D 24v13

ISO 27001 readiness version 2013

Objective

Objective of the module: Readiness for implementation, certification, maintenance and improvement of your information security management system (ISO 27001) in order to:

• guarantee the confidentiality, integrity, availability and traceability of information
• reduce information security risks
• seize opportunities for continual improvement

1 Information security

1.1 History

The information, hardware and software that an organization owns is a valuable investment that must be protected. One of the best ways to take care of this treasure is to set up an Information Security Management System (ISMS).

In 1989 the User's Code of Practice was released, based on Shell's security policy, at the request of the UK government (Department of Trade and Industry).

In 1995, the British standard BS 7799 was published.

In 1996 the ISO 13335 standard was published which after its last version in 2004 will be replaced by ISO / IEC 27001.

ISO (International Organization for Standardization) was created in 1947. ISO comes from the Greek for "isos" (equal). For simplicity we use ISO instead of ISO / IEC.

The history of transformations and versions of the ISO 27000 family of standards is shown in Figure 1-1.

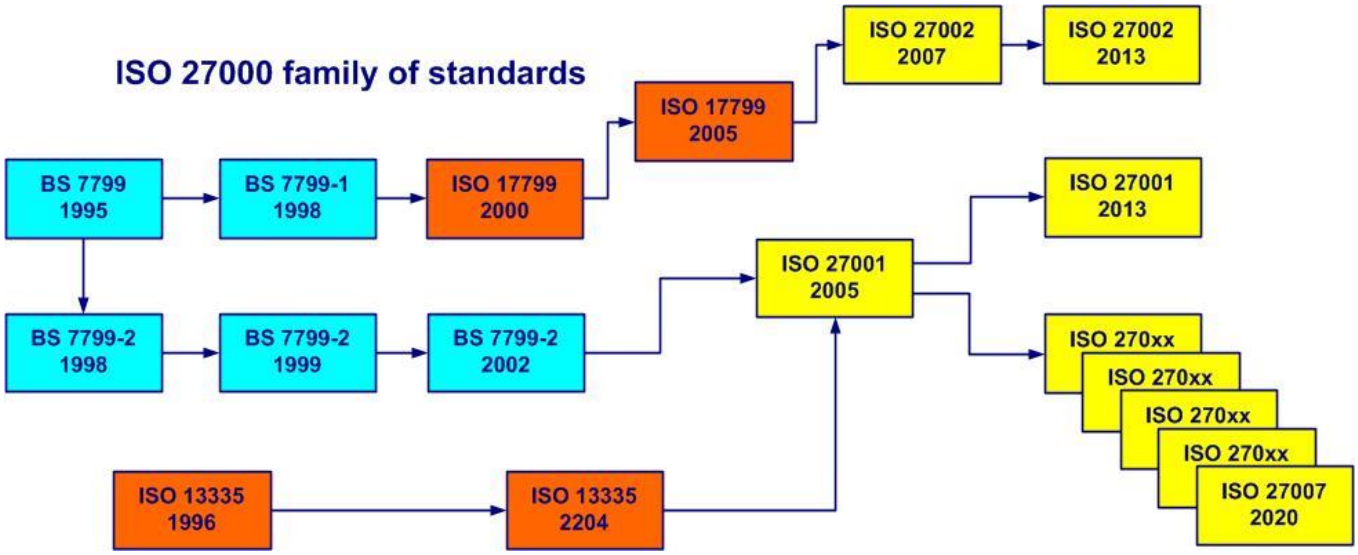


Figure 1-1. History of the ISO 27000 family of standards

Since 2005 ISO / IEC 27001: 2005 offers the possibility of certification of an information security management system.

In 2013, the ISO / CEI 27001: 2013 and ISO / CEI 27002: 2013 standards were released. A large number of standards followed which forms the ISO / IEC 27000 family. For more details see paragraph 2.2.

1.2 Scope

Information security is everyone's business

The ISO 27001 standard (Information technologies - Security techniques - Information security management systems - Requirements) is generic because it applies to the management system of any organization, without any constraints relating to the size, activity or type. It is an international voluntary standard that allows certification by an accredited (certification) body.

The implementation of an information security management system is always:

- resulting from a strategic decision by top management
- in agreement with:
  - the objectives of the organization
  - corporate culture
  - business processes

Applying the ISO 27001 standard and complying with its requirements helps preserve the confidentiality, integrity, availability and traceability of information.

Compliance with the requirements related to the assessment and treatment of risks (based on the ISO 31000 standard) helps to reassure interested parties about the management of information security.

1.3 Principles and steps

Security is a process. John Mallery

The information security (IS) approach is a state of mind that starts with top management as a priority strategic decision and extends to all staff. Top management defines the information security policy, in which the information security objectives are set, which are applicable to all activities. The tool used to achieve the objectives is the information security management system. Prevention is the essential concept of the information security management system.

The three essential properties of information security are confidentiality, integrity and availability as shown in Figure 1-2.

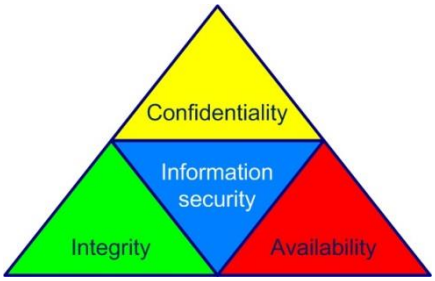


Figure 1-2. Information security properties

Take your bank account as an example. Account information must be protected:

- its confidentiality - the information must remain secret
- its integrity - the total information must be accurate and must not change
- its availability - the information must remain accessible in a timely manner

Any information security management system includes three distinct and interdependent approaches:

- process approach
- risk-based thinking
- continual improvement

The seven principles of quality management (cf. figure 1-3) will help us obtain sustainable performance (cf. ISO 9000: 2015, § 2.3).

