INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

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

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Reference number
ISO/IEC 27002:2013(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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);

c) responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handled by the employee or contractor (see Clause 8);

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

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

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

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 assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

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

Care should be taken when specifying access control rules to consider:

a) establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";

b) changes in information labels (see 8.2.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

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

d) rules which require specific approval before enactment and those which do not.

Access control rules should be supported by formal procedures (see 9.2, 9.3, 9.4) and defined responsibilities (see 6.1.1, 9.3).

Role based access control is an approach used successfully by many organisations to link access rights with business roles.

Two of the frequent principles directing the access control policy are:

a) Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile);

b) Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

9.1.2 Access to networks and network services

Control

Users should only be provided with access to the network and network services that they have been specifically authorized to use.

Implementation guidance

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

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

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

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

d) the means used to access networks and network services (e.g. use of VPN or wireless network);

e) user authentication requirements for accessing various network services;

f) monitoring of the use of network services.

The policy on the use of network services should be consistent with the organization's access control policy (see 9.1.1).

Other information

Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's information security management and control.

9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

9.2.1 User registration and de-registration

Control

A formal user registration and de-registration process should be implemented to enable assignment of access rights.

Implementation guidance

The process for managing user IDs should include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;

b) immediately disabling or removing user IDs of users who have left the organization (see 9.2.6);

c) periodically identifying and removing or disabling redundant user IDs;

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

Other information

Providing or revoking access to information or information processing facilities is usually a two-step procedure:

a) assigning and enabling, or revoking, a user ID;

b) providing, or revoking, access rights to such user ID (see 9.2.2).

9.2.2 User access provisioning

Control

A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

Implementation guidance

The provisioning process for assigning or revoking access rights granted to user IDs should include:

a) obtaining authorization from the owner of the information system or service for the use of the information system or service (see control 8.1.2); separate approval for access rights from management may also be appropriate;

b) verifying that the level of access granted is appropriate to the access policies (see 9.1) and is consistent with other requirements such as segregation of duties (see 6.1.2);

c) ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed;

d) maintaining a central record of access rights granted to a user ID to access information systems and services;

e) adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization;

f) periodically reviewing access rights with owners of the information systems or services (see 9.2.5).

Other information

Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews (see 9.2.4) are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or contractors (see 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 Management of privileged access rights

Control

The allocation and use of privileged access rights should be restricted and controlled.

Implementation guidance

The allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access control policy (see control 9.1.1). The following steps should be considered:

a) the privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom they need to be allocated should be identified;

b) privileged access rights should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (see 9.1.1), i.e. based on the minimum requirement for their functional roles;

c) an authorization process and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorization process is complete;

d) requirements for expiry of privileged access rights should be defined;

e) privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID;

f) the competences of users with privileged access rights should be reviewed regularly in order to verify if they are in line with their duties;

g) specific procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities;

h) for generic administration user IDs, the confidentiality of secret authentication information should be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

Other information

Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

9.2.4 Management of secret authentication information of users

Control

The allocation of secret authentication information should be controlled through a formal management process.

Implementation guidance

The process should include the following requirements:

a) users should be required to sign a statement to keep personal secret authentication information confidential and to keep group (i.e. shared) secret authentication information solely within the members of the group; this signed statement may be included in the terms and conditions of employment (see 7.1.2);

b) when users are required to maintain their own secret authentication information they should be provided initially with secure temporary secret authentication information`, which they are forced to change on first use;

c) procedures should be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information;

d) temporary secret authentication information should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided;

e) temporary secret authentication information should be unique to an individual and should not be guessable;

f) users should acknowledge receipt of secret authentication information;

g) default vendor secret authentication information should be altered following installation of systems or software.

Other information

Passwords are a commonly used type of secret authentication information and are a common means of verifying a user's identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes.

9.2.5 Review of user access rights

Control

Asset owners should review users' access rights at regular intervals.

Implementation guidance

The review of access rights should consider the following:

a) users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment (see Clause 7);

b) user access rights should be reviewed and re-allocated when moving from one role to another within the same organization;

c) authorizations for privileged access rights should be reviewed at more frequent intervals;

d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

e) changes to privileged accounts should be logged for periodic review.

Other information

This control compensates for possible weaknesses in the execution of controls 9.2.1, 9.2.2 and 9.2.6.

9.2.6 Removal or adjustment of access rights

Control

The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Implementation guidance

Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended. This will determine whether it is necessary to remove access rights. Changes of employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.

Access rights for information and assets associated with information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a) whether the termination or change is initiated by the employee, the external party user or by management, and the reason for termination;

b) the current responsibilities of the employee, external party user or any other user;

c) the value of the assets currently accessible.

Other information

In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees and external party users involved to no longer share this information with the person departing.

In cases of management-initiated termination, disgruntled employees or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they may be tempted to collect information for future use.

9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

9.3.1 Use of secret authentication information

Control

Users should be required to follow the organization's practices in the use of secret authentication information.

Implementation guidance

All users should be advised to:

a) keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority;

b) avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. password vault);

c) change secret authentication information whenever there is any indication of its possible compromise;

d) when passwords are used as secret authentication information, select quality passwords with sufficient minimum length which are:

   1) easy to remember;

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

   3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);

   4) free of consecutive identical, all-numeric or all-alphabetic characters;

   5) if temporary, changed at the first log-on;

e) not share individual user's secret authentication information;

f) ensure proper protection of passwords when passwords are used as secret authentication information in automated log-on procedures and are stored;

g) not use the same secret authentication information for business and non-business purposes.

Other information

Provision of Single Sign On (SSO) or other secret authentication information management tools reduces the amount of secret authentication information that users are required to protect and thus can increase the effectiveness of this control. However, these tools can also increase the impact of disclosure of secret authentication information.

9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

9.4.1 Information access restriction

Control

Access to information and application system functions should be restricted in accordance with the access control policy.

Implementation guidance

Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy.

