

Information security management

Part 1. Code of practice for information security management systems

ICS 35.020; 35.110

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee BSFD/12, Information Security Management, upon which the following bodies were represented:

- The BOC Group plc
- British Computer Society
- British Telecommunications plc
- CCTA
- Department of Trade and Industry
- Marks & Spencer plc
- Midland Bank plc
- Nationwide Building Society
- Prudential Assurance Corporation
- SEMA Group Consulting
- Shell International Petroleum Co Ltd.
- Shell UK Ltd.
- Unilever plc

This British Standard, having been prepared under the direction of the DISC Board (BRD/-), was published under the authority of the Standards Board and comes into effect on 15 February 1995

© BSI 1998

The following BSI references relate to the work on this standard:
Committee reference BSFD/12
Draft for comment 94/600027 DC

ISBN 0 580 23642 0

Amendments issued since publication

Amd. No.	Date	Text affected
9911	February 1998	Renumbered as Part 1 and title changed

Summary of pages

The following table identifies the current issue of each page. Issue 1 indicates that a page has been introduced for the first time by amendment. Subsequent issue numbers indicate an updated page. Vertical sidelining on replacement pages indicates the most recent changes (amendment, addition, deletion).

Page	Issue	Page	Issue
Front cover	2	iii	original
Inside front cover	2	iv	blank
a	1	1 to 50	original
b	blank	Inside back cover	original
i	original	Back cover	2
ii	original		

Change of identifier

Wherever BS 7799 : 1995 appears in this standard, it should be read as BS 7799 : Part 1 : 1995.

Contents

	Page
Committees responsible	Inside front cover
Foreword	iii
Code of practice	
Introduction	1
Section 0. General	
0.1 Scope	4
0.2 Informative references	4
0.3 Definitions	4
Section 1. Security policy	
1.1 Information security policy	5
Section 2. Security organization	
2.1 Information security infrastructure	6
2.2 Security of third party access	8
Section 3. Assets classification and control	
3.1 Accountability for assets	9
3.2 Information classification	9
Section 4. Personnel security	
4.1 Security in job definition and resourcing	11
4.2 User training	11
4.3 Responding to incidents	11
Section 5. Physical and environmental security	
5.1 Secure areas	13
5.2 Equipment security	15
Section 6. Computer and network management	
6.1 Operational procedures and responsibilities	17
6.2 System planning and acceptance	18
6.3 Protection from malicious software	20
6.4 Housekeeping	20
6.5 Network management	21
6.6 Media handling and security	21
6.7 Data and software exchange	23
Section 7. System access control	
7.1 Business requirement for system access	25
7.2 User access management	25
7.3 User responsibilities	26
7.4 Network access control	27
7.5 Computer access control	29
7.6 Application access control	31
7.7 Monitoring system access and use	32
Section 8. Systems development and maintenance	
8.1 Security requirements of systems	34
8.2 Security in application systems	35
8.3 Security of application system files	36
8.4 Security in development and support environments	36

	Page
Section 9. Business continuity planning	
9.1 Aspects of business continuity planning	38
Section 10. Compliance	
10.1 Compliance with legal requirements	40
10.2 Security reviews of IT systems	42
10.3 System audit considerations	42
Annex	
A (normative) Summary of controls used in BS 7799	43
Index	49
List of references	Inside back cover

Foreword

This British Standard has been prepared by BSFD/12, Information Security Management. It is intended for use as a reference document by managers and employees who are responsible for initiating, implementing and maintaining information security within their organization. It may therefore be considered as a basis for organizational security standards.

This British Standard is based on PD 0003, *A code of practice for information security management*, developed by the Department of Trade and Industry with the assistance of leading UK companies and organizations. It provides a comprehensive set of security controls comprising the best information security practices in current use, both in the UK and internationally.