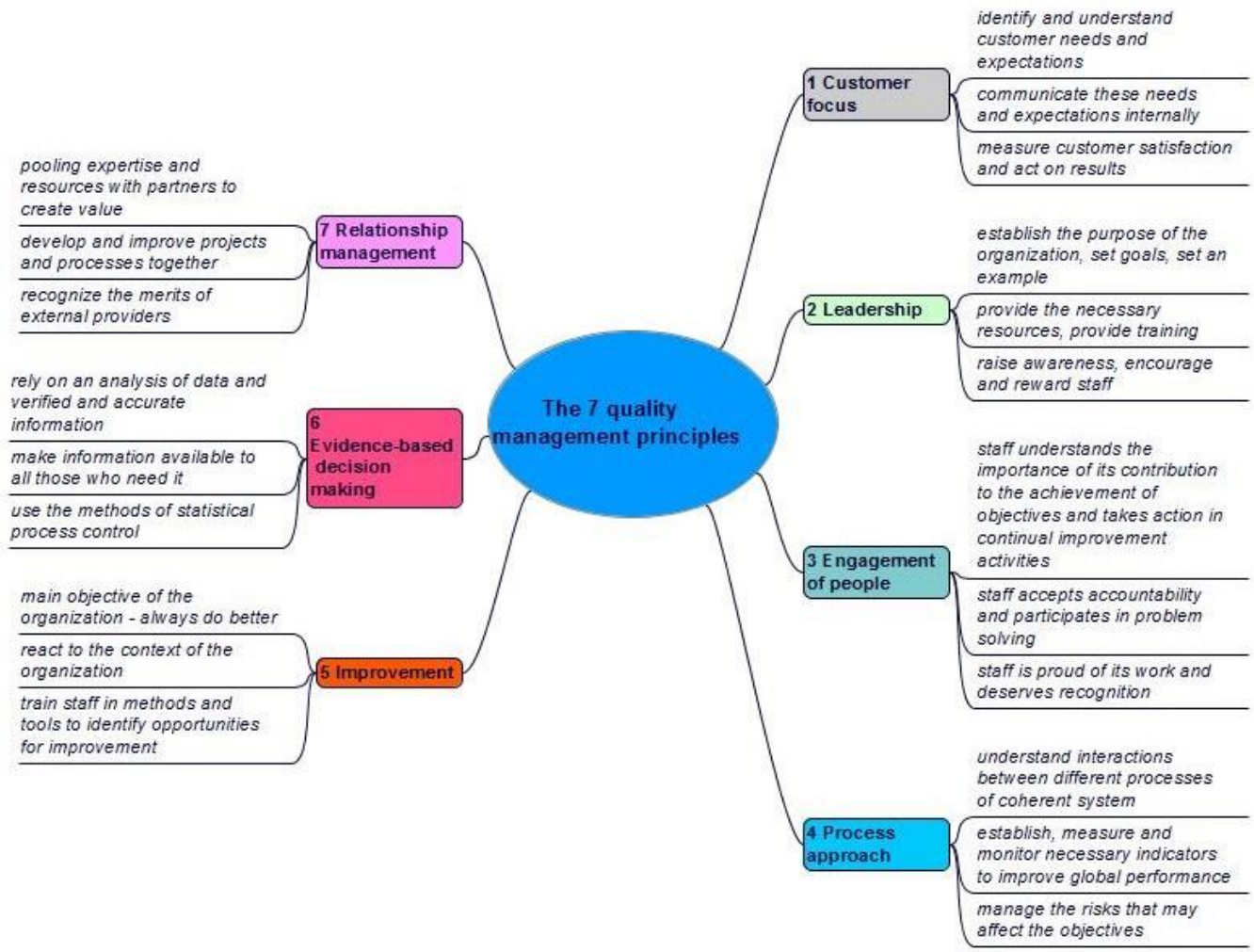


Figure 1-3. The 7 quality management principles

A well-prepared approach is halfway to success

The process for implementing an information security management system goes through several steps. An example of preparation is shown in Figure 1-4.

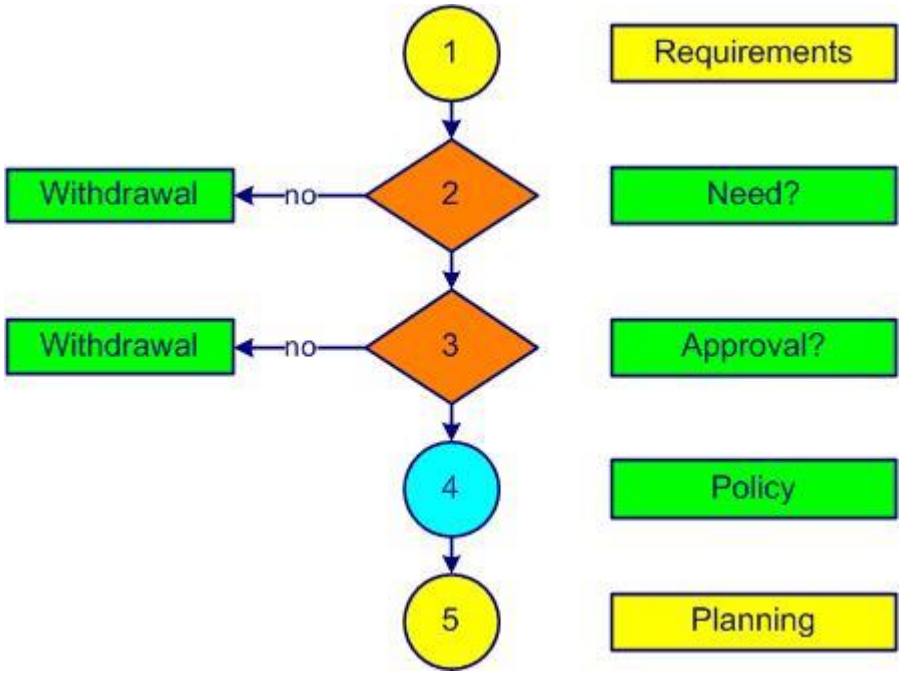


Figure 1-4. ISMS preparation

Step 1 involves identifying the needs and expectations (**requirements**) of interested parties:

- staff
- customers, consumers
- competitors
- shareholders, investors
- external providers (suppliers, subcontractors, partners)
- organizations and branch associations
- statutory and regulatory authorities

The involvement of top management at its highest level is truly indispensable. The advice of a consultant is often solicited. Determining the current status of the management system (whole or partial) would be welcome at this stage. An external certification body is chosen.

One of the key questions that comes up quickly (**step 2**) is the **need** for this decision. If this is not really necessary or if the estimated costs of the certification approach exceed the available resources, it is better to reject this idea immediately.

The benefits of implementing an information security management system are often:

- increased security of information systems
- enhanced resistance to threats and malware
- the information is only available to people who have permission
- the information is protected against any modification by unauthorized personnel
- improved protection of:
  - operational information
  - business secrets
  - intellectual property
  - personal data
- better defined responsibilities and obligations
- decreased likelihood of occurrence of information security incidents
- high level of risk control
- business disruptions avoided
- reduced insurance costs
- active involvement of staff in improving information security
- updated legal obligations
- strong integration of information security into business processes
- culture of continual improvement of information security
- you can sleep more peacefully 

The benefits of the certification of an information security management system are often:

- an improved image of the company
- being one step ahead of the competition
- new customers
- improved confidence of interested parties
- increased market share
- an increase in sales
- better financial performance

More than one and a half million businesses worldwide cannot be wrong!

The **third step** shall determine whether this approach receives the **approval** of the staff. A communication campaign is launched in-house on the objectives of an information security

management system (ISMS). The staff is aware and understands that, without their participation, the project cannot succeed.

Have confidence: success will come with the involvement and effort of all!

The vision (what we want to be), the mission (why we exist) and the business plan of the company are determined. The **following step** (**4**) includes the establishment of an outline of the information security **policy** and objectives. If you do not have a copy of the ISO 27001 standard, now is the time to get it (cf. sub-clause 2.1 of the present course).

Planning is the last **step** (**5**) of the project preparation for obtaining ISO 27001 certification. A reasonable period is between 12 to 24 months (each company is unique and specific). The financial resources and staff are confirmed by top management. A management representative is appointed as project leader. Top management commitment is formalized in a document communicated to all staff. A person is appointed as project leader for obtaining ISO 27001 certification.

The establishment and implementation of an ISO 27001 information security management system are shown in figure 1-5.

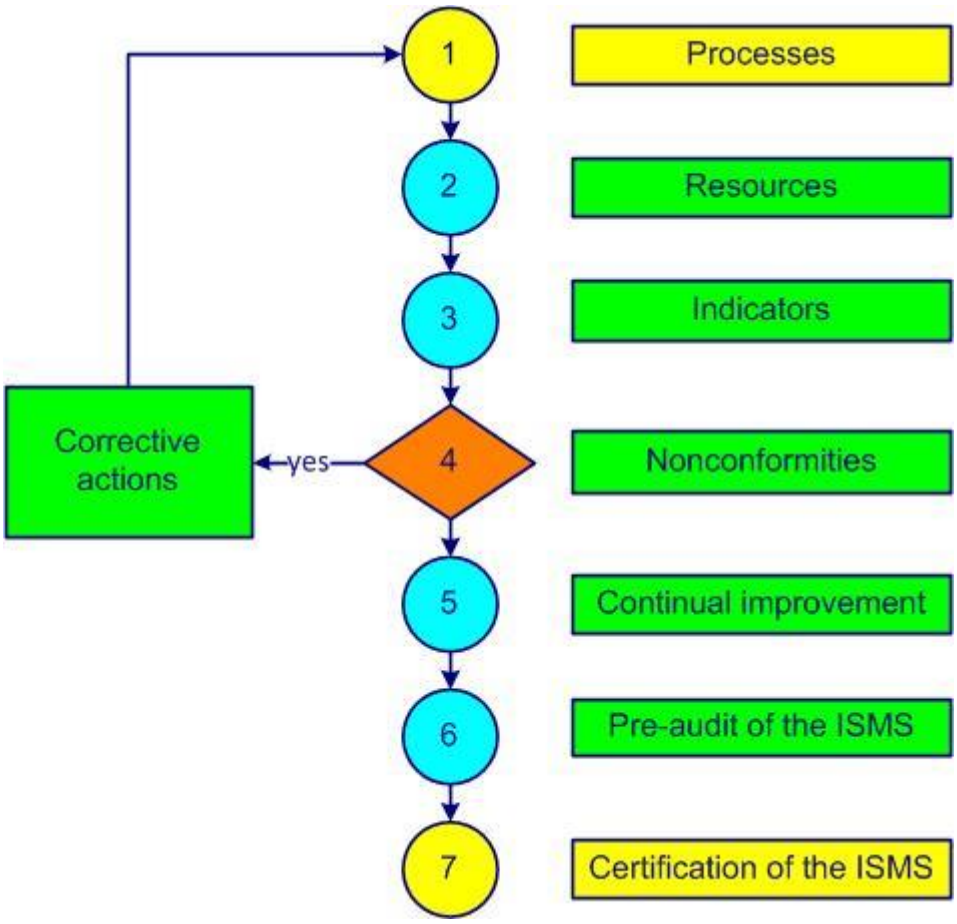


Figure 1-5. ISMS implementation

Step 1 aims to identify and determine the **processes**, interactions, owners, responsibilities and drafts of certain documented information. The first versions of process sheets, job descriptions and work instructions are written with the participation of the maximum number of available persons.

