

BS EN ISO/IEC 27002:2017

Incorporating corrigenda September 2014 and November 2015



BSI Standards Publication

**Information technology —
Security techniques —
Code of practice for
information security controls
(ISO/IEC 27002:2013)**

bsi.

AVA Documents
Document Sharing Hub

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27002:2017. It is identical to ISO/IEC 27002:2013, incorporating corrigenda September 2014 and November 2015. It supersedes BS ISO/IEC 27002:2013 which is withdrawn.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum September 2014 is indicated in the text by AC1 AC1.

The UK participation in its preparation was entrusted by Technical Committee IST/33, IT - Security techniques, to Subcommittee IST/33/-/1, Requirements, security services and guidelines.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017.
Published by BSI Standards Limited 2017

ISBN 978 0 580 95520 4

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 1 October 2013.

Amendments/corrigenda issued since publication

Date	Text affected
31 October 2014	Implementation of ISO/IEC corrigendum September 2014
30 November 2015	Implementation of ISO/IEC corrigendum November 2015: Subclause 14.2.8 modified
31 March 2017	This corrigendum renumbers BS ISO/IEC 27002:2013 as BS EN ISO/IEC 27002:2017.

English Version

Information technology - Security techniques - Code of
practice for information security controls (ISO/IEC
27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité
- Code de bonne pratique pour le management de la
sécurité de l'information (ISO/IEC 27002:2013 y
compris Cor 1:2014 et Cor 2:2015)

Informationstechnik - Sicherheitsverfahren - Leitfaden
für Informationssicherheitsmaßnahmen (ISO/IEC
27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

This European Standard was approved by CEN on 26 January 2017.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27002:2017.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 has been approved by CEN as EN ISO/IEC 27002:2017 without any modification.

Contents

Page

Foreword	v
0 Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this standard	1
4.1 Clauses	1
4.2 Control categories	1
5 Information security policies	2
5.1 Management direction for information security	2
6 Organization of information security	4
6.1 Internal organization	4
6.2 Mobile devices and teleworking	6
7 Human resource security	9
7.1 Prior to employment	9
7.2 During employment	10
7.3 Termination and change of employment	13
8 Asset management	13
8.1 Responsibility for assets	13
8.2 Information classification	15
8.3 Media handling	17
9 Access control	19
9.1 Business requirements of access control	19
9.2 User access management	21
9.3 User responsibilities	24
9.4 System and application access control	25
10 Cryptography	28
10.1 Cryptographic controls	28
11 Physical and environmental security	30
11.1 Secure areas	30
11.2 Equipment	33
12 Operations security	38
12.1 Operational procedures and responsibilities	38
12.2 Protection from malware	41
12.3 Backup	42
12.4 Logging and monitoring	43
12.5 Control of operational software	45
12.6 Technical vulnerability management	46
12.7 Information systems audit considerations	48
13 Communications security	49
13.1 Network security management	49
13.2 Information transfer	50
14 System acquisition, development and maintenance	54
14.1 Security requirements of information systems	54
14.2 Security in development and support processes	57
14.3 Test data	62
15 Supplier relationships	62
15.1 Information security in supplier relationships	62

15.2	Supplier service delivery management	66
16	Information security incident management	67
16.1	Management of information security incidents and improvements	67
17	Information security aspects of business continuity management	71
17.1	Information security continuity	71
17.2	Redundancies	73
18	Compliance	74
18.1	Compliance with legal and contractual requirements	74
18.2	Information security reviews	77
Bibliography		79

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

This second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structurally revised.

0 Introduction

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001^[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. An ISMS such as that specified in ISO/IEC 27001^[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001^[10] and this standard. 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. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

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

- a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;
- b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

- c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk 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.

ISO/IEC 27005^[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

0.3 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.^[11]

0.4 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

Information technology — Security techniques — Code of practice for information security controls

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

- a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;^[10]
- b) implement commonly accepted information security controls;
- c) develop their own information security management guidelines.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Structure of this standard

This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

4.1 Clauses

Each clause defining security controls contains one or more main security categories.

The order of the clauses in this standard does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organization applying this standard should identify applicable controls, how important these are and their application to individual business processes. Furthermore, lists in this standard are not in priority order.

4.2 Control categories

Each main security control category contains:

- a) a control objective stating what is to be achieved;
- b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control

Defines the specific control statement, to satisfy the control objective.

Implementation guidance

Provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements. .