The guidance in this code of practice is intended to be as comprehensive as possible. It is intended to serve as a single reference point for identifying the range of controls (summarized in annex A) needed for most situations encountered in industry and commerce and may therefore be applied by a wide range of organizations, large, medium and small. With increasing electronic networking between organizations there is a clear benefit in having a common reference document for information security management. It enables mutual trust to be established between networked sites and trading partners and provides a basis for management of facilities between IT users and service providers.

Not all of 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. Consequently, this code of practice may require to be augmented by further guidance before it can be used as a basis (for example) for corporate policy or an intercompany trading agreement.

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.

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

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

Introduction

What is information security?

The purpose of information security (see **0.3.6**) is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. Information security management (see **0.3.7**) enables information to be shared, while ensuring the protection of information and computing assets. It has three basic components:

- a) confidentiality (see **0.3.2**): protecting sensitive information from unauthorized disclosure or intelligible interception;
- b) integrity (see **0.3.9**): safeguarding the accuracy and completeness of information and computer software;
- c) availability (see **0.3.1**): ensuring that information and vital services are available to users (see **0.3.14**) when required.

Information (see **0.3.5**) takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations. From a security perspective, appropriate protection should be applied to all forms of information, including papers, databases, films, view foils, models, tapes, diskettes, conversations and any other methods used to convey knowledge and ideas.

Why action is needed

Your information and the IT systems and networks that support it are important business assets. Their availability, integrity and confidentiality may be essential to maintain your competitive edge, cash-flow, profitability, legal compliance and respected organization image. Your organizations may now be facing increasing security threats from a wide range of sources. Your IT systems and networks may be the target of a range of serious threats, including computer-based fraud, espionage, sabotage, vandalism and other sources of failure or disaster. New sources of damage, such as the highly publicized threats of computer viruses and computer hackers, continue to emerge. Such threats to information security are expected to become more widespread, more ambitious and increasingly sophisticated. At the same time, because of increasing dependence on IT systems and services, your organization may be becoming more vulnerable to security threats. The growth of networking presents new opportunities for unauthorized access to computer systems and the trend to distributed computing reduces the scope for central, specialist control of IT facilities. Security measures are considerably cheaper and more effective if incorporated into IT systems and services at the requirements specification and design stages. The sooner you take action to safeguard your information systems, the cheaper and more effective it will be for your organization in the long run.

How the code is set out

This code of practice is divided into 10 sections as follows.

- Section 1: Security policy.
- Section 2: Security organization.
- Section 3: Assets classification and control.
- Section 4: Personnel security.
- Section 5: Physical and environmental security.
- Section 6: Computer and network management.
- Section 7: System access control.
- Section 8: System development and maintenance.
- Section 9: Business continuity planning.
- Section 10: Compliance.

These sections provide a comprehensive set of security controls, based on the actual information security measures currently being implemented by UK and international organizations. These controls and the recommendations on which they are based are summarized in annex A.

Are all the controls applicable?

Some controls are not applicable to every IT environment and should be used selectively, according to local circumstances. The descriptions of these controls make this clear. However, most of the controls documented are widely accepted by large, experienced organizations as recommended good practices for all situations, subject of course to limiting factors such as environmental or technological constraints. These generally accepted controls are often referred to as baseline security controls, because they collectively define an industry baseline of good security practice.

Ten of the controls in this code of practice (designated key controls) are considered to be especially important. These key controls provide a good starting point for information security management. They are explained in more detail below under the heading 'Key controls'.

A few controls, e.g. data encryption, may require specialist security advice and an assessment of risks to establish if they are required, and to determine how they should be implemented. In some cases, further (stronger) controls, outside the scope of this code of practice, may be required to provide enhanced protection for especially valuable assets or to counter exceptionally high levels of security threat.