The following should be considered in order to support access restriction requirements:

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

b) controlling which data can be accessed by a particular user;

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

d) controlling the access rights of other applications;

e) limiting the information contained in outputs;

f) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

9.4.2 Secure log-on procedures

Control

Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

Implementation guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance. A good log-on procedure should:

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

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

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

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

e) protect against brute force log-on attempts;

f) log unsuccessful and successful attempts;

g) raise a security event if a potential attempted or successful breach of log-on controls is detected;

h) display the following information on completion of a successful log-on:

   1) date and time of the previous successful log-on;

   2) details of any unsuccessful log-on attempts since the last successful log-on;

i) not display a password being entered;

j) not transmit passwords in clear text over a network;

k) terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on mobile devices;

l) restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Other information

Passwords are a common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user authentication should be appropriate for the classification of the information to be accessed.

If passwords are transmitted in clear text during the log-on session over a network, they can be captured by a network "sniffer" program.

9.4.3 Password management system

Control

Password management systems should be interactive and should ensure quality passwords.

Implementation guidance

A password management system should:

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

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

c) enforce a choice of quality passwords;

d) force users to change their passwords at the first log-on;

e) enforce regular password changes and as needed;

f) maintain a record of previously used passwords and prevent re-use;

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

h) store password files separately from application system data;

i) store and transmit passwords in protected form.

Other information

Some applications require user passwords to be assigned by an independent authority; in such cases, points b), d) and e) of the above guidance do not apply. In most cases the passwords are selected and maintained by users.

9.4.4 Use of privileged utility programs

Control

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Implementation guidance

The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be considered:

a) use of identification, authentication and authorization procedures for utility programs;

b) segregation of utility programs from applications software;

c) limitation of the use of utility programs to the minimum practical number of trusted, authorized users (see 9.2.3);

d) authorization for ad hoc use of utility programs;

e) limitation of the availability of utility programs, e.g. for the duration of an authorized change;

f) logging of all use of utility programs;

g) defining and documenting of authorization levels for utility programs;

h) removal or disabling of all unnecessary utility programs;

i) not making utility programs available to users who have access to applications on systems where segregation of duties is required.

Other information

Most computer installations have one or more utility programs that might be capable of overriding system and application controls.

9.4.5 Access control to program source code

Control

Access to program source code should be restricted.

Implementation guidance

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines should then be considered to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

a) where possible, program source libraries should not be held in operational systems;

b) the program source code and the program source libraries should be managed according to established procedures;

c) support personnel should not have unrestricted access to program source libraries;

d) the updating of program source libraries and associated items and the issuing of program sources to programmers should only be performed after appropriate authorization has been received;

e) program listings should be held in a secure environment;

f) an audit log should be maintained of all accesses to program source libraries;

g) maintenance and copying of program source libraries should be subject to strict change control procedures (see 14.2.2).

If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

10 Cryptography

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

Control

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Implementation guidance

When developing a cryptographic policy the following should be considered:

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

b) based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required;

c) the use of encryption for protection of information transported by mobile or removable media devices or across communication lines;

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

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

   1) the implementation of the policy;

   2) the key management, including key generation (see 10.1.2);

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

g) the impact of using encrypted information on controls that rely upon content inspection (e.g. malware detection).

When implementing the organization's cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see 18.1.5).

Cryptographic controls can be used to achieve different information security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b) integrity/authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information;

c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;

d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

Other information

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

Specialist advice should be sought in selecting appropriate cryptographic controls to meet the information security policy objectives.

10.1.2 Key management

Control

A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.

Implementation guidance

The policy should include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

Cryptographic algorithms, key lengths and usage practices should be selected according to best practice. Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

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

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

b) issuing and obtaining public key certificates;

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

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

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

f) dealing with compromised keys;

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

h) recovering keys that are lost or corrupted;

i) backing up or archiving keys;

j) destroying keys;

k) logging and auditing of key management related activities.

In order to reduce the likelihood of improper use, activation and deactivation dates for keys should be defined so that the keys can only be used for the period of time defined in the associated key management policy.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates, which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see 15.2).

Other information

The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770[2][3][4] provides further information on key management.

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

11 Physical and environmental security

11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

11.1.1 Physical security perimeter

Control

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

Implementation guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

b) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;

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

d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;

e) all fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner;

f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;

g) information processing facilities managed by the organization should be physically separated from those managed by external parties.

Other information

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.

A secure area may be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter. Special attention to physical access security should be given in the case of buildings holding assets for multiple organizations.

The application of physical controls, especially for the secure areas, should be adapted to the technical and economic circumstances of the organization, as set forth in the risk assessment.

11.1.2 Physical entry controls

Control

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

Implementation guidance

The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means;

b) access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN;

c) a physical log book or electronic audit trail of all access should be securely maintained and monitored;

d) all employees, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

e) external party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorized and monitored;

f) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see 9.2.5 and 9.2.6).

11.1.3 Securing offices, rooms and facilities

Control

Physical security for offices, rooms and facilities should be designed and applied.

Implementation guidance

The following guidelines should be considered to secure offices, rooms and facilities:

a) key facilities should be sited to avoid access by the public;

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

c) facilities should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;

d) directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

11.1.4 Protecting against external and environmental threats

Control

Physical protection against natural disasters, malicious attack or accidents should be designed and applied.

Implementation guidance

Specialist advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

11.1.5 Working in secure areas

Control

Procedures for working in secure areas should be designed and applied.

Implementation guidance

The following guidelines should be considered:

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

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

c) vacant secure areas should be physically locked and periodically reviewed;

d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.

The arrangements for working in secure areas include controls for the employees and external party users working in the secure area and they cover all activities taking place in the secure area.

11.1.6 Delivery and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Implementation guidance

The following guidelines should be considered:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;

b) the delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;

c) the external doors of a delivery and loading area should be secured when the internal doors are opened;

d) incoming material should be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;

e) incoming material should be registered in accordance with asset management procedures (see Clause 8) on entry to the site;

f) incoming and outgoing shipments should be physically segregated, where possible;

g) incoming material should be inspected for evidence of tampering en route. If such tampering is discovered it should be immediately reported to security personnel.

