ISO/IEC 27001:2013 Information security management systems

Information – important asset that needs to be protected

ISO/IEC 27001 – a systematic framework to manage information security related risks and protect important information

ISO/IEC 27001 – requirements for an ISMS (Information Security Management System)
Annex A – list of control objectives and controls for information security

ISO/IEC 27002 – guidance for the implementation of controls in Annex A of ISO/IEC 27001

ISO/IEC 27001:2013 Information security management systems
- Information security concept-

Information security - the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information (Wikipedia)

Confidentiality
Information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity
To maintain and assure the accuracy and completeness of data over its entire life-cycle. Data cannot be modified in an unauthorized or undetected manner.

Availability
Information is available when needed.
For information to be available it means that the computing systems that process the information and the communication channels through which information is being sent are working correctly.

ISO/IEC 27001:2013 Information security management systems
- Information security concept-

Risk - the likelihood of something happening

Risk management - the process of identifying information security risks, evaluating them and dealing with risks

Threat – anything that can harm an information asset (it can be man-made or a natural event)

Vulnerability - a weakness that can be used to harm an information asset.

Information asset – content of valuable information and the hardware or software where it is contained

ISO/IEC 27001:2013 Information security management systems
- ISO 27k family-

ISO 27000 family of standards:

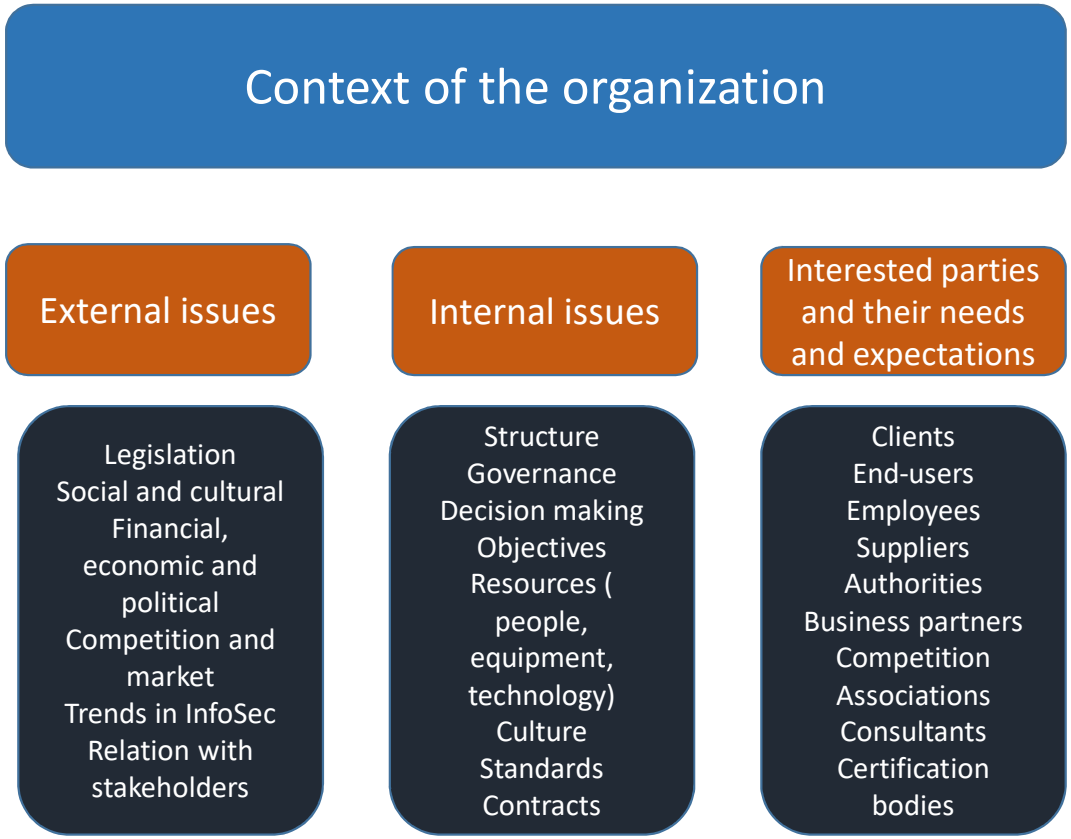
ISO/IEC 27001 –specifies the requirements for an ISMS
ISO/IEC 27002 –guideline for the implementation of the controls in Annex A

ISO/IEC 27000 – a general overview of information security and terms and definitions
ISO/IEC 27003 –general guidance for the implementation of an ISMS
ISO/IEC 27004 –advice on how organizations can monitor and measure the performance of their ISMS
ISO/IEC 27005 –guidance on risk management and
ISO/IEC 27006 –for audit and certification of ISMS
ISO/IEC 27007 - guideline on how to audit an ISMS
-sector specific -
ISO/IEC 27011 –application of security controls in telecommunication
ISO/IEC TR 27015 –information security management in financial services

… and others

ISO/IEC 27001:2013 Information security management systems

- Context of the organization-



ISO/IEC 27001:2013 Information security management systems
- Scope of the ISMS-

Scope = boundaries and applicability of the ISMS

Scope needs to be documented.

Scope can be limited to only parts of the organization or it can cover the whole organization.

What to take into consideration when defining the scope:
- Internal and external issues
- Needs and expectations of interested parties
- Interfaces and dependencies between activities of the organization and activities of others (suppliers, subcontractors, etc)

ISO/IEC 27001:2013 Information security management systems

- Leadership and commitment-

Top management needs to demonstrate leadership & commitment with respect to the ISMS.

Management support is vital for the ISMS

ISO/IEC 27001:2013 Information security management systems
- Leadership and commitment-

How?

- Ensure ISMS policy and objectives are established;
- Ensure information security is integrated with the business processes
- Provide resources for the ISMS
- Communicate on the importance of information security
- Monitor the management system
- Provide an example by promoting continual improvement
- Support others to demonstrate leadership

ISO/IEC 27001:2013 Information security management systems
- Information security policy-

Information security policy:

- Appropriate to the purpose
- Includes objectives or offer a framework to set them
- Includes a commitment to satisfy applicable security requirements
- Includes a commitment for continual improvement

Information security policy should be:
- documented;
- communicated inside the organization;
- available to interested parties (as needed).

ISO/IEC 27001:2013 Information security management system

- Organizational roles, responsibilities and authorities-

Top management should ensure that responsibilities and authorities relevant to information security are assigned and communicated to staff.

Nominate a person (structure) responsible for the ISMS:

- Ensure that the ISMS conforms to the requirements of ISO/IEC 27001;
- Report to top management about the performance of the ISMS

ISO/IEC 27001:2013 Information security management systems
- Information security risk assessment-

The organization is required to develop and apply a risk assessment process.

1. Start from information assets and try to identify the threats and vulnerabilities related to the assets

2. Evaluate impact if the confidentiality, integrity or availability of the information are compromised

3. Calculate the likelihood (or probability) of an event happening

4. Estimate the level of risk as a combination of impact and likelihood

5. Assign risk owners

6. Define what is considered acceptable risk and what is not acceptable

ISO/IEC 27001:2013 Information security management systems

- Information security risk assessment-

Asset	Threat	Vulnerabilities	Impact	Likelihood (probability)	Risk level	Acceptable? Y/N	Risk Owner
Information stored on mobile devices	Theft	No access security control (password or Touch ID). No settings for installed for remote wiping of data	Estimation of the damages	How probable is this to happen	Impact x Likelihood		

ISO/IEC 27001:2013 Information security management systems
- Information security risk assessment-

Estimation of impact, likelihood and risk level:

Qualitative – use levels (ex. "high", "low", "medium“)
Quantitative - use numbers
Semi-quantitative - using numerical ratings to generate a level

Establish criteria:
Acceptable risk / Not acceptable risk

Risk owners- persons (structures) who are accountable for the management of the management of the risk

ISO/IEC 27001:2013 Information security management systems

- Information security risk assessment-

Risk assessment is subjective!

…but you should create a list of risks as comprehensive as possible

ISO standards on risk assessment:
ISO 31000, IEC 31010, ISO/IEC 27005

Risk assessment should be documented

ISO/IEC 27001:2013 Information security management systems

- Information security risk treatment-

Possible options to treat risks:

- avoid the risk;
- control the risk and reduce risk level;
- transfer the risk;
- accept the risk;
- or a combination of those

The choice belongs to the organization and should be balanced taking into account resources and impact.

ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

Statement of Applicability - SoA

"the organization shall produce a Statement of Applicability"

SoA - is the map of implementation of the ISMS.
Includes all the controls, their justification for inclusion, whether they are implemented or not and justification for excluding any controls from the Annex A (of ISO/IEC 27001).

SoA should be revised as the activities of the organization suffer changes

ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

RiG CERT

Statement of applicability

No	Controls	Detailed	Justification for inclusion	Justification for exclusion	Implemented Y/N	Evidence of implementation
5.1.1.	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties	To define the expected levels of controls	-	Y	Documented policies - in the IS Manual Information security policy_code__ Access control policy_code, etc...
5.1.2.	Review of policies for information security		To ensure IS policies stay up to date	-	Y	The review of policies is done during management review (evidence kept in the management review minute)
14.2.6.	Secure developme nt policy	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle	-	Our organization does not develop information systems	N	-

ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

Risk treatment plan

The Risk Treatment Plan should include:

- the risk that is being addressed and its level according to the assessment;
- the actions proposed to treat the risk;
- who is in charge with implementing the actions;
- resources (budget);
- timeframe for implementation.

ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

Residual risk

The remaining risk after treatment actions are applied.
Residual risk needs to be evaluated similar to the initial process to see if it falls into the acceptable category.
If not, new treatment should be decided.

Obtain the approval of the risk owners for the risk treatment plan as well as for the residual risks

Risk treatment has to be documented.

ISO/IEC 27001:2013 Information security management systems
- Information security objectives-

Information security objectives:

- consistent with the information security policy;
- measurable (if practicable);
- take into account information security requirements, risk assessment and risk treatment;
- communicated and updated.

Information security objectives have to be documented.

ISO/IEC 27001:2013 Information security management systems
- Information security objectives-

The organization should develop plans for achieving objectives:

- what will be done
- what resources are required
- who is responsible
- what is the timeframe for accomplishment and
- how the results will be evaluated.

Achievement should be monitored.

ISO/IEC 27001:2013 Information security management systems
- Competence & Awareness-

Competence

The organization is required to:
- determine the necessary competence of persons whose work may affect information security;
- ensure that these persons are competent;
- take actions to acquire the needed competence and evaluate the effectiveness of those actions and
- retain appropriate documented information as evidence of competence

ISO/IEC 27001:2013 Information security management systems
- Competence & Awareness-

Personnel involved with the ISMS should:

- have knowledge about ISO/IEC 27001 standard;
- have an understanding of the security concepts, techniques, policies and procedures;
- know about risk assessment and risk treatment processes including the controls of Annex A and the guidelines provided by ISO/IEC 27002;
- understand the security requirements for the technology used.

ISO/IEC 27001:2013 Information security management systems
- Competence & Awareness-

Actions to raise competence:

- recruiting competent personnel;
- providing access to education and training on information security related matters;
- encouraging self-study;
- mentoring.

To be able to demonstrate competence of its personnel the organization shall retain documented information.

