system;

c) agrees and supports organization-wide information security initiatives, e.g. security awareness programme;

d) ensures that security is part of the information planning process;

e) assesses the adequacy and co-ordinates the implementation of specific information security controls for new systems or services;

f) reviews information security incidents;

g) promotes the visibility of business support for information security throughout the organization.

4.1.3 Allocation of information security responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined.

The information security policy (see clause 3) should provide general guidance on the allocation of security roles and responsibilities in the organization. This should be supplemented, where necessary, with more detailed guidance for specific sites, systems or services. Local responsibilities for individual physical and information assets and security processes, such as business continuity planning, should be clearly defined.

In many organizations an information security manager will be appointed to take overall responsibility for the development and implementation of security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each information asset who then becomes responsible for its day-to-day security.

Owners of information assets may delegate their security responsibilities to individual managers or service providers. Nevertheless the owner remains ultimately responsible for the security of the asset and should be able to determine that any delegated responsibility has been discharged correctly.

It is essential that the areas for which each manager is responsible are clearly stated; in particular the following should take place.

a) The various assets and security processes associated with each individual system should be identified and clearly defined.

b) The manager responsible for each asset or security process should be agreed and the details of this responsibility should be documented.

c) Authorization levels should be clearly defined and documented.

4.1.4 Authorization process for information processing facilities

A management authorization process for new information processing facilities should be established.

The following controls should be considered.

a) New facilities should have appropriate user management approval, authorizing their purpose and use. Approval should also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met.

b) Where necessary, hardware and software should be checked to ensure that they are compatible with other system components.

   NOTE Type approval may be required for certain connections.

c) The use of personal information processing facilities for processing business information and any necessary controls should be authorized.

d) The use of personal information processing facilities in the workplace may cause new vulnerabilities and should therefore be assessed and authorized.

These controls are especially important in a networked environment.

4.1.5 Specialist information security advice

Specialist security advice is likely to be required by many organizations. Ideally, an experienced in-house information security adviser should provide this. Not all organizations may wish to employ a specialist adviser. In such cases, it is recommended that a specific individual is identified to co-ordinate in-house knowledge and experiences to ensure consistency, and provide help in security decision making. They should also have access to suitable external advisers to provide specialist advice outside their own experience.

Information security advisers or equivalent points of contact should be tasked with providing advice on all aspects of information security, using either their own or external advice. The quality of their assessment of security threats and advice on controls will determine the effectiveness of the organization’s information security. For maximum effectiveness and impact they should be allowed direct access to management throughout the organization.

The information security adviser or equivalent point of contact should be consulted at the earliest possible stage following a suspected security incident or breach to provide a source of expert guidance or investigative resources. Although most internal security investigations will normally be carried out under management control, the information security adviser may be called on to advise, lead or conduct the investigation.

4.1.6 Co-operation between organizations

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators should be maintained to ensure that appropriate action can be quickly taken, and advice obtained, in the event of a security incident. Similarly, membership of security groups and industry forums should be considered.

Exchanges of security information should be restricted to ensure that confidential information of the organization is not passed to unauthorized persons.

4.1.7 Independent review of information security

The information security policy document (see 3.1) sets out the policy and responsibilities for information security. Its implementation should be reviewed independently to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective (see 12.2).

Such a review may be carried out by the internal audit function, an independent manager or a third party organization specialising in such reviews, where these candidates have the appropriate skills and experience.

4.2 Security of third party access

Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.

Access to the organization's information processing facilities by third parties should be controlled.

Where there is a business need for such third party access, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in a contract with the third party.

Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access.

This standard could be used as a basis for such contracts and when considering the outsourcing of information processing.

4.2.1 Identification of risks from third party access

4.2.1.1 *Types of access*

The type of access given to a third party is of special importance. For example, the risks of access across a network connection are different from risks resulting from physical access. Types of access that should be considered are:

a) physical access, e.g. to offices, computer rooms, filing cabinets;

b) logical access, e.g. to an organization's databases, information systems.

4.2.1.2 *Reasons for access*

Third parties may be granted access for a number of reasons. For example, there are third parties that provide services to an organization and are not located on-site but may be given physical and logical access, such as:

a) hardware and software support staff, who need access to system level or low level application functionality;

b) trading partners or joint ventures, who may exchange information, access information systems or share databases.

Information might be put at risk by access from third parties with inadequate security management. Where there is a business need to connect to a third party location a risk assessment should be carried out to identify any requirements for specific controls. It should take into account the type of access required, the value of the information, the controls employed by the third party and the implications of this access to the security of the organization's information.

4.2.1.3 *On-site contractors*

Third parties that are located on-site for a period of time as defined in their contract may also give rise to security weaknesses. Examples of on-site third party include:

a) hardware and software maintenance and support staff;

b) cleaning, catering, security guards and other outsourced support services;

c) student placement and other casual short term appointments;

d) consultants.

It is essential to understand what controls are needed to administer third party access to information processing facilities. Generally, all security requirements resulting from third party access or internal controls should be reflected by the third party contract (see also 4.2.2). For example, if there is a special need for confidentiality of the information, non-disclosure agreements might be used (see 6.1.3).

Access to information and information processing facilities by third parties should not be provided until the appropriate controls have been implemented and a contract has been signed defining the terms for the connection or access.

4.2.2 Security requirements in third party contracts

Arrangements involving third party access to organizational information processing facilities should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards. The contract should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of their supplier. The following terms should be considered for inclusion in the contract:

a) the general policy on information security;

b) asset protection, including:

  1) procedures to protect organizational assets, including information and software;
  2) procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred;
  3) controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
  4) integrity and availability;
  5) restrictions on copying and disclosing information;

c) a description of each service to be made available;

d) the target level of service and unacceptable levels of service;

e) provision for the transfer of staff where appropriate;

f) the respective liabilities of the parties to the agreement;

g) responsibilities with respect to legal matters, e.g. data protection legislation, especially taking into account different national legal systems if the contract involves co-operation with organizations in other countries (see also 12.1);

h) intellectual property rights (IPRs) and copyright assignment (see 12.1.2) and protection of any collaborative work (see also 6.1.3);

i) access control agreements, covering:

   1) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
   2) an authorization process for user access and privileges;
   3) a requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use;

j) the definition of verifiable performance criteria, their monitoring and reporting;

k) the right to monitor, and revoke, user activity;

l) the right to audit contractual responsibilities or to have those audits carried out by a third party;

m) the establishment of an escalation process for problem resolution; contingency arrangements should also be considered where appropriate;

n) responsibilities regarding hardware and software installation and maintenance;

o) a clear reporting structure and agreed reporting formats;

p) a clear and specified process of change management;

q) any required physical protection controls and mechanisms to ensure those controls are followed;

r) user and administrator training in methods, procedures and security;

s) controls to ensure protection against malicious software (see 8.3);

t) arrangements for reporting, notification and investigation of security incidents and security breaches;

u) involvement of the third party with subcontractors.

4.3 Outsourcing

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

Outsourcing arrangements should address the risks, security controls and procedures for information systems, networks and/or desk top environments in the contract between the parties.

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 should be addressed in a contract agreed between the parties.

For example, the contract should address:

a) how the legal requirements are to be met, e.g. data protection legislation;

b) what arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities;

c) how the integrity and confidentiality of the organization's business assets are to be maintained and tested;

d) what physical and logical controls will be used to restrict and limit the access to the organization's sensitive business information to authorized users;

e) how the availability of services is to be maintained in the event of a disaster;

f) what levels of physical security are to be provided for outsourced equipment;

g) the right of audit.

The terms given in the list in 4.2.2 should also be considered as part of this contract. The contract should allow the security requirements and procedures to be expanded in a security management plan to be agreed between the two parties.

Although outsourcing contracts can pose some complex security questions, the controls included in this code of practice could serve as a starting point for agreeing the structure and content of the security management plan.

5 Asset classification and control

5.1 Accountability for assets

Objective: To maintain appropriate protection of organizational assets.

All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

5.1.1 Inventory of assets

Inventories of assets help ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. The process of compiling an inventory of assets is an important aspect of risk management. An organization needs to be able to identify its assets and the relative value and importance of these assets. Based on this information an organization can then provide levels of protection commensurate with the value and importance of the assets. An inventory should be drawn up and maintained of the important assets associated with each information system. Each asset should be clearly identified and its ownership and security classification (see 5.2) agreed and documented, together with its current location (important when attempting to recover from loss or damage). Examples of assets associated with information systems are:

a) information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;

b) software assets: application software, system software, development tools and utilities;

c) physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PABXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;

d) services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

5.2 Information classification

Objective: To ensure that information assets receive an appropriate level of protection.

Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

5.2.1 Classification guidelines

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorized access or damage to the information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected.

Information and outputs from systems handling classified data should be labelled in terms of its value and sensitivity to the organization. It may also be appropriate to label information in terms of how critical it is to the organization, e.g. in terms of its integrity and availability. Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to an unnecessary additional business expense. Classification guidelines should anticipate and allow for the fact that the classification of any given item of information is not necessarily fixed for all time, and may change in accordance with some predetermined policy (see 9.1).

Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations which may have different definitions for the same or similarly named labels.

The responsibility for defining the classification of an item of information, e.g. for a document, data record, data file or diskette, and for periodically reviewing that classification, should remain with the originator or nominated owner of the information.

5.2.2 Information labelling and handling

It is important that an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by the organization. These procedures need to cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information processing activity:

a) copying;

b) storage;

c) transmission by post, fax, and electronic mail;

d) transmission by spoken word, including mobile phone, voicemail, answering machines;

e) destruction.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label (in the output). The labelling should reflect the classification according to the rules established in 5.2.1. Items for consideration include printed reports, screen displays, recorded media (tapes, disks, CDs, cassettes), electronic messages and file transfers.

Physical labels are generally the most appropriate forms of labelling. However, some information assets, such as documents in electronic form, cannot be physically labelled and electronic means of labelling need to be used.

6 Personnel security

6.1 Security in job definition and resourcing

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment.
Potential recruits should be adequately screened (see 6.1.2), especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality (non-disclosure) agreement.

6.1.1 Including security in job responsibilities

Security roles and responsibilities, as laid down in the organization's information security policy (see 3.1) should be documented where appropriate. They should include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

6.1.2 Personnel screening and policy

Verification checks on permanent staff should be carried out at the time of job applications. This should include the following controls:

a) availability of satisfactory character references, e.g. one business and one personal;

b) a check (for completeness and accuracy) of the applicant's curriculum vitae;

c) confirmation of claimed academic and professional qualifications;

d) independent identity check (passport or similar document).

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g. financial information or highly confidential information, the organization should also carry out a credit check. For staff holding positions of considerable authority this check should be repeated periodically.

A similar screening process should be carried out for contractors and temporary staff. Where these staff are provided through an agency the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern.

Management should evaluate the supervision required for new and inexperienced staff with authorization for access to sensitive systems. The work of all staff should be subject to periodic review and approval procedures by a more senior member of staff.

Managers should be aware that personal circumstances of their staff may affect their work. Personal or financial problems, changes in their behaviour or lifestyle, recurring absences and evidence of stress or depression might lead to fraud, theft, error or other security implications. This information should be handled in accordance with any appropriate legislation existing in the relevant jurisdiction.

6.1.3 Confidentiality agreements

Confidentiality or non-disclosure agreements are used to give notice that information is confidential or secret. Employees should normally sign such an agreement as part of their initial terms and conditions of employment.

Casual staff and third party users not already covered by an existing contract (containing the confidentiality agreement) should be required to sign a confidentiality agreement prior to being given access to information processing facilities.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.

6.1.4 Terms and conditions of employment

The terms and conditions of employment should state the employee’s responsibility for information security. Where appropriate, these responsibilities should continue for a defined period after the end of the employment. The action to be taken if the employee disregards security requirements should be included.

The employee’s legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation, should be clarified and included within the terms and conditions of employment. Responsibility for the classification and management of the employer’s data should also be included. Whenever appropriate, terms and conditions of employment should state that these responsibilities are extended outside the organization’s premises and outside normal working hours, e.g. in the case of home-working (see also 7.2.5 and 9.8.1).

6.2 User training

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.

Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

6.2.1 Information security education and training

All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages, before access to information or services is granted.

6.3 Responding to security incidents and malfunctions

Objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Incidents affecting security should be reported through appropriate management channels as quickly as possible.
All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of organizational assets. They should be required to report any observed or suspected incidents as quickly as possible to the designated point of contact. The organization should establish a formal disciplinary process for dealing with employees who commit security breaches. To be able to address incidents properly it might be necessary to collect evidence as soon as possible after the occurrence (see 12.1.7).

6.3.1 Reporting security incidents

Security incidents should be reported through appropriate management channels as quickly as possible.

A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an inc ident report. All employees and contractors should be made aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible. Suitable feedback processes should be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training (see 6.2) as examples of what could happen, how to respond to such incidents, and how to avoid them in the future (see also 12.1.7).

6.3.2 Reporting security weaknesses

Users of information services should be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services. They should report these matters either to their management or directly to their service provider as quickly as possible. Users should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

6.3.3 Reporting software malfunctions

Procedures should be established for reporting software malfunctions. The following actions should be considered.

a) The symptoms of the problem and any messages appearing on the screen should be noted.

b) The computer should be isolated, if possible, and use of it should be stopped. The appropriate contact should be alerted immediately. If equipment is to be examined, it should be disconnected from any organizational networks before being re-powered. Diskettes should not be transferred to other computers.

c) The matter should be reported immediately to the information security manager.

Users should not attempt to remove the suspected software unless authorized to do so. Appropriately trained and experienced staff should carry out recovery.

6.3.4 Learning from incidents

There should be mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. This information should be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process (see 3.1.2).

6.3.5 Disciplinary process

There should be a formal disciplinary process for employees who have violated organizational security policies and procedures (see 6.1.4 and, for retention of evidence, see 12.1.7). Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures. Additionally, it should ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.

7 Physical and environmental security

7.1 Secure areas

Objective: To prevent unauthorized access, damage and interference to business premises and information.

Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.

The protection provided should be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers, media and information processing facilities.

7.1.1 Physical security perimeter

Physical protection can be achieved by creating several physical barriers around the business premises and information processing facilities. Each barrier establishes a security perimeter, each increasing the total protection provided. Organizations should use security perimeters to protect areas which contain information processing facilities (see 7.1.3). A security perimeter is something which builds a barrier, e.g. a wall, a card controlled entry gate or a manned reception desk. The siting and strength of each barrier depends on the results of a risk assessment.

The following guidelines and controls should be considered and implemented where appropriate.

a) The security perimeter should be clearly defined.

b) The perimeter of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access, e.g. control mechanisms, bars, alarms, locks etc.

c) A manned reception area or other means to control physical access to the site or building should be in place. Access to sites and buildings should be restricted to authorized personnel only.

d) Physical barriers should, if necessary, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding.

e) All fire doors on a security perimeter should be alarmed and should slam shut.

7.1.2 Physical entry controls

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following controls should be considered.

a) Visitors to secure areas should be supervised or cleared and their date and time of entry and departure recorded. They should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures.

b) Access to sensitive information, and information processing facilities, should be controlled and restricted to authorized persons only. Authentication controls, e.g. swipe card plus PIN, should be used to authorize and validate all access. An audit trail of all access should be securely maintained.

c) All personnel should be required to wear some form of visible identification and should be encouraged to challenge unescorted strangers and anyone not wearing visible identification.

d) Access rights to secure areas should be regularly reviewed and updated.

7.1.3 Securing offices, rooms and facilities

A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of a secure area should take account of the possibility of damage from fire, flood, explosion, civil unrest, and other forms of natural or man-made disaster. Account should also be taken of relevant health and safety regulations and standards. Consideration should be given also to any security threats presented by neighbouring premises, e.g. leakage of water from other areas.

The following controls should be considered.

a) Key facilities should be sited to avoid access by the public.

b) Buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities.

c) Support functions and equipment, e.g. photocopiers, fax machines, should be sited appropriately within the secure area to avoid demands for access, which could compromise information.

d) Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.

e) Suitable intruder detection systems installed to professional standards and regularly tested should be in place to cover all external doors and accessible windows. Unoccupied areas should be alarmed at all times. Cover should also be provided for other areas, e.g. computer room or communications rooms.

f) Information processing facilities managed by the organization should be physically separated from those managed by third parties.

g) Directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public.

h) Hazardous or combustible materials should be stored securely at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area until required.

i) Fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster at the main site.

