ISO/IEC

Content

1) Information Security Policy
2) Organization of Information Security
3) Human Resource Security
4) Asset Management
5) Access Control
6) Cryptography
7) Physical and Environmental Security
8) Operations Security
9) Communications Security
10) System Acquisition, Development and Maintenance

Content

11) Supplier Relationship

12)Information security incident management

13) Information security of Business continuity management

14) Compliance

Introduction To ISO 27000 Series

Standard	Published	Title	Notes
ISO/IEC 27000	2016	Information security management systems - Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus a glossary of terms; FREE!
ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
ISO/IEC 27003	2017	Information security management system implementation guidance	Sound advice on implementing ISO27k, expanding section-by-section on the main body of ISO/IEC 27001, recommended
ISO/IEC 27004	2016	Information security management — Measurement	Much improved second version, recommended
ISO/IEC 27005	2011	Information security risk management	Discusses information risk management principles in general without specifying particular methods. Out of

Information Security Policy

❑Objective:

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

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

Information Security Policy

- 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.

Information Security Policy

- 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:

I. Access Control Policy
II. Information Classification

Information Security Policy

III. Physical and environmental security

IV. End user oriented topics such as:

- acceptable use of assets
- clear desk and clear screen
- information transfer
- mobile devices and teleworking
- restrictions on software installations and use

V. Backup

VI. Information transfer

VII. Protection from malware

VIII. Management of technical vulnerabilities

IX. Cryptographic controls

X. Communications security

Information Security Policy

XII. Privacy and protection of personally identifiable information

XIII. Supplier Relationship

- Review of the policies for information security:
- 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.

Organization of Information Security

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

- Information security roles and responsibilities:
  - Allocation of information security responsibilities should be done in accordance with the information security policies.
  - Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified

Organization of Information Security

❑Segregation of duties:

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

❑Contact with authorities:

- 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.

Organization of Information Security

❑Information security in project management:

- 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.

❑Mobile device policy:

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

Organization of Information Security

- 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.

Organization of Information Security

❑Teleworking:

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

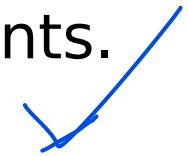
❑Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

Organization of Information Security

- 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;

Organization of Information Security

- 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 ofthe 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.



Human Resource Security

Objective:

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

Screening:

- Background verification checks on all candidates for employment should be caried out in accordance with relevant laws, regulations and ethics.
- Verification should take into account all relevant privacy, protection of personally identifiable information and employment based legislation, etc.

Human Resource Security

a) Availability of satisfactory character reference

b) A verification of applicant's curriculum vitae

c) Confirmation of claimed academic and professional qualification

d) Independent identity verification

e) More detailed verification; such as credit review or review of criminal records.

f) Candidate has the necessary competence to perform the security role

g) Candidate can be trusted to take on the role; specially if the role is critical for the organization

Human Resource Security

- Terms and conditions of employment:

a) Employee who are given access to confidential information should sign a confidentiality or non disclosure agreement

b) Employee's legal responsibilities and rights

c) Action to be taken if the employee or contractor disregards the organization's security requirements

Human Resource Security

❑Management Responsibilities:

a) That the employees are briefed on their roles and responsibilities prior to being granted the access to confidential information.

b) Employees are provided with guidelines to state information security expectation of their role within the organization

c) Employees are motivated to fulfil the information security policy of the organization

d) Continue to have the appropriate skills and qualifications and are educated on regular basis.

Human Resource Security

- Information security awareness, education and training:

- All the employee of organization and contractors should receive appropriate awareness education and training and regular updates in organizational policy and procedure, as relevant for their job

a) Awareness programme should include a number of awareness raising activities.

b) Delivery media should include classroom based, distance learning, web-based, self-paced and other

c) The training programme should include basic information security procedures and baseline controls with resources for advice.

Human Resource Security

❑Disciplinary process:

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

- The formal disciplinary process should consider 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.

Human Resource Security

Termination or Change of Employment Responsibilities:

- Information security responsibilities are duties that remain valid after termination or change of employment should be defined, communicated to the employee and enforced.
- The communication of termination responsibilities should include on-going information security requirement and legal responsibilities and, where appropriate, responsibilities contained within any confidential agreement and the terms and condition of employment continuing for a defined period after the end of employment.
- Changes of employment should be managed as a termination of current employment combined with the initiation of new employment.

Asset Management

Objective:

- To identify organizational assets and define appropriate protection responsibilities.

a) Inventory of assets
b) Ownership of assets
c) Acceptable use of assets
d) Return of assets
e) Information Classification
f) Labelling of information
g) Media handling
h) Disposal of media
i) Physical Media Transfer

Access Control

❑Objective:

- To identify organizational assets and define appropriate protection responsibilities.
- An access control policy should be established, documented and reviewed based on business and information security requirements.

a) Access to network and network services

b) User Access Management

   i. User Registration and de-registration
   ii. User Access Provisioning
   iii. Management of privileged access rights
   iv. Management of secret authentication info. of users
   v. Review of user access rights
   vi. Removal or adjustment of access right

Access Control

c) System and application access control
   i. Information Access Restriction
   ii. Secure Log-on Procedures
   iii. Password management system
   iv. Use of Privileged utility program
   v. Access Control to program source code

Crypto - Graphy

❑Objective:

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

a) Policy on the use of cryptographic controls

b) Key Management (Generating, Storing, Archiving, Retrieving, Distributing, Retiring and Destroying Keys.)