ISO/IEC 27001:2013 Information security management systems
- Competence & Awareness-

Awareness:

An awareness program to make people aware of:

- the information security policy;
- their personal contribution the ISMS and the benefits of improved security performance and
- the implications of not conforming with information security requirements

ISO/IEC 27001:2013 Information security management systems
- Competence & Awareness-

Awareness is key in improving the security level and make people see information security as an integral part of their day-to-day operations.

Awareness activities:
- training,
- posting on the social media of the organization,
- events like "information security day",
- newsletters, etc

Awareness activities should take place periodically and awareness topics should be in line with business needs.

ISO/IEC 27001:2013 Information security management systems
- Communication-

The organization shall determine the need for internal and external communications relevant to the ISMS.

Determine:
- on what to communicate;
- when to communicate;
- with whom to communicate;
- who shall communicate and
- the process by which communication shall be effected

The organization should have adequate communication channels.

ISO/IEC 27001:2013 Information security management systems

- Documented information-

Size of ISMS documentation depends on:

- size,
- activities,
- complexity of processes,
- products and services,
- competence of personnel.

ISO/IEC 27001:2013 Information security management systems
- Documented information-

Mandatory documents for the ISMS:

- the scope of the ISMS;
- information security policy and lower level policies;
- information security risk assessment and risk treatment;
- information security objectives;
- Statement of Applicability
- documented information on the results of monitoring and measuring performance and effectiveness of the ISMS;
- internal audit, management reviews, nonconformities and corrective actions

ISO/IEC 27001:2013 Information security management systems
- Documented information-

Creating and updating

- Identification and description (name, reference number, date, author)
- Format and media.

ISMS documents have to be reviewed and approved.

ISO/IEC 27001:2013 Information security management systems
- Documented information-

Controls for documented information refer to:

- making documents available in suitable format when needed;
- protect documented information from loss of confidentiality, improper use, loss of integrity;
- control the versions and ensure that only current versions are in use and obsolete documents are withdrawn;
- access controls;
- retention periods (and format).

ISO/IEC 27001:2013 Information security management systems
- Operational planning and control-

The organization shall plan, implement and control the processes needed to meet information security requirements and to implement the actions that were decided following the risk assessment and risk treatment processes.

The organization shall have a change management process – to handle changes in a controlled way.

Changes – should be planned with a review of consequences and risks involved.
Unintended changes – consequences should be reviewed and actions taken to mitigate undesired effects

In case of changes - perform risk assessments to evaluate new or modified risks and decide on risk treatment actions

ISO/IEC 27001:2013 Information security management systems
- Monitoring, measurement, analysis and evaluation-

The organization has to evaluate its information security performance and the effectiveness of the ISMS.
(*it is completely up to the organization to decide what it chooses to monitor and measure*)

Examples of what can be monitored and measured:

- information security events and out of them how many have been information security incidents;
- accomplishment of information security objectives;
- reported security vulnerabilities.

ISO/IEC 27001:2013 Information security management systems
- Monitoring, measurement, analysis and evaluation-

The information collected through monitoring and measurement has to be analyzed and evaluated to see what can be improved.

The organization shall retain documented information as evidence of monitoring, measuring, analysis and evaluation.

ISO/IEC 27004 - guidelines in evaluating the information security performance and the effectiveness of an ISMS.

ISO/IEC 27001:2013 Information security management systems
- Internal audit-

Organizations shall perform internal audits of the ISMS at planned intervals.

Internal audit programme – schedule of internal audits for a period of time.
For the development of internal audit programme the organization should take into consideration:

- importance of activities and processes;
- results of previous audits;
- security incidents;
- security performance.

ISO/IEC 27001:2013 Information security management systems
- Internal audit-

For each internal audit:

- Scope - what activities and locations are to be audited
- Criteria – ISO/IEC 27001, information security policies, internal regulations, legislation requirements, contract requirements, etc.

Auditors have knowledge of:

- information security terminology and principles,
- risk management,
- the security controls and techniques,
- current security threats and vulnerabilities,
- relevant legislation with regards to information security and of course
- the requirements of ISO/IEC 27001 including the controls from Annex A

Auditors should be independent from activities being audited

ISO/IEC 27001:2013 Information security management systems
- Internal audit-

Results of the audit – Audit report – Communicated to top management

Nonconformities should be managed – with corrections and corrective actions.

The organization should retain documented information as evidence of performing internal audits.

ISO/IEC 27001:2013 Information security management systems
- Management review-

Top management shall review at planned intervals the ISMS to ensure it continues to be suitable, adequate and effective.

<u>Input data:</u>

- actions from previous management reviews;
- changes in the organizational context;
- feedback on information security aspects;
- feedback from interested parties;
- the results of risk assessments and the status of the risk treatment plan and
- opportunities for improvement.

ISO/IEC 27001:2013 Information security management systems
- Management review-

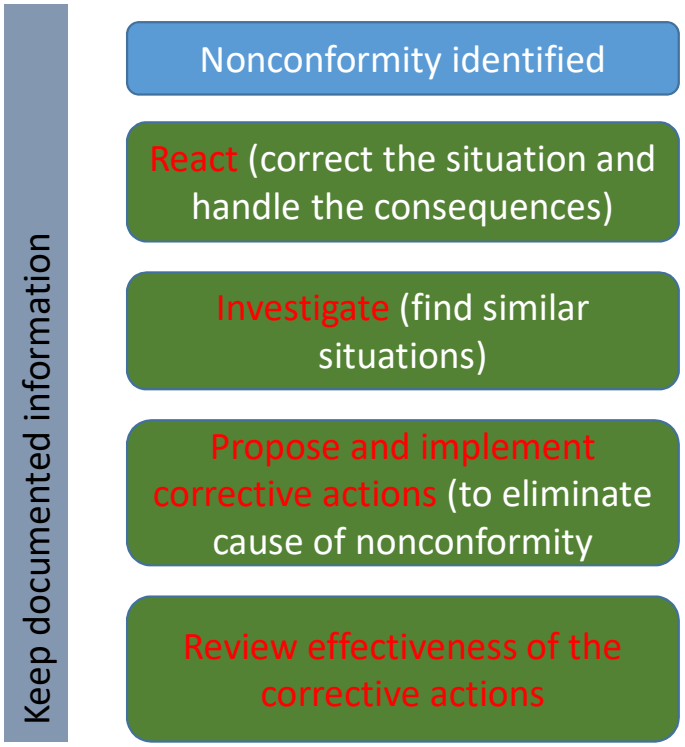
Output data:

- opportunities for the improvement of the ISMS;
- the need for changes to the ISMS.

Documented evidence as evidence of management review meetings shall be retained

ISO/IEC 27001:2013 Information security management systems
- Nonconformity and corrective action-

Nonconformity – non-fulfillment of a requirement.



ISO/IEC 27001:2013 Information security management systems

Controls listed in Annex A to ISO/IEC 27001:2013

14 security clauses:

Information security policies
Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operations security
Communications security
System acquisition, development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance

ISO/IEC 27001:2013 Information security management systems

Each security clause includes one or more security categories

35 security categories

Each security category includes one or more security controls

114 security controls

ISO/IEC 27001:2013 Information security management systems
-Management direction for information security-

Security category – 5.1. Management direction for information security

Control – 5.1.1. Policies for information security
The organization should define, publish and communicate to its employees and to any external parties as needed a set of information security policies.

First level – Information security policy
(definition of information security, the objectives and principles; reasoning for the ISMS; information security is actively supported by management; responsibilities for information security in the organization; references to lower level policies, regulations, manuals; how any deviations from the policy are to be handled by the management; etc)

Information security policy – communicated to staff, persons working for organization and external parties

ISO/IEC 27001:2013 Information security management systems
-Management direction for information security-

Lower level – Specific policies

- Access control,
- Information classification
- Physical and environmental security
- Acceptable use of resources
- Clear desk and clear screen
- Information transfer
- Mobile devices and teleworking
- Restrictions on software installation and use
- Backup
- Protection from malware
- Management of technical vulnerabilities
- Cryptographic controls
- Communications security
- Privacy and protection of personally identifiable information
- Supplier relationships

Its best if the policies are simple and easy to understand

ISO/IEC 27001:2013 Information security management systems
-Management direction for information security-

Control – 5.1.2. Review of policies for information security
The organization should review periodically the policies for information security to make sure they continue to be suitable, adequate and effective.

This review process – should take into consideration changes to the business environment, to legal requirements, to technology, to internal organization.

Whenever circumstances change the information security policies should be updated to reflect the new conditions

ISO/IEC 27001:2013 Information security management systems
-Roles, responsibilities and segregation of duties-

Security category – 6.1. Internal organization

Control – 6.1.1. Information security roles and responsibilities
The responsibilities for information security have to be defined and allocated.

Roles and responsibilities for all personnel should be defined and clearly communicated.

Explain to individuals in the organization what is expected of them.

All staff should have a basic responsibility for security included in job descriptions and should understand their security responsibility.

Information security manager – ok, but not enough.

ISO/IEC 27001:2013 Information security management systems
-Roles, responsibilities and segregation of duties-

Control – 6.1.2. Segregation of duties
There should be measures in place so that duties and areas of responsibility that are in conflict be segregated.

Segregation - reduces opportunities for unauthorized or unintentional modification of misuse of assets.

Principles:

- initiation of an event should be separated from its authorization;
- no single person should be able to access, modify or use assets without authorization or detection

ISO/IEC 27001:2013 Information security management systems

-Roles, responsibilities and segregation of duties-

Dividing the job between 2 or more staff provides a system of verification of one by the other (ex. 2 keys or passwords).

Barings bank collapse – classical example of a lack of segregation of duties (https://en.wikipedia.org/wiki/Barings_Bank)

Segregation of duties – more difficult to implement for small companies (if its not possible record all activities and to review the records independently to identify suspicious or unauthorized activity)

ISO/IEC 27001:2013 Information security management systems

-Contact with authorities and special interest groups-

Control – 6.1.3. Contact with authorities

The organization is required to maintain contacts with relevant authorities.

Procedures to specify:

- when authorities should be contacted
- by whom
- how security incidents should be reported to authorities (if required).

Nominate a person – in charge with contacts with authorities

ISO/IEC 27001:2013 Information security management systems

-Contact with authorities and special interest groups-

Control – 6.1.4. Contact with special interest groups

Contacts with security forums or any other forms of interest groups or associations specific to information security should be kept.

Benefits of memberships:

- improve knowledge on best practices
- gain an understanding of the information security environment
- receive warnings for security alerts
- get advice on security matters.

ISO/IEC 27001:2013 Information security management systems

-Contact with authorities and special interest groups-

Control – 6.1.5. Information security in project management
The organization needs to include information security in project management never mind the type of project.

Information security should be integrated into the organization's project management to ensure that security risks are identified and addressed as part of the projects.

2 risk assessments are recommended:
- one to consider the risks related to the activities of the project and
- the other to cover the risks related to the results.

Responsibilities for information security should be defined and allocated for each project

ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Security category – 6.2. Mobile devices and teleworking

Control – 6.2.1. Mobile devices policy
The organization should have a policy and security measures in place to manage risks associated to mobile devices use.

Mobile devices policy should consider:
- registration of mobile devices
- physical protection of mobile devices
- restrictions on software installation
- mobile device software versions and for applying patches
- restriction of connection to information services
- access controls
- cryptographic techniques
- malware protection
- remote disabling, erasure or lockout
- backups
- use of web services and apps

ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Care should be exercised when using mobile devices in public places.

Mobile devices should be protected physically against theft.

Users should be trained on the security measures for mobile devices.