11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

11.2.1 Equipment siting and protection

Control

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

Implementation guidance

The following guidelines should be considered to protect equipment:

a) equipment should be sited to minimize unnecessary access into work areas;

b) information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;

c) storage facilities should be secured to avoid unauthorized access;

d) items requiring special protection should be safeguarded to reduce the general level of protection required;

e) controls should be adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism;

f) guidelines for eating, drinking and smoking in proximity to information processing facilities should be established;

g) environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities;

h) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;

i) the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;

j) equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

11.2.2 Supporting utilities

Control

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Implementation guidance

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) should:

a) conform to equipment manufacturer's specifications and local legal requirements;

b) be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;

c) be inspected and tested regularly to ensure their proper functioning;

d) if necessary, be alarmed to detect malfunctions;

e) if necessary, have multiple feeds with diverse physical routing.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms.

Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

11.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.

Implementation guidance

The following guidelines for cabling security should be considered:

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

b) power cables should be segregated from communications cables to prevent interference;

c) for sensitive or critical systems further controls to consider include:

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

   2) use of electromagnetic shielding to protect the cables;

   3) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;

   4) controlled access to patch panels and cable rooms.

11.2.4 Equipment maintenance

Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

Implementation guidance

The following guidelines for equipment maintenance should be considered:

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

b) only authorized maintenance personnel should carry out repairs and service equipment;

c) records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance;

d) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared;

e) all maintenance requirements imposed by insurance policies should be complied with;

f) before putting equipment back into operation after its maintenance, it should be inspected to ensure that the equipment has not been tampered with and does not malfunction.

11.2.5 Removal of assets

Control

Equipment, information or software should not be taken off-site without prior authorization.

Implementation guidance

The following guidelines should be considered:

a) employees and external party users who have authority to permit off-site removal of assets should be identified;

b) time limits for asset removal should be set and returns verified for compliance;

c) where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned;

d) the identity, role and affiliation of anyone who handles or uses assets should be documented and this documentation returned with the equipment, information or software.

Other information

Spot checks, undertaken to detect unauthorized removal of assets, can also be performed to detect unauthorized recording devices, weapons, etc., and to prevent their entry into and exit from, the site. Such spot checks should be carried out in accordance with relevant legislation and regulations. Individuals should be made aware that spot checks are carried out, and the verifications should only be performed with authorization appropriate for the legal and regulatory requirements.

11.2.6 Security of equipment and assets off-premises

Control

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Implementation guidance

The use of any information storing and processing equipment outside the organization's premises should be authorized by management. This applies to equipment owned by the organization and that equipment owned privately and used on behalf of the organization.

The following guidelines should be considered for the protection of off-site equipment:

a) equipment and media taken off premises should not be left unattended in public places;

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

c) controls for off-premises locations, such as home-working, teleworking and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office (see also ISO/IEC 27033[15][16][17][18][19]);

d) when off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.

Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Other information

Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.

More information about other aspects of protecting mobile equipment can be found in 6.2.

It may be appropriate to avoid the risk by discouraging certain employees from working off-site or by restricting their use of portable IT equipment;

11.2.7 Secure disposal or re-use of equipment

Control

All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Implementation guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Other information

Damaged equipment containing storage media may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk erasure, whole-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files, etc.);

b) the encryption keys are long enough to resist brute force attacks;

c) the encryption keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on encryption, see Clause 10.

Techniques for securely overwriting storage media differ according to the storage media technology. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

11.2.8 Unattended user equipment

Control

Users should ensure that unattended equipment has appropriate protection.

Implementation guidance

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

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

b) log-off from applications or network services when no longer needed;

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

11.2.9 Clear desk and clear screen policy

Control

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

Implementation guidance

The clear desk and clear screen policy should take into account the information classifications (see 8.2), legal and contractual requirements (see 18.1) and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:

a) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

b) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

c) unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented;

d) media containing sensitive or classified information should be removed from printers immediately.

Other information

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Consider the use of printers with PIN code function, so the originators are the only ones who can get their print-outs and only when standing next to the printer.

12 Operations security

12.1 Operational procedures and responsibilities

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

12.1.1 Documented operating procedures

Control

Operating procedures should be documented and made available to all users who need them.

Implementation guidance

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

The operating procedures should specify the operational instructions, including:

a) the installation and configuration of systems;

b) processing and handling of information both automated and manual;

c) backup (see 12.3);

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

e) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see 9.4.4);

f) support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;

g) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (see 8.3 and 11.2.7);

h) system restart and recovery procedures for use in the event of system failure;

i) the management of audit-trail and system log information (see 12.4);

j) monitoring procedures.

Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

12.1.2 Change management

Control

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

Implementation guidance

In particular, the following items should be considered:

a) identification and recording of significant changes;

b) planning and testing of changes;

c) assessment of the potential impacts, including information security impacts, of such changes;

d) formal approval procedure for proposed changes;

e) verification that information security requirements have been met;

f) communication of change details to all relevant persons;

g) fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events;

h) provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident (see 16.1).

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.

Other information

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (see 14.2.2).

12.1.3 Capacity management

Control

The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Implementation guidance

Capacity requirements should be identified, taking into account the business criticality of the concerned system. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or information systems management tools.

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

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. Examples of managing capacity demand include:

a) deletion of obsolete data (disk space);

b) decommissioning of applications, systems, databases or environments;

c) optimising batch processes and schedules;

d) optimising application logic or database queries;

e) denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

Other information

This control also addresses the capacity of the human resources, as well as offices and facilities.

12.1.4 Separation of development, testing and operational environments

Control

Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

Implementation guidance

The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

a) rules for the transfer of software from development to operational status should be defined and documented;

b) development and operational software should run on different systems or computer processors and in different domains or directories;

c) changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems;

d) other than in exceptional circumstances, testing should not be done on operational systems;

e) compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;

f) users should use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error;

g) sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system (see 14.3).

Other information

Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the operational environment.

Where development and testing personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud or introduce untested or malicious code, which can cause serious operational problems.

Development and testing personnel also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, testing and operational environments is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data (see 14.3 for the protection of test data).