Key controls

Ten controls are either essential requirements, e.g. legislative requirements, or are considered to be fundamental building blocks for information security, e.g. security education. These controls, designated 'key controls', apply to all organizations and environments and are marked with the key symbol. These key controls are intended as a basis for use by organizations setting out to implement information security controls. The key controls are as follows:



- information security policy document (see 1.1.1);
- allocation of information security responsibilities (see 2.1.3)
- information security education and training (see 4.2.1);
- reporting of security incidents (see 4.3.1);
- virus controls (see 6.3.1);
- business continuity planning process (see 9.1.1);
- control of proprietary software copying (see 10.1.1);
- safeguarding of organizational records (see 10.1.2);
- data protection (see 10.1.3);
- compliance with security policy (see 10.2.1).



How to establish your security requirements

There are three main sources of security requirement in any organization.

The first source of security requirements is the unique set of security risks, comprising both threats and vulnerabilities, to assets and the potential impact of these security risks on business. Most of these risks are addressed and can be effectively countered by using the guidance in this code of practice. However, there will be some risks that require special treatment, and these will need to be addressed by risk assessment of each individual organization or component system.

The second source of requirements is the set of statutory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, with an increasing need for standardization as interorganizational networking proliferates. This code of practice is intended to serve as a consistent reference point for generic requirements of this type.

The third source of requirements is the unique set of principles, objectives and requirements for information processing that an organization has developed to support its business operations. It is important, e.g. for competitive edge, that the security policy supports these requirements, and vital that the implementation, or absence, of security controls in the IT infrastructure do not impede efficient business operations.

Incorporation of the right controls and the required degree of flexibility from the start of the IT planning process is critical to the successful outcome of the work.

Assessing your security risks

Expenditure on IT security controls needs to be balanced against, and appropriate to, the business value of the information and other IT assets at risk, and the business harm likely to result from security failures. A periodic review of business risks and IT security controls, to address changing business requirements and priorities, is therefore a regular feature of information security management.

Generally, risk analysis techniques (see 0.3.12) are applied to complete information systems and facilities, but they can also be directed to individual system components or services where this is practicable, realistic and helpful. Assessment of risks involves systematic consideration of the following items:

- a) the business harm likely to result from a significant breach of IT security, taking account of the potential consequences of failures of information confidentiality, integrity and availability;
- b) the realistic likelihood of such a breach occurring in the light of prevailing threats and controls.

The results of this assessment will help to guide and determine the appropriate management action and priorities for managing information security risks and for implementing the controls recommended in this code of practice. Assessment of these two aspects of risk depends upon the following factors:

- 1) the nature of the business information and systems;
- 2) the business purpose for which the information is used;
- 3) the environment in which the system is used and operated;
- 4) the protection provided by the controls in place.

The risk assessment might identify exceptional business security risks requiring stronger controls that are additional to the recommendations given in this standard. These controls will need to be justified on the basis of the conclusions of the 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 objectives and activities being based on business objectives and requirements, and led by business management;
- b) visible support and commitment from top management;
- c) a good understanding of the security risks, both threats and vulnerabilities, to organization assets and of the level of security inside the organization, which should be based on the value and importance of the assets;
- d) effective marketing of security to all managers and employees;
- e) distribution of comprehensive guidance on information security policy and standards to all employees and contractors.

Developing your own guidelines

There is no single best structure for security guidance. Each category of user (see **0.3.14**) or IT specialist in a particular environment will have a different set of requirements, problems and priorities depending on the particular function, organization and business or computing environment.

Many organizations have addressed this problem by developing a portfolio of individual interpretation guides for particular groups of employees, to ensure more effective dissemination of security guidance. Organizations that decide to adopt a different structure (or perhaps develop a local interpretation guide) are advised to retain cross-references to the text of this code of practice to enable future business partners or auditors to establish a direct link between it and organizational security guidelines.

Section 0. General

0.1 Scope

This British Standard gives recommendations for information security management. It is intended to provide a common basis for organizations to develop, implement and measure effective security management practice and to provide confidence in interorganizational dealings.

NOTE. It can be used as a common reference standard for interorganizational dealings and for subcontracting or procurement of information technology (IT) services or products.