7.1.4 Working in secure areas

Additional controls and guidelines may be required to enhance the security of a secure area. This includes controls for the personnel or third parties working in the secure area, as well as third party activities taking place there. The following controls should be considered.

a) Personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis.

b) Unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities.

c) Vacant secure areas should be physically locked and periodically checked.

d) Third party support services personnel should be granted restricted access to secure areas or sensitive information processing facilities only when required. This access should be authorized and monitored. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.

e) Photographic, video, audio or other recording equipment should not be allowed, unless authorized.

7.1.5 Isolated delivery and loading areas

Delivery and loading areas should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. Security requirements for such areas should be determined by a risk assessment. The following controls should be considered.

a) Access to a holding area from outside of the building should be restricted to identified and authorized personnel.

b) The holding area should be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building.

c) The external door(s) of a holding area should be secured when the internal door is opened.

d) Incoming material should be inspected for potential hazards [see 7.2.1d)] before it is moved from the holding area to the point of use.

e) Incoming material should be registered, if appropriate (see 5.1), on entry to the site.

7.2 Equipment security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

Equipment should be physically protected from security threats and environmental hazards.

Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

7.2.1 Equipment siting and protection

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. The following controls should be considered.

a) Equipment should be sited to minimize unnecessary access into work areas.

b) Information processing and storage facilities handling sensitive data should be positioned to reduce the risk of overlooking during their use.

c) Items requiring special protection should be isolated to reduce the general level of protection required.

d) Controls should be adopted to minimize the risk of potential threats including:

   1) theft;

   2) fire;

   3) explosives;

   4) smoke;

   5) water (or supply failure);

   6) dust;

   7) vibration;

   8) chemical effects;

   9) electrical supply interference;

   10) electromagnetic radiation.

e) An organization should consider its policy towards eating, drinking and smoking on in proximity to information processing facilities.

f) Environmental conditions should be monitored for conditions which could adversely affect the operation of information processing facilities.

g) The use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments.

h) The impact of a disaster happening in nearby premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street should be considered.

7.2.2 Power supplies

Equipment should be protected from power failures and other electrical anomalies. A suitable electrical supply should be provided that conforms to the equipment manufacturer's specifications.

Options to achieve continuity of power supplies include:

a) multiple feeds to avoid a single point of failure in the power supply;

b) uninterruptable power supply (UPS);

c) back-up generator.

A UPS to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Contingency plans should cover the action to be taken on failure of the UPS. UPS equipment should be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

A back-up generator should be considered if processing is to continue in case of a prolonged power failure. If installed, generators should be regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period.

In addition, emergency power switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure. Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all external communications lines.

7.2.3 Cabling security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. The following controls should be considered.

a) Power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection.

b) Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas.

c) Power cables should be segregated from communications cables to prevent interference.

d) For sensitive or critical systems further controls to consider include:

   1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

   2) use of alternative routings or transmission media;

   3) use of fibre optic cabling;

   4) initiation of sweeps for unauthorized devices being attached to the cables.

7.2.4 Equipment maintenance

Equipment should be correctly maintained to ensure its continued availability and integrity. The following controls should be considered.

a) Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.

b) Only authorized maintenance personnel should carry out repairs and service equipment.

c) Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.

d) Appropriate controls should be taken when sending equipment off premises for maintenance (see also 7.2.6 regarding deleted, erased and overwritten data). All requirements imposed by insurance policies should be complied with.

7.2.5 Security of equipment off-premises

Regardless of ownership, the use of any equipment outside an organization's premises for information processing should be authorized by management. The security provided should be equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside the organization's premises. Information processing equipment includes all forms of personal computers, organizers, mobile phones, paper or other form, which is held for home working or being transported away from the normal work location. The following guidelines should be considered.

a) Equipment and media taken off the premises should not be left unattended in public places. Portable computers should be carried as hand luggage and disguised where possible when travelling.

b) Manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields.

c) Home-working controls should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, and access controls for computers.

d) Adequate insurance cover should be in place to protect equipment off site.

Security risks, e.g. of damage, theft and eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls. More information about other aspects of protecting mobile equipment can be found in 9.8.1.

7.2.6 Secure disposal or re-use of equipment

Information can be compromised through careless disposal or re-use of equipment (see also 8.6.4). Storage devices containing sensitive information should be physically destroyed or securely overwritten rather than using the standard delete function.

All items of equipment containing storage media, e.g. fixed hard disks, should be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Damaged storage devices containing sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

7.3 General controls

Objective: To prevent compromise or theft of information and information processing facilities.

Information and information processing facilities should be protected from disclosure to, modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage.
Handling and storage procedures are considered in 8.6.3.

7.3.1 Clear desk and clear screen policy

Organizations should consider adopting a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. The policy should take into account the information security classifications (see 5.2), the corresponding risks and cultural aspects of the organization.

Information left out on desks is also likely to be damaged or destroyed in a disaster such as a fire, flood or explosion.

The following controls should be considered.

a) Where appropriate, paper and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.

b) Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.

c) Personal computers and computer terminals and printers should not be left logged on when unattended and should be protected by key locks, passwords or other controls when not in use.

d) Incoming and outgoing mail points and unattended fax and telex machines should be protected.

e) Photocopiers should be locked (or protected from unauthorized use in some other way) outside normal working hours.

f) Sensitive or classified information, when printed, should be cleared from printers immediately.

7.3.2 Removal of property

Equipment, information or software should not be taken off-site without authorization. Where necessary and appropriate, equipment should be logged out and logged back in when returned. Spot checks should be undertaken to detect unauthorized removal of property. Individuals should be made aware that spot checks will take place.

8 Communications and operations management

8.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures.
Segregation of duties (see 8.1.4) should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

8.1.1 Documented operating procedures

The operating procedures identified by the security policy should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by management.

The procedures should specify the instructions for the detailed execution of each job including:

a) processing and handling of information;

b) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

c) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see 9.5.5);

d) support contacts in the event of unexpected operational or technical difficulties;

e) special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs;

f) system restart and recovery procedures for use in the event of system failure.

Documented procedures should also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.

8.1.2 Operational change control

Changes to information processing facilities and systems should be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. Operational programs should be subject to strict change control. When programs are changed, an audit log containing all relevant information should be retained. Changes to the operational environment can impact on applications. Wherever practicable, operational and application change control procedures should be integrated (see also 10.5.1). In particular, the following controls should be considered:

a) identification and recording of significant changes;

b) assessment of the potential impact of such changes;

c) formal approval procedure for proposed changes;

d) communication of change details to all relevant persons;

e) procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

8.1.3 Incident management procedures

Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents (see also 6.3.1). The following controls should be considered.

a) Procedures should be established to cover all potential types of security incident, including:

   1) information system failures and loss of service;

   2) denial of service;

   3) errors resulting from incomplete or inaccurate business data;

   4) breaches of confidentiality.

b) In addition to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures should also cover (see also 6.3.4):

   1) analysis and identification of the cause of the incident;

   2) planning and implementation of remedies to prevent recurrence, if necessary;

   3) collection of audit trails and similar evidence;

   4) communication with those affected by or involved with recovery from the incident;

   5) reporting the action to the appropriate authority.

c) Audit trails and similar evidence should be collected (see 12.1.7) and secured, as appropriate, for:

   1) internal problem analysis;

   2) use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;

   3) negotiating for compensation from software and service suppliers.

d) Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures should ensure that:

   1) only clearly identified and authorized staff are allowed access to live systems and data (see also 4.2.2 for third party access);

   2) all emergency actions taken are documented in detail;

   3) emergency action is reported to management and reviewed in an orderly manner;

   4) the integrity of business systems and controls is confirmed with minimal delay.

8.1.4 Segregation of duties

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, should be considered.

Small organizations may find this method of control difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent.

Care should be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization. The following controls should be considered.

a) It is important to segregate activities which require collusion in order to defraud, e.g. raising a purchase order and verifying that the goods have been received.

b) If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.

8.1.5 Separation of development and operational facilities

Separating development, test and operational facilities is important to achieve segregation of the roles involved. Rules for the transfer of software from development to operational status should be defined and documented.

Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment, or of system failure. The level of separation that is necessary, between operational, test and development environments, to prevent operational problems should be considered. A similar separation should also be implemented between development and test functions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.

Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code. Untested or malicious code can cause serious operational problems. Developers and testers also pose a threat to the confidentiality of operational information.

Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data. The following controls should be considered.

a) Development and operational software should, where possible, run on different computer processors, or in different domains or directories.

b) Development and testing activities should be separated as far as possible.

c) Compilers, editors and other system utilities should not be accessible from operational systems when not required.

d) Different log-on procedures should be used for operational and test systems, to reduce the risk of error. Users should be encouraged to use different passwords for these systems, and menus should display appropriate identification messages.

e) Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed after use.

8.1.6 External facilities management

The use of an external contractor to manage information processing facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractor’s site. These risks should be identified in advance, and appropriate controls agreed with the contractor and incorporated into the contract (see also 4.2.2 and 4.3 for guidance on third party contracts involving access to organizational facilities and outsourcing contracts).

Particular issues that should be addressed include:

a) identifying sensitive or critical applications better retained in-house;

b) obtaining the approval of business application owners;

c) implications for business continuity plans;

d) security standards to be specified, and the process for measuring compliance;

e) allocation of specific responsibilities and procedures to effectively monitor all relevant security activities;

f) responsibilities and procedures for reporting and handling security incidents (see 8.1.3).

8.2 System planning and acceptance

Objective: To minimize the risk of systems failures.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources.
Projections of future capacity requirements should be made, to reduce the risk of system overload.
The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

8.2.1 Capacity planning

Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections should take account of new business and system requirements and current and projected trends in the organization’s information processing.

Mainframe computers require particular attention, because of the much greater cost and lead time for procurement of new capacity. Managers of mainframe services should monitor the utilization of key system resources, including processors, main storage, file storage, printers and other output devices, and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system tools.

Managers should use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services, and plan appropriate remedial action.

8.2.2 System acceptance

Acceptance criteria for new information systems, upgrades and new versions should be established and suitable tests of the system carried out prior to acceptance. Managers should ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented and tested. The following controls should be considered:

a) performance and computer capacity requirements;

b) error recovery and restart procedures, and contingency plans;

c) preparation and testing of routine operating procedures to defined standards;

d) agreed set of security controls in place;

e) effective manual procedures;

f) business continuity arrangements, as required by 11.1;

g) evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end;

h) evidence that consideration has been given to the effect the new system has on the overall security of the organization;

i) training in the operation or use of new systems.

For major new developments, the operations function and users should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria are fully satisfied.

8.3 Protection against malicious software

Objective: To protect the integrity of software and information.

Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses (see also 10.5.4) and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software, and managers should, where appropriate, introduce special controls to detect or prevent its introduction. In particular, it is essential that precautions be taken to detect and prevent computer viruses on personal computers.

8.3.1 Controls against malicious software

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Protection against malicious software should be based on security awareness, appropriate system access and change management controls. The following controls should be considered:

a) a formal policy requiring compliance with software licences and prohibiting the use of unauthorized software (see 12.1.2.2);

b) a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken (see also 10.5, especially 10.5.4 and 10.5.5);

c) installation and regular update of anti-virus detection and repair software to scan computers and media either as a precautionary control or on a routine basis;

d) conducting regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated;

e) checking any files on electronic media of uncertain or unauthorized origin, or files received over untrusted networks, for viruses before use;

f) checking any electronic mail attachments and downloads for malicious software before use. This check may be carried out at different places, e.g. at electronic mail servers, desk top computers or when entering the network of the organization;

g) management procedures and responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks (see 6.3 and 8.1.3);

h) appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements (see clause 11);

i) procedures to verify all information relating to malicious software, and ensure that warning bulletins are accurate and informative. Managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or anti-virus software suppliers, are used to differentiate between hoaxes and real viruses. Staff should be made aware of the problem of hoaxes and what to do on receipt of them.

These controls are especially important for network file servers supporting large numbers of workstations.

8.4 Housekeeping

Objective: To maintain the integrity and availability of information processing and communication services.

Routine procedures should be established for carrying out the agreed back-up strategy (see 11.1) taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

8.4.1 Information back-up

Back-up copies of essential business information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans (see clause 11). The following controls should be considered.

a) A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information should be retained for important business applications.

b) Back-up information should be given an appropriate level of physical and environmental protection (see clause 7) consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.

c) Back-up media should be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

d) Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

The retention period for essential business information, and also any requirement for archive copies to be permanently retained (see 12.1.3), should be determined.

8.4.2 Operator logs

Operational staff should maintain a log of their activities. Logs should include, as appropriate:

a) system starting and finishing times;

b) system errors and corrective action taken;

c) confirmation of the correct handling of data files and computer output;

d) the name of the person making the log entry.

Operator logs should be subject to regular, independent checks against operating procedures.

8.4.3 Fault logging

Faults should be reported and corrective action taken. Faults reported by users regarding problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:

a) review of fault logs to ensure that faults have been satisfactorily resolved;

b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

8.5 Network management

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

The security management of networks which may span organizational boundaries requires attention.
Additional controls may also be required to protect sensitive data passing over public networks.

8.5.1 Network controls

A range of controls is required to achieve and maintain security in computer networks. Network managers should implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access. In particular, the following controls should be considered.

a) Operational responsibility for networks should be separated from computer operations where appropriate (see 8.1.4).

b) Responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established.

c) If necessary, special controls should be established to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems (see 9.4 and 10.3). Special controls may also be required to maintain the availability of the network services and computers connected.

d) Management activities should be closely co-ordinated both to optimize the service to the business and to ensure that controls are consistently applied across the information processing infrastructure.

8.6 Media handling and security

Objective: To prevent damage to assets and interruptions to business activities.
Media should be controlled and physically protected.

Appropriate operating procedures should be established to protect documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorized access.

8.6.1 Management of removable computer media

There should be procedures for the management of removable computer media, such as tapes, disks, cassettes and printed reports. The following controls should be considered.

a) If no longer required, the previous contents of any re-usable media that are to be removed from the organization should be erased.

b) Authorization should be required for all media removed from the organization and a record of all such removals to maintain an audit trail should be kept (see 8.7.2).

c) All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications.

All procedures and authorization levels should be clearly documented.

8.6.2 Disposal of media

Media should be disposed of securely and safely when no longer required. Sensitive information could be leaked to outside persons through careless disposal of media. Formal procedures for the secure disposal of media should be established to minimize this risk. The following controls should be considered.

a) Media containing sensitive information should be stored and disposed of securely and safely, e.g. by incineration or shredding, or emptied of data for use by another application within the organization.

b) The following list identifies items that might require secure disposal:

   1) paper documents;

   2) voice or other recordings;

   3) carbon paper;

   4) output reports;

   5) one-time-use printer ribbons;

   6) magnetic tapes;

   7) removable disks or cassettes;

   8) optical storage media (all forms and including all manufacturer software distribution media);

   9) program listings;

   10) test data;

   11) system documentation.

c) It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items.

d) Many organizations offer collection and disposal services for papers, equipment and media. Care should be taken in selecting a suitable contractor with adequate controls and experience.

e) Disposal of sensitive items should be logged where possible in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive than a small quantity of classified information.

8.6.3 Information handling procedures

Procedures for the handling and storage of information should be established in order to protect such information from unauthorized disclosure or misuse. Procedures should be drawn up for handling information consistent with its classification (see 5.2) in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of fax machines and any other sensitive items, e.g. blank cheques, invoices. The following controls should be considered (see also 5.2 and 8.7.2):

a) handling and labelling of all media [see also 8.7.2a]];

b) access restrictions to identify unauthorized personnel;

c) maintenance of a formal record of the authorized recipients of data;

d) ensuring that input data is complete, that processing is properly completed and that output validation is applied;

e) protection of spooled data awaiting output to a level consistent with its sensitivity;

f) storage of media in an environment which accords with manufacturers' specifications;

g) keeping the distribution of data to a minimum;

h) clear marking of all copies of data for the attention of the authorized recipient;

i) review of distribution lists and lists of authorized recipients at regular intervals.

8.6.4 Security of system documentation

System documentation may contain a range of sensitive information, e.g. descriptions of applications processes, procedures, data structures, authorization processes (see also 9.1). The following controls should be considered to protect system documentation from unauthorized access.

a) System documentation should be stored securely.

b) The access list for system documentation should be kept to a minimum and authorized by the application owner.

c) System documentation held on a public network, or supplied via a public network, should be appropriately protected.

8.7 Exchanges of information and software

Objective: To prevent loss, modification or misuse of information exchanged between organizations.