In case of remote connections to the organization's site or databases the authentication should cover not only the device but also for the user.

When using private devices for business purposes:
- separate business and private use of the devices (ex. with a software)
- give access to business information only after the user has signed an agreement acknowledging duties, waiving the ownership of business data and allowing remote wiping of data by the organization in case of theft or loss of the device

ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Control – 6.2.2. Teleworking
The organization should have a policy and security measures implemented to protect information that is accessed, is processed or stored at teleworking sites.

Teleworking = “remote work” or “flexible workplace”, or “virtual work”

Decide whether to allow private owned equipment for teleworking or provide equipment.

Define a policy – conditions and restrictions for teleworking

ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Conditions and restrictions on teleworking (ISO/IEC 27002 guidelines):

- physical security of the location;
- permissions (hours of work, the information and services);
- communication security;
- use of virtual desktop access;
- potential for unauthorized access (ex. family, friends, visitors)
- use of home networks and restrictions;
- possible need to obtain access to privately owned equipment;
- software licensing;
- malware protection and firewall;
- hardware and software maintenance
- backup and business continuity;
- revocation of authority and access rights

ISO/IEC 27001:2013 Information security management systems

-HR Security – Prior to employment-

Security category – 7.1. Prior to employment

Control – 7.1.1. Screening

There have to be background checks for all candidates for employment done in accordance with the legislation and ethics. The checks are to be proportional to the sensitivity of the information to be accessed by the employee, the risks involved and the business requirements.

Screening is meant to prevent the organization hiring the wrong person.

There have to be procedures for screening:

- *criteria and limitations;*
- *who is eligible to screen people;*
- *how is screening performed and when;*
- *why perform verifications.*

ISO/IEC 27001:2013 Information security management systems

-HR Security – Prior to employment-

Screening should respect legislation (privacy, personally identifiable information and employment legislation).

Screening may include:

- character references;
- verification of the CV;
- confirmation of claimed academic and professional qualifications;
- independent verification of identity of the candidate;
- more detailed review (such as credit review, review of criminal records).

The level of detail for the verifications during screening are correlated with the access held by the individual to confidential information.

Screening applies employees, contractors, third-party users.

ISO/IEC 27001:2013 Information security management systems

-HR Security – Prior to employment-

Control – 7.1.2. Terms and conditions of employment

The responsibilities of employees and contractors for information security as well as the responsibilities of the organization should be documented in the contractual agreements.

ISO/IEC 27002 guidelines for the terms and conditions of employment:

- all individuals who have access to confidential information have to sign a confidentiality or non-disclosure agreement before accessing information;
- what are the employee's legal responsibilities and rights, (ex. with regards to copyright legislation, privacy and protection of personally identifiable information, etc)
- responsibilities for the classification of information and management of organizational assets handled by the employee or contractor;
- actions that can be taken by the organization in case the employee disregards security requirements.

ISO/IEC 27001:2013 Information security management systems
-HR Security – During employment-

Security category – 7.2. During employment

Control – 7.2.1. Management responsibilities
The employees and contractors shall be required by the management to apply information security according to the policies and procedures of the organization.

Management should make sure that employees and contractors:

- are informed of their information security roles and responsibilities before obtaining access to confidential information;
- are informed on the information security expectations for their roles
- are motivated to fulfil the security policies;
- receive awareness on information security;
- conform to the terms and conditions of employment;
- are trained regularly to be able to keep skills and qualification up to date;
- can report anonymously violations of security policies and procedures.

Management should exercise control and check the compliance with policies, procedures and regulations in the day-to-day work.

ISO/IEC 27001:2013 Information security management systems

-HR Security – During employment-

Control – 7.2.2. Information security awareness, education and training

There has to be appropriate awareness and training on information security aspects for all employees and contractors as relevant for their positions.

Untrained individuals are a risk for information security.

The organization should develop a security awareness programme to make individuals aware of their responsibilities for information security and how they should act.

All personnel should be trained on information security procedures and policies and on the use of equipment and software relevant to their jobs (internal or external training).

ISO/IEC 27001:2013 Information security management systems

-HR Security – During employment-

Control – 7.2.3. Disciplinary process

The organization should develop and enforce a disciplinary process to be applied in case of security breaches committed by employees. The disciplinary process has to be formal and communicated.

Non-compliance with security policies or controls needs to be dealt with properly.

<u>The disciplinary process:</u>

- shall ensure the treatment is fair and correct and
- shall not commence without prior verification and confirmation that a security breach has occurred
- should provide for a graduated response.

Employees have to be informed about the disciplinary process

ISO/IEC 27001:2013 Information security management systems

-HR Security – Termination or change of employment-

Security category – 7.3. Termination or change of employment

Control – 7.3.1. Termination or change of employment responsibilities
The organization has to define and communicate to its employees and its contractors their duties and responsibilities related to information security that remain valid after their employment is terminated or changed.

Termination or change of employment not handled correctly may cause security problems.

Aspects on termination or change of employment:
- ensure logical and physical access rights are removed;
- ensure equipment belonging to the organization is returned;
- responsibilities and duties valid after termination should be included in the terms and conditions of employment (ex. confidentiality).

Change of employment = termination of a job and beginning of another.

ISO/IEC 27001:2013 Information security management systems
-Responsibility for assets-

Security category – 8.1. Responsibility for assets

Control – 8.1.1. Inventory of assets
The organization has to identify all assets associated with information and information processing facilities and should create and establish an inventory of assets.

The inventory is expected to include:
- physical assets - equipment identity, location, maker, model, serial number and inventory tag
- documentation - including system documentation, contracts, procedures and business continuity plans, etc
- software products - including licensing information and where they are used
- services - including utilities.

Asset inventory should be kept up to date.

ISO/IEC 27001:2013 Information security management systems
-Responsibility for assets-

Control – 8.1.2. Ownership of assets
Assets should have owners.

Ownership should be assigned to assets.
The asset owner (individual or entity) is responsible for the asset protection.

Asset owner should:
- ensure that asset is included in the inventory;
- ensure that the asset is appropriately protected;
- define and review access restrictions to the asset;
- ensure proper handling when the asset is deleted or destroyed.

ISO/IEC 27001:2013 Information security management systems
-Responsibility for assets-

Control – 8.1.3. Acceptable use of assets
The organization should identify, document and implement rules for the acceptable use of assets associated with information and information processing facilities

Individuals should be made aware of the security requirements associated with the assets and should be responsible for the use of the resources.

Organizations are vulnerable to misuse of their assets by employees – intentional or not – refers to use of assets in a way that is different than their business purposes.

There have to be rules describing the acceptable use or resources and users should be made aware of the rules and agree with them.

ISO/IEC 27001:2013 Information security management systems
-Responsibility for assets-

Control – 8.1.4. Return of assets
Upon termination of employment, contract or agreement the users should return the assets belonging to the organization

Procedures should ensure assets are returned when the job is terminated.

If the employee purchases the organization's equipment or if it uses its own personal equipment for business purposes - rules should be in place to ensure that relevant information is transferred to the organization and the equipment is securely erased.

ISO/IEC 27001:2013 Information security management systems
-Information classification-

Security category – 8.2. Information classification

Control – 8.2.1. Classification of information
Information needs to be classified taking into consideration legal requirements, value of the information, criticality and sensitivity to unauthorized disclosure or modification.

The organization has to develop a classification scheme.
Owners of information assets are accountable for their classification.

Recommended to have an easy to understand classification scheme.

Classification should be done by taking into consideration the level of protection needed to ensure the confidentiality, integrity and availability of information.

The classification scheme has to be consistent across the whole organization.

ISO/IEC 27001:2013 Information security management systems
-Information classification-

ISO/IEC 27002 provides an example of classification scheme that uses 4 levels:

Public - disclosure causes no harm.

Internal use - disclosure causes minor embarrassment or minor operational inconvenience.

Confidential - disclosure has a significant short term impact on operations or tactical objectives.

Top secret - disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

ISO/IEC 27001:2013 Information security management systems
-Information classification-

Control – 8.2.2. Labelling of information
Starting from the classification scheme the organization should develop procedures for the labelling of information.

Labelling reflect the level of classification.

Procedures for information labelling need to cover information and its related assets in physical and electronic formats.

Employees and contractors should be made aware of the labelling procedures.

When receiving information from other organizations - care should be given to the labels of documents as other organizations may have different definitions for same labels.

ISO/IEC 27001:2013 Information security management systems
-Information classification-

Control – 8.2.3. Handling of assets
The organization should implement procedures for the handling of assets in line with the classification scheme.

Procedures for asset handling are meant to prevent the risk of sensitive information being mishandled and should detail:

- access restrictions for each level of classification;
- protection of copies (temporary or permanent) in the same way as the originals;
- storage requirements according to the classification level;
- declassification and destruction according to classification

ISO/IEC 27001:2013 Information security management systems
-Media handling-

Security category – 8.3. Media handling

Control – 8.3.1. Management of removable media

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

Removable media (flash disks, removable hard drives, CDs, DVDs, printed media, etc) containing the organization's data presents a vulnerability to loss of data and breaches of confidentiality.

Controls implemented have to address issues like:

- using removable media only if there is a business reason to do so;
- storing media in safe and secure environments;
- contents of re-usable media to be removed from the organization should be made unrecoverable;
- the organization may use encryption of data on removable media;
- transfer useful data on fresh media to prevent media degrading in time;
- have multiple copies of valuable information on separate media.

ISO/IEC 27001:2013 Information security management systems
-Media handling-

Control – 8.3.2. Disposal of media
When no longer needed media shall be disposed of according to procedures.

Procedures for secure disposal reduce the risk of confidential information leakage to unauthorized persons.

ISO/IEC 27002 guidance on disposal of media:

- identify the items that require secure disposal;
- store and dispose securely media with confidential information (with methods like incineration, shredding, erasure of data - depending on the media);
- perform a careful selecting of the provider for collection and disposal services (if such a provider is used for the disposal of media);
- keep a log of the disposal of sensitive items.

ISO/IEC 27001:2013 Information security management systems
-Media handling-

Control – 8.3.3. Physical media transfer
Media that contains information has to be protected during transportation against unauthorized access, misuse or corruption.

Transportation of media = risks for loss, corruption, unauthorized access and misuse.

Guidelines for transportation of media:

- use of reliable couriers and make verification of courier identity
- use suitable packaging to protect the contents from physical damage and protection from environmental factors - like heat or electromagnetic fields;
- to mitigate the risk of breach of confidentiality if media are lost or stolen - data to be transported should be encrypted and of course the encryption key should never be sent together with the encrypted data.

ISO/IEC 27001:2013 Information security management systems

-Business requirements for access control-

Security category – 9.1. Business requirements for access control

Control – 9.1.1. Access control policy

The organization should document an access control policy.

***Access control refers to both logical and physical access*.**

Access control rules, access rights and restrictions for specific user roles should be established.

Asset owners decide access rights to assets based on business needs

ISO/IEC 27001:2013 Information security management systems
-Business requirements for access control-

An access control policy should exist and should address some elements:

- security requirements for different business applications;
- consistency between access rights and information classification;
- legislation and contractual obligations regarding limitation of access to data or services;
- segregation of roles that refer to access control;
- periodic review of access rights;
- removal of access rights;
- roles that have privileged access.