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

- a) business strategy;
- b) regulations, legislation and contracts;
- c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

- a) definition of information security, objectives and principles to guide all activities relating to information security;
- b) assignment of general and specific responsibilities for information security management to defined roles;
- c) processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of such policy topics include:

- a) access control (see [Clause 9](#));

- b) information classification (and handling) (see [8.2](#));
- c) physical and environmental security (see [Clause 11](#));
- d) end user oriented topics such as:
 - 1) acceptable use of assets (see [8.1.3](#));
 - 2) clear desk and clear screen (see [11.2.9](#));
 - 3) information transfer (see [13.2.1](#));
 - 4) mobile devices and teleworking (see [6.2](#));
 - 5) restrictions on software installations and use (see [12.6.2](#));
- e) backup (see [12.3](#));
- f) information transfer (see [13.2](#));
- g) protection from malware (see [12.2](#));
- h) management of technical vulnerabilities (see [12.6.1](#));
- i) cryptographic controls (see [Clause 10](#));
- j) communications security (see [Clause 13](#));
- k) privacy and protection of personally identifiable information (see [18.1.4](#));
- l) supplier relationships (see [Clause 15](#)).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an “information security awareness, education and training programme” (see [7.2.2](#)).

Other information

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single “information security policy” document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information.

Some organizations use other terms for these policy documents, such as “Standards”, “Directives” or “Rules”.

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization’s policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

The review of policies for information security should take the results of management reviews into account. Management approval for a revised policy should be obtained.

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

Implementation guidance

Allocation of information security responsibilities should be done in accordance with the information security policies (see [5.1.1](#)). Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined. These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes should be defined.

Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless they remain accountable and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be stated. In particular the following should take place:

- a) the assets and information security processes should be identified and defined;
- b) the entity responsible for each asset or information security process should be assigned and the details of this responsibility should be documented (see [8.1.2](#));
- c) authorization levels should be defined and documented;
- d) to be able to fulfil responsibilities in the information security area the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments;
- e) coordination and oversight of information security aspects of supplier relationships should be identified and documented.

Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information 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 asset who then becomes responsible for its day-to-day protection.

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties 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.

Other information

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Implementation guidance

Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may have been broken).

Other information

Organizations under attack from the Internet may need authorities to take action against the attack source.

Maintaining such contacts may be a requirement to support information security incident management (see [Clause 16](#)) or the business continuity and contingency planning process (see [Clause 17](#)). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).

6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

Implementation guidance

Membership in special interest groups or forums should be considered as a means to:

- a) improve knowledge about best practices and stay up to date with relevant security information;
- b) ensure the understanding of the information security environment is current and complete;
- c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;
- d) gain access to specialist information security advice;

- e) share and exchange information about new technologies, products, threats or vulnerabilities;
- f) provide suitable liaison points when dealing with information security incidents (see [Clause 16](#)).

Other information

Information sharing agreements can be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of confidential information.

6.1.5 Information security in project management

Control

Information security should be addressed in project management, regardless of the type of the project.

Implementation guidance

Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes. The project management methods in use should require that:

- a) information security objectives are included in project objectives;
- b) an information security risk assessment is conducted at an early stage of the project to identify necessary controls;
- c) information security is part of all phases of the applied project methodology.

Information security implications should be addressed and reviewed regularly in all projects. Responsibilities for information security should be defined and allocated to specified roles defined in the project management methods.

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Implementation guidance

When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;
- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;

- f) access controls;
- g) cryptographic techniques;
- h) malware protection;
- i) remote disabling, erasure or lockout;
- j) backups;
- k) usage of web services and web apps.

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques (see [Clause 10](#)) and enforcing use of secret authentication information (see [9.2.4](#)).

Mobile devices 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. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of mobile devices. Devices carrying important, sensitive 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 devices.

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

Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

- a) separation of private and business use of the devices, including using software to support such separation and protect business data on a private device;
- b) providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.

Other information

Mobile device wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are:

- a) some wireless security protocols are immature and have known weaknesses;
- b) information stored on mobile devices may not be backed-up because of limited network bandwidth or because mobile devices may not be connected at the times when backups are scheduled.

Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organization's premises.

6.2.2 Teleworking

Control

A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

Implementation guidance

Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters 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 physical 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 passed over the communication link and the sensitivity of the internal system;
- d) the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;
- e) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;
- f) the use of home networks and requirements or restrictions on the configuration of wireless network services;
- g) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;
- h) access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;
- i) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users;
- j) malware protection and firewall requirements.

The guidelines and arrangements to be considered should include:

- a) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed;
- 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 provision of insurance;
- h) the procedures for backup and business continuity;
- i) audit and security monitoring;
- j) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

Other information

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible workplace”, “remote work” and “virtual work” environments.