0.2 Informative references

This British Standard refers to other publications that provide information or guidance. Editions of these publications current at the time of issue of this standard are listed on the inside back cover, but reference should be made to the latest editions.

0.3 Definitions

For the purposes of this British Standard the following definitions apply.

0.3.1 availability

Element of information security (see **0.3.6**).

0.3.2 confidentiality

Element of information security (see **0.3.6**).

0.3.3 data

The representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or by automatic means.

0.3.4 duress alarm

Mechanism by which a user (see **0.3.15**) can indicate to the host system that a logon is being attempted under duress.

NOTE. An alternative password, or the substitution or inclusion of special characters in a password, could be used to trigger the alarm.

0.3.5 information

The meaning that is currently assigned to data by means of the conventions applied to those data.

0.3.6 information security

Protection of information for:

- a) confidentiality: protecting sensitive information from unauthorized disclosure or intelligible interception;
- b) integrity: safeguarding the accuracy and completeness of information and computer software;
- c) availability: ensuring that information and vital services are available to users when required.

0.3.7 information security management

Provision of a mechanism to enable the implementation of information security (see **0.3.6**).

0.3.8 information technology

The scientific, technological and engineering discipline and the management of techniques used in data handling and processing; their applications; computers and their interactions with people and machines; and associated social, economic and cultural matters.

0.3.9 integrity

Element of information security (see **0.3.6**).

0.3.10 organization

Group of people collectively responsible for a defined set of activities.

NOTE. For example, a company, a local authority, an academic institution.

0.3.11 owner

Individual or organization having responsibility for specified information asset(s) and for the maintenance of appropriate security measures.

0.3.12 risk analysis

Comprehensive concept for defining and analysing threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimize investment in security countermeasures.

0.3.13 security incident

Any event that has, or could have, resulted in loss or damage to organizational assets, or an action that is in breach of organizational security procedures.

0.3.14 special privilege

Any feature or facility of a multi-user IT system that enables a user (see **0.3.15**) to override system or application controls.

0.3.15 user

Individual or organization that makes use of information technology (see **0.3.8**).

NOTE. See also BS ISO 2382-1.

Section 1. Security policy

1.1 Information security policy

Objective

To provide management direction and support for information security.

Top management should set a clear direction and demonstrate their support for and commitment to information security through the issue of an information security policy across the organization.

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

c) an explanation of specific security policies, principles, standards and compliance requirements, including:

- 1) compliance with legislative and contractual requirements;
- 2) security education requirements;
- 3) virus prevention and detection policy;
- 4) business continuity planning policy.

d) a definition of general and specific responsibilities for all aspects of information security;

e) an explanation of the process for reporting suspected security incidents.

There should be a defined review process, including responsibilities and review dates, for maintaining the policy document.

1.1.1 Information security policy document



A written policy document should be available to all employees responsible for information security.

The top management team should issue a written statement of information security policy to all parts of the organization. It should contain, as a minimum, the following guidance:

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

Section 2. Security organization

2.1 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 forums should be established to approve information security policy, to assign security roles, and to coordinate 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, standards and assessments, and to establish suitable liaison points for dealing with security incidents. Multidisciplined approaches to information security should be encouraged, e.g. auditors, users and administrators working together to address the problem effectively.

2.1.1 Management information security forum

Information security is a business responsibility shared by all members of the management team. The need for a high level management forum to ensure there is clear direction and visible management support for security initiatives should therefore be considered. If there are insufficient agenda items to justify regular meetings devoted exclusively to information security, the subject should be addressed by a suitable existing forum.

Typically, such a forum undertakes the following:

- a) review and approval of information security policy and overall responsibilities;
- b) monitoring of exposure to major threats to information assets;
- c) review and monitoring of security incidents;
- d) approval of major initiatives to enhance information security.

It is recommended that one member of the management team take lead responsibility for coordinating information security policy.

2.1.2 Information security coordination

In a large organization it might be necessary to coordinate information security measures through a cross-functional forum.