Principles: ***Need–to–Know and Need-to-Use***

Use: "**Everything is generally forbidden unless expressly permitted**“
instead of
"**Everything is generally permitted unless expressly forbidden**"

ISO/IEC 27001:2013 Information security management systems

-Business requirements for access control-

Control – 9.1.2. Access to networks and network services

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

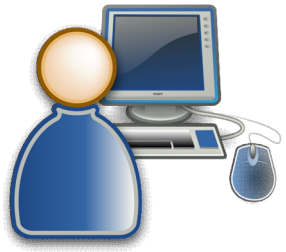
ISO/IEC 27002 recommends a policy on the access to networks that should cover:

- the networks and networks services which are allowed to be accessed;
- authorization procedures for determining who is allowed to access which networks and services;
- what controls are in place to protect access to networks and services;
- how are the networks and network services accessed (ex. use of VPN or wireless)
- what are the requirements for user authentication to allow access to networks and services;
- how the use of network services is monitored.

Users logging to a network, computer or application should have access only to the information and services required for their business function that they have been authorized to use.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Security category – 9.2. User access management



Control – 9.2.1. User registration and de-registration
There has to be a formal user registration and de-registration process to enable assignment of access rights.

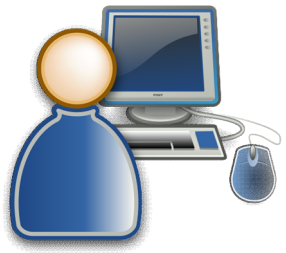
Every user should be formally authorized and registered to each information system, network or service that it accesses for the business needs.

Management of user IDs:

- use unique user IDs to enable users to be linked to their actions;
- immediately disable or remove user IDs of users who have left the organization;
- periodically identify and remove or disable redundant user IDs and
- ensure that redundant user IDs are not issued to other users.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.2. User access provisioning
The organization should implement a formal user access provisioning process to assign or to revoke access rights for all user types to all systems and services.



- the owner of the information system is responsible to approve or revoking of access rights to user IDs;
- access rights should not be activated before authorization;
- a central record of access rights granted to each user ID should be kept;
- access rights should be adapted for users who change roles or jobs and removed for users who left the organization.

An easier way to manage access rights is by using role based access - defining user profiles for different roles and positions in the organization.

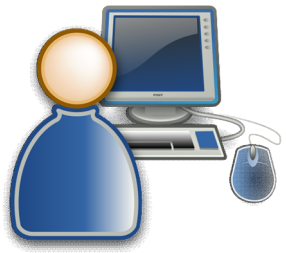
Define sanctions for unauthorized access

ISO/IEC 27001:2013 Information security management systems

-User access management-

Control – 9.2.3. Management of privileged access rights

The allocation of privileged access rights should be controlled and there should be a formal process for this.



Privileges = means to shortcut controls.

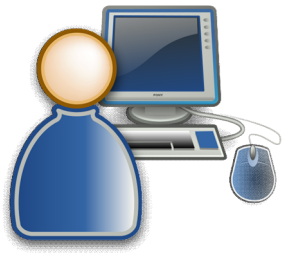
Unnecessary allocation and use of privileges may lead to to security breaches.

ISO/IEC 27002 recommendations on the allocation of privileged access rights:

- clear identification of privilege access rights and the users for every application, operating system, database; etc
- allocation of privileged access rights on a need-to-use basis and preferably on an event-by-event basis;
- use an authorization process for granting privileged access rights and not grant them until authorization is obtained;
- assign the privilege access rights to a user ID that is different from the ones used for regular business activities.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.4. Management of secret authentication information of users
There should be a formal process for the allocation of secret authentication information.



Secret authentication is done usually through passwords.

Requirements for allocation of secret authentication information:

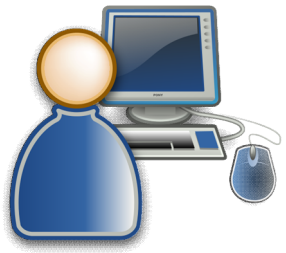
- users should be asked to sign a statement to keep personal secret authentication information (passwords) confidential;
- if the users select their own passwords - they should be provided initially with a temporary password that they should be forced to change;
- passwords should be given to users in a secure manner and users should acknowledge their receipt.

ISO/IEC 27001:2013 Information security management systems

-User access management-

Control – 9.2.5. Review of users access rights

Asset owners should periodically review user's access rights.

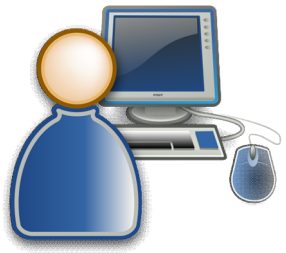


Access rights have to be based on business needs and when the business need changes or passes the access should be cancelled.

Periodically access rights should be reviewed and if found that some access rights are not needed they have to be withdrawn.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.6. Removal of users of access rights
At the end of employment or contract the access rights of employees or external parties should be removed. In case of changing positions the access rights should be adjusted.



If an employment is terminated the access rights associated should be removed.

If the user is part of a group – and access rights are allocated at group level – the individuals leaving should be removed from the group and the other members should be informed to no longer share information with the person departing.

ISO/IEC 27001:2013 Information security management systems

-User responsibilities-

Security category – 9.3. User responsibilities

Control – 9.3.1. Use of secret authentication information

The users are to be required to follow the organization's procedures for the use of secret authentication information.

Users need to be aware of the fact that they can be held accountable for someone else using their passwords.

ISO/IEC 27001:2013 Information security management systems

-User responsibilities-

ISO/IEC 27002 guidelines for users choosing and managing passwords:

- users should be advised to keep secret passwords confidential;
- avoid keeping a record of passwords (unless there is a password vault app);
- if possible compromise - change the password;
- advice users not to use the same password for both business and non-business purposes
- select quality passwords
    - sufficient length but be easy to remember;
    - not based on things easy to guess (name, birthdate),
    - not vulnerable to dictionary attacks.

Single Sign On – convenience (don't have to remember multiple passwords)
- security risk (in case it is compromised)

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Security category – 9.4. System and application access control

Control – 9.4.1. Information access restriction
Access to information and applications should be restricted in line with the access control policy.

Restrictions of access to information should be based on individual business requirements.

Some guidelines on the restriction requirements include:
- control the access of users in terms of what they can do - read, write, delete, execute;
- control which data can be accessed by each particular user;
- control the access rights of applications;
- provide menus to control access to application system functions.

ISO/IEC 27001:2013 Information security management systems

-System and application access control-

Control – 9.4.2. Secure log-on procedures

Access to systems and applications should be controlled with a secure log-on procedure.

The log-on procedure needs to be:

- ***easy to understand;***
- ***user-friendly;***
- ***must not give information about the system or application that the user is trying to access (before accessing it);***
- ***should minimize the opportunity for unauthorized access.***

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

ISO/IEC 27002 guidelines for a good log-on procedures:

a) not displaying system or application identifiers until the log-on is completed;
b) display a general notice warning that the computer should only be accessed by authorized users;
c) not providing help messages during the log-on;
d) validate the log-on information only on completion;
e) protect against brute force log-on attempts;
f) record unsuccessful and successful attempts;
g) raise a security event if a potential attempted or successful breach of log-on;
h) display the following information on completion of a successful log-on: date and time of the previous successful log-on; details of any unsuccessful log-on attempts;
i) do not display the password being entered;
j) do not transmit passwords in clear text over a network;
k) terminate inactive sessions after a defined period of inactivity;
l) restrict connection times to provide additional security for high-risk applications.

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Control – 9.4.3. Password management system
The organization should use interactive password management systems that ensure quality passwords.

A password management system should:

- enforce the use of individual user IDs and passwords to maintain accountability;
- allow users to select and change their own passwords and include a confirmation procedure;
- enforce a choice of quality passwords;
- force users to change their passwords at the first log-on;
- enforce regular password changes and as needed;
- maintain a record of previously used passwords and prevent the re-use of past passwords;
- not display passwords on the screen when being entered;
- store password files separately from application system data;
- store and transmit passwords in protected form.

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Control – 9.4.4. Use of privileged utility programs
The organization should restrict and strictly control the use of utility programs that are capable of overriding system and application controls.

Because utility programs may provide access to the parts of the system by overriding controls they can be a risk for security.

The use of such programs should be controlled:

- users have to be identified and authorized for their use and logs should be maintained;
- the use of utility programs should be limited to the minimum needed;
- utility programs should be segregated from application software and users should not have access to privilege functions from their normal user accounts.

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Control – 9.4.5. Access to program source code
Access to program source code should be restricted.

Unauthorized access to program source code can be a great opportunity for an intruder to modify the system.

Use of libraries – method to protect source code

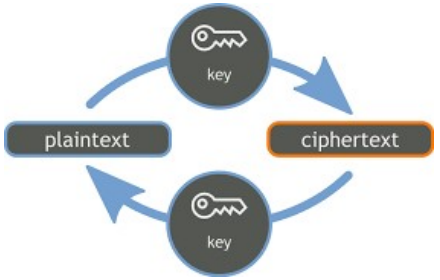
There are a few requirements for the source code libraries :

- as much as possible libraries should not be held in operational systems;
- there have to be some rules for the management of program source code and libraries where they are stored;
- the updating of program source libraries should only be done with authorization;
- all accesses to program source libraries should be logged;
- maintenance and copying of program source libraries should be subject to strict change control procedures.

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

Security category – 10.1. Cryptographic controls

Control – 10.1.1. Policy on the use of cryptographic controls
The organization should develop and implement a policy for the use of cryptographic controls.



Cryptography is a system of coding information so it can be accessible selectively.

Symmetric - uses a single key to encrypt and to decrypt data
Asymmetric - uses what is called "public key

The blog of Panayotis Vryonis offers a very clear, simple and easy to understand for non-technical people explanation of cryptography.
https://blog.vrypan.net/2013/08/28/public-key-cryptography-for-non-geeks/

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

Among the uses of cryptography:

- protecting information that goes out of the organization;
- limiting access to files or folders on the servers;
- protecting confidential information sent by e-mail;
- protecting passwords;
- securing payments;
- digital signatures, …

The decision whether to use or not cryptographic controls belongs to the organization and to its needs to protect the information.

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

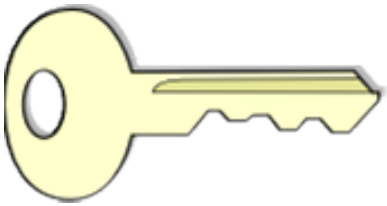
ISO/IEC 27002 recommends a policy for the use of cryptographic controls that should address a few aspects:

- general principles under which business information should be protected and the approach on the use of cryptographic controls;
- encryption algorithm used
- approach about using encryption for protection of information taken outside the organization;
- approach to key management – how are they protected and what happens in case keys are lost or compromised;
- responsibilities – who is in charge for the implementation of this policy and the management of the keys
- consistent implementation of the cryptographic controls throughout the whole organization

There are regulations and restrictions to the use of cryptographic controls that may exist in different countries and jurisdictions.

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

Control – 10.1.2. Key management
There should be a policy on the use, protection and lifetime of cryptographic keys.



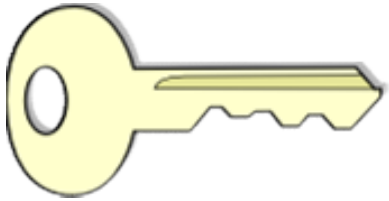
The organization has to protect the cryptographic keys against loss, modification, unauthorized access and disclosure.

Key management process should cover the whole lifecycle of the keys – generating, storing it, archiving, retrieving, distributing, retiring and destroying of keys.

