PRÀCTICA 2 ESTRUCTURA:

ALIÁNDOSE A LAS ISOS 27002-27005

This standard contains 11 security control clauses collectively containing a total of 39 main security categories and one introductory clause introducing risk assessment and treatment.

a) Security Policy

b) Organizing Information Security

c) Asset Management

d) Human Resources Security

e) Physical and Environmental Security

f) Communications and Operations Management

g) Access Control

h) Information Systems Acquisition, Development and Maintenance ->

i) Information Security Incident Management

j) Business Continuity Management

k) Compliance ->

Each main security category contains: a) a control objective stating what is to be achieved; and b) one or more controls that can be applied to achieve the control objective.

Implementation guidance Provides more detailed information to support the implementation of the control and meeting the control objective.

**- WHAT IS INFORMATION SECURITY**

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

**- HOW TO ESTABLISH SECURITY REQUIREMENTS**

There are three main sources of security requirements.

1. One source is derived from assessing risks to the organization.

2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization have to satisfy, and their socio-cultural environment.

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

**-ASSESSING SECURITY RISKS**

The results of the risk assessment will help to guide and determine the **appropriate management action and priorities for managing information security risks**, and for implementing controls selected to protect against these risks.

**- SELECTING CONTROLS**

**The selection of security 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**.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*THE 11 CLAUSES**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**SECURITY POLICY**

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

**- Information security policy document**

Control An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance The information security policy document should state management commitment and set out the organization’s approach to managing information security. The policy document should contain statements concerning:

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

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

1) compliance with legislative, regulatory, and contractual requirements;

2) security education, training, and awareness requirements;

3) business continuity management;

4) consequences of information security policy violations;

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

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

**ORGANIZATION OF INFORMATION SECURITY**

**Objective: To manage information security within the organization.**

**- Allocation of information security responsibilities**

Control :

All information security responsibilities should be clearly defined.

Implementation guidance: Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly identified.

a)the assets and security processes associated with each particular system should be identified and clearly defined;

b) the entity responsible for each asset or security process should be assigned and the details of this responsibility should be documented

c) authorization levels should be clearly defined and documented.

**ASSET MANAGEMENT**

**Objective: To achieve and maintain appropriate protection of organizational assets. All assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets**

**- Inventory of assets**

Control: All assets should be clearly identified and an inventory of all important assets drawn up and maintained

Implementation guidance: The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned. In addition, ownership and information classification should be agreed and documented for each of the assets.

There are many types of assets, including:

a) information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;

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

c) physical assets: computer equipment, communications equipment, removable media, and other equipment;

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

e) people, and their qualifications, skills, and experience;

f) intangibles, such as reputation and image of the organization.

**- Ownership of assets**

Control :All information and assets associated with information processing facilities should be owned by a designated part of the organization.

Implementation guidance: The asset owner should be responsible for:

a) ensuring that information and assets associated with information processing facilities are appropriately classified;

b) defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

Ownership may be allocated to:

a) a business process;

b) a defined set of activities;

c) an application; or

d) a defined set of data.

**-Acceptable use of asset**

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

Implementation guidance: All employees, contractors and third party users should follow rules for the acceptable use of information and assets associated with information processing facilities

**HUMAN RESOURCES SECURITY**

**Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities**

**- Roles and responsibilities**

Control: Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization’s information security policy.

Implementation guidance: Security roles and responsibilities should include the requirement to:

a) implement and act in accordance with the organization’s information security policies

b) protect assets from unauthorized access, disclosure, modification, destruction or interference;

c) execute particular security processes or activities;

d) ensure responsibility is assigned to the individual for actions taken;

e) report security events or potential events or other security risks to the organization

**- Terms and conditions of employment**

Control: As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization’s responsibilities for information security.

Implementation guidance: The terms and conditions of employment should reflect the organization’s security policy in addition to clarifying and stating:

a) that all employees, contractors and third party users who are given access to sensitive information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;

b) the employee’s, contractor’s and any other user’s legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (see also 15.1.1 and 15.1.2);

c) responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee.

d) responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;

**- Information security awareness, education, and training**

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

Implementation guidance: Awareness training should commence with a formal induction process designed to introduce the organization’s security policies and expectations before access to information or services is granted.

Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process (see 8.2.3).

**-Disciplinary process**

Control: There should be a formal disciplinary process for employees who have committed a security breach.

Implementation guidance: The disciplinary process should not be commenced without prior verification that a security breach has occurred (see also 13.2.3 for collection of evidence).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of 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. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

**PHYSICAL AND ENVIRONMENTAL SECURITY**

**Objective: To prevent unauthorized physical access, damage, and interference to the organization’s premises and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks.**

**-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.

b) access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained;

c) all employees, contractors and third party users and all visitors 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;

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

e) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary

**- Protecting against external and environmental threats**

Control: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

Implementation guidance: Consideration should be given to any security threats presented by neighboring premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street.

The following guidelines should be considered to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

a) hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area;

b) fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster affecting the main site;

c) appropriate fire fighting equipment should be provided and suitably placed

**- Working in secure areas**

Control Physical protection and guidelines 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 checked;

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

**- 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 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, sensitive information should be cleared from the equipment, or the maintenance personnel should be sufficiently cleared;

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

ISO

**COMMUNICATIONS AND OPERATIONS MANAGEMENT**

**Objective: To ensure the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures. Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.**

**- Documented operating procedures**

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

Implementation guidance Documented procedures should be prepared for system 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 instructions for the detailed execution of each job including:

a) processing and handling of information;

b) backup

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

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

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

f) 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

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

h) the management of audit-trail and system log information

**-Monitoring and review of third party services**

Control The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

Implementation guidance Monitoring and review of third party 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 and process between the organization and the third party to:

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

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

c) provide information about information security incidents and review of this information by the third party and the organization as required by the agreements and any supporting guidelines and procedures;

d) review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

e) resolve and manage any identified problems.

**- 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 For each new and ongoing activity, capacity requirements should be identified. 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.

**-Controls against malicious code**

Control Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

Implementation guidance Protection against malicious code should be based on malicious code detection and repair software, 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 15.1.2);

b) 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;

c) 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;

d) installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis;

e) defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks (see 13.1 and 13.2);

f) preparing appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements (see clause 14);

g) implementing procedures to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malicious code;

h) implementing procedures to verify information relating to malicious code, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources,

**- Information back-up**

Control Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Implementation guidance Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information back up should be considered:

a) the necessary level of back-up information should be defined;

b) accurate and complete records of the back-up copies and documented restoration procedures should be produced;

c) 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;

d) the back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

e) back-up information should be given an appropriate level of physical and environmental protection (see clause 9) consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;

f) back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;

**- Network controls**

Control Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Implementation guidance Network managers should implement controls 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) operational responsibility for networks should be separated from computer operations where appropriate (see 10.1.3);

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

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 11.4 and 12.3); 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 of security relevant actions;

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

ISO

**- Information exchange policies and procedures**

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

Implementation guidance The procedures and controls to be followed when using electronic communication facilities for information exchange should consider the following items:

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

b) procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications (see Clause 10.4.1);

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

d) policy or guidelines outlining acceptable use of electronic communication facilities (see 7.1.3);

e) procedures for the use of wireless communications, taking into account the particular risks involved;

f) employee, contractor and any other user’s responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.;

g) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Clause 12.3);

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

**ACCESS CONTROL**

**Objective: To control access to information. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorization.**

**-Access control policy**

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

Implementation guidance Access control rules and rights for each user or group of users should be clearly stated in an access control policy. Access controls are both logical and physical (see also section 9) 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 individual business applications;

b) identification of all information related to the business applications and the risks the information is facing;

c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information (see 7.2);

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

e) relevant legislation and any contractual obligations regarding protection of access to data or services (see 15.1);

f) standard user access profiles for common job roles in the organization;

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

h) segregation of access control roles, e.g. access request, access authorization, access administration;

i) requirements for formal authorization of access requests (see 11.2.1);

j) requirements for periodic review of access controls (see 11.2.4);

k) removal of access rights (see 8.3.3).

