ISO 27001 Controls and Objectives

A.5 Security policy

A.5.1 Information security policy

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

A.5.1.1 Information security policy document
Control
An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.

A.5.1.2 Review of the information security policy
Control
The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

A.6 Organization of information security

A.6.1 Internal organization

Objective: To manage information security within the organization.

A.6.1.1 Management commitment to information security
Control
Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

A.6.1.2 Information security coordination
Control
Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.

A.6.1.3 Allocation of information security responsibilities
Control
All information security responsibilities shall be clearly defined.

A.6.1.4 Authorization process for information processing facilities
Control
A management authorization process for new information processing facilities shall be defined and implemented.

A.6.1.5
Confidentiality agreements
Control
Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.

A.6.1.6
Contact with authorities
Control
Appropriate contacts with relevant authorities shall be maintained.

A.6.1.7 Contact with special interest groups
Control
Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.1.8 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) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

A.6.2 External parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

A.6.2.1 Identification of risks related to external parties
Control
The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.

A.6.2.2 Addressing security when dealing with customers
Control
All identified security requirements shall be addressed before giving customers access to the organization's information or assets.

A.6.2.3 Addressing security in third party agreements
Control
Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

A.7 Asset management

A.7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

A.7.1.1
Inventory of assets
Control
All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

A.7.1.2
Ownership of assets
Control
All information and assets associated with information processing facilities shall be 'owned' by a designated part of the organization.

A.7.1.3
Acceptable use of assets
Control
Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

A.7.2 Information classification

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

A.7.2.1
Classification guidelines
Control
Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.

A.7.2.2 Information labelling and handling
Control
An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.

A.8 Human resources security

A.8.1 Prior to employment

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.

A.8.1.1
Roles and responsibilities
Control
Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

A.8.1.2
Screening
Control
Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

A.8.1.3 Terms and conditions of employment
Control
As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

A.8.2 During employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

A.8.2.1
Management responsibilities
Control
Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

A.8.2.2 Information security awareness, education and training
Control
All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

A.8.2.3
Disciplinary process
Control
There shall be a formal disciplinary process for employees who have committed a security breach.

A.8.3 Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

A.8.3.1
Termination responsibilities
Control
Responsibilities for performing employment termination or changeof employment shall be clearly defined and assigned.

A.8.3.2
Return of assets
Control
All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

A.8.3.3
Removal of access rights
Control
The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9 Physical and environmental security

A.9.1 Secure areas

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

A.9.1.1
Physical security perimeter
Control
Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.

A.9.1.2
Physical entry controls
Control
Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

A.9.1.3 Securing offices, rooms and facilities
Control
Physical security for offices, rooms, and facilities shall be designed and applied.

A.9.1.4 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 shall be designed and applied.

A.9.1.5
Working in secure areas
Control
Physical protection and guidelines for working in secure areas shall be designed and applied.

A.9.1.6 Public access, delivery and loading areas
Control
Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

A.9.2 Equipment security

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

A.9.2.1 Equipment siting and protection
Control
Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

A.9.2.2
Supporting utilities
Control
Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.9.2.3
Cabling security
Control
Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

A.9.2.4
Equipment maintenance
Control
Equipment shall be correctly maintained to ensure its continued availability and integrity.

A.9.2.5 Security of equipment off premises
Control
Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.

A.9.2.6 Secure disposal or re-use of equipment
Control
All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

A.9.2.7
Removal of property
Control
Equipment, information or software shall not be taken off-site without prior authorization.

A.10 Communications and operations management

A.10.1 Operational procedures and responsibilities

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

A.10.1.1 Documented operating procedures
Control
Operating procedures shall be documented, maintained, and made available to all users who need them.

A.10.1.2
Change management
Control
Changes to information processing facilities and systems shall be controlled.

A.10.1.3
Segregation of duties
Control
Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

A.10.1.4 Separation of development, test and operational facilities
Control
Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.

A.10.2 Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

A.10.2.1

Service delivery

Control

It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

A.10.2.2 Monitoring and review of third party services

Control

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

A.10.2.3 Managing changes to third party services

Control

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

A.10.3 System planning and acceptance

Objective: To minimize the risk of systems failures.