7 Human resource security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Control

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Implementation guidance

Verification should take into account all relevant privacy, protection of personally identifiable information and employment based legislation, and should, where permitted, include the following:

- a) availability of satisfactory character references, e.g. one business and one personal;
- b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;
- c) confirmation of claimed academic and professional qualifications;
- d) independent identity verification (passport or similar document);
- e) more detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, organizations should make sure the candidate:

- a) has the necessary competence to perform the security role;
- b) can be trusted to take on the role, especially if the role is critical for the organization.

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 confidential information, e.g. financial information or highly confidential information, the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process should also be ensured for contractors. In these cases, the agreement between the organization and the contractor should specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organization should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

7.1.2 Terms and conditions of employment

Control

The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

Implementation guidance

The contractual obligations for employees or contractors should reflect the organization's policies for information security in addition to clarifying and stating:

- a) that all employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities (see [13.2.4](#));
- b) the employee's or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (see [18.1.2](#) and [18.1.4](#));
- AC1 c) responsibilities for the classification of information and management of organizational information, other assets associated with information, information processing facilities and information services handled by the employee or contractor (see Clause 8); AC1
- d) responsibilities of the employee or contractor for the handling of information received from other companies or external parties;
- e) actions to be taken if the employee or contractor disregards the organization's security requirements (see [7.2.3](#)).

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The organization should ensure that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see [7.3](#)).

Other information

A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. An external party, with which a contractor is associated, can be required to enter into contractual arrangements on behalf of the contracted individual.

7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1 Management responsibilities

Control

Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

Implementation guidance

Management responsibilities should include ensuring that employees and contractors:

- a) are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems;
- b) are provided with guidelines to state information security expectations of their role within the organization;

- c) are motivated to fulfil the information security policies of the organization;
- d) achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see [7.2.2](#));
- e) conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working;
- f) continue to have the appropriate skills and qualifications and are educated on a regular basis;
- g) are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

Management should demonstrate support of information security policies, procedures and controls, and act as a role model.

Other information

If employees and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organization. For example, poor management can lead to information security being neglected or potential misuse of the organization's assets.

7.2.2 Information security awareness, education and training

Control

All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation guidance

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

An information security awareness programme should be established in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

The awareness programme should be planned taking into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. The awareness programme should also be updated regularly so it stays in line with organizational policies and procedures, and should be built on lessons learnt from information security incidents.

Awareness training should be performed as required by the organization's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others.

Information security education and training should also cover general aspects such as:

- a) stating management's commitment to information security throughout the organization;

- b) the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements;
- c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and external parties;
- d) basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks);
- e) contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

Information security education and training should take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

The organization should develop the education and training programme in order to conduct the education and training effectively. The programme should be in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The programme should consider different forms of education and training, e.g. lectures or self-studies.

Other information

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why'. It is important that employees understand the aim of information security and the potential impact, positive and negative, on the organization of their own behaviour.

Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills.

An assessment of the employees' understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.

7.2.3 Disciplinary process

Control

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

Implementation guidance

The disciplinary process should not be commenced without prior verification that an information security breach has occurred (see [16.1.7](#)).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of information security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

The disciplinary process should also be used as a deterrent to prevent employees from violating the organization's information security policies and procedures and any other information security breaches. Deliberate breaches may require immediate actions.

Other information

The disciplinary process can also become a motivation or an incentive if positive sanctions are defined for remarkable behaviour with regards to information security.

7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

7.3.1 Termination or change of employment responsibilities

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

Implementation guidance

The communication of termination responsibilities should include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement (see 13.2.4) and the terms and conditions of employment (see 7.1.2) continuing for a defined period after the end of the employee's or contractor's employment.

Responsibilities and duties still valid after termination of employment should be contained in the employee's or contractor's terms and conditions of employment (see 7.1.2).

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Other information

The human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the information security aspects of the relevant procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

It may be necessary to inform employees, customers or contractors of changes to personnel and operating arrangements.

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

Control

[AC1] Information, other assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. **[AC1]**

Implementation guidance

An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.

The asset inventory should be accurate, up to date, consistent and aligned with other inventories.

For each of the identified assets, ownership of the asset should be assigned (see 8.1.2) and the classification should be identified (see 8.2).

Other information

Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

ISO/IEC 27005^[11] provides examples of assets that might need to be considered by the organization when identifying assets. The process of compiling an inventory of assets is an important prerequisite of risk management (see also ISO/IEC 27000 and ISO/IEC 27005^[11]).

8.1.2 Ownership of assets

Control

Assets maintained in the inventory should be owned.

Implementation guidance

Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.

A process to ensure timely assignment of asset ownership is usually implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle.

The asset owner should:

- a) ensure that assets are inventoried;
- b) ensure that assets are appropriately classified and protected;
- c) define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;
- d) ensure proper handling when the asset is deleted or destroyed.