The necessary **resources** to achieve the information security objectives are determined in **step 2**. Planning tasks, responsibilities and time frames are established. Training of internal auditors is taken into account.

Step 3 allows you to set and implement methods for measuring the **effectiveness** and efficiency of each process. Internal audits help to evaluate the degree of implementation of the system.

Nonconformities of all kinds are listed in **step 4**. A first draft for dealing with waste is established. Corrective actions are implemented and documented.

A first encounter with the tools and application areas of **continual improvement** is made in **step 5**. Risks are determined, actions are planned and opportunities for improvement are sized. An approach to preventing nonconformities and eliminating causes is established. The internal and external communication is established and formalized.

To conduct the **pre-audit of the ISMS** (**step 6**), documented information is checked and approved by the appropriate people. A management review allows evaluation of compliance with applicable requirements. The information security policy and objectives are finalized. An information security manager from another company or a consultant can provide valuable feedback, suggestions and recommendations.

When the system is accurately implemented and followed, the **certification of the ISMS** by an external body is a breeze, a formality (**step 7**).

An example of a certification project plan with 26 steps is shown in annex 01.

An appropriate method for evaluating the performance of your information security management system is the RADAR logic model of excellence EFQM (European Foundation for Quality Management) with its 9 criteria and overall score of 1000 points.

The Deming cycle (figure 1-5) is applied to control any process. The PDCA cycles (Plan, Do, Check, Act) are a universal base for continual improvement.

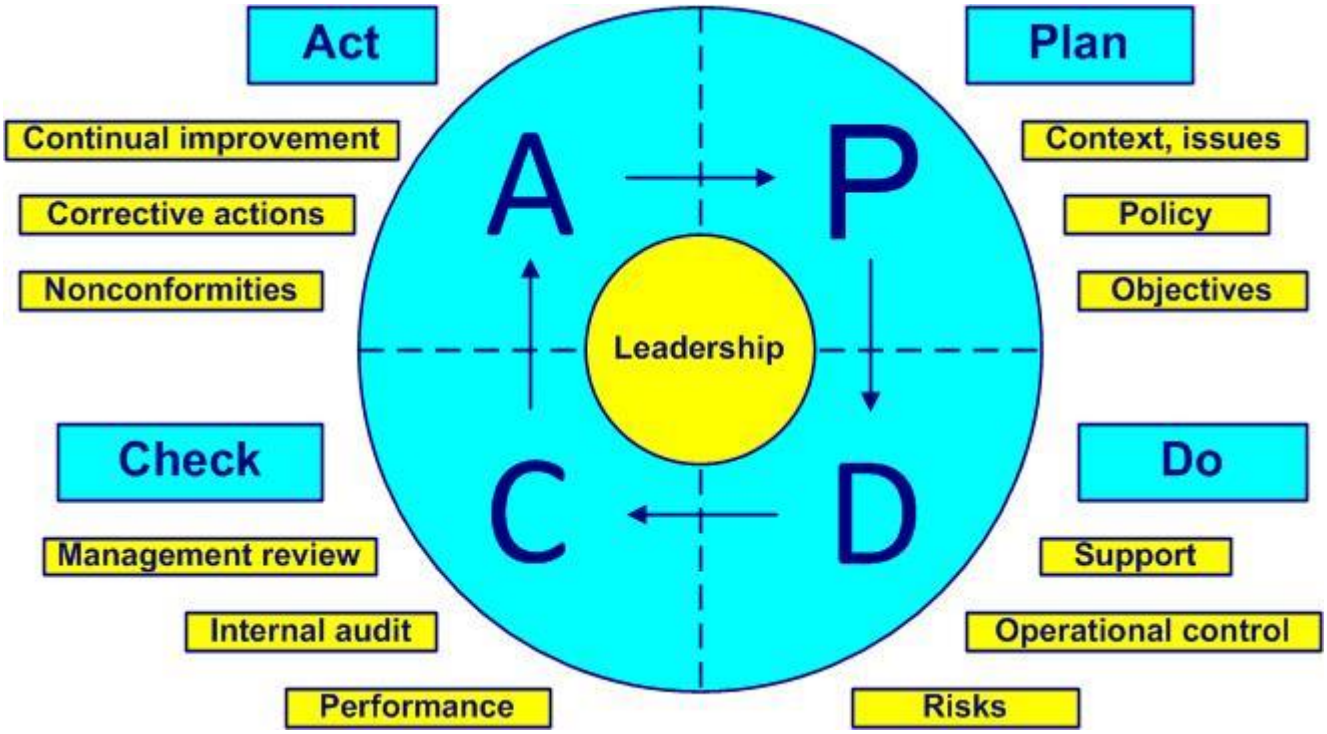


Figure 1-6. The Deming cycle

- Plan – define context, issues and processes, demonstrate leadership, establish policy and objectives (clauses 4, 5 and 6)
- Do – realize the product, treat risks, develop, implement and control processes, demonstrate leadership and bring support (clauses 5, 7 et 8)
- Check – compare, verify, evaluate risks, performance, inspect, analyze data, conduct audits and management reviews and demonstrate leadership (clauses 5 and 9)
- Act – adapt, demonstrate leadership, treat nonconformities, react with corrective actions and find new improvements (new PDCA cycle), (clauses 5 and 10)

For more information on the Deming cycle and its 14 points of management theory, you can consult the classic book "Out of the crisis", W. Edwards Deming, MIT press, 1982.

2 Standards, definitions, books

2.1 Standards

Plan ahead to avoid suffering

The ISO 27000 family includes a large number of standards. Some of the most used standards are shown in figure 2-1:

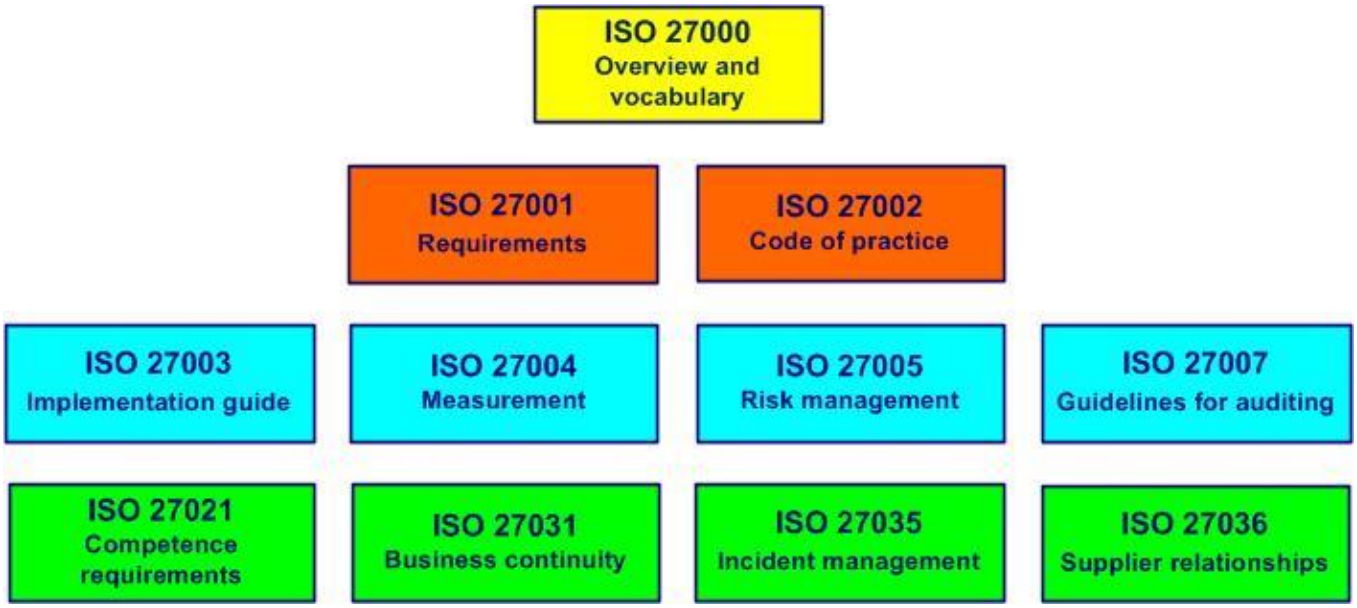


Figure 2-1. ISO 27000 family

- ISO 27000: 2018 - Information technology - Security techniques - Information security management systems (free - PAS - Publicly available specifications) - Overview and vocabulary
- ISO 27001: 2013 - Information technologies - Security techniques - Information security management systems - Requirements
- ISO 27002: 2013 Information technology - Security techniques - Code of practice for information security controls
- ISO 27003: 2017 - Information technology - Security techniques - Information security management systems - Guidance
- ISO 27004: 2016 - Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation
- ISO 27005: 2018 - Information technology - Security techniques - Information security risk management
- ISO 27007: 2020 - Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing
- ISO 27008: 2019 - Information technology - Security techniques - Guidelines for the assessment of information security controls
- ISO 27021: 2017 - Information technology - Security techniques - Competence requirements for information security management systems professionals
- ISO 27031: 2011 - Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity
- ISO 27035-1: 2016 - Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management
- ISO 27035-2: 2016 - Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response

- ISO 27035-3: 2020 - Information technology - Information security incident management - Part 3: Guidelines for ICT incident response operations
- ISO 27036-1: 2014 - Information technology - Security techniques (free - PAS - Publicly available specifications) - Information security for supplier relationships - Part 1: Overview and concepts
- ISO 27036-2: 2014 - Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements

Note: some "more recent" versions (example for ISO 27001 and ISO 27002 version 2017), include minor fixes and revert to the current version in full (in this case those from 2013).

The standard on auditing is:

ISO 19011 (2018): Guidelines for auditing management systems

The standard ISO 31000: 2018 Risk Management - Guidelines establishes the principles and process for risk management, risk assessment and treatment.

The technical report ISO / TR 31004: 2013 Risk management - Guidelines for the implementation of ISO 31000 provides a better understanding of the principles and organizational framework of risk management.

The standard on business continuity is: ISO 22301 (2019) Security and resilience - Business continuity management systems - Requirements.

ISO standards (over 21,000) are used in countless fields and are recognized around the world.

Over 28,000 standards (in English and other languages) are available free of charge on the Public.resource.Org site.

2.2 Definitions

The beginning of wisdom is the definition of terms. Socrates

Some specific terms:

Asset: *any element of value to the organization*
Availability: *property of information to be usable in time (see also ISO 27000, 3.7)*
Backup: *copy of data in order to archive and protect against loss*
Competence: *personal skills, knowledge and experiences (see also ISO 9000, 3.10.4)*
Confidentiality: *property of information to be accessible only to authorized persons (see also ISO 27000, 3.10)*
Conformity: *fulfillment of a specified requirement (see also ISO 9000, 3.6.11)*
Corrective action: *action to eliminate the causes of nonconformity or any other undesirable event and to prevent their recurrence (see also ISO 9000, 3.12.2)*
Cryptography: *activities of codification and decoding of information*
Customer satisfaction: *top priority objective of every quality management system related to the satisfaction of customer requirements (see also ISO 9000, 3.9.2)*
Customer: *anyone who receives a product (see also ISO 9000, 3.2.4)*
Effectiveness: *capacity to realize planned activities with minimum effort (see also ISO 9000, 3.7.11)*
Efficiency: *financial relationship between achieved results and resources used (see also ISO 9000, 3.7.10)*
Incident (information security): *unwanted and unexpected event that can compromise information security (see also ISO 27000, 3.31)*

Indicator: *value of a parameter, associated with a process objective, allowing the objective measure of its effectiveness (see also FD X50-171, 2.1)*
Information security (IS): *controls to protect the confidentiality, integrity and availability of information (see also ISO 27000, 3.28)*
Integrity: *property of information to be unaltered (see also ISO 27000, 3.36)*
Interested party: *person, group or company affected by the impacts from an organization (see also ISO 9000, 3.2.3)*
IS: *information security*
ISMS: *information security management system*
Management system: *set of processes allowing objectives to be achieved (see also ISO 9000, 3.5.3)*
Nonconformity: *non-fulfillment of a specified requirement (see also ISO 9000, 3.6.9)*
Objective: *measurable goal to be achieved*
Organization (company): *structure that satisfies a need (see also ISO 9000, 3.2.1)*
Process: *activities that transform inputs into outputs (see also ISO 9000, 3.4.1)*
Product (or service): *any outcome of a process or activity (see also ISO 9000, 3.4.2)*
Quality: *aptitude to fulfill requirements (see also ISO 9000, 3.6.2)*
Requirement: *explicit or implicit need or expectation (see also ISO 9000, 3.6.4)*
Residual risk: *risk accepted (see also ISO Guide 73, 3.8.1.6)*
Risk assessment: *risk identification, analysis and evaluation process (see also ISO Guide 73, 3.4.1)*
Risk treatment: *risk reduction activities (see also ISO Guide 73, 3.8.1)*
Risk: *likelihood of occurrence of a threat or an opportunity (see also ISO Guide 73, 1.1)*
Statement of applicability (SoA): *document describing the objectives and security controls*
Supplier (external provider): *an entity that provides a product (see also ISO 9000, 3.2.5)*
Top management: *group or persons in charge of the organizational control at the highest level (see also ISO 9000, 3.1.1)*
Traceability: *aptitude to memorize or restore all or part of a trace of executed functions (see also ISO 9000, 3.6.13)*
VLAN : *Virtual Local Area Network*
Vulnerability: *weakness of an asset that could lead to unauthorized access (see also ISO 27000, 3.77)*

In the terminology of management systems, do not confuse:

- accident and incident
  - an accident is an unexpected serious event
  - an incident is an event which can lead to an accident
- anomaly, defect, dysfunction, failure, nonconformity, reject and waste:
  - anomaly is a deviation from what is expected
  - defect is the non-fulfillment of a requirement related to an intended use
  - dysfunction is a degraded function which can lead to a failure
  - failure is when a function has become unfit
  - nonconformity is the non-fulfillment of a requirement in production
  - reject is a nonconforming product which will be destroyed
  - waste is when there are added costs but no value
- audit program and plan
  - an audit program is the annual planning of the audits
  - an audit plan is the description of the audit activities
- audit, inspection, auditee and auditor
  - an audit is the process of obtaining audit evidence
  - an inspection is conformity verification of a process or product
  - an auditee is the one who is audited
  - an auditor is the one who conducts the audit
- control and optimize

    - control is meeting the objectives
    - optimize is searching for the best possible results
- customer, external provider and subcontractor
    - a customer receives a product
    - an external provider provides a product on which specific work is done
    - a subcontractor provides service or product on which specific work is done
- effectiveness and efficiency
    - effectiveness is the level of achievement of planned results
    - efficiency is the ratio between results and resources
- follow-up and review
    - follow-up is the verification of the obtained results of an action
    - review is the analysis of the effectiveness in achieving objectives
- inform and communicate
    - to inform is to give someone meaningful data
    - to communicate is to pass on a message, to listen to the reaction and discuss
- objective and indicator
    - an objective is a sought after commitment
    - an indicator is the information on the difference between the pre-set objective and the achieved result
- organization and enterprise, society, company
    - organization is the term used by the ISO 9001 standard as the entity between the supplier and the customer
    - enterprise, society, company are examples of organizations
- process, procedure, product, activity and task
    - a process is how we satisfy the customer using people to achieve the objectives
    - a procedure is the description of how we should conform to the rules
    - a product is the result of a process
    - an activity is a set of tasks
    - a task is a sequence of simple operations
- safety and security
    - safety is prevention against malicious risks
    - security is prevention against risks of unintentional origin

Information is stored in multiple ways such as:

- digital (data stored electronically)
- physical form (on paper or other)
- knowledge (the know-how of the staff)

Information is transmitted in different ways such as:

- digital (electronic mail)
- physically (post)
- verbally (meetings)

Remark 1: the use of ISO 27000 and ISO 9000 definitions is recommended. The most important thing is to determine a common and unequivocal vocabulary for everyone in the company.