Exchanges of information and software between organizations should be controlled, and should be compliant with any relevant legislation (see clause 12).
Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit should be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

8.7.1 Information and software exchange agreements

Agreements, some of which may be formal, including software escrow agreements when appropriate, should be established for the exchange of information and software (whether electronic or manual) between organizations. The security content of such an agreement should reflect the sensitivity of the business information involved. Agreements on security conditions should consider:

a) management responsibilities for controlling and notifying transmission, despatch and receipt;

b) procedures for notifying sender, transmission, despatch and receipt;

c) minimum technical standards for packaging and transmission;

d) courier identification standards;

e) responsibilities and liabilities in the event of loss of data;

f) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;

g) information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations (see 12.1.2 and 12.1.4);

h) technical standards for recording and reading information and software;

i) any special controls that may be required to protect sensitive items, such as cryptographic keys (see 10.3.5).

8.7.2 Security of media in transit

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. The following controls should be applied to safeguard computer media being transported between sites.

a) Reliable transport or couriers should be used. A list of authorized couriers should be agreed with management and a procedure to check the identification of couriers implemented.

b) Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.

c) Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. Examples include:

1) use of locked containers;

2) delivery by hand;

3) tamper-evident packaging (which reveals any attempt to gain access);

4) in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes;

5) use of digital signatures and confidentiality encryption, see 10.3.

8.7.3 Electronic commerce security

Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and on line transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls should be applied to protect electronic commerce from such threats. Security considerations for electronic commence should include the following controls.

a) Authentication. What level of confidence should the customer and trader require in each others claimed identity?

b) Authorization. Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?

c) Contract and tendering processes. What are the requirements for confidentiality, integrity and proof of despatch and receipt of key documents and the non-repudiation of contracts?

d) Pricing information. What level of trust can be put in the integrity of the advertised price list and the confidentiality of sensitive discount arrangements?

e) Order transactions. How is the confidentiality and integrity of order, payment and delivery address details, and confirmation of receipt, provided?

f) Vetting. What degree of vetting is appropriate to check payment information supplied by the customer?

g) Settlement. What is the most appropriate form of payment to guard against fraud?

h) Ordering. What protection is required to maintain the confidentiality and integrity of order information, and to avoid the loss or duplication of transactions?

i) Liability. Who carries the risk for any fraudulent transactions?

Many of the above considerations can be addressed by the application of cryptographic techniques outlined in 10.3, taking into account compliance with legal requirements (see 12.1, especially 12.1.6 for cryptography legislation).

Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization [see b) above]. Other agreements with information service and value added network providers may be necessary.

Public trading systems should publicize their terms of business to customers.

Consideration should be given to the resilience to attack of the host used for electronic commerce, and the security implications of any network interconnection required for its implementation (see 9.4.7).

8.7.4 Security of electronic mail

8.7.4.1 *Security risks*

Electronic mail is being used for business communications, replacing traditional forms of communication such as telex and letters. Electronic mail differs from traditional forms of business communications by, for example, its speed, message structure, degree of informality and vulnerability to unauthorized actions. Consideration should be given to the need for controls to reduce security risks created by electronic mail. Security risks include:

a) vulnerability of messages to unauthorized access or modification or denial of service;

b) vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service;

c) impact of a change of communication media on business processes, e.g. the effect of increased speed of despatch or the effect of sending formal messages from person to person rather than company to company;

d) legal considerations, such as the potential need for proof of origin, despatch, delivery and acceptance;

e) implications of publishing externally accessible staff lists;

f) controlling remote user access to electronic mail accounts.

8.7.4.2 *Policy on electronic mail*

Organizations should draw up a clear policy regarding the use of electronic mail, including:

a) attacks on electronic mail, e.g. viruses, interception;

b) protection of electronic mail attachments;

c) guidelines on when not to use electronic mail;

d) employee responsibility not to compromise the company, e.g. sending defamatory electronic mail, use for harassment, unauthorized purchasing;

e) use of cryptographic techniques to protect the confidentiality and integrity of electronic messages (see 10.3);

f) retention of messages which, if stored, could be discovered in case of litigation;

g) additional controls for vetting messaging which cannot be authenticated.

8.7.5 Security of electronic office systems

Policies and guidelines should be prepared and implemented to control the business and security risks associated with electronic office systems. These provide opportunities for faster dissemination and sharing of business information using a combination of: documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities and fax machines.

Consideration given to the security and business implications of interconnecting such facilities should include:

a) vulnerabilities of information in office systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of faxes, opening mail, distribution of mail;

b) policy and appropriate controls to manage information sharing, e.g. the use of corporate electronic bulletin boards (see 9.1);

c) excluding categories of sensitive business information if the system does not provide an appropriate level of protection (see 5.2);

d) restricting access to diary information relating to selected individuals, e.g. staff working on sensitive projects;

e) the suitability, or otherwise, of the system to support business applications, such as communicating orders or authorizations;

f) categories of staff, contractors or business partners allowed to use the system and the locations from which it may be accessed (see 4.2);

g) restricting selected facilities to specific categories of user;

h) identifying the status of users, e.g. employees of the organization or contractors in directories for the benefit of other users;

i) retention and back-up of information held on the system (see 12.1.3 and 8.4.1);

j) fallback requirements and arrangements (see 11.1).

8.7.6 Publicly available systems

Care should be taken to protect the integrity of electronically published information to prevent unauthorized modification which could harm the reputation of the publishing organization. Information on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules and regulations in the jurisdiction in which the system is located or where trade is taking place. There should be a formal authorization process before information is made publicly available.

Software, data and other information requiring a high level of integrity, made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures (see 10.3.3). Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that:

a) information is obtained in compliance with any data protection legislation (see 12.1.4);

b) information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner;

c) sensitive information will be protected during the collection process and when stored;

d) access to the publishing system does not allow unintended access to networks to which it is connected.

8.7.7 Other forms of information exchange

Procedures and controls should be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities. Information could be compromised due to lack of awareness, policy or procedures on the use of such facilities, e.g. being overheard on a mobile phone in a public place, answering machines being overheard, unauthorised access to dial-in voice-mail systems or accidentally sending facsimiles to the wrong person using facsimile equipment.

Business operations could be disrupted and information could be compromised if communications facilities fail, are overloaded or interrupted (see 7.2 and clause 11). Information could also be compromised if these are accessed by unauthorized users (see clause 9).

A clear policy statement of the procedures staff are expected to follow in using voice, facsimile and video communications should be established. This should include:

a) reminding staff that they should take appropriate precautions, e.g. not to reveal sensitive information so as to avoid being overheard or intercepted when making a phone call by:

   1) people in their immediate vicinity particularly when using mobile phones;

   2) wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers when using analogue mobile phones;

   3) people at the recipient's end;

b) reminding staff that they should not have confidential conversations in public places or open offices and meeting places with thin walls;

c) not leaving messages on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;

d) reminding staff about the problems of using facsimile machines, namely:

   1) unauthorized access to built-in message stores to retrieve messages;

   2) deliberate or accidental programming of machines to send messages to specific numbers;

   3) sending documents and messages to the wrong number either by misdialling or using the wrong stored number.

9 Access control

9.1 Business requirement for access control

Objective: To control access to information.

Access to information, and business processes should be controlled on the basis of business and security requirements.
This should take account of policies for information dissemination and authorization.

9.1.1 Access control policy

9.1.1.1 *Policy and business requirements*

Business requirements for access control should be defined and documented. Access control rules and rights for each user or group of users should be clearly stated in an access policy statement. Users and service providers should be given a clear statement of the business requirements to be met by access controls.
The policy should take account of the following:

a) security requirements of individual business applications;

b) identification of all information related to the business applications;

c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information;

d) consistency between the access control and information classification policies of different systems and networks;

e) relevant legislation and any contractual obligations regarding protection of access to data or services (see clause 12);

f) standard user access profiles for common categories of job;

g) management of access rights in a distributed and networked environment which recognizes all types of connections available.

9.1.1.2 *Access control rules*

In specifying the access control rules, care should be taken to consider the following:

a) differentiating between rules that must always be enforced and rules that are optional or conditional;

b) establishing rules based on the premise “What must be generally forbidden unless expressly permitted” rather than the weaker rule “Everything is generally permitted unless expressly forbidden”;

c) changes in information labels (see 5.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

d) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;

e) rules which require administrator or other approval before enactment and those which do not.

9.2 User access management

Objective: To prevent unauthorized access to information systems.

Formal procedures should be in place to control the allocation of access rights to information systems and services.

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

9.2.1 User registration

There should be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.

Access to multi-user information services should be controlled through a formal user registration process, which should include:

a) using unique user IDs so that users can be linked to and made responsible for their actions. The use of group IDs should only be permitted where they are suitable for the work carried out;

b) checking that the user has authorization from the system owner for the use of the information system or service. Separate approval for access rights from management may also be appropriate;

c) checking that the level of access granted is appropriate to the business purpose (see 9.1) and is consistent with organizational security policy, e.g. it does not compromise segregation of duties (see 8.1.4);

d) giving users a written statement of their access rights;

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring service providers do not provide access until authorization procedures have been completed;

g) maintaining a formal record of all persons registered to use the service;

h) immediately removing access rights of users who have changed jobs or left the organization;

i) periodically checking for, and removing, redundant user IDs and accounts;

j) ensuring that redundant user IDs are not issued to other users.

Consideration should be given to including clauses in staff contracts and service contracts that specify sanctions if unauthorized access is attempted by staff or service agents (see also 6.1.4 and 6.3.5).

9.2.2 Privilege management

The allocation and use of privileges (any feature or facility of a multi-user information system that enables the user to override system or application controls) should be restricted and controlled. Inappropriate use of system privileges is often found to be a major contributory factor to the failure of systems that have been breached.

Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process. The following steps should be considered.

a) The privileges associated with each system product, e.g. operating system, database management system and each application, and the categories of staff to which they need to be allocated should be identified.

b) Privileges should be allocated to individuals on a need-to-use basis and on an event-by-event basis, i.e. the minimum requirement for their functional role only when needed.

c) An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.

d) The development and use of system routines should be promoted to avoid the need to grant privileges to users.

e) Privileges should be assigned to a different user identity from those used for normal business use.

9.2.3 User password management

Passwords are a common means of validating a user's identity to access an information system or service. The allocation of passwords should be controlled through a formal management process, the approach of which should:

a) require users to sign a statement to keep personal passwords confidential and work group passwords solely within the members of the group (this could be included in the terms and conditions of employment, see 6.1.4);

b) ensure, where users are required to maintain their own passwords, that they are provided initially with a secure temporary password which they are forced to change immediately. Temporary passwords provided when users forget their password should only be supplied following positive identification of the user;

c) require temporary passwords to be given to users in a secure manner. The use of third parties or unprotected (clear text) electronic mail messages should be avoided. Users should acknowledge receipt of passwords.

Passwords should never be stored on computer system in an unprotected form (see Other technologies for user identification and authentication, such as biometrics, e.g. finger-print verification, signature verification and use of hardware tokens, e.g. chip-cards, are available, and should be considered if appropriate.

9.2.4 Review of user access rights

To maintain effective control over access to data and information services, management should conduct a formal process at regular intervals to review users' access rights so that:

a) users' access rights are reviewed at regular intervals (a period of 6 months is recommended) and after any changes (see 9.2.1);

b) authorizations for special privileged access rights (see 9.2.2) should be reviewed at more frequent intervals; a period of 3 months is recommended;

c) privilege allocations are checked at regular intervals to ensure that unauthorized privileges have not been obtained.

9.3 User responsibilities

Objective: To prevent unauthorized user access.

The co-operation of authorized users is essential for effective security.
Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

9.3.1 Password use

Users should follow good security practices in the selection and use of passwords.

Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services. All users should be advised to:

a) keep passwords confidential;

b) avoid keeping a paper record of passwords, unless this can be stored securely;

c) change passwords whenever there is any indication of possible system or password compromise;

d) select quality passwords with a minimum length of six characters which are:

   1) easy to remember;

   2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;

   3) free of consecutive identical characters or all-numeric or all-alphabetical groups.

e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

f) change temporary passwords at the first log-on;

g) do not include passwords in any automated log-on process, e.g. stored in a macro or function key;

h) do not share individual user passwords.

If users need to access multiple services or platforms and are required to maintain multiple passwords, they should be advised that they may use a single, quality password [see d) above] for all services that provide a reasonable level of protection for stored password.

9.3.2 Unattended user equipment

Users should ensure that unattended equipment has appropriate protection. Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period. All users and contractors should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

b) log-off mainframe computers when the session is finished (i.e. not just switch off the PC or terminal);

c) secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

9.4 Network access control

Objective: Protection of networked services.

Access to both internal and external networked services should be controlled.
This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring:

a) appropriate interfaces between the organization's network and networks owned by other organizations, or public networks;

b) appropriate authentication mechanisms for users and equipment;

c) control of user access to information services.

9.4.1 Policy on use of network services

Insecure connections to network services can affect the whole organization. Users should only be provided with direct access to the services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's security management and control.

A policy should be formulated concerning the use of networks and network services. This should cover:

a) the networks and network services which are allowed to be accessed;

b) authorization procedures for determining who is allowed to access which networks and networked services;

c) management controls and procedures to protect the access to network connections and network services.

This policy should be consistent with the business access control policy (see 9.1).

9.4.2 Enforced path

The path from the user terminal to the computer service may need to be controlled. Networks are designed to allow maximum scope for a sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorized access to business applications, or unauthorized use of information facilities. Incorporating controls that restrict the route between a user terminal and the computer services its user is authorized to access, e.g. creating an enforced path, can reduce such risks.

The objective of an enforced path is to prevent any users selecting routes outside the route between the user terminal and the services that the user is authorized to access.

This usually requires the implementation of a number of controls at different points in the route. The principle is to limit the routing options at each point in the network, through predefined choices.

Examples of this are as follows:

a) allocating dedicated lines or telephone numbers;

b) automatically connecting ports to specified application systems or security gateways;

c) limiting menu and submenu options for individual users;

d) preventing unlimited network roaming;

e) enforcing the use of specified application systems and/or security gateways for external network users;

f) actively controlling allowed source to destination communications via security gateways, e.g. firewalls;

g) restricting network access by setting up separate logical domains, e.g. virtual private networks, for user groups within the organization (see also 9.4.6).

The requirements for an enforced path should be based on the business access control policy (see 9.1).

9.4.3 User authentication for external connections

External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. Therefore, access by remote users should be subject to authentication. There are different types of authentication method, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.

Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Dedicated private lines or a network user address checking facility can also be used to provide assurance of the source of connections.

Dial-back procedures and controls, e.g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization’s information processing facilities. This type of control authenticates users trying to establish a connection to an organization’s network from remote locations. When using this control, an organization should not use network services which include call forwarding or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. It is also important that the call back process includes ensuring that an actual disconnection on the organization’s side occurs. Otherwise, the remote user could hold the line open pretending that call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.

9.4.4 Node authentication

A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. Connections to remote computer systems should therefore be authenticated. This is especially important if the connection uses a network that is outside the control of the organization’s security management. Some examples of authentication and how it can be achieved are given in 9.4.3 above.

Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility (see 9.4.3).

9.4.5 Remote diagnostic port protection

Access to diagnostic ports should be securely controlled. Many computers and communication systems are installed with a dial-up remote diagnostic facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access. They should therefore be protected by an appropriate security mechanism, e.g. a key lock and a procedure to ensure that they are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

9.4.6 Segregation in networks

Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, the introduction of controls within the network, to segregate groups of information services, users and information systems, should be considered.

One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. Such a perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains (see 9.4.7 and 9.4.8) and to block unauthorized access in accordance with the organization's access control policy (see 9.1). An example of this type of gateway is what is commonly referred to as a firewall.

The criteria for segregation of networks into domains should be based on the access control policy and access requirements (see 9.1), and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology (see 9.4.7 and 9.4.8).

9.4.7 Network connection control

Access control policy requirements for shared networks, especially those extending across organizational boundaries, may require the incorporation of controls to restrict the connection capability of the users. Such controls can be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be based on the access policy and requirements of the business applications (see 9.1), and should be maintained and updated accordingly.

Examples of applications to which restrictions should be applied are:

a) electronic mail;

b) one-way file transfer;

c) both-ways file transfer;

d) interactive access;

e) network access linked to time of day or date.

9.4.8 Network routing control

Shared networks, especially those extending across organizational boundaries, may require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications (see 9.1). This control is often essential for networks shared with third party (non-organization) users.

Routing controls should be based on positive source and destination address checking mechanisms. Network address translation is also a very useful mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another. They can be implemented in software or hardware. Implementers should be aware of the strength of any mechanisms deployed.

9.4.9 Security of network services

A wide range of public or private network services is available, some of which offer value-added services. Network services may have unique or complex security characteristics. Organizations using network services should ensure that a clear description of the security attributes of all services used is provided.