12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

Control

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Implementation guidance

Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The following guidance should be considered:

a) establishing a formal policy prohibiting the use of unauthorized software (see 12.6.2 and 14.2.);

b) implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);

c) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting);

d) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken;

e) reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management (see 12.6);

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

g) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:

   1) scan any files received over networks or via any form of storage medium, for malware before use;

   2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;

   3) scan web pages for malware;

h) defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;

i) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (see 12.3);

j) implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware;

k) implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them;

l) isolating environments where catastrophic impacts may result.

Other information

The use of two or more software products protecting against malware across the information processing environment from different vendors and technology can improve the effectiveness of malware protection.

Care should be taken to protect against the introduction of malware during maintenance and emergency procedures, which may bypass normal malware protection controls.

Under certain conditions, malware protection might cause disturbance within operations.

Use of malware detection and repair software alone as a malware control is not usually adequate and commonly needs to be accompanied by operating procedures that prevent introduction of malware.

12.3 Backup

Objective: To protect against loss of data.

12.3.1 Information backup

Control

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

Implementation guidance

A backup policy should be established to define the organization's requirements for backup of information, software and systems.

The backup policy should define the retention and protection requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

When designing a backup plan, the following items should be taken into consideration:

a) accurate and complete records of the backup copies and documented restoration procedures should be produced;

b) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved and the criticality of the information to the continued operation of the organization;

c) the backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

d) backup information should be given an appropriate level of physical and environmental protection (see Clause 11) consistent with the standards applied at the main site;

e) backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss;

f) in situations where confidentiality is of importance, backups should be protected by means of encryption.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.

Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information should be determined, taking into account any requirement for archive copies to be permanently retained.

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Implementation guidance

Event logs should include, when relevant:

a) user IDs;

b) system activities;

c) dates, times and details of key events, e.g. log-on and log-off;

d) device identity or location if possible and system identifier;

e) records of successful and rejected system access attempts;

f) records of successful and rejected data and other resource access attempts;

g) changes to system configuration;

h) use of privileges;

i) use of system utilities and applications;

j) files accessed and the kind of access;

k) network addresses and protocols;

l) alarms raised by the access control system;

m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;

n) records of transactions executed by users in applications.

Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

Other information

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (see 18.1.4).

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 12.4.3).

12.4.2 Protection of log information

Control

Logging facilities and log information should be protected against tampering and unauthorized access.

Implementation guidance

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

a) alterations to the message types that are recorded;

b) log files being edited or deleted;

c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence (see 16.1.7).

Other information

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

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.

12.4.3 Administrator and operator logs

Control

System administrator and system operator activities should be logged and the logs protected and regularly reviewed.

Implementation guidance

Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.

Other information

An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

12.4.4 Clock synchronisation

Control

The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.

Implementation guidance

External and internal requirements for time representation, synchronisation and accuracy should be documented. Such requirements can be legal, regulatory, contractual requirements, standards compliance or requirements for internal monitoring. A standard reference time for use within the organization should be defined.

The organization's approach to obtaining a reference time from external source(s) and how to synchronise internal clocks reliably should be documented and implemented.

Other information

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

Control

Procedures should be implemented to control the installation of software on operational systems.

Implementation guidance

The following guidelines should be considered to control changes of software on operational systems:

a) the updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorization (see 9.4.5);

b) operational systems should only hold approved executable code and not development code or compilers;

c) applications and operating system software should only be implemented after extensive and successful testing; the tests should cover usability, security, effects on other systems and user-friendliness and should be carried out on separate systems (see 12.1.4); it should be ensured that all corresponding program source libraries have been updated;

d) a configuration control system should be used to keep control of all implemented software as well as the system documentation;

e) a rollback strategy should be in place before changes are implemented;

f) an audit log should be maintained of all updates to operational program libraries;

g) previous versions of application software should be retained as a contingency measure;

h) old versions of software should be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. Software patches should be applied when they can help to remove or reduce information security weaknesses (see 12.6).

Physical or logical access should only be given to suppliers for support purposes when necessary and with management approval. The supplier's activities should be monitored (see 15.2.1).

Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Control

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Implementation guidance

A current and complete inventory of assets (see Clause 8) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

Appropriate and timely action should be taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

a) the organization should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;

b) information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list, see 8.1.1); these information resources should be updated based on changes in the inventory or when other new or useful resources are found;

c) a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;

d) once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls;

e) depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management (see 12.1.2) or by following information security incident response procedures (see 16.1.5);

f) if a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);

g) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:

   1) turning off services or capabilities related to the vulnerability;

   2) adapting or adding access controls, e.g. firewalls, at network borders (see 13.1);

   3) increased monitoring to detect actual attacks;

   4) raising awareness of the vulnerability;

h) an audit log should be kept for all procedures undertaken;

i) the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;

j) systems at high risk should be addressed first;

k) an effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur;

l) define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

Other information

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see 12.1.2 and 14.2.2).

Vendors are often under significant pressure to release patches as soon as possible. Therefore, there is a possibility that a patch does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling a patch cannot be easily achieved once the patch has been applied.

If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031[14] can be beneficial.

12.6.2 Restrictions on software installation

Control

Rules governing the installation of software by users should be established and implemented.

Implementation guidance

The organization should define and enforce strict policy on which types of software users may install.

The principle of least privilege should be applied. If granted certain privileges, users may have the ability to install software. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted having regard to the roles of the users concerned.

Other information

Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights.

12.7 Information systems audit considerations

Objective: To minimise the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Control

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.

Implementation guidance

The following guidelines should be observed:

a) audit requirements for access to systems and data should be agreed with appropriate management;

b) the scope of technical audit tests should be agreed and controlled;

c) audit tests should be limited to read-only access to software and data;

d) access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

e) requirements for special or additional processing should be identified and agreed;

f) audit tests that could affect system availability should be run outside business hours;

g) all access should be monitored and logged to produce a reference trail.

13 Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

Control

Networks should be managed and controlled to protect information in systems and applications.

Implementation guidance

Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a) responsibilities and procedures for the management of networking equipment should be established;

b) operational responsibility for networks should be separated from computer operations where appropriate (see 6.1.2);

c) special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (see Clause 10 and 13.2); special controls may also be required to maintain the availability of the network services and computers connected;

d) appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security;

e) management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;

f) systems on the network should be authenticated;

g) systems connection to the network should be restricted.