Remark 2: the customer can also be the user, the beneficiary, the trigger, the ordering party or the consumer.

Remark 3: documented information is any information which we must maintain (procedure) or retain (record).

Remark 4: an asset is a broad concept. An asset can be:

- *an information*
- *a document*
- *an archive*
- *an infrastructure*
- *a technical equipment*
- *a software*
- *the staff*
- *the reputation of the organization*
- *a process*
- *a service*

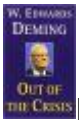
For other definitions, comments, explanations and interpretations that you do not find in this module and Annex 06 you can consult:

- ISO online consultation platform (OBP)
- IEC Electropedia

2.3 Books

When I think of all the books still left for me to read, I am certain of further happiness.
Jules Renard

Books for further reading on quality and information security:

- 

Edwards Deming, Out of the crisis, MIT Press, 1982
- 

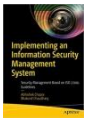
Eliyahu Goldratt, Jeff Cox, The Goal, A Process of Ongoing Improvement, North River Press, 1984
- 

Masaaki Imai, KAIZEN, The key to Japan's competitive success, McGraw-Hill, 1986
- 

Edward Humphreys, Implementing the ISO/IEC 27001 2013 ISMS Standard, Artech House, 2016
- 
Douglas Landoll, Information security policies, procedures, and standards, Auerbach Publications, 2016

- 

Dejan Kosutic, Secure & simple, A small-business guide to implementing iso 27001 on your own, Advisera Expert Solutions, 2016
- 
Dejan Kosutic, ISO 27001 Risk management in plain english, step-by-step handbook for information security practitioners in small businesses, Advisera Expert Solutions, 2016
- 
Dejan Kosutic, ISO 27001 annex A controls in plain english, Step-by-step handbook for information security practitioners in small businesses, Advisera Expert Solutions, 2016
- 
Raphaël Hertzog et al, Kali Linux Revealed: Mastering the Penetration Testing Distribution, OFFSEC Press, 2017
- 

Cees van der Wens, ISO 27001 handbook: Implementing and auditing an 'Information Security Management System' in small and medium-sized businesses, Brave New Books, 2020
- 

Abhishek Chopra, Mukund Chaudary, Implementing an Information Security Management System, Apress, 2020

3 Process approach

3.1 Process

If you cannot describe what you are doing as a process, you do not know what you're doing. Edwards Deming

The word process comes from the Latin root procedere = go, development, progress (Pro = forward, cedere = go). Each process transforms inputs into outputs, creating added value and potential nuisances.

A process has three basic elements: inputs, activities and outputs. 

A process can be very complex (launch a rocket) or relatively simple (audit a product). A process is:

- repeatable
- foreseeable
- measurable
- definable
- dependent on its context
- responsible for its external providers

A process is, among others things, determined by its:

- title and type
- purpose (why?)
- beneficiary (for whom?)
- scope and activities
- initiators
- documented information
- inputs
- outputs (intentional and not intentional)
- restraints
- people
- material resources
- objectives and indicators
- person in charge (owner) and actors (participants)
- means of inspection (monitoring, measurement)
- mapping
- interaction with other processes
- risks and potential deviations
- opportunities for continual improvement

A process review is conducted periodically by the process owner (cf. annex 02).

Review: *a survey of a file, product, process so as to verify if pre-set objectives are achieved*

The components of a process are shown in figure 3-1: 

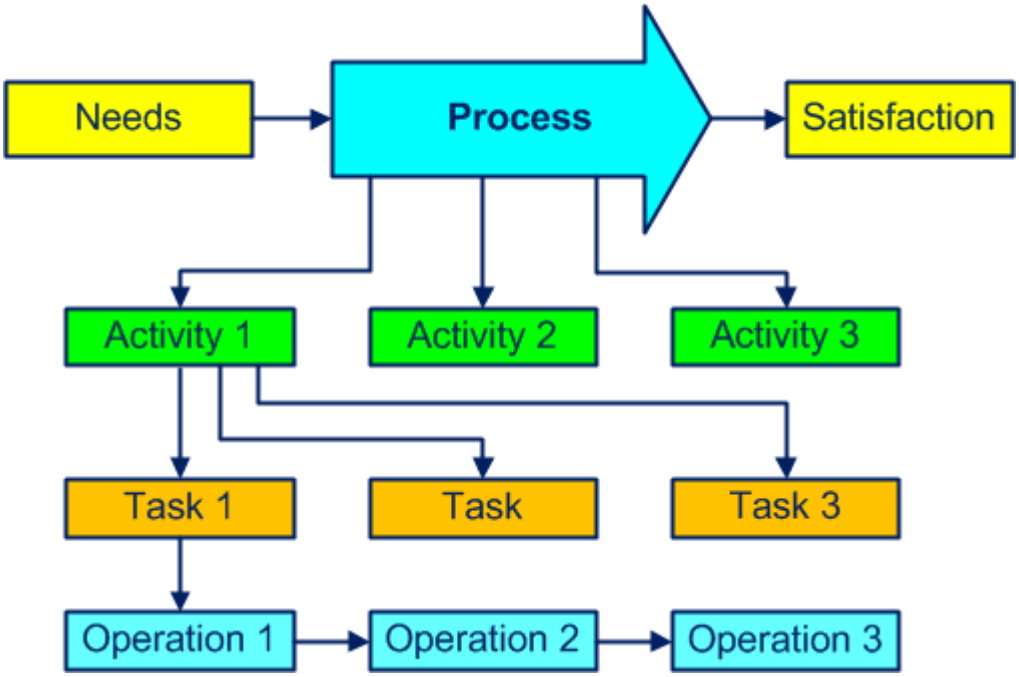


Figure 3-1. Components of a process

Figure 3-2 shows an example that helps to answer some questions:

- which materials, which documents, which tooling? (inputs)
- which title, what objective, which activities, requirements, constraints? (process)
- which products, which documents? (outputs)
- how, which inspections? (methods)
- what is the level of performance? (indicators)
- who, with what competence? (people)
- with what, which machines, which equipment? (material resources)

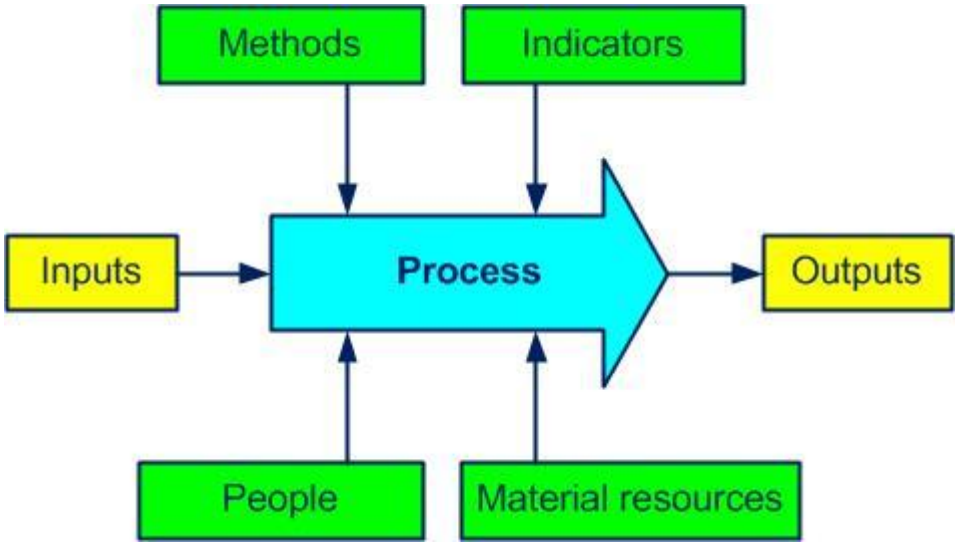


Figure 3-2. Some elements of a process

Often the output of a process is the input of the next process.

You can find some examples of process sheets in the document pack D 02 and a list of processes in annex 03.

Any organization (company) can be considered as a macro process, with its purpose, its inputs (customer needs and expectations) and its outputs (products/services to meet customer requirements).

Our preference is to identify a process using a verb (buy, produce, sell) instead of a noun (purchases, production, sales) to differentiate the process from the company's department or documented information to maintain and recall the purpose of the process.

The processes are (as we shall see in the following paragraphs) of management, realization and support types. Do not attach too much importance to process categorizing (sometimes it's very relative) but ensure that all the company's activities at least fall into one process.