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

Policy on key management - **a set of rules that will apply to a number of activities like:**

- generating keys for different types of cryptographic systems and applications;
- issuing and obtaining public key certificates;
- distributing keys and their activation when received;
- storing keys;
- changing and updating keys;
- dealing with compromised keys;
- revoking keys – how are they withdrawn or deactivated;
- recovering keys that have been lost or corrupted;
- backup and archiving keys;
- destroying keys;
- logging and auditing key management related activities.



To reduce the likelihood of improper use ISO/IEC 27002 recommends defining activation and deactivation dates for keys - so that they can only be used for a period of time.

ISO/IEC 11770 – Key management

ISO/IEC 27001:2013 Information security management systems

-Physical and environmental security – Secure areas-

Security category – 11.1. Physical and environmental security

Control – 11.1.1. Physical security perimeter

The organization should define and use security perimeters to protect areas that contain either sensitive or critical information and information processing facilities.

The premises of the organization may be at the risk of unauthorized access.

Guidelines for securing physical perimeters refer to:

- define perimeters and establish controls depending on the security requirements of the assets in each perimeter;
- ensure protection of the perimeters – doors, windows, roofs, walls, flooring;
- reception or similar area to control the physical access;
- fire doors should be alarmed, monitored and tested;
- intruder detection systems should be installed and unoccupied areas should be alarmed at all times.

Have multiple barriers or systems to prevent unauthorized access so the failure of one barrier does not compromise the security immediately.

ISO/IEC 27001:2013 Information security management systems

-Physical and environmental security – Secure areas-

Control – 11.1.2. Physical entry controls

There should be entry controls to ensure that only authorized personnel are allowed to access secure areas.

Guidelines for designing entry controls:

- date and time of entry and departure should be recorded;
- identity of the visitors should be confirmed and recorded;
- visitors should be supervised;
- access to areas where confidential information is processed or stored should be restricted to authorized individuals;
- all access should be logged;
- employees, contractors and external parties should wear visual identification; - external parties personnel should not be allowed to areas where confidential information is being processed (unless its critical and they should be monitored);
- physical access rights to areas should be reviewed regularly.

ISO/IEC 27001:2013 Information security management systems

-Physical and environmental security – Secure areas-

Control – 11.1.3. Securing offices, rooms and facilities

The organization should design and apply physical protection measures for offices, rooms and facilities.

Control measures for offices, rooms and facilities should be suitable to the value and importance of assets inside.

- key facilities should be sited to avoid access by the public;
- the organization should avoid the use of signs about the information processing facilities inside the rooms (ex. server room);
- Facilities should be configured to prevent confidential information or activities from being visible and audible from outside. Electromagnetic shielding may be needed;
- directories and phone books should not be readily accessible to anyone from outside the organization

ISO/IEC 27001:2013 Information security management systems

-Physical and environmental security – Secure areas-

Control – 11.1.4. Protecting against external and environmental threats

The organization needs to have physical protection against natural disasters, malicious attack or accidents.

Damage due to earthquake, fire, flooding, explosions, civil unrest or other forms of natural or man-made disasters.

For many of those in most countries there is specific legislation and ISO/IEC 27002 recommends the use of specialist advice on this matter

ISO/IEC 27001:2013 Information security management systems

-Physical and environmental security – Secure areas-

Control – 11.1.5. Working in secure areas

The organization should develop and use procedures for working in secure areas.

Secure areas - locations where critical information is being processed or stored, information that has great commercial value to the organization.

Guidelines for working in secure areas:

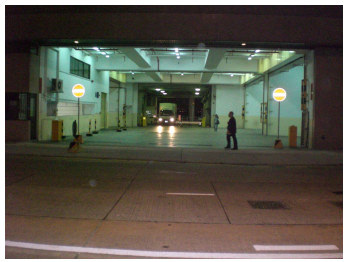
- personnel should only be aware of the existence of, or activities within a secure area on a need-to-know basis;
- only authorized personnel shall be allowed inside;
- unsupervised work in secure area should be avoided as much as possible and depending of course on the specifics of the area
- vacant secure areas should be locked and checked periodically
- photographic, video and audio recording equipment should not be allowed in secure areas unless specifically authorized.

ISO/IEC 27001:2013 Information security management systems

-Physical and environmental security – Secure areas-

Control – 11.1.6. Delivery and loading areas

Delivery and loading areas, as well as any other access points where unauthorized persons could enter the premises should be controlled and if its possible they should be isolated from the information processing facilities to avoid unauthorized access.



Uncontrolled access of public from outside can lead to security breaches.

Guidance on handling the security of delivery and loading areas include:

- delivery and loading areas should be designed so that delivery and loading personnel cannot access other parts of the building from those areas
- external doors of delivery and loading areas should be closed when internal doors that lead inside the organization are open
- If possible incoming material should be checked for explosives, chemicals or hazardous material before entering the delivery and loading area
- As much as possible it is recommended to segregate incoming and outgoing shipments
- Records of deliveries and dispatches should be kept (on paper or by video recording)

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (1)-

Security category – 11.2. Equipment

Control – 11.2.1. Equipment sitting and protection
The equipment needs to be sited and protected from environmental threats and hazards and unauthorized access.

Equipment is vulnerable to damage, to unauthorized viewing and to interference.

Guidelines provided by ISO/IEC 27002:
- equipment should be sited to minimize unnecessary access to work areas
- equipment where sensitive information is processed should be positioned so that the risk of information being viewed by unauthorized persons is reduced;
- controls should be in place to reduce the risk of physical or environmental threats;
- guidelines in place for eating, drinking and smoking;
- temperature and humidity should be monitored (if needed);
- use of special protection methods (ex. keyboard membranes) – if needed

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (1)-

Control – 11.2.2. Supporting utilities
The organization should protect its equipment from power failures and other disruptions caused by failures in supporting utilities.

Supporting utilities include electricity supply, telecommunications, water supply, gas, sewage, ventilation, air conditioning, heating.

A problem with any supporting utility should by identified by an alarm system.
Supporting utilities should be in line with the legal requirements and meet the needs of business growth.
They should be inspected regularly to ensure proper functioning.

Redundant connections for network connectivity should be obtained through the use of more than one provider.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (1)-

Control – 11.2.3. Cabling security
Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference of damage.

Guidelines for cabling security:

- power and telecommunication lines should be underground where possible;
- power cables should be segregated from communication cables to prevent interference;
- for critical systems further controls include: armoured conduit and locked rooms or boxes at inspection and termination points; use of electromagnetic shielding of cables; controlled access to patch panels and cable rooms as well as inspection for unauthorized devices attached.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (1)-

Control – 11.2.4. Equipment maintenance
Equipment should be maintained to ensure its integrity and availability.

The guidelines for equipment maintenance:

- respecting the supplier's recommended service intervals and specifications;
- using only authorized maintenance personnel for repairs;
- clearing confidential information from the equipment scheduled for maintenance or verifying maintenance personnel (depending on the case);
- complying with the maintenance requirements in the insurance policies;
- before putting the equipment back in operation after maintenance ensuring that it has not been tampered with and does not malfunction.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.5. Removal of assets
Taking equipment, information or software off-site should be done only with authorization.

The organization should have rules covering and a process to authorize taking assets out of the premises.

The rules regarding removal of assets may include aspects like:

- who authorizes taking assets out of premises;
- time limits for taking assets off premises;
- record the assets taken outside and the identity of the person(s).

Unauthorized removal of assets should be forbidden and employees need to be aware that spot checks can be done to verify this.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.6. Security of equipment and assets off premises
Assets off-site should be protected taking into consideration the different risks involved by working outside the organization premises.

The use of equipment outside the premises involves many security threats.

When using equipment or media outside:

- it should not be left unattended in public places and it should be protected (according to its manufacturer specifications – ex. protection from electromagnetic fields)
- if the equipment is transferred between individuals there should be a log that defines the chain of custody.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.7. Secure disposal or re-use of equipment
Before disposal or re-use, all equipment containing storage media shall be verified to ensure sensitive data and licensed software has been removed or securely overwritten.

Have controls in place to ensure that equipment to be disposed of or re-used does not contain sensitive information.

If storage media contains confidential or copyrighted information then this has to be securely deleted or overwritten so it can not be retrieved.
Consider destroying of media containing sensitive information as a method of disposal.

Simple deleting of files is usually not enough.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.8. Unattended user equipment
Unattended equipment should be protected.

Unattended equipment may provide an opportunity for security breaches.

Users should be advised to:

- terminate active sessions when finished or secure them with a password;
- log-off from application or network services when no longer needed;
- use a lock system for all computers or mobile devices.

ISO/IEC 27001:2013 Information security management systems
-Physical and environmental security – Equipment (2)-

Control – 11.2.9. Clear desk and clear screen policy
The organization should develop and implement a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

Defining and applying a clear desk/ clear screen policy reduces the risks of unauthorized access, loss and damage of information.

Guidelines on cs/cd policy include:
- sensitive or critical business information should be locked away preferably in a safe when not required and especially when the office is vacated
- computers should be logged off when unattended
- use of cameras and recording devices may be forbidden;
- media containing sensitive information should be removed from the printers after printing.

ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

Security category – 12.1. Operational procedures and responsibilities

Control – 12.1.1. Documented operating procedures
The organization should document and make available to all users operating procedures.

Documented procedures should be prepared for operational activities associated with information processing and communication activities.

The operating procedures should specify operational instructions like:
- installation and configuration of systems;
- processing and handling of information;
- backup;
- scheduling requirements - earliest job start and latest job completion times;
- instructions for handling errors and other exceptional conditions;
- support and escalation contacts in the event of unexpected difficulties;
- system restart and recovery procedures for use in the event of system failure…

ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

Control – 12.1.2. Change management
The organization should control changes that affect information security.

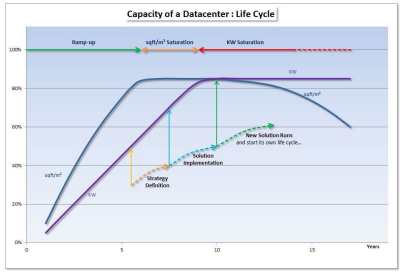
Uncontrolled changes to systems, processes or information processing facilities can cause major problems to business.

Guidelines of ISO/IEC 27002 with regards to change management:

- planning and testing of changes prior to implementation;
- assessing the potential impacts of changes, including security impacts, before implementation;
- a formal approval process for proposed changes;
- communication of change details to all relevant persons;
- how and when to abort change and actions to recover from unsuccessful changes.

ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

Control – 12.1.3. Capacity management
The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.



Capacity management refers to information processing facilities but also to office space and human resources.

Sufficient capacity can be achieved by increasing capacity or reducing demand for resources.

Critical systems like network gateways or main database servers should be prioritized and there should be a documented capacity plan made for those resources

ISO/IEC 27001:2013 Information security management systems
-Operational procedures and responsibilities-

Control – 12.1.4. Separation of development, testing and operational environments
The organization should separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment.

The operational systems must be kept reliable and using the same equipment or software for both current operation and development and testing of new systems - can affect the operational environment's integrity and availability.

Its desirable that development and operational software be segregated through strong access controls.

- separate domains completely segregated from each other (if not separate log-on procedures)
- users should use different profiles for operational and testing systems;
- compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required.