9.5 Operating system access control

Objective: To prevent unauthorized computer access.

Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of the following:

a) identifying and verifying the identity, and if necessary the terminal or location of each authorized user;

b) recording successful and failed system accesses;

c) providing appropriate means for authentication; if a password management system is used, it should ensure quality passwords [see 9.3.1 d]];

d) where appropriate, restricting the connection times of users.

Other access control methods, such as challenge-response, are available if these are justified on the basis of business risk.

9.5.1 Automatic terminal identification

Automatic terminal identification should be considered to authenticate connections to specific locations and to portable equipment. Automatic terminal identification is a technique that can be used if it is important that the session can only be initiated from a particular location or computer terminal. An identifier in, or attached to, the terminal can be used to indicate whether this particular terminal is permitted to initiate or receive specific transactions. It may be necessary to apply physical protection to the terminal, to maintain the security of the terminal identifier. A number of other techniques can also be used to authenticate users (see 9.4.3).

9.5.2 Terminal log-on procedures

Access to information services should be attainable via a secure log-on process. The procedure for logging into a computer system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with unnecessary assistance. A good log-on procedure should:

a) not display system or application identifiers until the log-on process has been successfully completed;

b) display a general notice warning that the computer should only be accessed by authorized users;

c) not provide help messages during the log-on procedure that would aid an unauthorized user;

d) validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

e) limit the number of unsuccessful log-on attempts allowed (three is recommended) and consider:
    1) recording unsuccessful attempts;
    2) forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization;
    3) disconnecting data link connections;

f) limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on;

g) display the following information on completion of a successful log-on:
    1) date and time of the previous successful log-on;
    2) details of any unsuccessful log-on attempts since the last successful log-on.

9.5.3 User identification and authentication

All users (including technical support staff, such as operators, network administrators, system programmers and database administrators) should have a unique identifier (user ID) for their personal and sole use so that activities can subsequently be traced to the responsible individual. User IDs should not give any indication of the user's privilege level (see 9.2.2), e.g. manager, supervisor.

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented for such cases. Additional controls may be required to maintain accountability.

There are various authentication procedures, which can be used to substantiate the claimed identity of a user. Passwords (see also 9.3.1 and below) are a very common way to provide identification and authentication (I&A) based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols.

Objects such as memory tokens or smart cards that users possess can also be used for I & A. Biometric authentication technologies that use the unique characteristics or attributes of an individual can also be used to authenticate the person's identity. A combination of technologies and mechanisms securely linked will result in stronger authentication.

9.5.4 Password management system

Passwords are one of the principal means of validating a user's authority to access a computer service. Password management systems should provide an effective, interactive facility, which ensures quality passwords (see 9.3.1 for guidance on use of passwords).

Some applications require user passwords to be assigned by an independent authority. In most cases the passwords are selected and maintained by users.

A good password management system should:

a) enforce the use of individual passwords to maintain accountability;

b) where appropriate, allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

c) enforce a choice of quality passwords as described in 9.3.1;

d) where users maintain their own passwords, enforce password changes as described in 9.3.1;

e) where users select passwords, force them to change temporary passwords at the first log-on (see 9.2.3);

f) maintain a record of previous user passwords, e.g. for the previous 12 months, and prevent re-use;

g) not display passwords on the screen when being entered;

h) store password files separately from application system data;

i) store passwords in encrypted form using a one-way encryption algorithm;

j) alter default vendor passwords following installation of software.

9.5.5 Use of system utilities

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled. The following controls should be considered:

a) use of authentication procedures for system utilities;

b) segregation of system utilities from applications software;

c) limitation of the use of system utilities to the minimum practical number of trusted, authorized users;

d) authorization for ad hoc use of systems utilities;

e) limitation of the availability of system utilities, e.g. for the duration of an authorized change;

f) logging of all use of system utilities;

g) defining and documenting of authorization levels for system utilities;

h) removal of all unnecessary software based utilities and system software.

9.5.6 Duress alarm to safeguard users

Provision of a duress alarm should be considered for users who might be the target of coercion. The decision whether to supply such an alarm should be based on an assessment of risks. There should be defined responsibilities and procedures for responding to a duress alarm.

9.5.7 Terminal time-out

Inactive terminals in high risk locations, e.g. public or external areas outside the organization’s security management, or serving high risk systems, should shut down after a defined period of inactivity to prevent access by unauthorized persons. This time-out facility should clear the terminal screen and close both application and network sessions after a defined period of inactivity. The time-out delay should reflect the security risks of the area and the users of the terminal.

A limited form of terminal time-out facility can be provided for some PCs which clears the screen and prevents unauthorized access but does not close down the application or network sessions.

9.5.8 Limitation of connection time

Restrictions on connection times should provide additional security for high-risk applications. Limiting the period during which terminal connections are allowed to computer services reduces the window of opportunity for unauthorized access. Such a control should be considered for sensitive computer applications, especially those with terminals installed in high risk locations, e.g. public or external areas that are outside the organization's security management. Examples of such restrictions include:

a) using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration;

b) restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation.

9.6 Application access control

Objective: To prevent unauthorized access to information held in information systems.
Security facilities should be used to restrict access within application systems.
Logical access to software and information should be restricted to authorized users. Application systems should:

a) control user access to information and application system functions, in accordance with a defined business access control policy;

b) provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls;

c) not compromise the security of other systems with which information resources are shared;

d) be able to provide access to information to the owner only, other nominated authorized individuals, or defined groups of users.

9.6.1 Information access restriction

Users of application systems, including support staff, should be provided with access to information and application system functions in accordance with a defined access control policy, based on individual business application requirements and consistent with organizational information access policy (see 9.1). Application of the following controls should be considered in order to support access restriction requirements:

a) providing menus to control access to application system functions;

b) restricting users' knowledge of information or application system functions which they are not authorized to access, with appropriate editing of user documentation;

c) controlling the access rights of users, e.g. read, write, delete and execute;

d) ensuring that outputs from application systems handling sensitive information contain only the information that are relevant to the use of the output and are sent only to authorized terminals and locations, including periodic review of such outputs to ensure that redundant information is removed.

9.6.2 Sensitive system isolation

Sensitive systems might require a dedicated (isolated) computing environment. Some application systems are sufficiently sensitive to potential loss that they require special handling. The sensitivity may indicate that the application system should run on a dedicated computer, should only share resources with trusted applications systems, or have no limitations. The following considerations apply.

a) The sensitivity of an application system should be explicitly identified and documented by the application owner (see 4.1.3).

b) When a sensitive application is to run in a shared environment, the application systems with which it will share resources should be identified and agreed with the owner of the sensitive application.

9.7 Monitoring system access and use

Objective: To detect unauthorized activities.

Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents.
System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model (see 9.1) to be verified.

9.7.1 Event logging

Audit logs recording exceptions and other security-relevant events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs should also include:

a) user IDs;

b) dates and times for log-on and log-off;

c) terminal identity or location if possible;

d) records of successful and rejected system access attempts;

e) records of successful and rejected data and other resource access attempts.

Certain audit logs may be required to be archived as part of the record retention policy or because of requirements to collect evidence (see also clause 12).

9.7.2 Monitoring system use

9.7.2.1 *Procedures and areas of risk*

Procedures for monitoring use of information processing facilities should be established. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be considered include:

a) authorized access, including detail such as:

   1) the user ID;

   2) the date and time of key events;

   3) the types of events;

   4) the files accessed;

   5) the program/utilities used;

b) all privileged operations, such as:

   1) use of supervisor account;

   2) system start-up and stop;

   3) I/O device attachment/detachment;

c) unauthorized access attempts, such as:

   1) failed attempts;

   2) access policy violations and notifications for network gateways and firewalls;
   3) alerts from proprietary intrusion detection systems;

d) system alerts or failures such as:
   1) console alerts or messages;
   2) system log exceptions;
   3) network management alarms.

9.7.2.2 *Risk factors*

The result of the monitoring activities should be reviewed regularly. The frequency of the review should depend on the risks involved. Risk factors that should be considered include:

a) the criticality of the application processes;

b) the value, sensitivity or criticality of the information involved;

c) the past experience of system infiltration and misuse;

d) the extent of system interconnection (particularly public networks).

9.7.2.3 *Logging and reviewing events*

A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of security incidents are given in 9.7.1.

System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered.

When allocating the responsibility for log review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Particular attention should be given to the security of the logging facility because if tampered with it can provide a false sense of security. Controls should aim to protect against unauthorized changes and operational problems including:

a) the logging facility being de-activated;

b) alterations to the message types that are recorded;

c) log files being edited or deleted;

d) log file media becoming exhausted, and either failing to record events or over-writing itself.

9.7.3 Clock synchronization

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal Co-ordinated Time (UCT) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.

9.8 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the teleworking site and ensure that suitable arrangement are in place for this way of working.

9.8.1 Mobile computing

When using mobile computing facilities, e.g. notebooks, palmtops, laptops and mobile phones, special care should be taken to ensure that business information is not compromised. A formal policy should be adopted that takes into account the risks of working with mobile computing facilities, in particular in unprotected environments. For example such a policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques (see 10.3).

It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date (see 8.3). Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

Suitable protection should be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication, and with suitable access control mechanisms in place (see 9.4).

Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment. More information about the physical protection of mobile equipment can be found in 7.2.5.

Training should be arranged for staff using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that should be implemented.

9.8.2 Teleworking

Teleworking uses communications technology to enable staff to work remotely from a fixed location outside of their organization. Suitable protection of the teleworking site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. It is important that teleworking is both authorized and controlled by management, and that suitable arrangements are in place for this way of working.

Organizations should consider developing a policy, procedures and standards to control teleworking activities. Organizations should only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the organization's security policy. The following should be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed teleworking environment;

c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system;

d) the threat of unauthorized access to information or resources from other people using the accommodation, e.g. family and friends.

The controls and arrangements to be considered include:

a) the provision of suitable equipment and storage furniture for the teleworking activities;

b) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;

c) the provision of suitable communication equipment, including methods for securing remote access;

d) physical security;

e) rules and guidance on family and visitor access to equipment and information;

f) the provision of hardware and software support and maintenance;

g) the procedures for back-up and business continuity;

h) audit and security monitoring;

i) revocation of authority, access rights and the return of equipment when the teleworking activities cease.

10 Systems development and maintenance

10.1 Security requirements of systems

Objective: To ensure that security is built into information systems.

This will include infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems.
All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

10.1.1 Security requirements analysis and specification

Statements of business requirements for new systems, or enhancements to existing systems should specify the requirements for controls. Such specifications should consider the automated controls to be incorporated in the system, and the need for supporting manual controls. Similar considerations should be applied when evaluating software packages for business applications. If considered appropriate, management may wish to make use of independently evaluated and certified products.

Security requirements and controls should reflect the business value of the information assets involved, and the potential business damage, which might result from a failure or absence of security. The framework for analysing security requirements and identifying controls to fulfil them is risk assessment and risk management.

Controls introduced at the design state are significantly cheaper to implement and maintain than those included during or after implementation.

10.2 Security in application systems

Objective: To prevent loss, modification or misuse of user data in application systems.

Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical organizational assets. Such controls should be determined on the basis of security requirements and risk assessment.

10.2.1 Input data validation

Data input to application systems should be validated to ensure that it is correct and appropriate. Checks should be applied to the input of business transactions, standing data (names and addresses, credit limits, customer reference numbers) and parameter tables (sales prices, currency conversion rates, tax rates). The following controls should be considered:

a) dual input or other input checks to detect the following errors:
   1) out-of-range values;
   2) invalid characters in data fields;
   3) missing or incomplete data;
   4) exceeding upper and lower data volume limits;
   5) unauthorized or inconsistent control data;

b) periodic review of the content of key fields or data files to confirm their validity and integrity;

c) inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized);

d) procedures for responding to validation errors;

e) procedures for testing the plausibility of the input data;

f) defining the responsibilities of all personnel involved in the data input process.

10.2.2 Control of internal processing

10.2.2.1 *Areas of risk*

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks should be incorporated into systems to detect such corruption. The design of applications should ensure that restrictions are implemented to minimize the risk of processing failures leading to a loss of integrity. Specific areas to consider include:

a) the use and location in programs of add and delete functions to implement changes to data;

b) the procedures to prevent programs running in the wrong order or running after failure of prior processing (see also 8.1.1);

c) the use of correct programs to recover from failures to ensure the correct processing of data.

10.2.2.2 *Checks and controls*

The controls required will depend on the nature of the application and the business impact of any corruption of data. Examples of checks that can be incorporated include the following:

a) session or batch controls, to reconcile data file balances after transaction updates;

b) balancing controls, to check opening balances against previous closing balances, namely:

   1) run-to-run controls;

   2) file update totals;

   3) program-to-program controls;

c) validation of system-generated data (see 10.2.1);

d) checks on the integrity of data or software downloaded, or uploaded, between central and remote computers (see 10.3.3);

e) hash totals of records and files;

f) checks to ensure that application programs are run at the correct time;

g) checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved.

10.2.3 Message authentication

Message authentication is a technique used to detect unauthorized changes to, or corruption of, the contents of a transmitted electronic message. It can be implemented in hardware or software supporting a physical message authentication device or a software algorithm.

Message authentication should be considered for applications where there is a security requirement to protect the integrity of the message content, e.g. electronic funds transfer, specifications, contracts, proposals etc with high importance or other similar electronic data exchanges. An assessment of security risks should be carried out to determine if message authentication is required and to identify the most appropriate method of implementation.

Message authentication is not designed to protect the contents of a message from unauthorized disclosure. Cryptographic techniques (see 10.3.2 and 10.3.3) can be used as an appropriate means of implementing message authentication.

10.2.4 Output data validation

Data output from an application system should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Typically, systems are constructed on the premise that having undertaken appropriate validation, verification and testing the output will always be correct. This is not always the case. Output validation may include:

a) plausibility checks to test whether the output data is reasonable;

b) reconciliation control counts to ensure processing of all data;

c) providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision and classification of the information;

d) procedures for responding to output validation tests;

e) defining the responsibilities of all personnel involved in the data output process.

10.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information.
Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

10.3.1 Policy on the use of cryptographic controls

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of a wider process of assessing risks and selecting controls. A risk assessment should be carried out to determine the level of protection that information should be given. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

An organization should develop a policy on its use of cryptographic controls for protection of its information. Such a policy is necessary to maximize benefits and minimize the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use. When developing a policy the following should be considered:

a) the management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected;

b) the approach to key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys;

c) roles and responsibilities, e.g. who is responsible for:

d) the implementation of the policy;

e) the key management;

f) how the appropriate level of cryptographic protection is to be determined;

g) the standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes).

10.3.2 Encryption

Encryption is a cryptographic technique that can be used to protect the confidentiality of information. It should be considered for the protection of sensitive or critic al information.

Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used.

When implementing the organization's cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information. In addition, consideration should be given to the controls that apply to the export and import of cryptographic technology (see also 12.1.6).

Specialist advice should be sought to identify the appropriate level of protection, to select suitable products that will provide the required protection and the implementation of a secure system of key management (see also 10.3.5). In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the organization's intended use of encryption.

10.3.3 Digital signatures

Digital signatures provide a means of protecting the authenticity and integrity of electronic documents. For example they can be used in electronic commerce where there is a need to verify who signed an electronic document and check whether the contents of the signed document have been changed.

Digital signatures can be applied to any form of document being processed electronically, e.g. they can be used to sign electronic payments, funds transfers, contracts and agreements. Digital signatures can be implemented using a cryptographic technique based on a uniquely related pair of keys where one key is used to create a signature (the private key) and the other to check the signature (the public key).

Care should be taken to protect the confidentiality of the private key. This key should be kept secret since anyone having access to this key can sign documents, e.g. payments, contracts, thereby forging the signature of the owner of that key. In addition, protecting the integrity of the public key is important. This protection is provided by the use of a public key certificate (see 10.3.5).

Consideration needs to be given to the type and quality of the signature algorithm used and the length of keys to be used. Cryptographic keys used for digital signatures should be different from those used for encryption (see 10.3.2).

When using digital signatures, consideration should be given to any relevant legislation that describes the conditions under which a digital signature is legally binding. For example, in the case of electronic commerce it is important to know the legal standing of digital signatures. It may be necessary to have binding contracts or other agreements to support the use of digital signatures where the legal framework is inadequate. Legal advice should be sought regarding the laws and regulations that might apply to the organization's intended use of digital signatures.

10.3.4 Non-repudiation services

Non-repudiation services should be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action, e.g. a dispute involving the use of a digital signature on an electronic contract or payment. They can help establish evidence to substantiate whether a particular event or action has taken place, e.g. denial of sending a digitally signed instruction using electronic mail. These services are based on the use of encryption and digital signature techniques (see also 10.3.2 and 10.3.3).