3.1.1 Management processes

Management processes are also known as piloting, decision, key or major processes. They take part in the overall organization, elaboration of the policy, deployment of the objectives and all needed checks. They are the glue of all the realization and support processes.

The following processes can be part of this family (* mandatory):

- assess risks*
- treat risks*
- communicate*
- conduct an audit *
- plan the ISMS
- establish process ownership
- develop strategy
- establish policy
- deploy objectives
- conduct management review
- improve

3.1.2 Realization processes

The realization (operational) processes are related to the product, increase the added value and contribute directly to customer satisfaction.

They are mainly (* mandatory):

- meet security requirements*
- control outsourced processes*
- register and unsubscribe*
- distribute access*
- manage authentication*
- develop and support security*
- manage security continuity*
- implement security*
- inspect security*
- design and develop
- purchase
- maintain equipment
- manage networks
- manage changes
- control nonconformities
- implement corrective actions

3.1.3 Support processes

The support processes provide the resources necessary for the proper functioning of all other processes. They are not directly related to a contribution of the product's added value, but are still essential.

The support processes are often (* mandatory):

- apply discipline*
- manage the employment contract*
- maintain regulatory watch
- acquire and maintain infrastructure
- manage inspection means
- provide training
- provide information
- control documentation

3.2 Process mapping

Par excellence process “mapping” is a multidisciplinary work. This is not a formal requirement of the ISO 27001 standard but is always welcome.

The 3 types of processes and some interactions are shown in figure 3-3.

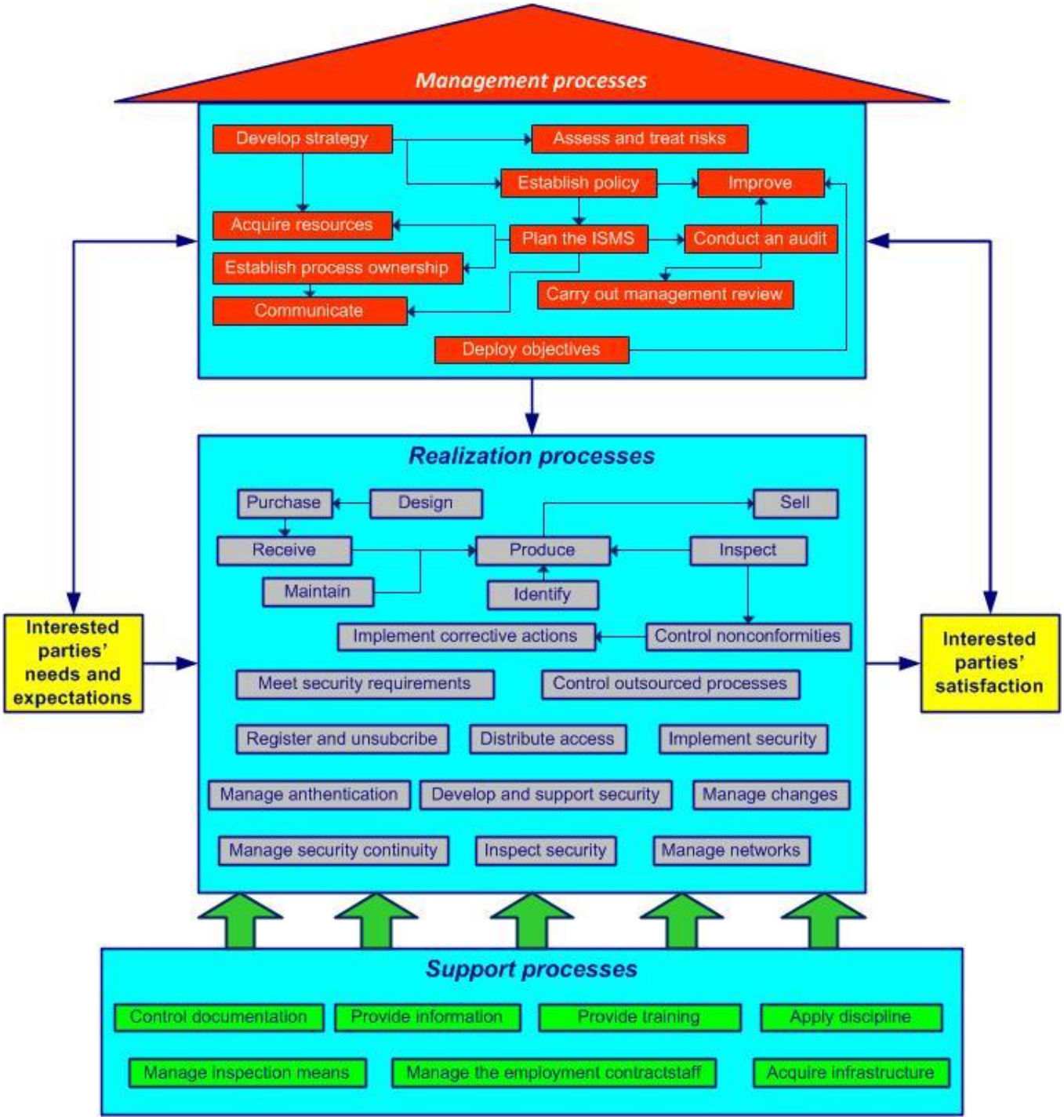


Figure 3-3. The process house

In the outputs, do not underestimate unwanted products such as rubbish, pollution, rejects.

Mapping, among other things, allows you to:

- obtain a global vision of the company
- identify the beneficiaries (customers), flows and interactions
- define rules (simple) for communication between processes

To obtain a clearer picture, you can simplify by using a total of about fifteen core processes. A core process can contain several sub-processes: for example, the process "develop the ISMS" can involve:

- develop strategy
- establish policy
- assess risks
- treat risks
- plan the ISMS
- deploy objectives
- establish process ownership
- improve

An example of “design” process is shown in figure 3-4:

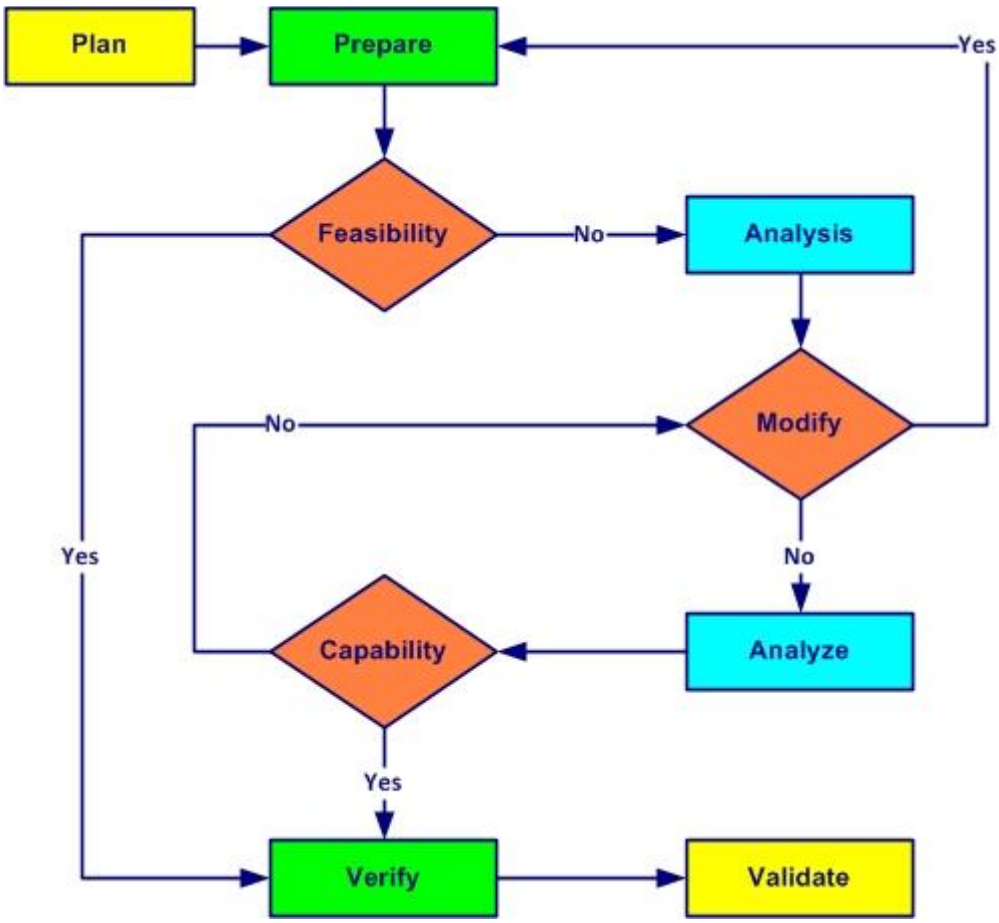


Figure 3-4. Design process

3.3 Process approach

Simple solutions for now, perfection for later

Process approach: *management by the processes to better satisfy customers, improve the effectiveness of all processes and increase global efficiency*

The process approach contributes enormously to the efficient management of the company (cf. annex 04).