ISO/IEC 27001:2013 Information security management systems
-Protection from malware-

Security category – 12.2. Protection from malware

Control – 12.2.1. Controls against malware
The organization should have detection, prevention and recovery controls to protect against malware and they should be combined with appropriate user awareness.

ISO/IEC 27002 recommends protection against malware to be based on detection and repair software, awareness, system access control and controlled change management.

ISO/IEC 27001:2013 Information security management systems
-Protection from malware-

Guidance on protection from malware:

- define a policy to prohibit the use of unauthorized software and implement controls to detect the use of such software;
- blacklist suspected malicious websites and prevent their use;
- have a policy aimed to protect against risks associated with obtaining files and software from or via external networks;
- use and regular update of malware detection and repair software and scan computers and media on a regular basis;
- have some plans to recover from malware attacks;
- keep in touch with latest information on malware attacks;
- isolating environments where malware infection can lead to catastrophic impacts for the organization - if there are such environments.

For systems where sensitive information is being processed, the use of more than one vendor's antivirus software may improve detection rate.

ISO/IEC 27001:2013 Information security management systems
-Backup-

Security category – 12.3. Backup

Control – 12.3.1. Information backup
The organization should have a backup policy to ensure that backups of information and software are taken and tested regularly.

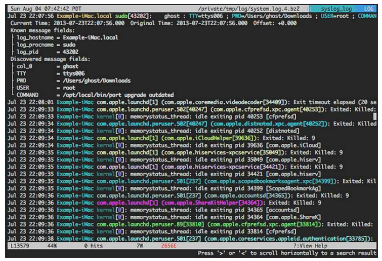
Guidelines for the backup policy:

- the extent of backup should be in line with the business requirements and the criticality of the information being backed-up;
- the backups should be located where they cannot be damaged by a disaster at the main site;
- if the information backed up require so - encryption should be used;
- backup media should be tested periodically to ensure they can be relied upon;
- testing of the capacity to restore backup data should be performed.

Real time backup/ Automated backup/ User initiated backup

ISO/IEC 27001:2013 Information security management systems
-Logging and monitoring-

Security category – 12.4. Logging and monitoring



Control – 12.4.1. Event logging

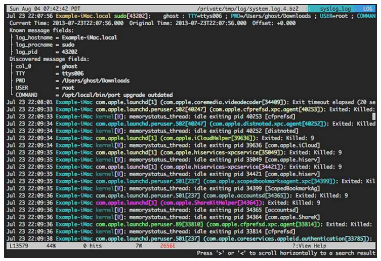
Event logs record user activities, exceptions, faults and security events. The organization should ensure that such logs are produced, kept and regularly reviewed.

Logs are valuable to investigate incidents, events that led to security problems and to determine who is accountable for different activities.

For every information processing facility there should be an event log kept – that is independent and not accessible by the user.

ISO/IEC 27001:2013 Information security management systems
-Logging and monitoring-

Some guidelines for what event logs should refer to:



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;
e) records of successful and rejected system access attempts;
f) changes to system configuration;
g) use of privileges;
h) use of system utilities and applications;
i) files accessed;
j) alarms raised;
k) activation and de-activation of protection systems, such as the anti-virus systems;
l) records of transactions executed by users in applications…

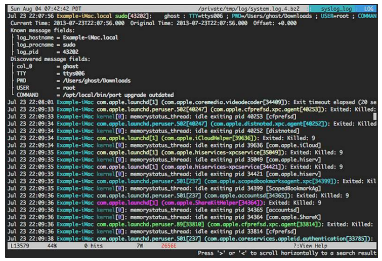
Review of logs should respect the segregation of duty principle.
Logs should be kept for a sufficient period of time so that they can be used if needed for an investigation.

ISO/IEC 27001:2013 Information security management systems

-Logging and monitoring-

Control – 12.4.2. Protection of log information

The organization should protect logging facilities and log information against tampering and unauthorized access.



The information contained in logs is valuable as log as its integrity is preserved.

Controls should aim to protect against unauthorized changes like: editing or deleting the information recorded; modifying the type of information that is being recorded or overwriting logs because storage capacity is exceeded***.***

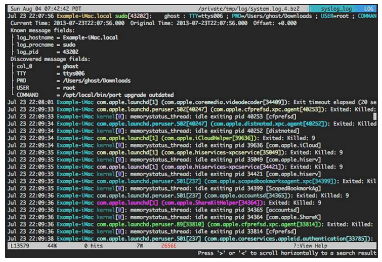
A method to safeguard logs is to copy them in real time to a system outside the control of the system administrator.

ISO/IEC 27001:2013 Information security management systems

-Logging and monitoring-

Control – 12.4.3. Administrator and operator logs

The activities of system administrators and the activities of operators should be logged and the logs should be protected and reviewed regularly.



A user with privileges may be able to manipulate logs so its necessary to employ some protection for such situations.

An intrusion detection system managed outside the control of the administrator is a solution proposed by ISO/IEC 27002 for the control of logs.

ISO/IEC 27001:2013 Information security management systems
-Logging and monitoring-

Control – 12.4.4. Clock synchronization
The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source.

An internal reference time should be established, documented and implemented.

Clock synchronization is needed because most logs are time and date stamped.

In most cases – reference time is local time.
For organizations with multiple locations – a reference time should be decided.

All system clocks should be automatically synchronized with a master clock.

ISO/IEC 27001:2013 Information security management systems
-Control of operational software-

Security category – 12.5. Control of operational software

Control – 12.5.1. Installation of software on operational systems
The organization should have procedures for the installation of software on operational systems.

Systems can be affected by the installation of unauthorized software and by unauthorized changes to software.

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

ISO/IEC 27001:2013 Information security management systems
-Control of operational software-

Guidelines for the installation of software, according to ISO/IEC 27002:

a) updating of the operational software, applications and program libraries should only be performed by trained personnel and with authorization;
b) operational systems should only hold approved executable code and not development code or compilers;
c) applications and operating system software should be implemented only after successful testing;
d) there has to be a strategy for situations where changes to software go wrong;
e) previous versions of application software should be retained as for contingency purposes;
f) old versions of software should be archived.

Physical or logical access to suppliers for software support should only be given for specific activities, under approval from management and be it should be monitored.

ISO/IEC 27001:2013 Information security management systems
-Technical vulnerability management-

Security category – 12.6. Technical vulnerability management

Control – 12.6.1. Management of technical vulnerabilities
The organization should be able to obtain information about vulnerabilities of its information systems, its exposure to such vulnerabilities should be evaluated and appropriate measures should be taken to address the risks.

Technical vulnerabilities being exploited is among the most common type of attacks on organizations' information systems.

ISO/IEC 27001:2013 Information security management systems
-Technical vulnerability management-

Guidelines of ISO/IEC 27002 for the management of vulnerabilities:

- defining responsibilities for vulnerability management;
- find a suitable software to identify technical vulnerabilities;
- set timelines to react since being notified about a potential vulnerability;
- once a technical vulnerability has been identified – assess associated risks and decide actions;
- if a patch is available from a legitimate source the risks associated with installing the patch should be assessed and patches should be tested before being installed. There should be a possibility to uninstall a patch and go back to the previous state;
- if no patch is available some other actions should be taken - turning off services related to the vulnerability, changing or adding access controls (like firewalls); increasing monitoring to detect attacks and raising awareness.

ISO/IEC 27001:2013 Information security management systems
-Technical vulnerability management-

Control – 12.6.2. Restrictions on software installation
The organization should establish and implement rules for the installation of software by users.

In most organizations a certain group of users enjoy increased privileges - allowing them to install software.

But uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and security incidents.

Use of least privilege to be applied.

Rules on what types of software installations are permitted and what installations are prohibited.

ISO/IEC 27001:2013 Information security management systems
-Information systems audit considerations-

Security category – 12.7. Information systems audit considerations

Control – 12.7.1. Information systems audit considerations
Audit activities, especially those that involve verification of operational systems, should be planned and agreed so that the disruption to business activities is minimal.

The audits of information systems should be carefully planned and the schedule of audit activities should be agreed.

No information should be changed during audit activities and access should be logged as in the case of any other operation.

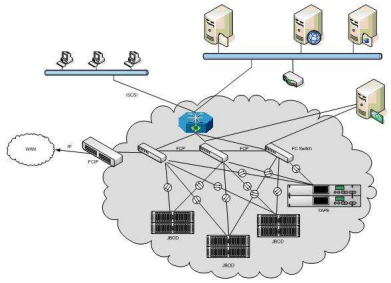
The audit should be limited to read-only access to software and data.
If some audit tests that could affect systems availability are needed to be performed during the audit - they should be scheduled to run outside business hours.

Audit activities should cause as little interruptions to business activities as possible.

ISO/IEC 27001:2013 Information security management systems
-Network security management-

Security category – 13.1. Network security management

Control – 13.1.1. Network controls
The networks have to be controlled and managed so that the information in systems and applications is protected.

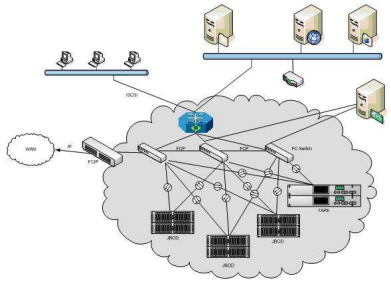


Networks are vulnerable to unauthorized access, to misuse or abuse and to unintentional fallings of technology.

ISO/IEC 27001 requires the organization to implement controls to ensure the security of information passing through networks and the protection of devices connected to the networks.

ISO/IEC 27001:2013 Information security management systems

-Network security management-



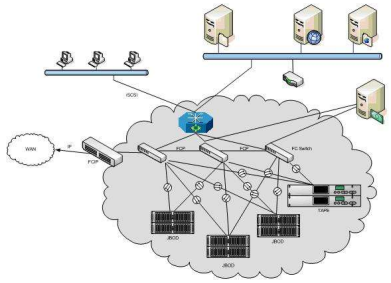
General guidelines from ISO/IEC 27002 on network security management:

- define responsibilities and procedures for the management of network equipment;
- define and apply some supplementary controls to protect the confidentiality and integrity of data passing over public networks or through wireless networks – as the risks are considerably higher;
- constantly monitor of the network ;
- ensure the authentication of systems connected to the network and restrict connections.

ISO/IEC 27033 – about network security

ISO/IEC 27001:2013 Information security management systems
-Network security management-

Control – 13.1.2. Security of network services
The organization should identify and include in network service agreements security mechanisms, service levels and management requirements for all network services. This is applicable irrespective whether the network services are provided in-house or by a third party.



Third party supplied network services carry a risk of unauthorized access attempts that may lead to security breaches.

Network services may include – provision of connections, private network services, security solutions for the networks (like firewalls or intrusion detection systems)…

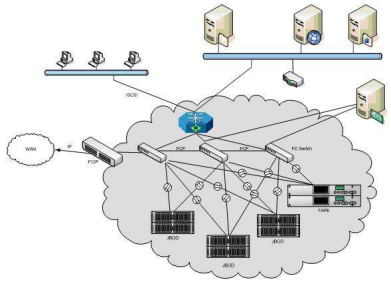
The organization should agree with the service provider (and document in the contracts) on the security features for the services it provides and should monitor the services to see if they meet requirements.