Physical and Environmental Security

Objective:

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

a) Secure Areas
   i. Physical Entry Control
   ii. Securing Offices, Rooms and Facilities
   iii. Protection against external and environmental threats
   iv. Working in secure areas
   v. Delivery and Loading areas

b) Equipment
   i. Supporting Utilities (i.e. electricity, telecommunication, water supplies, gas, sewage, ventilation and air conditioning)

Physical and Environmental Security

ii. Equipment siting and protection
iii. Cabling Security
iv. Equipment maintenance
v. Removal of assets
vi. Security of equipment and assets off-premises
vii. Secure disposal or re-use of equipment
viii. Unattended user equipment

Operations Security

❑Objective:

- To ensure correct and secure operations of information processing facilities.

- 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.

Operations Security

- Change management
- Capacity management
- Separation of development, testing and operational environments
- Protection from malware
- Backup
- Logging and monitoring
- Protection of log information
- Administrator and operator logs
- Clock synchronisation
- Control of operational software
- Technical vulnerability management
- Restrictions on software installation
- Information systems audit considerations

Operations Security

- Event logs should include, when relevant: (Logging and Monitoring):
- 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.

Communication Security

❑Objective:

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

a) Security of Network Services:

b) Segregation in Networks:

c) Information Transfer:
   - To maintain the security of information transferred within an organization and with any external entity.

d) Information-transfer Policies and Procedures:
   - Transferred information from interception, copying, modification, mis-routing and destruction.

Communication Security

- Transferred information from interception, copying, modification, mis-routing and destruction.
- protection against malware that may be transmitted through the use of electronic communications
- acceptable use of communication facilities
- use of cryptographic techniques
- controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses.

e) Confidentiality or non-disclosure agreements:

System Acquisition, Development

❑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.

a) Information security requirements analysis and specification:

- 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.

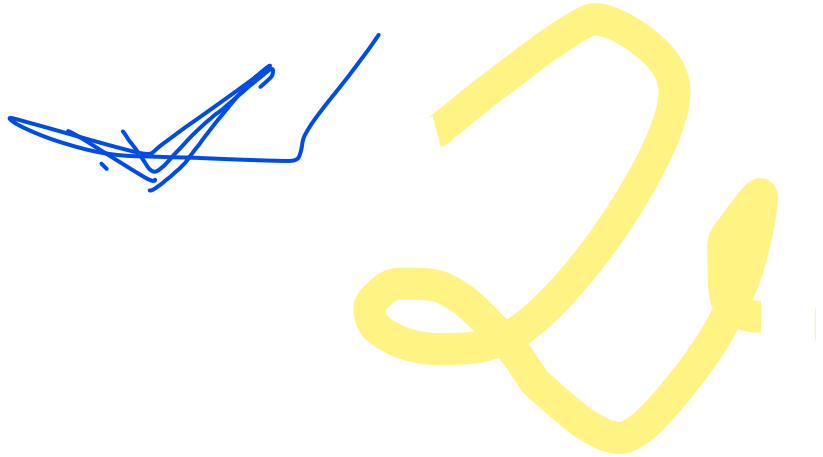
System Acquisition, Development

b) Securing application services on public networks:

c) Protecting application services transactions:

d) Security in development and support processes:

e) Test data:



Information Security Incident

❑Objective:

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

- procedures for incident response planning and preparation;
- procedures for monitoring, detecting, analysing and reporting of information security events and incidents;
- procedures for logging incident management activities;
- procedures for handling of forensic evidence;
- procedures for assessment of and decision on information security events and assessment of information security weaknesses;

Information Security Incident

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

- Reporting information security events:
- Reporting information security weaknesses:
- Assessment of and decision on information security events:
- Response to information security incidents:
- Learning from information security incidents:
- Collection of evidence:

Information Security aspects of Busine

❑Objective:

- Information security continuity should be embedded in the organization's business continuity management systems

- 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.

Information Security aspects of Busine

❑ **Implementing information security continuity:**

- 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

Information Security aspects of Busine

- 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.

Information Security aspects of Busine

- 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.

Information Security aspects of Busine

❑Redundancies:

- To ensure availability of information processing facilities.

- 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.

Compliance

- 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.

- Identification of applicable legislation and contractual requirements
- Intellectual property rights:
- Protection of records:
- Privacy and protection of personally identifiable information:
- Regulation of cryptographic controls

Compliance

- **Information security reviews:**
- **Independent review of information security:**
- **Compliance with security policies and standards:**
- **Technical compliance review:**
- 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.

ISO 27001/2

Truth, Transparency and Tactics Are the Characteristics of a good Auditor