10.3.5 Key management

10.3.5.1 *Protection of cryptographic keys*

The management of cryptographic keys is essential to the effective use of cryptographic techniques. Any compromise or loss of cryptographic keys may lead to a compromise of the confidentiality, authenticity and/or integrity of information. A management system should be in place to support the organization's use of the two types of cryptographic techniques, which are:

a) secret key techniques, where two or more parties share the same key and this key is used both to encrypt and decrypt information. This key has to be kept secret since anyone having access to it is able to decrypt all information being encrypted with that key, or to introduce unauthorized information;

b) public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret). Public key techniques can be used for encryption (see 10.3.2) and to produce digital signatures (see 10.3.3).

All keys should be protected against modification and destruction, and secret and private keys need protection against unauthorized disclosure. Cryptographic techniques can also be used for this purpose. Physical protection should be used to protect equipment used to generate, store and archive keys.

10.3.5.2 *Standards, procedures and methods*

A key management system should be based on an agreed set of standards, procedures and secure methods for:

a) generating keys for different cryptographic systems and different applications;

b) generating and obtaining public key certificates;

c) distributing keys to intended users, including how keys should be activated when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;

g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);

h) recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;

i) archiving keys, e.g. for information archived or backed up;

j) destroying keys;

k) logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, keys should have defined activation and deactivation dates so they can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used and the perceived risk.

Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.

In addition to the issue of securely managed secret and private keys, the protection of public keys should also be considered. There is a threat of someone forging a digital signature by replacing a user's public key with their own. This problem is addressed by the use of a public key certificate. These certificates should be produced in a way that uniquely binds information related to the owner of the public/private key pair to the public key. It is therefore important that the management process that generates these certificates can be trusted. This process is normally carried out by a certification authority which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see 4.2.2).

10.4 Security of system files

Objective: To ensure that IT projects and support activities are conducted in a secure manner. Access to system files should be controlled.

Maintaining system integrity should be the responsibility of the user function or development group to whom the application system or software belongs.

10.4.1 Control of operational software

Control should be provided for the implementation of software on operational systems. To minimize the risk of corruption of operational systems, the following controls should be considered.

a) The updating of the operational program libraries should only be performed by the nominated librarian upon appropriate management authorization (see 10.4.3).

b) If possible, operational systems should only hold executable code.

c) Executable code should not be implemented on an operational system until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated.

d) An audit log should be maintained of all updates to operational program libraries.

e) Previous versions of software should be retained as a contingency measure.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Any decision to upgrade to a new release should take into account the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses.

Physical or logical access should only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities should be monitored.

10.4.2 Protection of system test data

Test data should be protected and controlled. System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data. The use of operational databases containing personal information should be avoided. If such information is used, it should be depersonalized before use. The following controls should be applied to protect operational data, when used for testing purposes.

a) The access control procedures, which apply to operational application systems, should also apply to test application systems.

b) There should be separate authorization each time operational information is copied to a test application system.

c) Operational information should be erased from a test application system immediately after the testing is complete.

d) The copying and use of operational information should be logged to provide an audit trail.

10.4.3 Access control to program source library

In order to reduce the potential for corruption of computer programs; strict control should be maintained over access to program source libraries as follows (see also 8.3).

a) Where possible, program source libraries should not be held in operational systems.

b) A program librarian should be nominated for each application.

c) IT support staff should not have unrestricted access to program source libraries.

d) Programs under development or maintenance should not be held in operational program source libraries.

e) The updating of program source libraries and the issuing of program sources to programmers should only be performed by the nominated librarian upon authorization from the IT support manager for the application.

f) Program listings should be held in a secure environment (see 8.6.4).

g) An audit log should be maintained of all accesses to program source libraries.

h) Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.

i) Maintenance and copying of program source libraries should be subject to strict change control procedures (see 10.4.1).

10.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

Project and support environments should be strictly controlled.
Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

10.5.1 Change control procedures

In order to minimize the corruption of information systems, there should be strict control over the implementation of changes. Formal change control procedures should be enforced. They should ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Changing application software can impact the operational environment. Wherever practicable, application and operational change control procedures should be integrated (see also 8.1.2). This process should include:

a) maintaining a record of agreed authorization levels;

b) ensuring changes are submitted by authorized users;

c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

d) identifying all computer software, information, database entities and hardware that require amendment;

e) obtaining formal approval for detailed proposals before work commences;

f) ensuring that the authorized user accepts changes prior to any implementation;

g) ensuring that implementation is carried out to minimize business disruption;

h) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

i) maintaining a version control for all software updates;

j) maintaining an audit trail of all change requests;

k) ensuring that operating documentation (see 8.1.1) and user procedures are changed as necessary to be appropriate;

l) ensuring that the implementation of changes takes place at the right time and is not disturbing the business processes involved.

Many organizations maintain an environment in which users test new software and which is segregated from development and production environments. This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes.

10.5.2 Technical review of operating system changes

Periodically it is necessary to change the operating system, e.g. to install a newly supplied software release or patches. When changes oc cur, the application systems should be reviewed and tested to ensure that there is no adverse impact on operation or security. This process should cover:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;

b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;

c) ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation;

d) ensuring that appropriate changes are made to the business continuity plans (see clause 11).

10.5.3 Restrictions on changes to software packages

Modifications to software packages should be discouraged. As far as possible, and practicable, vendor-supplied software packages should be used without modification. Where it is deemed essential to modify a software package, the following points should be considered:

a) the risk of built-in controls and integrity processes being compromised;

b) whether the consent of the vendor should be obtained;

c) the possibility of obtaining the required changes from the vendor as standard program updates;

d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes.

If changes are deemed essential the original software should be retained and the changes applied to a clearly identified copy. All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades.

10.5.4 Covert channels and Trojan code

A covert channel can expose information by some indirect and obscure means. It may be activated by changing a parameter accessible by both secure and insecure elements of a computing system, or by embedding information into a data stream. Trojan code is designed to affect a system in a way that is not authorized and not readily noticed and not required by the recipient or user of the program. Covert channels and Trojan code rarely occur by accident. Where covert channels or Trojan code are a concern, the following should be considered:

a) buying programs only from a reputable source;

b) buying programs in source code so the code may be verified;

c) using evaluated products;

d) inspecting all source code before operational use;

e) controlling access to, and modification of, code once installed;

f) use staff of proven trust to work on key systems.

10.5.5 Outsourced software development

Where software development is outsourced, the following points should be considered:

a) licensing arrangements, code ownership and intellectual property rights (see **12.1.**2);

b) certification of the quality and accuracy of the work carried out;

c) escrow arrangements in the event of failure of the third party;

d) rights of access for audit of the quality and accuracy of work done;

e) contractual requirements for quality of code;

f) testing before installation to detect Trojan code.

11 Business continuity management

11.1 Aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

The consequences of disasters, security failures and loss of service should be analysed. Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans should be maintained and practised to become an integral part of all other management processes.
Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

11.1.1 Business continuity management process

There should be a managed process in place for developing and maintaining business continuity throughout the organization. It should bring together the following key elements of business continuity management:

a) understanding the risks the organization is facing in terms of their likelihood and their impact, including an identification and prioritization of critical business processes;

b) understanding the impact which interruptions are likely to have on the business (it is important that solutions are found that will handle smaller incidents, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information processing facilities;

c) considering the purchase of suitable insurance which may form part of the business continuity process;

d) formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities;

e) formulating and documenting business continuity plans in line with the agreed strategy;

f) regular testing and updating of the plans and processes put in place;

g) ensuring that the management of business continuity is incorporated in the organization's processes and structure. Responsibility for co-ordinating the business continuity management process should be assigned at an appropriate level within the organization, e.g. at the information security forum (see 4.1.1).

11.1.2 Business continuity and impact analysis

Business continuity should begin by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This should be followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). Both of these activities should be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes, and is not limited to the information processing facilities.

Depending on the results of the risk assessment, a strategy plan should be developed to determine the overall approach to business continuity. Once this plan has been created, it should be endorsed by management.

11.1.3 Writing and implementing continuity plans

Plans should be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The business continuity planning process should consider the following:

a) identification and agreement of all responsibilities and emergency procedures;

b) implementation of emergency procedures to allow recovery and restoration in required time-scales. Particular attention needs to be given to the assessment of external business dependencies and the contracts in place;

c) documentation of agreed procedures and processes;

d) appropriate education of staff in the agreed emergency procedures and processes including crisis management;

e) testing and updating of the plans.

The planning process should focus on the required business objectives, e.g. restoring of specific services to customers in an acceptable amount of time. The services and resources that will enable this to occur should be considered, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities.

11.1.4 Business continuity planning framework

A single framework of business continuity plans should be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance. Each business continuity plan should specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, established emergency procedures, e.g. evacuation plans or any existing fallback arrangements, should be amended as appropriate.

A business continuity planning framework should consider the following:

a) the conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated;

b) emergency procedures which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities, e.g. police, fire service and local government;

c) fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales;

d) resumption procedures which describe the actions to be taken to return to normal business operations;

e) a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan;

f) awareness and education activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective;

g) the responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

Each plan should have a specific owner. Emergency procedures, manual fallback plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, should usually be the responsibility of the service providers.

11.1.5 Testing, maintaining and re-assessing business continuity plans

11.1.5.1 *Testing the plans*

Business continuity plans may fail on being tested, often because of incorrect assumptions, oversights, or changes in equipment or personnel. They should therefore be tested regularly to ensure that they are up to date and effective. Such tests should also ensure that all members of the recovery team and other relevant staff are aware of the plans.

The test schedule for business continuity plan(s) should indicate how and when each element of the plan should be tested. It is recommended to test the individual components of the plan(s) frequently. A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life. These should include:

a) table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions);

b) simulations (particularly for training people in their post-incident/crisis management roles);

c) technical recovery testing (ensuring information systems can be restored effectively);

d) testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site);

e) tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment);

f) complete rehearsals (testing that the organization, personnel, equipment, facilities and processes can cope with interruptions).

The techniques can be used by any organization and should reflect the nature of the specific recovery plan.

11.1.5.2 *Maintaining and re-assessing the plans*

Business continuity plans should be maintained by regular reviews and updates to ensure their continuing effectiveness (see 11.1.5.1 to 11.1.5.3). Procedures should be included within the organization’s change management programme to ensure that business continuity matters are appropriately addressed.

Responsibility should be assigned for regular reviews of each business continuity plan; the identification of changes in business arrangements not yet reflected in the business continuity plans should be followed by an appropriate update of the plan. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

Examples of situations that might necessitate updating plans include the acquisition of new equipment, or upgrading of operational systems and changes in:

a) personnel;

b) addresses or telephone numbers;

c) business strategy;

d) location, facilities and resources;

e) legislation;

f) contractors, suppliers and key customers;

g) processes, or new/withdrawn ones;

h) risk (operational and financial).

12 Compliance

12.1 Compliance with legal requirements

Objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual

obligations and of any security requirements.
The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements.
Advice on specific legal requirements should be sought from the organization’s legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and for information created in one country that is transmitted to another country (i.e. trans-border data flow).

12.1.1 Identification of applicable legislation

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

12.1.2 Intellectual property rights (IPR)

12.1.2.1 *Copyright*

Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trade marks. Copyright infringement can lead to legal action which may involve criminal proceedings.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization, or that is licensed or provided by the developer to the organization, can be used.

12.1.2.2 *Software copyright*

Proprietary software products are usually supplied under a licence agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. The following controls should be considered:

a) publishing a software copyright compliance policy which defines the legal use of software and information products;

b) issuing standards for the procedures for acquisition of software products;

c) maintaining awareness of the software copyright and acquisition policies, and giving notice of the intent to take disciplinary action against staff who breach them;

d) maintaining appropriate asset registers;

e) maintaining proof and evidence of ownership of licenses, master disks, manuals, etc;

f) implementing controls to ensure that any maximum number of users permitted is not exceeded;

g) carrying out checks that only authorized software and licensed products are installed;

h) providing a policy for maintaining appropriate licence conditions;

i) providing a policy for disposing or transferring software to others;

j) using appropriate audit tools;

k) complying with terms and conditions for software and information obtained from public networks (see also 8.7.6).

12.1.3 Safeguarding of organizational records

Important records of an organization should be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Examples of this are records that may be required as evidence that an organization operates within statutory or regulatory rules, or to ensure adequate defence against potential civil or criminal action, or to confirm the financial status of an organization with respect to shareholders, partners and auditors. The time period and data content for information retention may be set by national law or regulation.

Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys associated with encrypted archives or digital signatures (see 10.3.2 and 10.3.3), should be kept securely and made available to authorized persons when needed.

Consideration should be given to the possibility of degradation of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in a manner acceptable to a court of law, e.g. all records required can be retrieved in an acceptable timeframe and in an acceptable format.

The system of storage and handling should ensure clear identification of records and of their statutory or regulatory retention period. It should permit appropriate destruction of records after that period if they are not needed by the organization.

To meet these obligations, the following steps should be taken within an organization.

a) Guidelines should be issued on the retention, storage, handling and disposal of records and information.

b) A retention schedule should be drawn up identifying essential record types and the period of time for which they should be retained.

c) An inventory of sources of key information should be maintained.

d) Appropriate controls should be implemented to protect essential records and information from loss, destruction and falsification.

12.1.4 Data protection and privacy of personal information

A number of countries have introduced legislation placing controls on the processing and transmission of personal data (generally information on living individuals who can be identified from that information). Such controls may impose duties on those collecting, processing and disseminating personal information, and may restrict the ability to transfer that data to other countries.

Compliance with data protection legislation requires appropriate management structure and control. Often this is best achieved by the appointment of a data protection officer who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. It should be the responsibility of the owner of the data to inform the data protection officer about any proposals to keep personal information in a structured file, and to ensure awareness of the data protection principles defined in the relevant legislation.

12.1.5 Prevention of misuse of information processing facilities

The information processing facilities of an organization are provided for business purposes. Management should authorize their use. Any use of these facilities for non-business or unauthorized purposes, without management approval, should be regarded as improper use of the facilities. If such activity is identified by monitoring or other means, it should be brought to the attention of the individual manager concerned for appropriate disciplinary action.

The legality of monitoring the usage varies from country to country and may require employees to be advised of such monitoring or to obtain their agreement. Legal advice should be taken before implementing monitoring procedures.

Many countries have, or are in the process of introducing, legislation to protect against computer misuse. It may be a criminal offence to use a computer for unauthorized purposes. It is therefore essential that all users are aware of the precise scope of their permitted access. This can, for example, be achieved by giving users written authorization, a copy of which should be signed by the user and securely retained by the organization. Employees of an organization, and third party users, should be advised that no access be permitted except that which is authorized.

At log-on a warning message should be presented on the computer screen indicating that the system being entered is private and that unauthorized access is not permitted. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process.

12.1.6 Regulation of cryptographic controls

Some countries have implemented agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls. Such control may include:

a) import and/or export of computer hardware and software for performing cryptographic functions;

b) import and/or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) mandatory or discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with national law. Before encrypted information or cryptographic controls are moved to another country, legal advice should also be taken.

12.1.7 Collection of evidence

12.1.7.1 *Rules for evidence*

It is necessary to have adequate evidence to support an action against a person or organization. Whenever this action is an internal disciplinary matter the evidence necessary will be described by internal procedures.

Where the action involves the law, either civil or criminal, the evidence presented should 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. In general, these rules cover:

a) admissibility of evidence: whether or not the evidence can be used in court;

b) weight of evidence: the quality and completeness of the evidence;

c) adequate evidence that controls have operated correctly and consistently (i.e. process control evidence) throughout the period that the evidence to be recovered was stored and processed by the system.

12.1.7.2 *Admissibility of evidence*

To achieve admissibility of the evidence, organizations should ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.

12.1.7.3 *Quality and completeness of evidence*

To achieve quality and completeness of the evidence, a strong evidence trail is needed. In general, such a strong trail can be established under the following conditions.

a) For paper documents: the original is kept securely and it is recorded who found it, where it was found, when it was found and who witnessed the discovery. Any investigation should ensure that originals are not tampered with.

b) For information on computer media: copies of any removable media, information on hard disks or in memory should be taken to ensure availability. The log of all actions during the copying process should be kept and the process should be witnessed. One copy of the media and the log should be kept securely.

When an incident is first detected, it may not be obvious that it will result in possible court action. Therefore, the danger exists that necessary evidence is destroyed accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.

12.2 Reviews of security policy and technical compliance

Objective: To ensure compliance of systems with organizational security policies and standards.