Other information

Additional information on network security can be found in ISO/IEC 27033.[15][16][17][18][19]

13.1.2 Security of network services

Control

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Implementation guidance

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Other information

Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption and network connection controls;

b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;

c) procedures for the network service usage to restrict access to network services or applications, where necessary.

13.1.3 Segregation in networks

Control

Groups of information services, users and information systems should be segregated on networks.

Implementation guidance

One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks (e.g.virtual private networking).

The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy (see 9.1.1), access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy (see 13.1.1) before granting access to internal systems.

The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organization's internal network when properly implemented.

Other information

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Control

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Implementation guidance

The procedures and controls to be followed when using communication facilities for information transfer should consider the following items:

a) procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction;

b) procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications (see 12.2.1);

c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

d) policy or guidelines outlining acceptable use of communication facilities (see 8.1.3);

e) personnel, external party and any other user's responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.;

f) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Clause 10);

g) retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations;

h) controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

i) advising personnel to take appropriate precautions not to reveal confidential information;

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

k) advising personnel about the problems of using facsimile machines or services, namely:

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

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

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

In addition, personnel should be reminded that they should not have confidential conversations in public places or over insecure communication channels, open offices and meeting places.

Information transfer services should comply with any relevant legal requirements (see 18.1).

Other information

Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile and video.

Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products.

The business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls should be considered.

13.2.2 Agreements on information transfer

Control

Agreements should address the secure transfer of business information between the organization and external parties.

Implementation guidance

Information transfer agreements should incorporate the following:

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

b) procedures to ensure traceability and non-repudiation;

c) minimum technical standards for packaging and transmission;

d) escrow agreements;

e) courier identification standards;

f) responsibilities and liabilities in the event of information security incidents, such as loss of data;

g) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see 8.2);

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

i) any special controls that are required to protect sensitive items, such as cryptography (see Clause 10);

j) maintaining a chain of custody for information while in transit;

k) acceptable levels of access control.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit (see 8.3.3), and should be referenced in such transfer agreements.

The information security content of any agreement should reflect the sensitivity of the business information involved.

Other information

Agreements may be electronic or manual, and may take the form of formal contracts. For confidential information, the specific mechanisms used for the transfer of such information should be consistent for all organizations and types of agreements.

13.2.3 Electronic messaging

Control

Information involved in electronic messaging should be appropriately protected.

Implementation guidance

Information security considerations for electronic messaging should include the following:

a) protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organization;

b) ensuring correct addressing and transportation of the message;

c) reliability and availability of the service;

d) legal considerations, for example requirements for electronic signatures;

e) obtaining approval prior to using external public services such as instant messaging, social networking or file sharing;

f) stronger levels of authentication controlling access from publicly accessible networks.

Other information

There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications.

13.2.4 Confidentiality or non-disclosure agreements

Control

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.

Implementation guidance

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external parties or employees of the organization. Elements should be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);

b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

c) required actions when an agreement is terminated;

d) responsibilities and actions of signatories to avoid unauthorized information disclosure;

e) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

f) the permitted use of confidential information and rights of the signatory to use information;

g) the right to audit and monitor activities that involve confidential information;

h) process for notification and reporting of unauthorized disclosure or confidential information leakage;

i) terms for information to be returned or destroyed at agreement cessation;

j) expected actions to be taken in case of a breach of the agreement.

Based on an organization's information security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply (see 18.1).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other information

Confidentiality and non-disclosure agreements protect organizational information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner.

There may be a need for an organization to use different forms of confidentiality or non-disclosure agreements in different circumstances.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 Information security requirements analysis and specification

Control

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

Implementation guidance

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the identification should be documented and reviewed by all stakeholders.

Information security requirements and controls should reflect the business value of the information involved (see 8.2) and the potential negative business impact which might result from lack of adequate security.

Identification and management of information security requirements and associated processes should be integrated in early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage can lead to more effective and cost efficient solutions.

Information security requirements should also consider:

a) the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements;

b) access provisioning and authorization processes, for business users as well as for privileged or technical users;

c) informing users and operators of their duties and responsibilities;

d) the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity;

e) requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements;

f) requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems.

For applications that provide services over public networks or which implement transactions, the dedicated controls 14.1.2 and 14.1.3 should be considered.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality

in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls should be reconsidered prior to purchasing the product.

Available guidance for security configuration of the product aligned with the final software / service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined e.g. in terms of their functionality, which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Additional functionality should be reviewed to ensure it does not introduce unacceptable additional risks.

Other information

ISO/IEC 27005[11] and ISO 31000[27] provide guidance on the use of risk management processes to identify controls to meet information security requirements.

14.1.2 Securing application services on public networks

Control

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Implementation guidance

Information security considerations for application services passing over public networks should include the following:

a) the level of confidence each party requires in each other's claimed identity, e.g. through authentication;

b) authorization processes associated with who may approve contents of, issue or sign key transactional documents;

c) ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;

d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

e) the level of trust required in the integrity of key documents;

f) the protection requirements of any confidential information;

g) the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;

h) the degree of verification appropriate to verify payment information supplied by a customer;

i) selecting the most appropriate settlement form of payment to guard against fraud;

j) the level of protection required to maintain the confidentiality and integrity of order information;

k) avoidance of loss or duplication of transaction information;

l) liability associated with any fraudulent transactions;

m) insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls (see Clause 10), taking into account compliance with legal requirements (see Clause 18, especially see 18.1.5 for cryptography legislation).

Application service arrangements between partners should be supported by a documented agreement which commits both parties to the agreed terms of services, including details of authorization (see b) above).

Resilience requirements against attacks should be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.

Other information

Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Application services can make use of secure authentication methods, e.g. using public key cryptography and digital signatures (see Clause 10) to reduce the risks. Also, trusted third parties can be used, where such services are needed.

14.1.3 Protecting application services transactions

Control

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Implementation guidance

Information security considerations for application service transactions should include the following:

a) the use of electronic signatures by each of the parties involved in the transaction;

b) all aspects of the transaction, i.e. ensuring that:

   1) user's secret authentication information of all parties are valid and verified;

   2) the transaction remains confidential;

   3) privacy associated with all parties involved is retained;

c) communications path between all involved parties is encrypted;

d) protocols used to communicate between all involved parties are secured;

e) ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on a storage medium directly accessible from the Internet;

f) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

Other information

The extent of the controls adopted needs to be commensurate with the level of the risk associated with each form of application service transaction.