When the process approach is integrated during the development, implementation and continual improvement of an information security management system, it allows one to achieve objectives that are related to customer satisfaction, as is shown in figure 3-5.

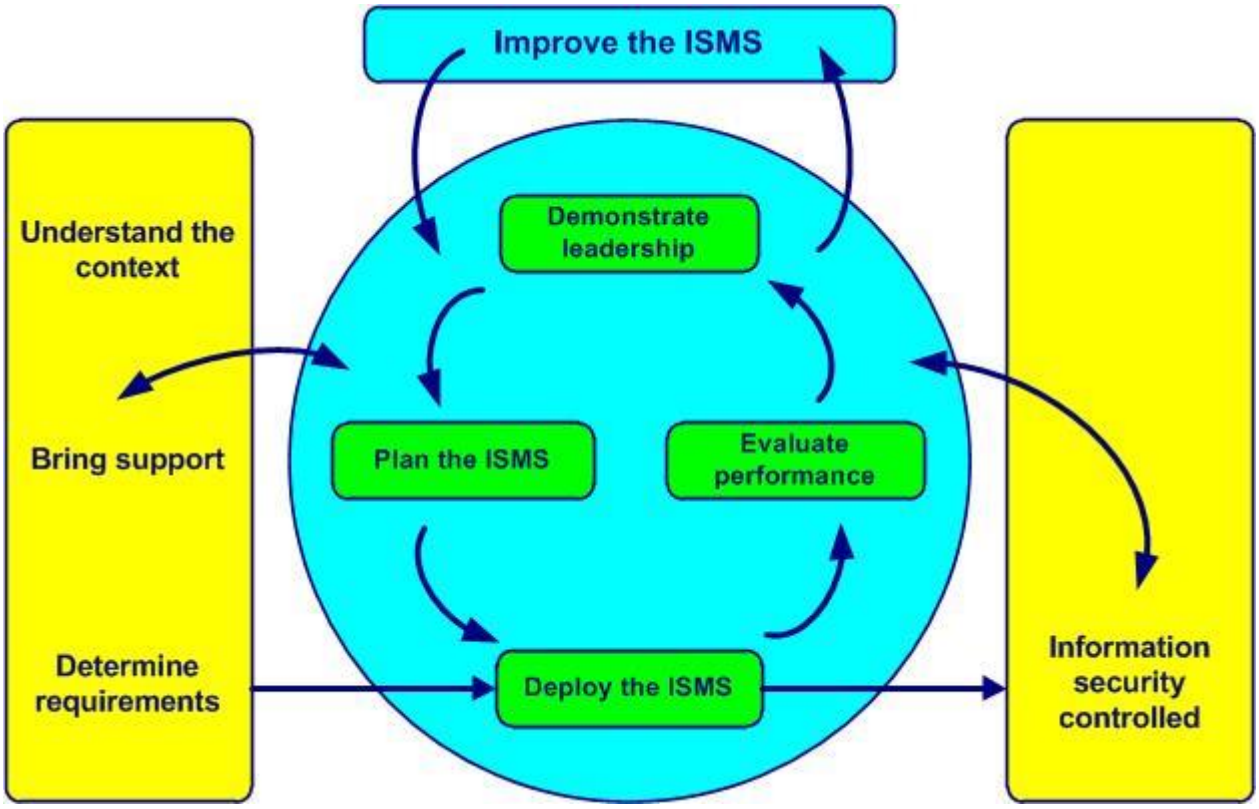


Figure 3-5. Model of an ISMS based on process approach and continual improvement

The process approach:

- emphasizes the importance of:
  - understanding and complying with customer requirements
  - prevention so as to react to unwanted elements such as:
    - customer returns
    - waste
  - measuring process performance, effectiveness and efficiency
  - permanently improving objectives based on pertinent measurements
  - process added value
- relies on:
  - methodical identification
  - interactions
  - the sequence and
  - process management which consists of:
    - determining objectives and their indicators
    - piloting related activities
    - analyzing obtained results
    - permanently undertaking improvements
- allows one to:
  - better view inputs and outputs and their relationship
  - clarify roles and responsibilities
  - judiciously assign necessary resources
  - break down barriers between departments
  - decrease costs, delays and wastes
- and ensures in the long run:
  - control
  - monitoring and
  - continual improvement of processes

The process approach **is not**:

- crisis management ("You will not solve the problems by addressing the effects")
- blaming people (“Poor quality is the result of poor management." Masaaki Imai)
- priority to investments (“Use your brain, not your money." Taiichi Ohno)

4 Context

4.1 The organisation and its context *(requirement 1)*

The two most important things in a company do not appear in its balance sheet: its reputation and its people. Henry Ford

Integrating ISMS requirements into business processes ensures that interested parties (i.e. customers) control the risks associated with information security. Adopting these requirements is a strategic top management decision.

To successfully implement an information security management system, it is necessary to understand and assess everything that can influence the purpose and performance of the organization. It is advisable to engage in in-depth reflection after a few essential activities:

- draw up an in-depth diagnosis of the unique context in which the organization finds itself, taking into account the issues:
  - external such as the environment:
    - social
    - regulatory
    - economical
    - political
    - technological
    - natural
  - internal like:
    - specific aspects of corporate culture:
      - vision
      - reason to exist, purpose, mission
      - core values
    - staff
    - products and services
    - processes, policies, procedures, instructions, objectives
    - infrastructure
- monitor and regularly review all information relating to external and internal issues
- analyze the factors that may influence the achievement of the organization's objectives

Each issue is identified by its level of influence and control. Priority is given to issues that are very influential and not at all under control. External and internal issues.

PESTEL and SWOT analyses (our strengths and weaknesses, opportunities and threats) can be useful for a relevant analysis of the context of the organization (see annex 05). SWOT analysis helps to understand our business environment. It also allows us to identify internal and external problems, which could have an impact on information security.

Good practices

- *diagnosis of the context includes the main external and internal issues*
- *the core values as part of the corporate culture are taken into account in the context of the company*
- *the results of the context analysis are widely diffused*
- *the SWOT analysis includes many relevant examples*
- *the SWOT analysis is a powerful tool for identifying the main threats and opportunities*

Bad practices

- *the issues of the context of the company, such as the competitive environment, are not taken into account*
- *in some cases, the corporate culture is not taken into account*
- *risk analysis does not take into account strategic issues*
- *no clear link between the SWOT analysis and the actions undertaken*
- *the scope of the ISMS procedure is classified as confidential*

4.2 Needs and expectations of interested parties *(requirements 2 to 3)*

There is only one valid definition of a business purpose: to create a customer. Peter Drucker

To fully understand the needs and expectations of interested parties, it is necessary to start by determining all those who may be affected by the information security management system, for example:

- employees
- top management
- customers
- external providers (suppliers, subcontractors, consultants)
- owners
- shareholders
- bankers
- distributors
- competitors
- citizens
- neighbors
- social and political organizations

The list of interested parties is created by a multidisciplinary team. Every interested party is identified by its level of influence and control. Priority is given to interested parties with great influence and poor control. List of interested parties.

The requirements of interested parties, which change over time, are reviewed regularly (see the Maintain regulatory watch process, annex 03).

True story

The customer is king but we still can fight against rudeness. This example is taken from the restaurant La petite Syrah in Nice and its coffee prices:

"A coffee"……7 €

"A coffee, please……..…4,25 €
"Hello, a coffee, please……1,40 €

Anticipating the reasonable and relevant needs and expectations of interested parties is:

- meeting the requirements of the ISMS
- preparing to address risks
- seize improvement opportunities

When a requirement is accepted, it becomes an internal requirement of the ISMS.