A cross-functional forum, made up of management representatives from each part of the organization, is often necessary to coordinate the implementation of information security measures. 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) coordinates the implementation of specific information security measures for new systems or services;
- f) promotes the visibility of business support for information security throughout the organization.

2.1.3 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 1.1.1) should provide general guidance on the allocation of security roles and responsibilities within the organization. This should be supplemented, where necessary, with a more detailed local interpretation for specific sites, systems or services which should clearly define local responsibilities for individual assets (both physical and information) and security processes, e.g. business continuity planning.

The security of an information system should be the responsibility of the owner of that system (see 3.1). Owners of information systems may delegate their security authority (power to act) to individual user managers or service providers. Nevertheless they remain ultimately accountable for protecting the security of the system.

To avoid any misunderstanding about individual responsibilities, it is essential that the areas for which each manager is responsible are clearly stated, in particular the following.

- 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 responsibility documented.
- c) Authorization levels should be clearly defined and documented.

2.1.4 Authorization process for IT facilities

A management approval process for new IT facilities should be established to ensure that the installation of equipment is for a defined business purpose, will provide an adequate level of security protection, and will not adversely affect the security of the existing infrastructure.

Two levels of authorization should be considered, as follows.

- a) *Business approval.* Each installation should have appropriate user management approval, authorizing its purpose and use. Approval should also be obtained from the manager responsible for maintaining the local IT security environment, to ensure that it conforms to all relevant security policies and requirements.
- b) *Technical approval.* Where necessary, it should be checked that all devices connected to communication networks or maintained by a particular service provider are of an approved device type.

NOTE. This control is especially important in a networked environment.

2.1.5 Specialist information security advice

Every organization, large or small, can benefit from specialist security advice. Ideally, this should be provided by an experienced in-house information security adviser. Small organizations are unlikely to be able to justify employing a specialist adviser. In this case, it is recommended that a single focal point is established to ensure consistency in security decision making, and to help develop maximum in-house knowledge and experience.

Information security advisers or focal points should be equipped to provide advice on all aspects of information security. The quality of their

assessment of security threats and advice on countermeasures will determine the effectiveness of the organization's information security programme. For maximum effectiveness and impact, they should be allowed direct access to IT and business managers throughout the organization.

The information security adviser or focal point 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 business line management control, the information security adviser may be called on to advise, lead or conduct the investigation.

2.1.6 Cooperation between organizations

Internal information security advisers should be encouraged to liaise with external security specialists (in industry or government) at their discretion. Such cooperation provides an opportunity to share experience and assessments of security threats and promote the development of consistent security practices across industry, helping to remove obstacles to interorganizational dealings.

It is also important to maintain appropriate contacts with law enforcement authorities, IT service providers and telecommunications authorities, to ensure that appropriate contacts can be quickly established, and advice obtained, in the event of a security incident.

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

2.1.7 Independent review of information security

The information security policy document (see 1.1.1) sets out responsibilities and policy for information security. The actual practice of information security should be reviewed independently to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.

NOTE. Possible candidates to undertake such a review are the internal audit function, an independent senior manager, or a third party organization specializing in compliance certification, where these candidates have the appropriate skills and experience.

2.2 Security of third party access

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

Access to company IT facilities by (non-organizational) third parties should be controlled.

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

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

It is recommended that this code of practice is used as a basis for such contracts.

2.2.1 Identification of risks from third party connections

The security of organizational IT systems might be put at risk by access from third party (non-organizational) locations with inadequate security management. Where there is a business need to connect to a third party location, a risk analysis should be carried out to identify any requirements for specific security measures. The risk analysis should take into account the type of access required, the value of the information, the security measures employed by the third party and the implications of the access for the security of the organizational IT infrastructure. This process should be facilitated by reference to published industry standards, such as this code of practice. Access to organizational facilities by third parties should not be provided until the appropriate measures have been implemented and a contract has been signed defining the terms for the connection.