Transactions may need to comply with legal and regulatory requirements in the jurisdiction which the transaction is generated from, processed via, completed at or stored in.

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

Control

Rules for the development of software and systems should be established and applied to developments within the organization.

Implementation guidance

Secure development is a requirement to build up a secure service, architecture, software and system. Within a secure development policy, the following aspects should be put under consideration:

a) security of the development environment;

b) guidance on the security in the software development lifecycle:

   1) security in the software development methodology;

   2) secure coding guidelines for each programming language used;

c) security requirements in the design phase;

d) security checkpoints within the project milestones;

e) secure repositories;

f) security in the version control;

g) required application security knowledge;

h) developers' capability of avoiding, finding and fixing vulnerabilities.

Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use. Developers should be trained in their use and testing and code review should verify their use.

If development is outsourced, the organization should obtain assurance that the external party complies with these rules for secure development (see 14.2.7).

Other information

Development may also take place inside applications, such as office applications, scripting, browsers and databases.

14.2.2 System change control procedures

Control

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

Implementation guidance

Formal change control procedures should be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts.

Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated (see 12.1.2). The change control procedures should include but not be limited to:

a) maintaining a record of agreed authorization levels;

b) ensuring changes are submitted by authorized users;

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

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

e) identifying and checking security critical code to minimize the likelihood of known security weaknesses;

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

g) ensuring authorized users accept changes prior to implementation;

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

i) maintaining a version control for all software updates;

j) maintaining an audit trail of all change requests;

k) ensuring that operating documentation (see 12.1.1) and user procedures are changed as necessary to remain appropriate;

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

Other information

Changing software can impact the operational environment and vice versa.

Good practice includes the testing of new software in an environment segregated from both the production and development environments (see 12.1.4). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Where automatic updates are considered, the risk to the integrity and availability of the system should be weighed against the benefit of speedy deployment of updates. Automated updates should not be used on critical systems as some updates can cause critical applications to fail.

14.2.3 Technical review of applications after operating platform changes

Control

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Implementation guidance

This process should cover:

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

b) ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation;

c) ensuring that appropriate changes are made to the business continuity plans (see Clause 17).

Other information

Operating platforms include operating systems, databases and middleware platforms. The control should also be applied for changes of applications.

14.2.4 Restrictions on changes to software packages

Control

Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.

Implementation guidance

As far as possible and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered:

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

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

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

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

e) compatibility with other software in use.

If changes are necessary the original software should be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software (see 12.6.1). All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

14.2.5 Secure system engineering principles

Control

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Implementation guidance

Secure information system engineering procedures based on security engineering principles should be established, documented and applied to in-house information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

These principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They

should also be regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

The established security engineering principles should be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization should confirm that the rigour of suppliers' security engineering principles is comparable with its own.

Other information

Application development procedures should apply secure engineering techniques in the development of applications that have input and output interfaces. Secure engineering techniques provide guidance on user authentication techniques, secure session control and data validation, sanitisation and elimination of debugging codes.

14.2.6 Secure development environment

Control

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Implementation guidance

A secure development environment includes people, processes and technology associated with system development and integration.

Organizations should assess risks associated with individual system development efforts and establish secure development environments for specific system development efforts, considering:

a) sensitivity of data to be processed, stored and transmitted by the system;

b) applicable external and internal requirements, e.g. from regulations or policies;

c) security controls already implemented by the organization that support system development;

d) trustworthiness of personnel working in the environment (see 7.1.1);

e) the degree of outsourcing associated with system development;

f) the need for segregation between different development environments;

g) control of access to the development environment;

h) monitoring of change to the environment and code stored therein;

i) backups are stored at secure offsite locations;

j) control over movement of data from and to the environment.

Once the level of protection is determined for a specific development environment, organizations should document corresponding processes in secure development procedures and provide these to all individuals who need them.

14.2.7 Outsourced development

Control

The organization should supervise and monitor the activity of outsourced system development.

Implementation guidance:

Where system development is outsourced, the following points should be considered across the organization's entire external supply chain:

a) licensing arrangements, code ownership and intellectual property rights related to the outsourced content (see 18.1.2);

b) contractual requirements for secure design, coding and testing practices (see 14.2.1);

c) provision of the approved threat model to the external developer;

d) acceptance testing for the quality and accuracy of the deliverables;

e) provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;

f) provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery;

g) provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;

h) escrow arrangements, e.g. if source code is no longer available;

i) contractual right to audit development processes and controls;

j) effective documentation of the build environment used to create deliverables;

k) the organization remains responsible for compliance with applicable laws and control efficiency verification.

Other information

Further information on supplier relationships can be found in ISO/IEC 27036.[21][22][23]

14.2.8 System security testing

Control

Testing of security functionality should be carried out during development.

Implementation guidance

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected (see 14.1.1 and 14.1.9). The extent of testing should be in proportion to the importance and nature of the system.

14.2.9 System acceptance testing

Control

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Implementation guidance

System acceptance testing should include testing of information security requirements (see 14.1.1 and 14.1.2) and adherence to secure system development practices (see 14.2.1). The testing should also be conducted on received components and integrated systems. Organizations can leverage automated tools,

such as code analysis tools or vulnerability scanners, and should verify the remediation of security-related defects.

Testing should be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organization's environment and that the tests are reliable.

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1 Protection of test data

Control

Test data should be selected carefully, protected and controlled.

Implementation guidance

The use of operational data containing personally identifiable information or any other confidential information for testing purposes should be avoided. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification (see ISO/IEC 29101[26]).