Other information

The identified owner can be either an individual or an entity who has approved management responsibility for controlling the whole lifecycle of an asset. The identified owner does not necessarily have any property rights to the asset.

Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the owner.

In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.

8.1.3 Acceptable use of assets

Control

Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.

Implementation guidance

^[AC1] Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's information, other assets associated with information and information processing facilities and resources. ^[AC1]

8.1.4 Return of assets

Control

All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

Implementation guidance

The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see [11.2.7](#)).

In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period of termination, the organization should control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification of information

Control

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

Implementation guidance

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Assets other than information can also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information assets should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. The level of protection in the scheme should be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered. The scheme should be aligned to the access control policy (see [9.1.1](#)).

Each level should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organization so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.

Classification should be included in the organization's processes, and be consistent and coherent across the organization. Results of classification should indicate value of assets depending on their sensitivity and criticality to the organization, e.g. in terms of confidentiality, integrity and availability. Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their life-cycle.

Other information

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease 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 the implementation of unnecessary controls resulting in additional expense or on the contrary under-classification can endanger the achievement of business objectives.

An example of an information confidentiality classification scheme could be based on four levels as follows:

- a) disclosure causes no harm;
- b) disclosure causes minor embarrassment or minor operational inconvenience;
- c) disclosure has a significant short term impact on operations or tactical objectives;
- d) disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

8.2.2 Labelling of information

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

“Implementation guidance”

Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established in [8.2.1](#). The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information to reduce workloads. Employees and contractors should be made aware of labelling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information

Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and metadata are a common form of labelling.

Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.

8.2.3 Handling of assets

Control

Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Implementation guidance

Procedures should be drawn up for handling, processing, storing and communicating information consistent with its classification (see [8.2.1](#)).

The following items should be considered:

- a) access restrictions supporting the protection requirements for each level of classification;
- b) maintenance of a formal record of the authorized recipients of assets;
- c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
- d) storage of IT assets in accordance with manufacturers' specifications;
- e) clear marking of all copies of media for the attention of the authorized recipient.

The classification scheme used within the organization may not be equivalent to the schemes used by other organizations, even if the names for levels are similar; in addition, information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical.

Agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organizations.

8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

Control

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Implementation guidance

The following guidelines for the management of removable media should be considered:

- a) if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable;
- b) where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail;
- c) all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;
- d) if data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media;
- e) to mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable;
- f) multiple copies of valuable data should be stored on separate media to further reduce the risk of coincidental data damage or loss;
- g) registration of removable media should be considered to limit the opportunity for data loss;
- h) removable media drives should only be enabled if there is a business reason for doing so;
- i) where there is a need to use removable media the transfer of information to such media should be monitored.

Procedures and authorization levels should be documented.

8.3.2 Disposal of media

Control

Media should be disposed of securely when no longer required, using formal procedures.

Implementation guidance

Formal procedures for the secure disposal of media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure disposal of media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

- a) media containing confidential information should be stored and disposed of securely, e.g. by incineration or shredding, or erasure of data for use by another application within the organization;
- b) procedures should be in place to identify the items that might require secure disposal;
- 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 media; care should be taken in selecting a suitable external party with adequate controls and experience;
- e) disposal of sensitive items should be logged in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

Other information

Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded (see [11.2.7](#)).

8.3.3 Physical media transfer

Control

Media containing information should be protected against unauthorized access, misuse or corruption during transportation.

Implementation guidance

The following guidelines should be considered to protect media containing information being transported:

- a) reliable transport or couriers should be used;
- b) a list of authorized couriers should be agreed with management;
- c) procedures to verify the identification of couriers should be developed;
- d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;
- e) logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

Other information

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. In this control, media include paper documents.

When confidential information on media is not encrypted, additional physical protection of the media should be considered.

9 Access control

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

Control

An access control policy should be established, documented and reviewed based on business and information security requirements.

Implementation guidance

Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

Access controls are both logical and physical (see [Clause 11](#)) and these should be considered together. 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 business applications;
- b) policies for information dissemination and authorization, e.g. the need-to-know principle and information security levels and classification of information (see [8.2](#));
- c) consistency between the access rights and information classification policies of systems and networks;
- d) relevant legislation and any contractual obligations regarding limitation of access to data or services (see [18.1](#));
- e) management of access rights in a distributed and networked environment which recognizes all types of connections available;
- f) segregation of access control roles, e.g. access request, access authorization, access administration;
- g) requirements for formal authorization of access requests (see [9.2.1](#) and [9.2.2](#));
- h) requirements for periodic review of access rights (see [9.2.5](#));
- i) removal of access rights (see [9.2.6](#));
- j) archiving of records of all significant events concerning the use and management of user identities and secret authentication information;
- k) roles with privileged access (see [9.2.3](#)).

Other information