Good practices

- *the list of interested parties is updated*
- *the needs and expectations of interested parties are established through meetings on site, surveys, roundtables and meetings (monthly or frequent)*
- *the application of statutory and regulatory requirements is a prevention approach and not a constraint*

Bad practices

- *statutory and regulatory requirements are not taken into account*
- *the delivery time is not validated by the customer*
- *the expectations of interested parties are not determined*
- *the list of interested parties does not contain their area of activity*

4.3 Scope *(requirements 4 to 8)*

In many areas, the winner is the one who is best informed. André Muller

The scope (or in other words the perimeter) of the information security management system is defined and validated by top management.

The Statement of Applicability - SoA (cf. sub-clause 6.1.3 and annex 07) allows us to: 

- determine what is or is not part of the ISMS
- identify and update the controls to be applied
- answer the questions for each control:
  - what needs to be done?
  - why?
  - how?
  - what is its status?
- plan and audit the ISMS

Each control of the statement of applicability is directly linked to the treatment of a risk.

To properly determine the scope of the ISMS, the specificities of the context of the organization are taken into account such as:

- the issues (see sub-clause 4.1)
- the activities of the organization, including support
- corporate culture
- the environment:
  - social

    - financial
    - technological
    - economical
- the requirements of the interested parties (see sub-clause 4.2)
- outsourced processes

The Scope of the ISMS is available as documented information.  It includes the scope (limits and interfaces):

- of the organization:
    - products
    - services
- information and communication:
    - software design and development
    - maintenance
- physical:
    - head office
    - subsidiaries

Good practices

- *the scope is relevant and available upon request*
- *non applicable requirements are justified in writing*
- *the department not included in the field of activity is treated as a supplier with all the consequences (contract, confidentiality agreement, performance monitoring)*

Bad practices

- *some products are outside the scope of the ISMS without justification*
- *the scope is obsolete (the new subsidiary is not included)*
- *the scope is not validated by top management*

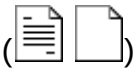
4.4 Information security management system *(requirement 9)*

The requirements of the ISO 27001 standard are linked to the control of:

- information security and
- organizational processes

To do this:

- the information security management system is:
    - planned (see the Plan the ISMS process, annex 03)
    - established
    - documented (a simple and sufficient documentary system is in place)
    - set up and
    - continually improved
- the information security policy, objectives, resources and working environment are determined
- threats are determined and actions to reduce them are established (see sub-clause 6.1)
- the essential processes necessary for the ISMS are controlled (cf. the process Establish process ownership, annex 03): 
    - the corresponding resources assured

    - the determined input and output elements
    - the necessary information available
    - the named owners (responsibilities and authorities defined)
    - determined sequences and interactions
    - each process is measured and monitored (criteria established), objectives are established and performance indicators analyzed
    - process performance is evaluated
    - necessary changes are introduced to achieve expected results
    - actions to obtain continual improvement of processes are established
- the strict minimum necessary ("as much as necessary") of Documented information on the processes is maintained and retained ()

The information security manual is not a requirement of the ISO 27001 standard but it is always a possible method to present the organization, its ISMS and its procedures, policies and processes (see annex 08).

 Pitfalls to avoid:

- going overboard on quality: 
    - a useless operation is performed without adding value and without the customer asking for it - it is a waste, cf. quality tools D 12
- having all procedures written by the information security manager: 
    - information security is everybody's business, "the staff is conscious of the relevance and importance of each to the contribution to information security objectives", which is even more true for department heads and process owners
- forgetting to take into account the specificities related to the corporate culture: 
    - innovation, luxury, secret, authoritarian management (Apple)
    - strong culture related to ecology, action and struggle, while cultivating secrecy (Greenpeace)
    - fun and quirky corporate culture (Michel & Augustin)
    - liberated company, the man is good, love his customer, shared dream (Favi)

The requirements of the ISO 27001 standard are shown in figures 4-1 and the dedicated page:

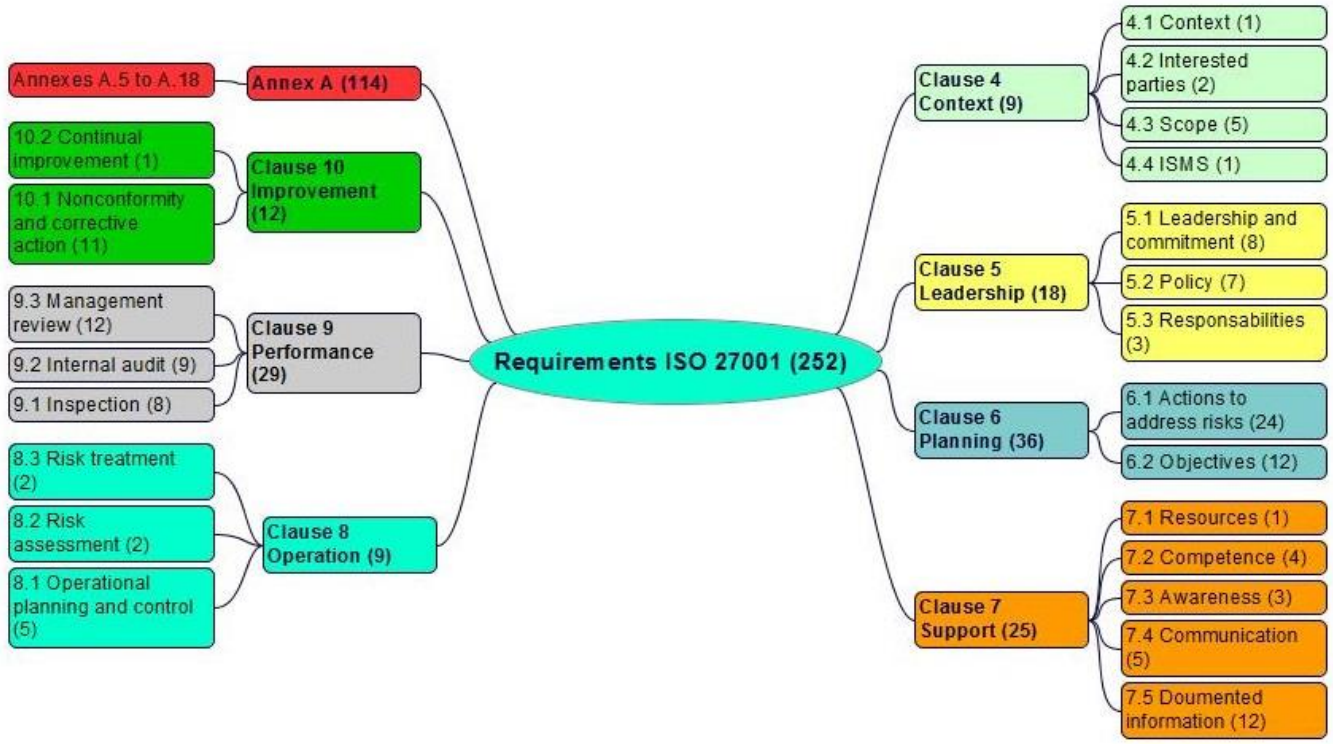


Figure 4-1. The requirements of the ISO 27001 standard

Information security requirements concern:

- the risks of the organization:
  - threats to assets
  - the vulnerability and likelihood of occurrence
  - the consequences
- legal and contractual requirements
- the principles, objectives and information control obligations related to business processes

Good practices

- *the process map has enough arrows to show who the customer (internal or external) is*
- *for a process, it is better to use a lot of arrows (several customers) rather than to forget one*
- *reveal the added value of the process during the process review*
- *the analysis of process performance is an example of continual improvement and evidence of the effectiveness of the ISMS*
- *top management regularly monitors the objectives and action plans*
- *the purpose of each process is clearly defined*
- *top management's commitments on continual improvement are widely diffused*
- *the innovation potential is confirmed by the increase in sales of new products*

Bad practices

- *some process outputs are not set correctly (customers not considered)*
- *process efficiency criteria are not established*
- *process owner is not formalized*
- *outsourced processes are not determined*
- *very real activities are not identified in any process*
- *control of outsourced services is not described*

- *sequences and interactions of certain processes are not determined*
- *criteria and methods for ensuring effective processes are not determined*
- *monitoring the effectiveness of certain processes is not established*
- *the ISMS resources do not allow achievement of information security objectives*
- *the ISMS is not updated (new processes are not determined)*
- *the threats and weaknesses identified in the SWOT analysis remain without actions*