The following guidelines should be applied to protect operational data, when used for testing purposes:

a) the access control procedures, which apply to operational application systems, should also apply to test application systems;

b) there should be separate authorization each time operational information is copied to a test environment;

c) operational information should be erased from a test environment immediately after the testing is complete;

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

Other information

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance

The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes

and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

a) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;

b) a standardised process and lifecycle for managing supplier relationships;

c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;

e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;

f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;

g) types of obligations applicable to suppliers to protect the organization's information;

h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;

i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;

j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;

k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;

l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;

m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information

Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

15.1.2 Addressing security within supplier agreements

Control

All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;

b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;

c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

e) rules of acceptable use of information, including unacceptable use if necessary;

f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;

g) information security policies relevant to the specific contract;

h) incident management requirements and procedures (especially notification and collaboration during incident remediation);

i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures;

j) relevant regulations for sub-contracting, including the controls that need to be implemented;

k) relevant agreement partners, including a contact person for information security issues;

l) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

m) right to audit the supplier processes and controls related to the agreement;

n) defect resolution and conflict resolution processes;

o) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

p) supplier's obligations to comply with the organization's security requirements.

Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers).

The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance

The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;

c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

d) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

e) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;

f) obtaining assurance that critical components and their origin can be traced throughout the supply chain;

g) obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

h) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

i) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information

The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Control

Organizations should regularly monitor, review and audit supplier service delivery.

Implementation guidance

Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organization and the supplier to:

a) monitor service performance levels to verify adherence to the agreements;

b) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

c) conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

d) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

e) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

f) resolve and manage any identified problems;

g) review information security aspects of the supplier's relationships with its own suppliers;

h) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing changes to supplier services

Control

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Implementation guidance

The following aspects should be taken into consideration:

a) changes to supplier agreements;

b) changes made by the organization to implement:

   1) enhancements to the current services offered;

   2) development of any new applications and systems;

   3) modifications or updates of the organization's policies and procedures;

   4) new or changed controls to resolve information security incidents and to improve security;.

c) changes in supplier services to implement:

   1) changes and enhancement to networks;

   2) use of new technologies;

   3) adoption of new products or newer versions/releases;

   4) new development tools and environments;

   5) changes to physical location of service facilities;

   6) change of suppliers;

   7) sub-contracting to another supplier.

16 Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

Control

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Implementation guidance

The following guidelines for management responsibilities and procedures with regard to information security incident management should be considered:

a) management responsibilities should be established to ensure that the following procedures are developed and communicated adequately within the organization:

   1) procedures for incident response planning and preparation;

   2) procedures for monitoring, detecting, analysing and reporting of information security events and incidents;

3) procedures for logging incident management activities;

4) procedures for handling of forensic evidence;

5) procedures for assessment of and decision on information security events and assessment of information security weaknesses;

6) procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations;

b) procedures established should ensure that:

1) competent personnel handle the issues related to information security incidents within the organization;

2) a point of contact for security incidents' detection and reporting is implemented;

3) appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained;

c) reporting procedures should include:

1) preparing information security event reporting forms to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event;

2) the procedure to be undertaken in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact and taking only coordinated actions;

3) reference to an established formal disciplinary process for dealing with employees who commit security breaches;

4) suitable feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

Other information

Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.

Detailed guidance on information security incident management is provided in ISO/IEC 27035.[20]

16.1.2 Reporting information security events

Control

Information security events should be reported through appropriate management channels as quickly as possible.

Implementation guidance

All employees and contractors should be made aware of their responsibility to report information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported.

Situations to be considered for information security event reporting include:

a) ineffective security control;

b) breach of information integrity, confidentiality or availability expectations;

c) human errors;

d) non-compliances with policies or guidelines;

e) breaches of physical security arrangements;

f) uncontrolled system changes;

g) malfunctions of software or hardware;

h) access violations.

Other information

Malfunctions or other anomalous system behaviour may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

16.1.3 Reporting information security weaknesses

Control

Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

Implementation guidance

All employees and contractors should report these matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible and available as possible.

Other information

Employees and contractors should be advised not to attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

16.1.4 Assessment of and decision on information security events

Control

Information security events should be assessed and it should be decided if they are to be classified as information security incidents.

Implementation guidance

The point of contact should assess each information security event using the agreed information security event and incident classification scale and decide whether the event should be classified as an information security incident. Classification and prioritization of incidents can help to identify the impact and extent of an incident.

In cases where the organization has an information security incident response team (ISIRT), the assessment and decision can be forwarded to the ISIRT for confirmation or reassessment.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

16.1.5 Response to information security incidents

Control

Information security incidents should be responded to in accordance with the documented procedures.

Implementation guidance

Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organization or external parties (see 16.1.1).

The response should include the following:

a) collecting evidence as soon as possible after the occurrence;

b) conducting information security forensics analysis, as required (see 16.1.7);

c) escalation, as required;

d) ensuring that all involved response activities are properly logged for later analysis;

e) communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;

f) dealing with information security weakness(es) found to cause or contribute to the incident;

g) once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis should take place, as necessary, to identify the source of the incident.

Other information

The first goal of incident response is to resume 'normal security level' and then initiate the necessary recovery.

16.1.6 Learning from information security incidents

Control

Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Implementation guidance

There should be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

Other information

The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process (see 5.1.2).

With due care of confidentiality aspects, anecdotes from actual information security incidents can be used in user awareness training (see 7.2.2) as examples of what could happen, how to respond to such incidents and how to avoid them in the future.

16.1.7 Collection of evidence

Control

The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Implementation guidance

Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.

In general, these procedures for evidence should provide processes of identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off. The procedures should take account of:

a) chain of custody;

b) safety of evidence;

c) safety of personnel;

d) roles and responsibilities of personnel involved;

e) competency of personnel;

f) documentation;

g) briefing.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Forensic evidence may transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as forensic evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.

Other information

Identification is the process involving the search for, recognition and documentation of potential evidence. Collection is the process of gathering the physical items that can contain potential evidence. Acquisition is the process of creating a copy of data within a defined set. Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence.

When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037[24] provides guidelines for identification, collection, acquisition and preservation of digital evidence.

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 Planning information security continuity

Control

The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

Implementation guidance

An organization should determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process. Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

Other information

In order to reduce the time and effort of an 'additional' business impact analysis for information security, it is recommended to capture information security aspects within the normal business continuity management or disaster recovery management business impact analysis. This implies that the information security continuity requirements are explicitly formulated in the business continuity management or disaster recovery management processes.