**- Privilege management**

Control The allocation and use of privileges should be restricted and controlled.

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

a) the access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated should be identified;

b) privileges 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 (11.1.1), i.e. the minimum requirement for their functional role only when needed;

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

d) the development and use of system routines should be promoted to avoid the need to grant privileges to users; e) the development and use of programs which avoid the need to run with privileges should be promoted;

f) privileges should be assigned to a different user ID from those used for normal business use.

**- Teleworking**

Control A policy, operational plans and procedures should be developed and implemented for teleworking activities.

Implementation guidance Organizations should only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization’s security policy.

Suitable protection of the teleworking site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization’s internal systems or misuse of facilities. Teleworking activities should both be authorized and controlled by management, and it should be ensured that suitable arrangements are in place for this way of working.

**INFORMATION SECURITY INCIDENT MANAGEMENT**

**Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.**

**- REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES**

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

Implementation guidance A formal information security event reporting procedure should be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact should be established for the reporting of information security events. It should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.

The reporting procedures should include:

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

b) 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;

c) the correct behaviour to be undertaken in case of an information security event, i.e.

d) reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches.

Control All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Implementation guidance All employees, contractors and third party users should report these matters either to their management or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible, and available as possible. They should be informed that they should not, in any circumstances, attempt to prove a suspected weakness.

**- 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 In addition to reporting of information security events and weaknesses (see also 13.1), the monitoring of systems, alerts, and vulnerabilities (10.10.2) should be used to detect information security incidents. The following guidelines for information security incident management procedures should be considered:

a) procedures should be established to handle different types of information security incident

b) in addition to normal contingency plans

c) audit trails and similar evidence should be collected

d) action to recover from security breaches and correct system failures should be carefully and formally controlled;

**BUSINESS CONTINUITY MANAGEMENT**

**Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumpt**

**- Business continuity and risk assessment**

Control Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.

Implementation guidance Information security aspects of business continuity should be based on identifying events (or sequence of events) that can cause interruptions to the organizations business processes, e.g. equipment failure, human errors, theft, fire, natural disasters and acts of terrorism. This should be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period.

**-Developing and implementing continuity plans including information security**

Control Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

Implementation guidance The business continuity planning process should consider the following:

a) identification and agreement of all responsibilities and business continuity procedures;

b) identification of the acceptable loss of information and services;

c) implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place;

d) operational procedures to follow pending completion of recovery and restoration;

e) documentation of agreed procedures and processes;

**- Data protection and privacy of personal information**

Control Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

Implementation guidance An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information.

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

**INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE**

**Objective: To ensure that security is an integral part of information systems. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.**

**-Security requirements analysis and specification**

Control Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

Implementation guidance Specifications for the requirements for controls should consider the automated controls to be incorporated in the information system, and the need for supporting manual controls. Similar considerations should be applied when evaluating software packages, developed or purchased, for business applications.

**-Change control procedures**

Control The implementation of changes should be controlled by the use of formal change control procedures.

Implementation guidance Formal change control procedures should be documented and enforced in order to minimize the corruption of information systems. 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 assessmen.

The change procedures should include:

a) maintaining a record of agreed authorization levels;

b) ensuring changes are submitted by authorized users;

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

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

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

f) ensuring authorized users accept changes prior to implementation;

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

h) maintaining a version control for all software updates;

i) maintaining an audit trail of all change requests;

**- Control of technical vulnerabilities**

Control Timely information about technical vulnerabilities of information systems being used should be obtained, 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 7.1) 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.

**COMPLIANCE**

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Advice on specific legal requirements should be sought from the organization’s legal advisers, or suitably qualified legal practitioners.

**- Intellectual property rights (IPR)**

Control Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the 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 licenses, master disks, manuals, etc;

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

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

h) providing a policy for maintaining appropriate licence conditions;

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

**-Protection of organizational records**

Control Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

Implementation guidance Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures (see 12.3), should also be stored to enable decryption of the records for the length of time the records are retained.