2.2.2 Security conditions in third party contracts

Arrangements involving third party access to organizational IT facilities should be based on a formal contract containing, or referring to, all of the necessary security conditions to ensure compliance with the organization's security policies and standards. The contract should be in place before access to the IT facilities is provided. The following items should be considered for inclusion in the contract:

- a) the general policy on information security;
 - b) permitted access methods, and the control and use of unique identifiers (user IDs) and passwords;
 - c) a description of each IT service to be made available;
 - d) a requirement to maintain a list of individuals authorized to use the service;
 - e) times and dates when the service is to be available;
- NOTE. Contingency arrangements should be considered where appropriate.
- f) the respective liabilities of the parties to the agreement;
 - g) procedures regarding protection of organizational assets, including information;
 - h) responsibilities with respect to legal matters, e.g. data protection legislation;
 - i) the right to monitor, and revoke, user activity;
 - j) responsibilities regarding hardware and software installation and maintenance;
 - k) the right to audit contractual responsibilities;
 - l) restrictions on copying and disclosing information;
 - m) measures to ensure the return or destruction of information and assets at the end of the contract;
 - n) any required physical protection measures;
 - o) mechanisms to ensure that security measures are followed;
 - p) user training in methods, procedures and security;
 - q) measures to ensure protection against the spread of computer viruses (see 6.3.1);
 - r) an authorization process for user access;
 - s) arrangements for reporting and investigating security incidents;
 - t) involvement by the third party of subcontractors and other participants.

Section 3. Assets classification and control

3.1 Accountability for assets

Objective: To maintain appropriate protection of organizational assets.

All major information assets should be accounted for and have a nominated owner (see 0.3.11).

Accountability for assets helps ensure that adequate security protection is maintained. Owners should be identified for major assets and assigned responsibility for the maintenance of appropriate security measures. Responsibility for implementing security measures may be delegated, though accountability should remain with the nominated owner of the asset.

3.1.1 Inventory of assets

Inventories of assets help to ensure that effective security protection is maintained, and may be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. An inventory should be drawn up of the major assets associated with each information system. Each asset should be clearly identified and its ownership and security classification (see 3.2) agreed and documented. Examples of assets associated with information systems include the following:

- a) *information assets*: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;
- b) *software assets*: application software, system software, development tools and utilities;
- c) *physical assets*: computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;
- d) *services*: computing and communications services, other technical services (heating, lighting, power, air-conditioning).

3.2 Information classification

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

Security classifications should be used to indicate the need and priorities for security protection.

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

3.2.1 Classification guidelines

Security classifications and associated protective measures for business information should take account of business needs for sharing or restricting information, and the business impacts associated with unauthorized access or damage to the information. In particular, consideration should be given to the following business needs:

- a) *confidentiality*: the business need to share or restrict access to information with regard to confidentiality and the controls required to restrict access to the information;
- b) *integrity*: the business need to control modifications to information and the controls required to protect the accuracy and completeness of the information;
- c) *availability*: the business need to have information available when required by the business and the controls required to achieve this.

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

NOTE. There is not yet an accepted standard for classification labels (see 3.2.2) between organizations.

Care should be taken in interpreting classification labels on documents from other organizations that may have different definitions for the same, or a similar sounding, label.

3.2.2 Classification labelling

Classified information and outputs from systems handling organizationally classified data should be labelled appropriately. Often, however, information ceases to be sensitive after a certain period of time, for example, when the information has been made public. This should be taken into account, as over- classification can lead to unnecessary, additional business expense.

Output from IT systems containing classified information should carry an appropriate classification label (in the output). The marking should reflect the classification of the most sensitive data in the output. Items for consideration include printed reports, screen displays, magnetic media (tapes, disks, cassettes), electronic messages and file transfers.

NOTE. Physical labels are generally the most appropriate form of labelling. However, in some cases, e.g. electronic transmissions, other means such as procedures, contracts or postal notifications may be necessary to accomplish the labelling function.