A.10.3.1

Capacity management

Control

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

A.10.3.2

System acceptance

Control

Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

A.10.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

A.10.4.1 Controls against malicious code

Control

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

A.10.4.2 Controls against mobile code

Control

Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.

A.10.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

A.10.5.1

Information back-up

Control

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

A.10.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

A.10.6.1

Network controls

Control

Networks shall 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.

A.10.6.2

Security of network services

Control

Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

A.10.7 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

A.10.7.1 Management of removable media

Control

There shall be procedures in place for the management of removable media.

A.10.7.2
Disposal of media
Control
Media shall be disposed of securely and safely when no longer required, using formal procedures.

A.10.7.3 Information handling procedures
Control
Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.

A.10.7.4 Security of system documentation
Control
System documentation shall be protected against unauthorized access.

A.10.8 Exchange of information

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

A.10.8.1 Information exchange policies and procedures
Control
Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.

A.10.8.2
Exchange agreements
Control
Agreements shall be established for the exchange of information and software between the organization and external parties.

A.10.8.3
Physical media in transit
Control
Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

A.10.8.4
Electronic messaging
Control
Information involved in electronic messaging shall be appropriately protected.

A.10.8.5 Business information systems
Control
Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

A.10.9 Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

A.10.9.1
Electronic commerce
Control
Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

A.10.9.2
On-line transactions
Control
Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

A.10.9.3 Publicly available information
Control
The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.

A.10.10 Monitoring

Objective: To detect unauthorized information processing activities.

A.10.10.1
Audit logging
Control
Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

A.10.10.2
Monitoring system use
Control
Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.

A.10.10.3
Protection of log information
Control
Logging facilities and log information shall be protected against tampering and unauthorized access.

A.10.10.4 Administrator and operator logs
Control
System administrator and system operator activities shall be logged.

A.10.10.5
Fault logging
Control
Faults shall be logged, analyzed, and appropriate action taken.

A.10.10.6
Clock synchronization
Control
The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

A.11 Access control

A.11.1 Business requirement for access control

Objective: To control access to information.

A.11.1.1
Access control policy
Control
An access control policy shall be established, documented, and reviewed based on business and security requirements for access.

A.11.2 User access management

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

A.11.2.1
User registration
Control
There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

A.11.2.2
Privilege management
Control
The allocation and use of privileges shall be restricted and controlled.

A.11.2.3
User password management
Control
The allocation of passwords shall be controlled through a formal management process.

A.11.2.4
Review of user access rights
Control
Management shall review users' access rights at regular intervals using a formal process.

A.11.3 User responsibilities

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

A.11.3.1
Password use
Control
Users shall be required to follow good security practices in the selection and use of passwords.

A.11.3.2
Unattended user equipment
Control
Users shall ensure that unattended equipment has appropriate protection.

A.11.3.3 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 shall be adopted.

A.11.4 Network access control

Objective: To prevent unauthorized access to networked services.

A.11.4.1 Policy on use of network services
Control
Users shall only be provided with access to the services that they have been specifically authorized to use.

A.11.4.2 User authentication for external connections
Control
Appropriate authentication methods shall be used to control access by remote users.

A.11.4.3 Equipment identification in networks
Control
Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

A.11.4.4 Remote diagnostic and configuration port protection
Control
Physical and logical access to diagnostic and configuration ports shall be controlled.

A.11.4.5
Segregation in networks
Control
Groups of information services, users, and information systems shall be segregated on networks.

A.11.4.6
Network connection control
Control
For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).

A.11.4.7
Network routing control
Control
Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

A.11.5 Operating system access control

Objective: To prevent unauthorized access to operating systems.

A.11.5.1
Secure log-on procedures
Control
Access to operating systems shall be controlled by a secure log-on procedure.

A.11.5.2 User identification and authentication
Control
All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

A.11.5.3 Password management system
Control
Systems for managing passwords shall be interactive and shall ensure quality passwords.