The security of information systems should be regularly reviewed.
Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards.

12.2.1 Compliance with security policy

Managers should ensure that all security procedures within their area of responsibility are carried out correctly. In addition, all areas within the organization should be considered for regular review to ensure compliance with security policies and standards. These should include the following:

a) information systems;

b) systems providers;

c) owners of information and information assets;

d) users;

e) management.

Owners of information systems (see 5.1) should support regular reviews of the compliance of their systems with the appropriate security policies, standards and any other security requirements. Operational monitoring of system use is covered in 9.7.

12.2.2 Technical compliance checking

Information systems should be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical assistance. It should be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer, or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.

Compliance checking also covers, for example, penetration testing, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities. Caution should be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

Any technical compliance check should only be carried out by, or under the supervision of, competent, authorized persons.

12.3 System audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the system audit process.

There should be controls to safeguard operational systems and audit tools during system audits.
Protection is also required to safeguard the integrity and prevent misuse of audit tools.

12.3.1 System audit controls

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. The following should be observed.

a) Audit requirements should be agreed with appropriate management.

b) The scope of the checks should be agreed and controlled.

c) The checks should be limited to read-only access to software and data.

d) Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed.

e) IT resources for performing the checks should be explicitly identified and made available.

f) Requirements for special or additional processing should be identified and agreed.

g) All access should be monitored and logged to produce a reference trail.

h) All procedures, requirements and responsibilities should be documented.

12.3.2 Protection of system audit tools

Access to system audit tools, i.e. software or data files, should be protected to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

Index

blank

National annex NA (informative) Editorial amendments required to convert from BS 7799-1:1999 to BS ISO/IEC 17799:2000

Table NA.1 shows the editorial amendments required to convert from BS 7799-1:1999 to BS ISO/IEC 17799:2000.

Table NA.1 — Editorial amendments required to convert from BS 7799-1:1999 to BS ISO/IEC 17799:2000

BS 7799-1:1999	BS ISO/IEC 17799:2000 (BS 7799-1:2000)
Title Title: "Information security management — Part 1: Code of practice for information security management"	**Title** Title of standard changed to: "Information technology — Information security management"
Introduction **Selecting controls**	**Introduction** **Selecting controls** Add the following **new** sentence at the end of the first paragraph: "As another example, **9.7** and **12.1** describe how system use can be monitored and evidence collected. The described controls e.g. event logging might conflict with applicable legislation, such as privacy protection for customers or in the workplace."
Introduction **Information security starting point** Second paragraph, bullet points: "a) intellectual property rights (see **12.1.2**); b) safeguarding of organizational records (see **12.1.3**); c) data protection and privacy of personal information (see **12.1.4**)."	**Introduction** **Information security starting point** In the second paragraph, re-order the bullet points as follows: "a) data protection and privacy of personal information (see **12.1.4**); b) safeguarding of organizational records (see **12.1.3**); c) intellectual property rights (see **12.1.2**)."

Table NA.1 — Editorial amendments required to convert from BS 7799-1:1999 to BS ISO/IEC 17799:2000 *(continued)*

BS 7799-1:1999	BS ISO/IEC 17799:2000 (BS 7799-1:2000)
Clause 1 Scope First sentence: "This part of BS 7799 gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization."	**Clause 1 Scope** Replace the first sentence in the Scope with: "This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization."
Clause 1 Scope	**Clause 1 Scope** Add the following **new** sentence at the end of the Scope: "Recommendations from this standard should be selected and used in accordance with applicable laws and regulations."
Clause 2.1 Information security Definition of "information security": "The preservation of confidentiality, integrity and availability of information. NOTE Confidentiality is defined as ensuring that information is accessible only to those authorized to have access. Integrity is defined as safeguarding the accuracy and completeness of information and processing methods. Availability is defined as ensuring that authorized users have access to information and associated assets when required."	**Clause 2.1 Information security** Replace the definition of "information security" with: "The preservation of confidentiality, integrity and availability of information. - Confidentiality is defined as ensuring that information is accessible only to those authorized to have access. - Integrity is defined as safeguarding the accuracy and completeness of information and processing methods. - Availability is defined as ensuring that authorized users have access to information and associated assets when required."
Clause 4 Security organization Clause title: "Security organization"	**Clause 4 Organizational security** Change the clause title to: "Organizational security"

Table NA.1 — Editorial amendments required to convert from BS 7799-1:1999 to BS ISO/IEC 17799:2000 *(continued)*

BS 7799-1:1999	BS ISO/IEC 17799:2000 (BS 7799-1:2000)
Clause 4.1.1 Bullet c): “c) reviewing and monitoring security incidents;”	**Clause 4.1.1** Replace bullet c) with: “c) reviewing and monitoring information security incidents;”
Clause 4.1.4 Second paragraph, first sentence: “The following should be considered.”	**Clause 4.1.4** Second paragraph, replace first sentence with: “The following controls should be considered.”
Clause 6.1.2 Second sentence, first paragraph: “This should include the following:”	**Clause 6.1.2** Replace second sentence, first paragraph with: “This should include the following controls:”
Clauses 7.1.4 and 7.2.1 First paragraph, last sentence: “The following should be considered.”	**Clauses 7.1.4 and 7.2.1** Replace first paragraph, last sentence with: “The following controls should be considered.”
Clauses 7.1.5 and 7.2.4 First paragraph, last sentence: “The following guidelines should be considered.”	**Clauses 7.1.5 and 7.2.4** Replace first paragraph, last sentence with: “The following controls should be considered.”
Clause 7.2.4 Bullet c): “c) Records should be kept of all suspected or actual faults and all preventative and corrective maintenance.”	**Clause 7.2.4** Replace bullet c) with: “c) Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.”

Table NA.1 — Editorial amendments required to convert from BS 7799-1:1999 to BS ISO/IEC 17799:2000 *(continued)*

BS 7799-1:1999	BS ISO/IEC 17799:2000 (BS 7799-1:2000)
Clause 7.3.1 Third paragraph: "The following guidelines should be applied."	**Clause 7.3.1** Replace third paragraph with: "The following controls should be considered."
Clause 8.1.2 First paragraph, final sentence. "In particular, the following items should be considered:"	**Clause 8.1.2** Replace first paragraph, final sentence with: "The following controls should be considered."
Clause 8.1.3 First paragraph, final sentence. "The following guidelines should be considered."	**Clause 8.1.3** Replace first paragraph, final sentence with: "The following controls should be considered."
Clause 8.1.4 Third paragraph, last sentence: "The following points should be considered."	**Clause 8.1.4** Replace the third paragraph, last sentence with: "The following controls should be considered."
Clauses 8.2.2 and 8.4.1 First paragraph, final sentence: "The following should be considered:"	**Clauses 8.2.2 and 8.4.1** Replace first paragraph, final sentence with: "The following controls should be considered:"
Clause 8.5.1 First paragraph, last sentence: "In particular, the following items should be considered."	**Clause 8.5.1** Replace first paragraph, last sentence with: "In particular, the following controls should be considered."
Clauses 8.6.1 and 8.6.2 First paragraph, final sentence: "The following guidelines should be considered."	**Clauses 8.6.1 and 8.6.2** Replace first paragraph, last sentence with: "The following controls should be considered."

Table NA.1 — Editorial amendments required to convert from BS 7799-1:1999 to BS ISO/IEC 17799:2000 *(continued)*

BS 7799-1:1999	BS ISO/IEC 17799:2000 (BS 7799-1:2000)
Clause 8.6.3 First paragraph, last sentence: "The following items should be considered (see also **5.2** and **8.7.2**):"	**Clause 8.6.3** Replace first paragraph, last sentence with: "The following controls should be considered (see also **5.2** and **8.7.2**):"
Clause 8.7.2 Bullet c).	**Clause 8.7.2** Bullet c), add **new** fifth sub-bullet: "5) use of digital signatures and confidentiality encryption, see **10.3**."
Clause 8.7.3 First paragraph, last sentence: "Security considerations for electronic commerce should include the following."	**Clause 8.7.3** Replace first paragraph, last sentence with: "Security considerations for electronic commerce should include the following controls."
Clause 10.2.3 Second paragraph, first sentence: "Message authentication should be considered for applications where there is a security requirement to protect the integrity of the message content, e.g. electronic funds transfer, specifications, contracts, proposals etc. with high importance or other similar electronic data exchanges."	**Clause 10.2.3** Replace second paragraph, first sentence with: "Message authentication should be considered for applications where there is a security requirement to protect the integrity of the message content, e.g. electronic funds transfer, specifications, contracts, proposals etc. with high importance or other similar electronic data exchanges."
Clause 11.1.5.2 First sentence, first paragraph.	**Clause 11.1.5.2** First sentence, first paragraph: An error has been introduced in ISO/IEC 17799 where it states incorrectly: "(see **11.1.5.1** to **11.1.5.3**)" It should be read as: "(see **11.1.1** to **11.1.3**)"

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: 020 8996 9000. Fax: 020 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: 020 8996 9001. Fax: 020 8996 7001. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: 020 8996 7111. Fax: 020 8996 7048.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: 020 8996 7002. Fax: 020 8996 7001. Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL

Information security management systems — Specification with guidance for use

ICS 03.100.01; 35.020

British Standards

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to BSI-DISC Committee BDD/2, Information security management, upon which the following bodies were represented:

@stake

Articsoft Ltd

Association of British Insurers

British Computer Society

British Telecommunications plc

British Security Industry Association

Department of Transport and Industry — Information Security Policy Group

EDS Ltd

Experian

Gamma Secure Systems Limited

GlaxoSmithKline plc

HMG Protective Security Authority

HSBC

I-Sec Ltd

Institute of Chartered Accountants in England and Wales

Institute of Internal Auditors — UK and Ireland

KPMG plc

Lloyds TSB

Logica UK Ltd

London Clearing House

Marks & Spencer plc

National Westminster Group

Nationwide Building Society

QinetiQ Ltd

Shell UK

Unilever

Wm. List & Co

XiSEC Consultants Ltd/AEXIS Security Consultants

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Policy and Strategy Committee and comes into effect on 5 September 2002

First published as Part 2 February 1998
Revised May 1999

The following BSI references relate to the work on this British Standard:
Committee reference BDD/2
Draft for comment 01/682010 DC

ISBN 0 580 40250 9

Amendments issued since publication

Amd. No.	Date	Comments

Contents

Foreword

This part of BS 7799 has been prepared by BDD/2, Information security management. It supersedes BS 7799-2:1999, which is obsolescent.

This new edition has been produced to harmonize it with other management system standards such as BS EN ISO 9001:2000 and BS EN ISO 14001:1996 to provide consistent and integrated implementation and operation of management systems. It also introduces a Plan-Do-Check-Act (PDCA) model as part of a management system approach to developing, implementing, and improving the effectiveness of an organization's information security management system.

The implementation of the PDCA model will also reflect the principles as set out in the OECD guidance (2002)[1] governing the security of information systems and networks. In particular, this new edition gives a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

The control objectives and controls referred to in this edition are directly derived from and aligned with those listed in BS ISO/IEC 17799:2000. The list of control objectives and controls in this British Standard is not exhaustive and an organization might 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 organization.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

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

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 33 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

[1] OECD. *OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.org

0 Introduction

0.1 General

This British Standard has been prepared for business managers and their staff to provide a model for setting up and managing an effective Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by business needs and objectives, resulting security requirements, 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 British Standard can be used by internal and external parties including certification bodies, to assess an organization's ability to meet its own requirements, as well as any customer or regulatory demands.

0.2 Process approach

This British Standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an organization's ISMS.

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

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".

A process approach encourages its users to emphasize 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 an organization's overall business risk;

c) monitoring and reviewing the performance and effectiveness of the ISMS;

d) continual improvement based on objective measurement.

The model, known as the "Plan-Do-Check-Act" (PDCA) model, can be applied to all ISMS processes, as adopted in this standard. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes (i.e. managed information security) that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses **4**, **5**, **6** and **7**.

EXAMPLE 1

A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2

An expectation might be that if a serious incident occurs — perhaps hacking of an organization's eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.

NOTE The term "procedure" is, by convention, used in information security to mean a "process" that is carried out by people as opposed to a computer or other electronic means.

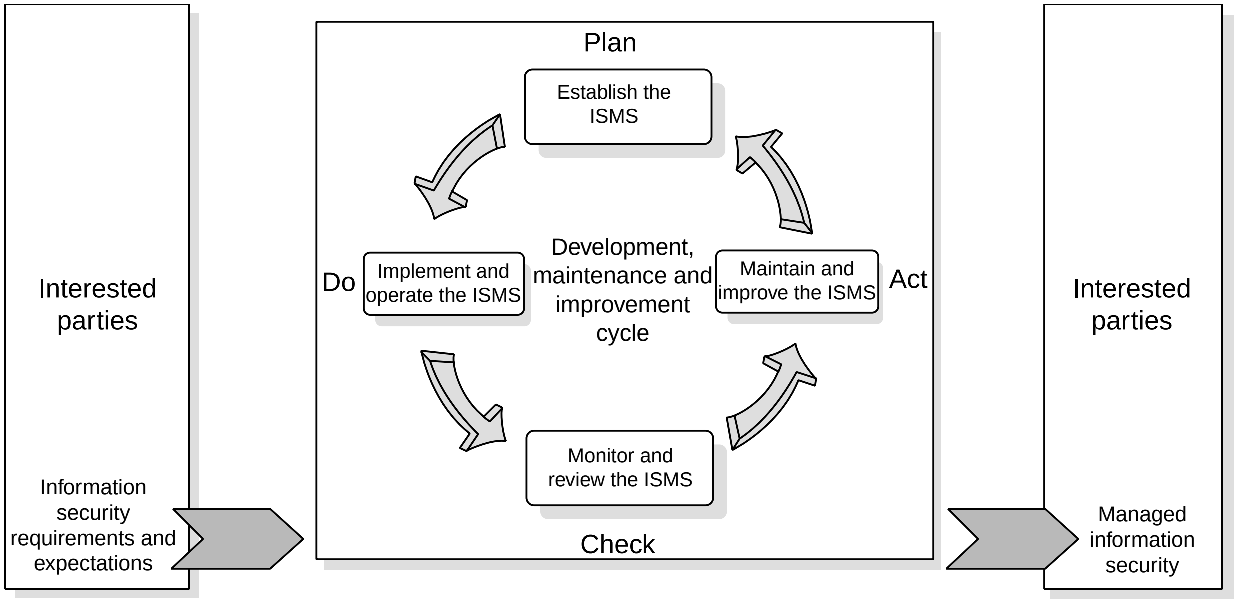
Interested parties
Information security requirements and expectations
Plan
Establish the ISMS
Do
Implement and operate the ISMS
Development, maintenance and improvement cycle
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested parties
Managed information security

Figure 1 — 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.

0.3 Compatibility with other management systems

This standard is aligned with BS EN ISO 9001:2000 and BS EN ISO 14001:1996 in order to support consistent and integrated implementation and operation with related management standards.

Table C.1 illustrates the relationship between the clauses of this British Standard, BS EN ISO 9001:2000 and BS EN ISO 14001:1996.

This British Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

1 Scope

1.1 General

This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof (see Annex B which provides informative guidance on the use of this standard).

The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.

1.2 Application

The requirements set out in this British 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, the requirement 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, 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.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies.

BS EN ISO 9001:2000, *Quality management systems — Requirements.*

BS ISO/IEC 17799:2000, *Information technology — Code of practice for information security management.*

ISO Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards.*

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1
availability
ensuring that authorized users have access to information and associated assets when required
[BS ISO/IEC 17799:2000]

3.2
confidentiality
ensuring that information is accessible only to those authorized to have access
[BS ISO/IEC 17799:2000]

3.3
information security
security preservation of confidentiality, integrity and availability of information

3.4
information security management system
ISMS
that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.5
integrity
safeguarding the accuracy and completeness of information and processing methods
[BS ISO/IEC 17799:2000]

3.6
risk acceptance
decision to accept a risk
[ISO Guide 73]

3.7
risk analysis
systematic use of information to identify sources and to estimate the risk
[ISO Guide 73]

3.8
risk assessment
overall process of risk analysis and risk evaluation
[ISO Guide 73]

3.9
risk evaluation
process of comparing the estimated risk against given risk criteria to determine the significance of risk
[ISO Guide 73]

3.10
risk management
coordinated activities to direct and control an organization with regard to risk
[ISO Guide 73]

3.11
risk treatment
treatment process of selection and implementation of measures to modify risk
[ISO Guide 73]

3.12
statement of applicability
document describing the control objectives and controls that are relevant and applicable to the organization’s ISMS, based on the results and conclusions of the risk assessment and risk treatment processes

4 Information security management system

4.1 General requirements

The organization shall develop, implement, maintain and continually improve a documented ISMS within the context of the organization's overall business activities and risk. For the purposes of this standard the process used is based on the PDCA model shown in Figure 1.