ISO/IEC 27001:2013 Information security management systems

-Network security management-

Control – 13.1.3. Segregation in networks

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



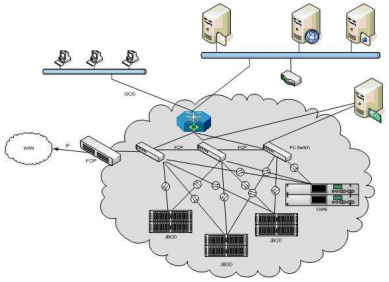
The bigger the network, the higher the risk.

Security can be managed easier if the network is divided into physical or logical domains and security measures are implemented to manage the gateways between the domains.

The segregation can be done using physically different networks or by applying connection and routing controls.

ISO/IEC 27001:2013 Information security management systems

-Network security management-



The perimeter for each domain should be well defined and the access between network domains should be controlled using a gateway.

Wireless networks - difficult to define exactly the perimeter – ISO/IEC 27002 recommends for sensitive environments (where critical data is stored or processed) to treat all wireless access as external connections and to segregate this access from internal networks and pass the wireless access through a gateway before accessing internal systems.

The domains and their relationship should be documented in a ***network map*** or similar document.

Special care for networks that spread beyond organization's boundaries.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

Security category – 13.2. Information transfer

Control – 13.2.1. Information transfer policies and procedures
The organization should have transfer policies, procedures and controls to protect the transfer of information for all types of communication facilities.

Exchange of information carry the risk of the information being compromised.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

General guidelines for rules and procedures on information transfer:

- rules to protect against malware that can be transmitted through the use of electronic communications;
- rules for the acceptable use of communication facilities;
- explicit rules forbidding employees to compromise the organization (ex. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing);
- encrypt information (if needed);
- rules on the retention and disposal of business correspondence;
- not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons;
- not leaving sensitive information in printers or fax machines;
- personnel reminded not to have confidential conversations in public places or through insecure communication channels.

Rules should be communicated to all staff.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

Control – 13.2.2. Agreements on information transfer
The organization should include in agreements with other parties the secure transfer of business information.

ISO/IEC 27002 recommends to document in the contracts the level of security expected for sensitive information passing between organizations and the controls applied.

Example elements to be included in the contracts:

- management responsibilities for controlling and notifying transmission, dispatch and receipt;
- procedures to ensure traceability and non-repudiation;
- minimum technical standards for packaging and transmission;
- escrow agreements;
- courier identification;
- responsibilities and authorities in case of security incidents;
- agreeing on a common system of labelling information between the parties.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

Control – 13.2.3. Electronic messaging
Information exchanged through electronic messaging should be appropriately protected.

Email involves many risks if used without appropriate controls.
(ex. financial fraud, infection, legal issues)

There should be some rules or procedures in place for the use of email and its essential that staff are aware of: the risks involved, the organization's requirements and the control mechanisms in place.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

Control – 13.2.4. Confidentiality or non-disclosure agreements
The organization should have suitable confidentiality and non-disclosure agreements that are in line with the needs for the protection of information.

Before giving access to confidential information - to employees or external personnel and organizations the organization should ensure that confidentiality agreements are signed.

Elements to be included in the non-disclosure agreements:
- a definition of the information to be protected (ex. confidential information);
- ownership of information and the rights to use confidential information by the signatories;
- expected duration of the agreement, including cases where confidentiality might need to be maintained indefinitely
- responsibilities and actions of the signatories to avoid information being disclosed;
- the process of notification and reporting in case of unauthorized access to confidential information;
- expected actions in case the agreement is breached

ISO/IEC 27001:2013 Information security management systems
-Security requirements of information systems-

Security category – 14.1. Security requirements of information systems

Control – 14.1.1. Information security requirements analysis and specification
The organization should include security related requirements in its requirements for new information systems or enhancements to existing information systems.

The organization needs to recognize information security requirements from the first stages of information systems acquisition or development.

There are 2 different situations:
- the information system is developed specifically for the organization, or by the organization itself;
- the system is acquired as a commercial product not personalized.

The level of security requirements and controls should reflect of course the business value of the information involved and the potential negative impact over the business in case this information is not adequately protected.

ISO/IEC 27001:2013 Information security management systems
-Security requirements of information systems-

Control – 14.1.2. Securing application services on public networks
Information from application services that are passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

E-commerce.

Many security requirements can be addressed by using cryptography:

- encryption to ensure the confidentiality of information like billing details and personal information;
- digital signatures to ensure the integrity of electronic transactions and to authenticate the partners in the transaction;
- both encryption and digital signatures to achieve non-repudiation that may be needed in case of disputes on the occurrence or non-occurrence of a certain event.

ISO/IEC 27001:2013 Information security management systems
-Security requirements of information systems-

If the organization is using or providing application services over public networks it should have clear regulations that define:

- who is allowed to carry out electronic commerce activities and what is the employee authorized to do;
- how segregation of duties is ensured - activities that in combination can be used to commit fraud should not be performed by the same person;
- what controls are in place to monitor activities and ensure protection of the information involved.

ISO/IEC 27001:2013 Information security management systems
-Security requirements of information systems-

Control – 14.1.3. Protecting application service transactions
Information used for transactions has to be protected against incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

The security considerations provided by ISO/ IEC 27002 refer to:

- the use of electronic signatures;
- aspects on the transaction - privacy of the parties, confidentiality of the transaction, verification and validation of the user's authentication information;
- encryption of the communications between parties;
- the use of secure protocols for communication between the parties involved in the transaction;
- storage of the transaction details outside any publicly accessible environment;

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Security category – 14.2. Security in development and support processes

Control – 14.2.1. Secure development policy
The organization should develop and apply rules for the development of software and systems.

The secure development policy should address aspects like:

- Security of the development environment;
- Guidelines for secure coding that should be used;
- Security checkpoints within the project milestones;
- Security in the version control.

Unsafe coding may lead to vulnerabilities
(www.securecoding.cert.org)

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Control – 14.2.2. System change control procedures
The organization should use a change control procedure to handle changes to systems within the development lifecycle.

A system is more vulnerable whenever it undergoes change.

A risk assessment and analysis on the impact of change should exist along with the specification of security controls needed.

Procedures for change control should address aspects like:
- authorization of changes;
- fallback arrangements;
- reviews and tests;
- version control of all software updates;
- audit trail of all changes;
- Update system documentation on the completion of the change;
- implementing changes so that disturbance to business processes is minimal

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Control – 14.2.3. Technical review of applications after operating platform changes
Whenever the organization is making changes to its operating platforms, critical applications should be reviewed and tested to ensure there is no adverse impact on operations or security.

Changes to operating system software should be under control.

ISO/IEC 27002 recommends to have a formal process to review the applications and test for possible vulnerabilities that may appear after a new operating system is implemented or the existing one is changed.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Control – 14.2.4. Restrictions to changes to software packages
The organization should discourage modifications to software packages and limit them to necessary changes. All changes should be strictly controlled.

Changes to software packages and especially to vendor-supplied software should be made only if there is a really critical business need to do so.

If a software package needs to be modified to suit a business need the following should be considered:
- risk assessment to identify the potential vulnerabilities;
- need for a consent from the vendor for the changes;
- if the changes result in vendor support for the software package to cease.
- retain the original of the software and make changes to a copy;
- test the software after implementing the changes before starting to use it.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Control – 14.2.5. Secure system engineering principles
The organization should establish, document, maintain and apply principles for engineering secure systems for all its implementation efforts.

Security engineering focuses on the security aspects in the design of systems that need to be able to deal with possible sources of disruption, ranging from natural disasters to malicious acts.

nist.org - SP 800-160 (Systems security engineering)

Principles for security engineering have to be reviewed periodically to ensure they are still up-to-date.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.6. Secure development environment
The organization should establish and protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Development environment includes people, processes and technology

Aspects to be considered in defining security requirements for the development environment:
- sensitivity of the data being processed, stored and transmitted;
- regulations applicable –external or internal policies;
- trustworthiness of personnel involved;
- outsourced activities;
- access control to the development environment;
- storing backups in secure offsite locations.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.7. Outsourced development
Outsourced system development should be supervised and monitored.

Development outsourcing involves risks since the process is not under the control of the organization.

The organization should have clear agreements with the software development suppliers to protect against risks and to ensure on-time delivery of the product and functionality aspects.

Control of the software development supplier depends on the risks involved:

- testing of deliverables
- auditing the supplier organization's development environment.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.8. System security testing
The organization should test security functionalities during development.

Security testing should be carried before operational implementation of the product.

For in-house developments such tests should be performed by the development team and the extent of testing should be of course proportional to the importance and nature of the system.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.9. System acceptance testing
The organization should establish acceptance testing programs and criteria for new information systems, upgrades and for new versions.

New or changed systems can bring in unknown vulnerabilities.

The organization should define ***acceptance criteria*** and ***testing to ensure*** that those ***criteria are met*** before the new system is introduced.

Automated tools can be used – like code analysis tools or vulnerability scanners and security related defects should be remediated.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Security category – 14.3. Test data

Control – 14.3.1. Protection of test data
Test data should be selected carefully, protected and controlled.

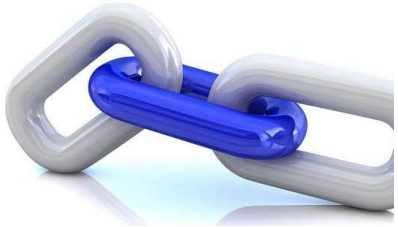
Avoid the use of operational data containing personally identifiable information or any other confidential information for testing purposes.

Guidelines of ISO/IEC 27002 for protecting operational data used for testing:
- Use the same access control procedures for test application systems as for operational systems;
- existence of an authorization each time operational information is used in a test environment;
- After testing is finalized the data no longer needed should be securely erased from the test system;
- Logging the use of operational information for testing purposes.

ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

Security category – 15.1. Information security in supplier relationships

Control – 15.1.1. Information security policy for supplier relationships
The organization needs to agree with its suppliers and to document the requirements for information security needed to mitigate risks that may arise from the supplier's access to its assets.

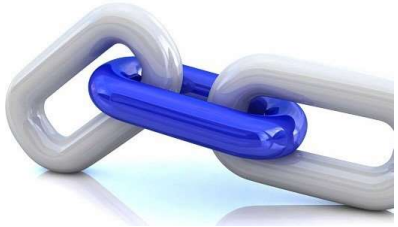


If a supplier is accessing the organization's assets there are risks involved.

There have to be rules and procedures specifying:
- what the supplier is allowed to do and to access,
- what are the obligations of the suppliers;
- how security incidents are to be handled;
- awareness of the organization's personnel involved in acquisition;
- documenting the security requirements in contracts.

ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

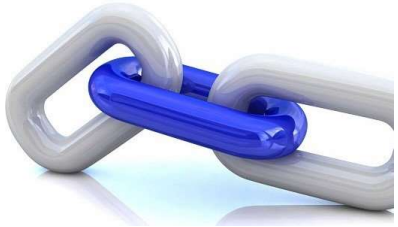
Control – 15.1.2. Addressing security within supplier agreements
The contracts signed with the suppliers should include all relevant information security requirements.



The contracts signed with supplier depend on the risks involved but the best practice is to make the contracts as detailed as possible in terms of information security.

Suppliers should not be allowed access to the organization's assets before the contracts are not agreed and signed and any other controls agreed by the parties are not implemented.

ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

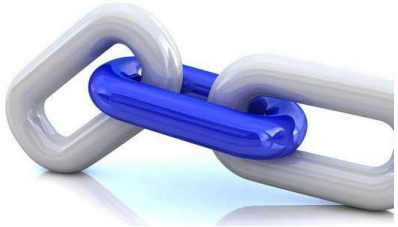


Guidance of ISO/IEC 27002 on elements to be included in supplier agreements:

- obligation of the supplier to comply to the organization's policies;
- information to be provided to or accessed by the supplier and how;
- the classification of information used within the agreement;
- any legal requirements applicable to the relations between the parties;
- what controls are to be implemented by each party;
- the list of supplier's personnel to access the organization's assets or a system to authorize personnel for the access including here the possibility to perform screening of suppliers personnel before granting access;
- how incidents are to be handled and how conflicts are to be resolved;
- rules and conditions for subcontracting by the supplier;
- if the parties agree that the organization can audit the supplier.

ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

Control – 15.1.3. Information and communication technology supply chain
The organization should include in its agreements with suppliers requirements related to the supply chain for IT&C products and services.



This is meant to address the risks associated with the suppliers' sub-suppliers.

So the organization should investigate its IT&C supply chain and document in the contracts with its suppliers some aspects on this topic, like:

- asking the supplier to propagate the organization's security requirements throughout the supply chain;
- getting assurance that critical components origin can be traced throughout the supply chain;
- how the supplier evaluates its own suppliers and how it chooses them.

ISO/IEC 27001:2013 Information security management systems
-Supplier service delivery management-

Security category – 15.2. Supplier service delivery management

Control – 15.2.1. Monitoring and review of supplier services
The delivery of services by the suppliers has to be monitored, reviewed and audited by the organization.

Organization needs to ensure that the services purchased conform to contracts

Monitoring can include:
- observation (for example observation of availability of a service);
- request and review service reports from the suppliers;
- have regular meetings with the supplier to discuss the conformity of the services to requirements;
- audit the supplier.

Important aspects: how the supplier deals with security incidents; if the supplier has security requirements for its own suppliers and if the supplier has the capability to ensure continuity of services in case of major problems or disasters.

ISO/IEC 27001:2013 Information security management systems

-Supplier service delivery management-

Control – 15.2.2. Managing changes to supplier services

The changes to services provided by the suppliers have to be carefully managed and should take into account the risks involved and the criticality of business information, systems and processes.

Changes need to be reviewed, information security risks have to be re-assessed and if needed controls need to be changed or new controls implemented to maintain the level of security

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Security category – 16.1. Management of information security incidents and improvements

Control – 16.1.1. Responsibilities and procedures
There should be responsibilities and procedures in place to respond effectively and in time to information security incidents.

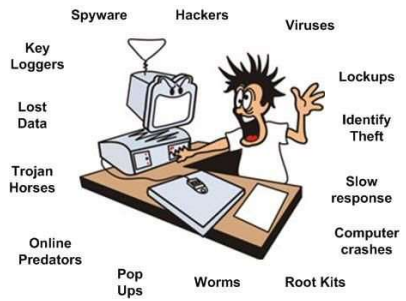
Consider the idea of creating a list of potential security incidents.

There should be procedures in place to ensure that security incidents are reviewed and investigated:
- planning and preparation of incident response
- monitoring, detecting, analyzing and reporting security events and incidents;
- logging incident management;
- handling of forensic evidence collected;
- escalation of incidents and recovery from an incident.

ISO/IEC 27035 - incident management.

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Control – 16.1.2. Reporting information security events
The organization is required to establish communication channels for reporting security events as quickly as possible.



What can be considered a security event that needs to be reported:

- a security control that is not effective;
- human errors;
- a virus detected on a system;
- breaches of physical security leading to theft;
- passwords being exposed;
- hardware or software that is not functioning correctly;
- uncontrolled system changes;
- unauthorized access to systems;
- non-compliance with legal requirements or procedures …

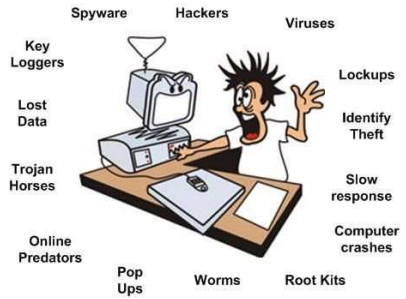
A security event can be considered anything that can result in loss or damage to assets or an action that is against the security policies of the organization

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Point of contact – a person or department where events are being reported and that is the first line of response to the incident.

All personnel should be aware of the contact point identity.

The reporting of events should be standardized and all staff should be advised to report events as soon as possible



ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Control – 16.1.3. Reporting information security weaknesses
All employees and contractors need to be trained to report any security weakness – be it observed or suspected.

Weaknesses need to be reported to the point of contact to prevent information security incidents.

The reporting mechanism has to be easy, accessible and efficient.

All users should understand that they are required to report any weaknesses and not try to test the weaknesses to be sure or exploit them.

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

Control – 16.1.4. Assessment and decision on information security events
Information security events are required to be assessed and the organization needs to decide whether they are to be considered information security incidents.

Contact point provides initial triage – review of each event and evaluate the Impact to decide whether it has to be classified as information security incident.

Criteria for classification of incidents to prioritize the actions.

The contact point may not be the single decision layer with regards to incidents – the organization may have an information security incident response team (ISIRT) and the incident will be escalated here for assessment and decision.

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

Control – 16.1.5. Response to information security incidents
After assessment the organization should respond to information security incidents according to documented procedures.

Incidents should be responded to with the first goal being to resume "normal security level" and then initiate recovery.

ISO/IEC 27002 provides some guidance on what the response should include:

- collect evidence as soon as possible after the occurrence of the incident;
- perform forensics analysis;
- escalate the incident if necessary;
- communicate to all parties that need-to-know about the incident (be it inside or outside the organization);
- find the weaknesses that lead to the incident and deal with them;
- record the incident and close it.

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

Control – 16.1.6. Learning from information security incidents
The organization is required to use the knowledge it gets from dealing with security incidents to learn reduce the likelihood and impact of future incidents.

Besides resolving security incidents its important that people learn from the security incidents to avoid them happening in the future or if they happen to deal with them more effectively.

Case studies and anecdotes from actual security incidents can be used in awareness training as examples of what can happen, how to avoid situations and how to respond

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (2)

Control – 16.1.7. Collection of evidence
The organization should collect and preserve information which can serve as evidence according to established procedures.

In most cases its not clear whether a certain incident will end up in court or not.
The organization should collect information that can serve as evidence for every information security incident.

The organization should have procedures to deal with evidence collected.

ISO/ IEC 27037 - guidelines for identification, collection, acquisition and preservation of digital evidence.

ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Security category – 17.1. Information security continuity

Control – 17.1.1. Planning information security continuity
The organization is required to ensure that in case of adverse situations like a crisis or a disaster, information security management is not neglected.

If there is a need for information security when things are ok, then there is a need for information security when things go wrong too.

Information security aspects should be inserted in the planning for business continuity and disaster recovery.

If there is no formal business continuity management implemented :

- either information security applicable in normal conditions remain the same in case of adverse conditions;
- or a business impact analysis is made to determine the requirements for information security in case of a crisis or disaster..

ISO 22301 – Business Continuity Management Systems

ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Control – 17.1.2. Implementing information security continuity
The requirement here is for the organization to have processes, procedures and controls in place to ensure the continuity of information security during an adverse situation.

The organization is required to:
- have a management structure in place that will prepare for and respond to an a disruptive event using personnel with sufficient competence and authority;
- nominate personnel with the specific tasks to maintain information security in case of an unexpected event;
- have plans and procedures for response and recovery that include aspects on how to maintain information security while managing the disruptive event.

Normally the information security controls should be able to operate in case of a disruptive event but if not, the organization should plan for other controls that will become effective in this situation to ensure an acceptable level of information security.

ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Control – 17.1.3. Verify, review and evaluate information security continuity
The controls implemented for information security continuity need to be verified to ensure they are still valid and effective in case of real adverse situation.

Information security continuity processes, procedures and controls need to be tested for functionality.

Whenever something changes information security continuity measures need to be reviewed and updated as necessary.

ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Security category – 17.2. Redundancies

Control – 17.2.1. Availability of information processing facilities
Redundancy should be sufficient to meet the requirements for availability.

Redundancy offers availability.

The organization needs to identify the business requirements for availability of information systems, see what the current systems provide and where the existing architecture cannot guarantee availability needed the organization should consider the use redundant components or systems to match the needs for availability.

Redundant should be tested.

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Security category – 18.1. Compliance with legal and contractual requirements

Control – 18.1.1. Identification of applicable legislation and contractual requirements
Identify, document and keep up to date all legal, regulatory and contractual requirements applicable to each information system of the organization.

Identification of legislation and contractual requirements – including a short description of the organization's approach to fulfill the requirement.

More difficult in case of organizations that operate in several countries.

Legal and contractual requirements change – so they need to be updated.

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.2. Intellectual property rights
There should be procedures to ensure compliance with requirements related to intellectual property rights and use of proprietary software.

The risk is for legal action against the organization for unauthorized use of copyright material.

The organization should implement rules on the use of intellectual property.

Guidelines:
- software should be acquired only from known sources;
- awareness of personnel on intellectual property rights and using the disciplinary process in case of breaches;
- make inventory checks at least once per year to ensure all software in use is licensed;
- keep proof and evidence of ownership for all software;
- have regulations for disposing of software or transfer of software to others.

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.3. Protection of records
The organization should protect records according to legislation, regulatory, contractual and business requirements.

Records have to be protected from breach of confidentiality, from loss or modification.

There is legislation defining retention periods for many types of records and the organization is required to comply.

When keeping records for long periods consideration should be given to the risk of deterioration.

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.4. Privacy and protection of personally identifiable information
The organization needs to protect the privacy of personally identifiable information in line with applicable legal requirements.

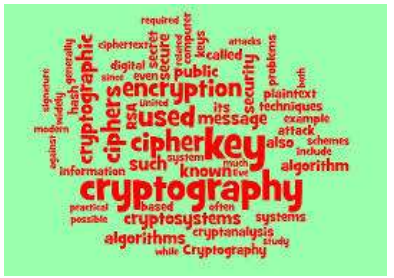
Most countries have legislation on the protection of personally identifiable information.

The organization should have a policy to ensure the compliance with relevant legislation related to privacy and personally identifiable information**.**

A solution is to nominate a "*Privacy officer".*

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.5. Regulation on cryptographic controls
The use of cryptography should respect legislation, regulations and relevant agreements.



Legislation on the use of digital signatures and other uses of cryptography.

Some countries prohibit the export of cryptography software, some restrict the import of such software; some legislations require licensing for the use of cryptography software.

Look for legal advice to make sure it complies with specific legislation on all the markets where it activates.

ISO/IEC 27001:2013 Information security management systems
-Information security reviews-

Security category – 18.2. Information security reviews

Control – 18.2.1. Independent review of information security
An independent review of the implementation of information security should be performed from time to time and also whenever significant changes occur.

An independent review is useful to ensure that the approach taken by the organization on information security is suitable and also to find opportunities for improvement.

The review should be done by individuals that are independent from the area under review.

Results of the review should be communicated to management

ISO/IEC 27001:2013 Information security management systems
-Information security reviews-

Control – 18.2.2. Technical compliance review
The managers of the organization are required to review compliance of procedures applied in their area or responsibility with the appropriate security policies, standards and requirements.

Technical compliance review requires skilled personnel and the help of automated tools:
- Penetration tests
- Vulnerability assessments.

Technical reviews have to be done with proper planning, have to be authorized and documented