A.11.5.4
Use of system utilities
Control
The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A.11.5.5
Session time-out
Control
Inactive sessions shall shut down after a defined period of inactivity.

A.11.5.6
Limitation of connection time
Control
Restrictions on connection times shall be used to provide additional security for high-risk applications.

A.11.6 Application and information access control

Objective: To prevent unauthorized access to information held in application systems.

A.11.6.1 Information access restriction
Control
Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

A.11.6.2
Sensitive system isolation
Control
Sensitive systems shall have a dedicated (isolated) computing environment.

A.11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

A.11.7.1 Mobile computing and communications
Control
A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

A.11.7.2
Teleworking
Control
A policy, operational plans and procedures shall be developed and implemented for teleworking activities.

A.12 Information systems acquisition, development and maintenance

A.12.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

A.12.1.1 Security requirements analysis and specification
Control
Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

A.12.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.

A.12.2.1
Input data validation
Control
Data input to applications shall be validated to ensure that this data is correct and appropriate.

A.12.2.2 Control of internal processing
Control
Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

A.12.2.3
Message integrity
Control
Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

A.12.2.4
Output data validation
Control
Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

A.12.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

A.12.3.1 Policy on the use of cryptographic controls
Control
A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A.12.3.2
Key management
Control
Key management shall be in place to support the organization’s use of cryptographic techniques.

A.12.4 Security of system files

Objective: To ensure the security of system files.

A.12.4.1 Control of operational software
Control
There shall be procedures in place to control the installation of software on operational systems.

A.12.4.2 Protection of system test data
Control
Test data shall be selected carefully, and protected and controlled.

A.12.4.3 Access control to program source code
Control
Access to program source code shall be restricted.

A.12.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

A.12.5.1
Change control procedures
Control
The implementation of changes shall be controlled by the use of formal change control procedures.

A.12.5.2 Technical review of applications after operating system changes
Control
When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

A.12.5.3 Restrictions on changes to software packages
Control
Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

A.12.5.4
Information leakage
Control
Opportunities for information leakage shall be prevented.

A.12.5.5 Outsourced software development
Control
Outsourced software development shall be supervised and monitored by the organization.

A.12.6 Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

A.12.6.1 Control of technical vulnerabilities
Control
Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

A.13 Information security incident management

A.13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

A.13.1.1 Reporting information security events
Control
Information security events shall be reported through appropriate management channels as quickly as possible.

A.13.1.2 Reporting security weaknesses
Control
All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

A.13.2 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

A.13.2.1 Responsibilities and procedures
Control
Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

A.13.2.2 Learning from information security incidents
Control
There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

A.13.2.3
Collection of evidence
Control
Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

A.14 Business continuity management

A.14.1 Information security aspects of 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 resumption.

A.14.1.1
Including information security in the business continuity management process
Control
A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

A.14.1.2 Business continuity and risk assessment
Control
Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

A.14.1.3
Developing and implementing continuity plans including information security
Control
Plans shall 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.

A.14.1.4 Business continuity planning framework
Control
A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

A.14.1.5 Testing, maintaining and reassessing business continuity plans
Control
Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

A.15 Compliance

A.15.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

A.15.1.1 Identification of applicable legislation
Control
All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.

A.15.1.2 Intellectual property rights (IPR)
Control
Appropriate procedures shall 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.

A.15.1.3 Protection of organizational records
Control
Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

A.15.1.4 Data protection and privacy of personal information
Control
Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

A.15.1.5 Prevention of misuse of information processing facilities
Control
Users shall be deterred from using information processing facilities for unauthorized purposes.

A.15.1.6 Regulation of cryptographic controls
Control
Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

A.15.2 Compliance with security policies and standards, and technical compliance

Objective: To ensure compliance of systems with organizational security policies and standards.

A.15.2.1 Compliance with security policies and standards
Control
Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

A.15.2.2 Technical compliance checking
Control
Information systems shall be regularly checked for compliance with security implementation standards.

A.15.3 Information systems audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

A.15.3.1 Information systems audit controls
Control
Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.

A.15.3.2 Protection of information systems audit tools
Control
Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.