4.2 Establishing and managing the ISMS

4.2.1 *Establish the ISMS*

The organization shall do the following.

a) *Define the scope of the ISMS* in terms of the characteristics of the business, the organization, its location, assets and technology.

b) *Define an ISMS policy* in terms of the characteristics of the business, the organization, its location, assets and technology that:

1) includes a framework for setting its objectives and establishes an overall sense of direction and principles for action with regard to information security;

2) takes into account business and legal or regulatory requirements, and contractual security obligations;

3) establishes the strategic organizational and risk management context in which the establishment and maintenance of the ISMS will take place;

4) establishes criteria against which risk will be evaluated and the structure of the risk assessment will be defined [see **4.2.1**c)];

5) has been approved by management.

c) *Define a systematic approach to risk assessment*

Identify a method of risk assessment that is suited to the ISMS, 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 and identify the acceptable levels of risk [see **5.1**f)].

d) *Identify the risks*

1) Identify the assets within the scope of the ISMS and the owners of these assets.

2) Identify the threats to those assets.

3) Identify the vulnerabilities that might be exploited by the threats.

4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

e) *Assess the risks*

1) Assess the business harm that might result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks.

4) Determine whether the risk is acceptable or requires treatment using the criteria established in **4.2.1**c).

f) *Identify and evaluate options for the treatment of risks*

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and the criteria for risk acceptance [see **4.2.1**c)];

3) avoiding risks;

4) transferring the associated business risks to other parties, e.g. insurers, suppliers.

g) *Select control objectives and controls for the treatment of risks*

Appropriate control objectives and controls shall be selected from Annex A of this standard and the selection shall be justified on the basis of the conclusions of the risk assessment and risk treatment process.

NOTE The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

h) *Prepare a Statement of Applicability*

The control objectives and controls selected in **4.2.1**g) and the reasons for their selection shall be documented in the Statement of Applicability. The exclusion of any control objectives and controls listed in Annex A shall also be recorded.

i) Obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS.

4.2.2 *Implement and operate the ISMS*

The organization shall do the following.

a) Formulate a risk treatment plan that identifies the appropriate management action, responsibilities and priorities for managing information security risks (see Clause **5**).

b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) Implement controls selected in **4.2.1**g) to meet the control objectives.

d) Implement training and awareness programmes (see **5.2.2**).

e) Manage operations.

f) Manage resources (see **5.2**).

g) Implement procedures and other controls capable of enabling prompt detection of and response to security incidents.

4.2.3 *Monitor and review the ISMS*

The organization shall do the following.

a) Execute monitoring procedures and other controls to:

1) detect errors in the results of processing promptly;

2) identify failed and successful security breaches and incidents promptly;

3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) determine the actions taken to resolve a breach of security reflecting business priorities.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting security policy and objectives, and review of security controls) taking into account results of security audits, incidents, suggestions and feedback from all interested parties.

c) Review the level of residual risk and acceptable risk, taking into account changes to:

1) the organization;

2) technology;

3) business objectives and processes;

4) identified threats;

5) external events, such as changes to the legal or regulatory environment and changes in social climate.

d) Conduct internal ISMS audits at planned intervals.

e) Undertake a management review of the ISMS on a regular basis (at least once a year) to ensure that the scope remains adequate and improvements in the ISMS process are identified (see Clause **6**).

f) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see **4.3.3**).

4.2.4 *Maintain and improve the ISMS*

The organization shall regularly do the following.

a) Implement the identified improvements in the ISMS.

b) Take appropriate corrective and preventive actions in accordance with **7.2** and **7.3**. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.

c) Communicate the results and actions and agree with all interested parties.

d) Ensure that the improvements achieve their intended objectives.

4.3 Documentation requirements

4.3.1 *General*

The ISMS documentation shall include the following.

a) Documented statements of the security policy [see **4.2.1**b)] and control objectives.

b) The scope of the ISMS [see **4.2.1**c)] and procedures and controls in support of the ISMS.

c) Risk assessment report [see **4.2.1**c) to **4.2.1**g)].

d) Risk treatment plan [see **4.2.2**b)].

e) Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes (see **6.1**).

f) Records required by this British Standard (see **4.3.3**).

g) Statement of Applicability.

All documentation shall be made available as required by the ISMS policy.

NOTE 1 Where the term "documented procedure" appears within this standard, this means that the procedure is established, documented, implemented and maintained.

NOTE 2 The extent of the ISMS documentation can differ from one organization to another owing to:

— the size of the organization and the type of its activities;

— the scope and complexity of the security requirements and the system being managed.

NOTE 3 Documents and records may be in any form or type of medium.

4.3.2 *Control of documents*

Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

a) approve documents for adequacy prior to issue;

b) review and update documents as necessary and re-approve documents;

c) ensure that changes and the current revision status of documents are identified;

d) ensure that the most recent versions of relevant 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 controlled;

h) prevent the unintended use of obsolete documents;

i) apply suitable identification to them if they are retained for any purpose.

4.3.3 ***Control of records***

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be controlled. The ISMS shall take account of any relevant legal requirements. Records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented. A management process shall determine the need for and extent 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.

EXAMPLE

Examples of records are a visitors' book, audit records and authorization of access.

5 Management responsibility

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing an information security policy;

b) ensuring that information security objectives and plans are established;

c) establishing roles and responsibilities for information security;

d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;

e) providing sufficient resources to develop, implement, operate and maintain the ISMS (see **5.2.1**);

f) deciding the acceptable level of risk;

g) conducting management reviews of the ISMS (see Clause **6**).

5.2 Resource management

5.2.1 ***Provision of resources***

The organization shall determine and provide the resources needed to:

a) establish, implement, operate and maintain an ISMS;

b) ensure that information security procedures support the business requirements;

c) identify and address legal and regulatory requirements and contractual security obligations;

d) maintain adequate security by correct application of all implemented controls;

e) carry out reviews when necessary, and to react appropriately to the results of these reviews;

f) where required, improve the effectiveness of the ISMS.

5.2.2 ***Training, awareness and competency***

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

a) determining the necessary competencies for personnel performing work effecting the ISMS;

b) providing competent training and, if necessary, employing competent personnel to satisfy these needs;

c) evaluating the effectiveness of the training provided and actions taken;

d) maintaining records of education, training, skills, experience and qualifications (see **4.3.3**).

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

6 Management review of the ISMS

6.1 General

Management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the security policy and security objectives. The results of the reviews shall be clearly documented and records shall be maintained (see **4.3.3**).

6.2 Review input

The input to a management review shall include information on:

a) results of ISMS audits and reviews;

b) feedback from interested parties;

c) techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;

d) status of preventive and corrective actions;

e) vulnerabilities or threats not adequately addressed in the previous risk assessment;

f) follow-up actions from previous management reviews;

g) any changes that could affect the ISMS;

h) recommendations for improvement.

6.3 Review output

The output from the management review shall include any decisions and actions related to the following.

a) Improvement of the effectiveness of the ISMS.

b) Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:

1) business requirements;

2) security requirements;

3) business processes effecting the existing business requirements;

4) regulatory or legal environment;

5) levels of risk and/or levels of risk acceptance.

c) Resource needs.

6.4 Internal ISMS audits

The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

a) conform to the requirements of this standard and relevant legislation or regulations;

b) conform to the identified information security requirements;

c) are effectively implemented and maintained;

d) perform as expected.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audits criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see **4.3.3**) shall be defined in a documented procedure.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Improvement activities shall include the verification of the actions taken and the reporting of verification results (see Clause **7**).

7 ISMS improvement

7.1 Continual improvement

The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

7.2 Corrective action

The organization shall take action to eliminate the cause of nonconformities associated with the implementation and operation of the ISMS in order to prevent recurrence. The documented procedures for corrective action shall define requirements for:

a) identifying nonconformities of the implementation and/or operation of the ISMS;

b) determining the causes of nonconformities;

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 (see **4.3.3**);

f) reviewing of corrective action taken.

7.3 Preventive action

The organization shall determine action to guard against future 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 implementing preventive action needed;

c) recording results of action taken (see **4.3.3**);

d) reviewing of preventive action taken;

e) identifying changed risks and ensuring that attention is focused on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment.

NOTE Action to prevent nonconformities is often more cost-effective than corrective action.

Annex A (normative) Control objectives and controls

A.1 Introduction

The control objectives and controls listed in **A.3** to **A.12** are directly derived from and aligned with those listed in BS ISO/IEC 17799:2000 Clauses **3** to **12**. The lists in these tables are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables shall be selected as part of the ISMS process specified in **4.2.1**.

A.2 Code of practice guidance

BS ISO/IEC 17799:2000 Clauses **3** to **12** provide implementation advice and guidance on best practice in support of the controls specified in **A.3** to **A.12**.

A.3 Security policy

			BS ISO/IEC 17799:2000 numbering
A.3.1 ***Information security policy*** *Control objective*: To provide management direction and support for information security.			**3.1**
Controls			
A.3.1.1	*Information security policy document*	A policy document shall be approved by management, published and communicated, as appropriate, to all employees.	**3.1.1**
A.3.1.2	*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 Organizational security

			BS ISO/IEC 17799:2000 numbering
A.4.1 ***Information security infrastructure*** *Control objective*: To manage information security within the organization.			**4.1**
Controls			
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. The management forum shall promote security through appropriate commitment and adequate resourcing.	**4.1.1**
A.4.1.2	*Information security coordination*	In large organizations, a cross-functional forum of management representatives from relevant parts of the organization shall be used to coordinate 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	*Authorization 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*	Specialist advice on information security shall be sought from either internal or external advisors and coordinated throughout the organization.	**4.1.5**
A.4.1.6	*Cooperation between organizations*	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.	**4.1.6**
A.4.1.7	*Independent review of information security*	The implementation of the information security policy shall be reviewed independently.	**4.1.7**

A.4 (*continued*)

			BS ISO/IEC 17799:2000 numbering
A.4.2 ***Security of third-party access*** *Control objective:* To maintain the security of organizational information processing facilities and information assets accessed by third parties.			**4.2**
Controls			
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**
A.4.3 ***Outsourcing*** *Control objective:* To maintain the security of information when the responsibility for information processing has been outsourced to another organization.			**4.3**
Controls			
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 desktop environments shall be addressed in a contract agreed between the parties.	**4.3.1**

A.5 Asset classification and control

			BS ISO/IEC 17799:2000 numbering
A.5.1 ***Accountability for assets*** *Control objective:* To maintain appropriate protection of organizational assets.			**5.1**
Controls			
A.5.1.1	*Inventory of assets*	An inventory of all important assets associated with each information system shall be drawn up and maintained.	**5.1.1**
A.5.2 ***Information classification*** *Control objective*: To ensure that information assets receive an appropriate level of protection.			**5.2**
Controls			
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*	A 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

			BS ISO/IEC 17799:2000 numbering
A.6.1 ***Security in job definition and resourcing*** *Control objective:* To reduce the risks of human error, theft, fraud or misuse of facilities.			**6.1**
Controls			
A.6.1.1	*Including security in job responsibilities*	Security roles and responsibilities, as laid down in the organization's information security policy shall be documented in job definitions.	**6.1.1**
A.6.1.2	*Personnel screening and policy*	Verification checks on permanent staff, contractors, and temporary 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**
A.6.2 ***User training*** *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.			**6.2**
Controls			
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.	**6.2.1**
A.6.3 ***Responding to security incidents and malfunctions*** *Control objective:* To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.			**6.3**
Controls			
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 put 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

			BS ISO/IEC 17799:2000 numbering
A.7.1 ***Secure areas*** *Control objective:* To prevent unauthorized physical access, damage and interference to business premises and information.			**7.1**
Controls			
A.7.1.1	*Physical security perimeter*	Organizations shall use security perimeters to protect areas that 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 secure areas.	**7.1.4**
A.7.1.5	*Isolated delivery and loading areas*	Delivery and loading areas shall be controlled, and where possible, isolated from information processing facilities to avoid unauthorized access.	**7.1.5**
A.7.2 ***Equipment security*** *Control objective:* To prevent loss, damage or compromise of assets and interruption to business activities.			**7.2**
Controls			
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 enable its continued availability and integrity.	**7.2.4**
A.7.2.5	*Security of equipment off-premises*	Any use of equipment for information processing outside an organization's premises shall require authorization by management.	**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**
A.7.3 ***General controls*** *Control objective:* To prevent compromise or theft of information and information processing facilities.			**7.3**
Controls			
A.7.3.1	*Clear desk and clear screen policy*	Organizations shall have a clear desk and a clear screen policy aimed at reducing 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 of the management.	**7.3.2**

A.8 Communications and operations management

			BS ISO/IEC 17799:2000 numbering
A.8.1 ***Operational procedures and responsibilities*** *Control objective:* To ensure the correct and secure operation of information processing facilities.			**8.1**
Controls			
A.8.1.1	*Documented operating procedures*	The operating procedures identified in the security policy shall be documented and maintained.	**8.1.1**
A.8.1.2	*Operational change controls*	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 and to collect incident related data such as audit trails and logs.	**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. Rules for the migration of software from development to operational status shall be defined and documented.	**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 a contract.	**8.1.6**
A.8.2 ***System planning and acceptance*** *Control objective:* To minimize the risk of systems failure.			**8.2**
Controls			
A.8.2.1	*Capacity planning*	Capacity demands shall be monitored and projections of future capacity requirements made to enable adequate processing power and storage to be made 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**
A.8.3 ***Protection against malicious software*** *Control objective:* To protect the integrity of software and information from damage by malicious software.			**8.3**
Controls			
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**
A.8.4 ***Housekeeping*** *Control objective:* To maintain the integrity and availability of information processing and communication services.			**8.4**
Controls			
A.8.4.1	*Information back-up*	Back-up copies of essential business information and software shall be taken and tested regularly.	**8.4.1**

A.8 (*continued*)

			BS ISO/IEC 17799:2000 numbering
A.8.4.2	*Operator logs*	Operational staff shall maintain a log of their activities. Operator logs shall be subject to regular, independent checks.	**8.4.2**
A.8.4.3	*Fault logging*	Faults shall be reported and corrective action taken.	**8.4.3**
A.8.5 ***Network management*** *Control objective:* To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.			**8.5**
Controls			
A.8.5.1	*Network controls*	A range of controls shall be implemented to achieve and maintain security in networks.	**8.5.1**
A.8.6 ***Media handling and security*** *Control objective:* To prevent damage to assets and interruptions to business activities.			**8.6**
Controls			
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**
A.8.7 ***Exchanges of information and software*** *Control objective:* To prevent loss, modification or misuse of information exchanged between organizations.			**8.7**
Controls			
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*	Policies, 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

			BS ISO/IEC 17799:2000 numbering
A.9.1 ***Business requirement for access control*** *Control objective:* To control access to information.			**9.1**
Controls			
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**
A.9.2 ***User access management*** *Control objective:* To ensure that access rights to information systems are appropriately authorized, allocated and maintained.			**9.2**
Controls			
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**
A.9.3 ***User responsibilities*** *Control objective:* To prevent unauthorized user access.			**9.3**
Controls			
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 is given appropriate protection.	**9.3.2**
A.9.4 ***Network access control*** *Control objective:* Protection of networked services.			**9.4**
Controls			
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 routeing control*	Shared networks shall have routeing 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 (*continued*)

			BS ISO/IEC 17799:2000 numbering
A.9.4.9	*Security of network services*	A clear description of the security attributes of all network services used by the organization shall be provided.	**9.4.9**
A.9.5 ***Operating system access control*** *Control objective:* To prevent unauthorized computer access.			**9.5**
Controls			
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 log-on 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. A suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	**9.5.3**
A.9.5.4	*Password management system*	Password management systems shall provide an effective, interactive facility which aims to ensure 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**
A.9.6 ***Application access control*** *Control objective:* To prevent unauthorized access to information held in information systems.			**9.6**
Controls			
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**
A.9.7 ***Monitoring system access and use*** *Control objective:* To detect unauthorized activities.			**9.7**
Controls			
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 the 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**

A.9 (*continued*)

			BS ISO/IEC 17799:2000 numbering
A.9.8 ***Mobile computing and teleworking*** *Control objective:* To ensure information security when using mobile computing and teleworking facilities.			**9.8**
Controls			
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

			BS ISO/IEC 17799:2000 numbering
A.10.1 ***Security requirements of systems*** *Control objective:* To ensure that security is built into information systems.			**10.1**
Controls			
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**
A.10.2 ***Security in application systems*** *Control objective:* To prevent loss, modification or misuse of user data in application systems.			**10.2**
Controls			
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 any 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**
A.10.3 ***Cryptographic controls*** *Control objective:* To protect the confidentiality, authenticity or integrity of information.			**10.3**
Controls			
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**

A.10 (*continued*)			**BS ISO/IEC 17799:2000 numbering**
A.10.4 ***Security of system files*** *Control objective:* To ensure that IT projects and support activities are conducted in a secure manner.			**10.4**
Controls			
A.10.4.1	*Control of operational software*	Procedures shall be in place to control 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**
A.10.5 ***Security in development and support processes*** *Control objective:* To maintain the security of application system software and information.			**10.5**
Controls			
A.10.5.1	*Change control procedures*	The implementation of changes shall be strictly controlled by the use of formal change control procedures.	**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

			BS ISO/IEC 17799:2000 numbering
A.11.1 ***Aspects of business continuity management*** *Control objective:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.			**11.1**
Controls			
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

			BS ISO/IEC 17799:2000 numbering
A.12.1 ***Compliance with legal requirements*** *Control objective:* To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.			**12.1**
Controls			
A.12.1.1	*Identification of applicable legislation*	All relevant statutory, regulatory and contractual requirements shall be defined explicitly 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 enable 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 organization 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**
A.12.2 ***Reviews of security policy and technical compliance*** *Control objective:* To ensure compliance of systems with organizational security policies and standards.			**12.2**
Controls			
A.12.2.1	*Compliance with security policy*	Managers shall take action to 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**
A.12.3 ***System audit considerations*** *Control objective:* To maximize the effectiveness of and to minimize interference to/from the system audit process.			**12.3**
Controls			
A.12.3.1	*System audit controls*	Audits of operational systems shall be planned carefully 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 (informative)
Guidance on use of the standard

B.1 Overview

B.1.1 *PDCA model*

Setting up and managing an 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, formalizing 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 used to reinforce, amend and improve the security solutions identified and implemented already. 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 computerized 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 or audits are needed to ensure that the whole management system is achieving its objectives.