Information on business continuity management can be found in ISO/IEC 27031,[14] ISO 22313[9] and ISO 22301.[8]

17.1.2 Implementing information security continuity

Control

The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Implementation guidance

An organization should ensure that:

a) an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;

b) incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;

c) documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives (see 17.1.1).

According to the information security continuity requirements, the organization should establish, document, implement and maintain:

a) information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;

b) processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;

c) compensating controls for information security controls that cannot be maintained during an adverse situation.

Other information

Within the context of business continuity or disaster recovery, specific processes and procedures may have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them should be protected. Therefore an organization should

involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures.

Information security controls that have been implemented should continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls should be established, implemented and maintained to maintain an acceptable level of information security.

17.1.3 Verify, review and evaluate information security continuity

Control

The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

"Implementation guidance"

Organizational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such cases, the continuity of processes, procedures and controls for information security should be reviewed against these changed requirements.

Organizations should verify their information security management continuity by:

a) exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;

b) exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives;

c) reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

Other information

The verification of information security continuity controls is different from general information security testing and verification and should be performed outside the testing of changes. If possible, it is preferable to integrate verification of information security continuity controls with the organization's business continuity or disaster recovery tests.

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Implementation guidance

Organizations should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures should be considered.

Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

Other information

The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems.

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

Control

All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization.

Implementation guidance

The specific controls and individual responsibilities to meet these requirements should also be defined and documented.

Managers should identify all legislation applicable to their organization in order to meet the requirements for their type of business. If the organization conducts business in other countries, managers should consider compliance in all relevant countries.

18.1.2 Intellectual property rights

Control

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

Implementation guidance

The following guidelines should be considered to protect any material that may be considered intellectual property:

a) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;

b) acquiring software only through known and reputable sources, to ensure that copyright is not violated;

c) maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them;

d) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;

e) maintaining proof and evidence of ownership of licences, master disks, manuals, etc.;

f) implementing controls to ensure that any maximum number of users permitted within the licence is not exceeded;

g) carrying out reviews that only authorized software and licensed products are installed;

h) providing a policy for maintaining appropriate licence conditions;

i) providing a policy for disposing of or transferring software to others;

j) complying with terms and conditions for software and information obtained from public networks;

k) not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law;

l) not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. The importance and awareness of intellectual property rights should be communicated to staff for software developed by the organization.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which may involve fines and criminal proceedings.

18.1.3 Protection of records

Control

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

Implementation guidance

When deciding upon protection of specific organizational records, their corresponding classification based on the organization's classification scheme, should be considered. Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of allowable storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys and programs associated with encrypted archives or digital signatures (see Clause 10), should also be stored to enable decryption of the records for the length of time the records are retained.

Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

To meet these record safeguarding objectives, the following steps should be taken within an organization:

a) guidelines should be issued on the retention, storage, handling and disposal of records and information;

b) a retention schedule should be drawn up identifying records and the period of time for which they should be retained;

c) an inventory of sources of key information should be maintained.

Other information

Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organization operates within statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status of an organization to shareholders, external parties and auditors. National law or regulation may set the time period and data content for information retention.

Further information about managing organizational records can be found in ISO 15489-1.[5]

18.1.4 Privacy and protection of personally identifiable information

Control

Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

Implementation guidance

An organization's data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information.

Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented.

Other information

ISO/IEC 29100[25] provides a high-level framework for the protection of personally identifiable information within information and communication technology systems. A number of countries have introduced legislation placing controls on the collection, processing and transmission of personally identifiable information (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing and disseminating personally identifiable information, and may also restrict the ability to transfer personally identifiable information to other countries.

18.1.5 Regulation of cryptographic controls

Control

Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.

Implementation guidance

The following items should be considered for compliance with the relevant agreements, laws and regulations:

a) restrictions on import or export of computer hardware and software for performing cryptographic functions;

b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) restrictions on the usage of encryption;

d) mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with relevant legislation and regulations. Before encrypted information or cryptographic controls are moved across jurisdictional borders, legal advice should also be taken.

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

18.2.1 Independent review of information security

Control

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

Implementation guidance

Management should initiate the independent review. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

Such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience.

The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained.

If the independent review identifies that the organization's approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies (see 5.1.1), management should consider corrective actions.

Other information

ISO/IEC 27007[12], "Guidelines for information security management systems auditing" and ISO/IEC TR 27008[13], "Guidelines for auditors on information security controls" also provide guidance for carrying out the independent review.

18.2.2 Compliance with security policies and standards

Control

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

Implementation guidance

Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

a) identify the causes of the non-compliance;

b) evaluate the need for actions to achieve compliance;

c) implement appropriate corrective action;

d) review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews (see 18.2.1) when an independent review takes place in the area of their responsibility.

Other information

Operational monitoring of system use is covered in 12.4.

18.2.3 Technical compliance review

Control

Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.

Implementation guidance

Technical compliance should be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed.

If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.

Any technical compliance review should only be carried out by competent, authorized persons or under the supervision of such persons.

Other information

Technical compliance reviews involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance review requires specialist technical expertise.

Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorized access due to these vulnerabilities.

Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). Penetration testing and vulnerability assessments are not a substitute for risk assessment.

ISO/IEC TR 27008[13] provides specific guidance regarding technical compliance reviews.

Bibliography

[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1, *Information technology Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[4] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[5] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[6] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[7] ISO/IEC 20000-2,[1)]*Information technology — Service management — Part 2: Guidance on the application of service management systems*

[8] ISO 22301, *Societal security — Business continuity management systems — Requirements*

[9] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[10] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[11] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[12] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[13] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[14] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[15] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[16] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[17] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[18] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[19] ISO/IEC 27033-5, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)*

[20] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[21] ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

1) ISO/IEC 20000-2:2005 has been cancelled and replaced by ISO/IEC 20000-2:2012, *Information technology — Service management — Part 2: Guidance on the application of service management systems*.

[22] ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements*

[23] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security*

[24] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[27] ISO 31000, *Risk management — Principles and guidelines*

ICS 35.040
Price based on 80 pages