B.1.4 *Summary of controls*

The organization may find it beneficial to make available a Summary of Controls (SoC) that is relevant and applicable to the organization's ISMS. This can facilitate business relationships such as electronic outsourcing by providing a summary of the controls in place. The SoC may contain sensitive information. Therefore care that it is appropriate to the recipient should be taken when making the SoC available both internally and externally.

NOTE The SoC is not a substitute for the SoA [see **4.2.1**h)]. The SoA is a mandatory requirement for certification.

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 *Information security policy*

4.2.1b) requires the organization and its management to define the information security policy that includes a framework for setting its objectives and targets, and establishes an overall sense of direction and principles for action with regard to information security. Guidance on the content of such a policy is given in BS ISO/IEC 17799:2000.

B.2.3 *Scope of the ISMS*

The ISMS may cover all or part of an organization. Dependencies, interfaces and assumptions concerning 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 to make subsequent risk management tasks simpler. The ISMS scope documentation should cover:

a) the processes used to establish the scope and context of the ISMS;

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, another Management System or another ISMS (of the same or a third-party organization). In such cases, only those controls the ISMS have management control over can be considered as being within the scope of the ISMS.

B.2.4 *Risk identification and assessment*

The risk assessment documentation should explain which risk assessment approach has been chosen, and why this approach is appropriate to the security requirements, the business environment, the size of the business and the risks the organization faces. 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, explain why they are suitable for the ISMS scope and risks, and how they should be used correctly 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, when it is not monetary;

b) identification of threats and vulnerabilities;

c) assessment of threats exploiting vulnerabilities, and of the impacts caused by such incidents;

d) calculation of the risks based on the results of the assessment, and identification of residual risks.

B.2.5 *Risk treatment plan*

Organizations 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.

An acceptable level of risk needs to be identified. For each of the risks at an unacceptable level, appropriate action should be chosen from the following:

a) decide to accept the risk, e.g. because other actions are not possible or too expensive;

b) transfer the risk; or

c) reduce the risk to an acceptable level.

The risk treatment plan is a coordination document defining the actions to reduce unacceptable levels of risk and implement the controls required to protect information.

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

The Statement of Applicability [see **4.2.1**h)] documents the control objectives and controls selected from Annex A. This document is one of the working documents required for ISMS certification. BS 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.

Controls designed to deter, detect, limit, prevent and recover from, security violations (in accordance with the ISMS) are very important in the implementation of the PDCA model and should be put in place early enough to be effective, along with those governing 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 designed to implement selected controls and promote the action necessary 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*

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

The aim of the awareness programme is to generate a well-founded risk management 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 organizational structures such as partnership and joint ventures. In such cases, it should be ensured that the organization(s) to which the risks are transferred understand the nature of those risks and are able to manage them 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. Where a business has decided to accept risks that are higher than the acceptance level, sign-off from management should be obtained.

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 Check activity is designed to ensure that the controls are working effectively and as intended, and that the ISMS remains effective. In addition, any change to the assumptions or scope of the risk assessment should be considered. If the controls 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 realize 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 Check activity 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, in order to anticipate future changes to the ISMS and 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.

The nature of the Check activity depends on the character of the PDCA cycle concerned, as in the following examples:

EXAMPLE 1

The automatic actions of intrusion detection technology. A network intrusion detector checks whether the security of other components has been penetrated.

EXAMPLE 2

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 given in **B.4.2** to **B.4.7**.

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. They might include: reconciliation of bank accounts, inventory counts, and resolving customer complaints. 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 unauthorized changes to parameters governing the actions of software, that there are no unintended and unauthorized changes to data displayed on websites;

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 so 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. for equipment failures or errors) and raises an alarm. The alarm alerts the responsible people to the problem, and they 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 organization's procedures are suboptimal is to identify where other organizations 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. Organizations should refer to these frequently and make the necessary updates to their software.

Information on management techniques is exchanged and discussed in many forums, including conferences, professional societies, and user groups and there are many articles in the technical and management press. Such exchanges enable organizations to learn how others tackle similar problems.

B.4.5 *Internal ISMS 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) an appropriate risk assessment methodology is being used;

c) the documented procedures are being followed (i.e. within the scope of the ISMS), and are meeting their desired objectives;

d) technical controls (e.g. firewalls, physical access controls) are in place, are correctly configured and working as intended;

e) the residual risks have been assessed correctly and are still acceptable to the management of the organization;

f) the agreed actions from previous audits and reviews have been implemented;

g) the ISMS is compliant with this standard.

The audits will need samples of current documents and records and involve interviews with 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. 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 in order to anticipate future changes to the ISMS and ensure its continued effectiveness.

B.4.7 *Trend analysis*

Trend analysis undertaken on a regular basis will help organizations identify those areas in which a need for improvement is indicated and should form an essential part of the continuous improvement cycle.

B.5 Act phase

B.5.1 *Introduction*

In order for the ISMS to remain effective it should be regularly improved on the basis of information collected during the Check phase.

The purpose of the Act activity is to take action as a result of the Check activity. The action will be to address a nonconformity or take other corrective action as explained in **B.5.2** and **B.5.3**. The action might also be to advance immediately to a Plan or Do activity. An example of the former would be when a new threat has been identified, the Plan activity being to update the risk assessment. An example of the latter would be to put an existing business continuity plan into action, the Check activity having identified the need to do that. Note that if changes are made to the ISMS as a result of the Act or subsequent Plan activities, then it is vital that all interested parties are advised promptly about the changes and that additional training should be given as required.

B.5.2 *Nonconformity*

A nonconformity (from the application guidance to the clauses of ISO/IEC Guide 62) is:

a) the absence of, or the failure to implement and maintain one or more ISMS requirements; or

b) a situation which would, on the basis of available objective evidence, raise significant doubt as to the capability of the ISMS to fulfil the information security policy and security objectives of the organization.

It is important that where reviews during the Check phase highlight areas of nonconformity, 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 minimize and prevent recurrence. Corrective action should be consistent with the severity of the nonconformity and the risk to the ability of the ISMS to meet specified requirements.

B.5.3 ***Corrective and preventive actions***

Corrective (or reactive) action should be taken to eliminate the cause of a nonconformity or other undesirable situation to prevent recurrence. Preventive (or proactive) action should be taken to eliminate the cause of a potential noncompliance or other undesirable potential situation.

It is never possible to entirely eliminate isolated nonconformities. On the other hand, what may appear to be an isolated event may in fact be symptomatic of a weakness that may have an impact across the entire organization if not addressed. Isolated events should be considered from this point of view when identifying and implementing any 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 recurring.

B.5.4 ***OECD principles and BS 7799-2:2002***

The principles given in the OECD Guidelines for the Security of Information Systems and Networks [1] apply to all policy and operational levels that govern the security of information systems and networks. This British Standard provides an information security management system framework for implementing some of the OECD principles using the PDCA model and the processes described in Clauses **4**, **5**, **6** and **7**, as indicated in Table B.1.

Table B.1 — OECD principles and the PDCA model

OECD principle	Corresponding ISMS process and PDCA phase
Awareness Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.	This activity is part of the **Do** phase (see **4.2.2** and **5.2.2**).
Responsibility All participants are responsible for the security of information systems and networks.	This activity is part of the **Do** phase (see **4.2.2** and **5.1**).
Response Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.	This is in part a monitoring activity **Check** phase (see **4.2.3** and **6.1** to **6.4**) and a responding activity **Act** phase (see **4.2.4** and **7.1** to **7.3**). This can also be covered by some aspects of the **Plan** and **Check** phases.
Risk assessment Participants should conduct risk assessments.	This activity is part of the **Plan** phase (see **4.2.1**) and risk reassessment is part of the **Check** phase (see **4.2.3** and **6.1** to **6.4**).
Security design and implementation Participants should incorporate security as an essential element of information systems and networks.	Once a risk assessment has been completed, controls are selected for the treatment of risks as part of the **Plan** phase (see **4.2.1**). The **Do** phase (see **4.2.2** and **5.2**) then covers the implementation and operational use of these controls.
Security management Participants should adopt a comprehensive approach to security management.	The management of risk is a process which includes the prevention, detection and response to incidents, ongoing maintenance, review and audit. All of these aspects are encompassed in the **Plan**, **Do**, **Check** and **Act** phases.
Reassessment Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.	Reassessment of information security is a part of the **Check** phase (see **4.2.3** and **6.1** to **6.4**) where regular reviews should be undertaken to check the effectiveness of the information security management system, and improving the security is part of the **Act** phase (see **4.2.4** and **7.1** to **7.3**).

Annex C (informative) Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002

Table C.1 shows the correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002.

Table C.1 — Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002

BS 7799-2:2002	BS EN ISO 9001:2000	BS EN ISO 14001:1996
0 Introduction	**0 Introduction**	**Introduction**
0.1 General	0.1 General	
0.2 Process approach	0.2 Process approach	
	0.3 Relationship with ISO 9004	
0.3 Compatibility with other management systems	0.4 Compatibility with other management systems	
1 Scope	**1 Scope**	**1 Scope**
1.1 General	1.1 General	
1.2 Application	1.2 Application	
2 Normative references	**2 Normative reference**	**2 Normative reference**
3 Terms and definitions	**3 Terms and definitions**	**3 Terms and definitions**
4 ISMS requirements	**4 QMS requirements**	**4 EMS requirements**
4.1 General requirements	4.1 General requirements	4.1 General requirements
4.2 Establishing and managing the ISMS		
4.2.1 Establish the ISMS		
4.2.2 Implement and operate the ISMS		4.4 Implementation and operation
4.2.3 Monitor and review the ISMS		4.5.1 Monitoring and measurement
4.2.4 Maintain and improve the ISMS		4.5.2 Non-conformance and corrective and preventive action
4.3 Documentation requirements	4.2 Documentation requirements	
4.3.1 General	4.2.1 General	
	4.2.2 Quality manual	
4.3.2 Control of documents	4.2.3 Control of documents	4.4.5 Documentation control
4.3.3 Control of records	4.2.4 Control of records	4.5.3 Records
5 Management responsibility	**5 Management responsibility**	
5.1 Management commitment	5.1 Management commitment	
	5.2 Customer focus	
	5.3 Quality policy	4.2 Environmental policy
	5.4 Planning	4.3 Planning
	5.5 Responsibility, authority and communication	

Table C.1 — Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002 (*concluded*)

BS 7799-2:2002	BS EN ISO 9001:2000	BS EN ISO 14001:1996
5.2 Resource management	**6 Resource management**	
5.2.1 Provision of resources	6.1 Provision of resources	
	6.2 Human resources	
5.2.2 Training, awareness and competency	6.2.2 Competence, awareness and training	4.2.2 Training, awareness and competence
	6.3 Infrastructure	
	6.4 Work environment	
6 Management review of the ISMS	**5.6 Management review**	**4.6 Management review**
6.1 General	5.6.1 General	
6.2 Review input	5.6.2 Review input	
6.3 Review output	5.6.3 Review output	
6.4 Internal ISMS audits	8.2.2 Internal audits	4.5.4 EMS audit
7 ISMS improvement	**8 Improvement**	
7.1 Continual improvement	8.5.1 Continual improvement	
7.2 Corrective action	8.5.2 Corrective actions	4.5.2 Non-conformance and corrective and preventive action
7.3 Preventive action	5.5.3 Preventive actions	
Annex A Control objectives and controls		
Annex B Guidance on use of the standard		**Annex A Guidance on use of the specification**
Annex C Correspondence between different management system standards	**Annex A Links between ISO 14001 and ISO 9001**	**Annex B Links between ISO 14001 and ISO 9001**

Annex D (informative) Changes to internal numbering

Table D.1 shows the relationship between the clause numbering in BS 7799-2:1999 and the clause numbering in this British Standard, BS 7799-2:2002.

Table D.1 — Relationship between internal numbering in different editions of BS 7799-2

Clause number in BS 7799-2:1999	Clause number in BS 7799-2:2002
—	0 Introduction
1 Scope	1 Scope
—	2 Normative references
2 Terms and definitions	3 Terms and definitions
—	3.1 Information security management system
2.1 Statement of applicability	3.12 Statement of applicability
3 Information security management system requirements	4 Information security management system
3.1 General	4.1 General requirements
3.2 Establishing a management framework	4.2 Establishing and managing the ISMS
	4.2.1 Establish the ISMS
3.3 Implementation	4.2.2 Implement and operate the ISMS
—	4.2.3 Monitor and review the ISMS
—	4.2.4 Maintain and improve the ISMS
3.4 Documentation	4.3 Documentation requirements
—	4.3.1 General
3.5 Document control	4.3.2 Control of documents
3.6 Records	4.3.3 Control of records
—	5 Management responsibility
—	5.1 Management commitment
—	5.2 Resource management
—	6 Management review of the ISMS
—	6.1 General
—	6.2 Review input
—	6.3 Review output
—	6.4 Internal ISMS audits
—	7 ISMS improvement
—	7.1 Continual improvement
—	7.2 Corrective action
—	7.3 Preventive action
4 Detailed controls	Annex A Control objectives and controls
—	A.1 Introduction
—	A.2 Code of practice guidance
4.1 Security policy	A.3 Security policy
4.2 Organizational security	A.4 Organizational security
4.3 Asset classification and control	A.5 Asset classification and control
4.4 Personnel security	A.6 Personnel security
4.5 Physical and environmental security	A.7 Physical and environmental security

Table D.1 — Relationship between internal numbering in different editions of BS 7799-2 (*concluded*)

Clause number in BS 7799-2:1999	Clause number in BS 7799-2:2002
4.6 Communications and operations management	A.8 Communications and operations management
4.7 Access control	A.9 Access control
4.8 System development and maintenance	A.10 System development and maintenance
4.9 Business continuity management	A.11 Business continuity management
4.10 Compliance	A.12 Compliance
—	Annex B Guidance on the use of the standard
—	Annex C Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002

blank

Bibliography

Standards publications

BS 7799-2:1999, *Information security management — Part 2: Specification for information security management systems.*

BS EN ISO 14001:1996, *Environmental management systems — Specification with guidance for use.*

BS ISO/IEC TR 13335-3:1998, *Guidelines for the Management of IT Security — Part 3: Techniques for the management of IT security.*

BS ISO/IEC TR 13335-4:2000, *Guidelines for the Management of IT Security — Part 4: Selection of safeguards.*

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

Other publications

[1] OECD. *OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.org

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001.
Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.
Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.
Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001.
Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

Details and advice can be obtained from the Copyright & Licensing Manager.
Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553.
Email: copyright@bsi-global.com.

BSI
389 Chiswick High Road
London
W4 4AL