Learning Objectives

By the end of this training course, the participants will be able to:

1. Explain the fundamental concepts and principles of an information security management system (ISMS) based on ISO/IEC 27001
2. Interpret the ISO/IEC 27001 requirements for an ISMS from the perspective of an implementer
3. Initiate and plan the implementation of an ISMS based on ISO/IEC 27001, by utilizing PECB's IMS2 Methodology and other best practices
4. Support an organization in operating, maintaining, and continually improving an ISMS based on ISO/IEC 27001
5. Prepare an organization to undergo a third-party certification audit

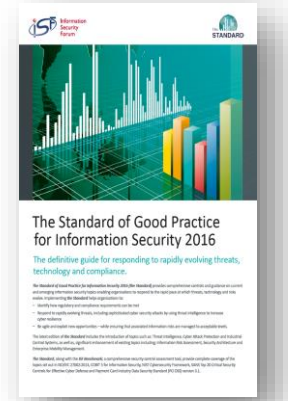
Information Security Framework Landscape

PCI DSS

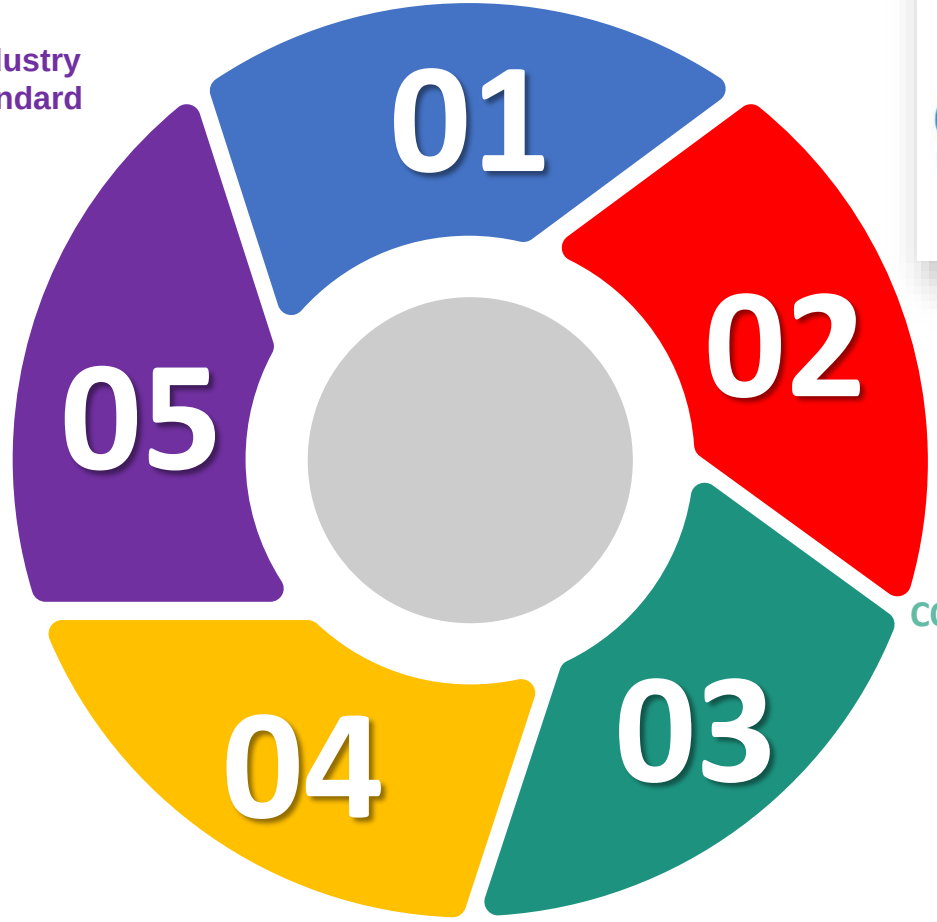
Payment Card Industry
Data Security Standard

ISO 27001

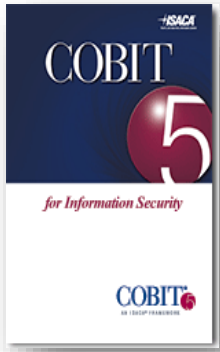
ISF Standard for Good Practice



SANS Critical security controls



COBIT 5 For information Security



What Is ISO?

ISO is an international organization of national standards bodies from over 160 countries.

The final results of ISO works are published as international standards.

ISO has published over 24,000 standards since 1947.

The ISO/IEC 27000 family of standards is a series of information security standards. It includes the following:

- **ISO/IEC 27000:** Presents the basic concepts and the vocabulary that applies when establishing an information security management system (A free copy of this standard can be downloaded on the ISO website.)
- **ISO/IEC 27001:** Defines the requirements for an information security management system (ISMS) and provides a reference set of security controls in its Annex A
- **ISO/IEC 27701:** Specifies the requirements and provides guidance for establishing, maintaining, and continually improving a privacy information management system (PIMS) as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management (as a result of the processing of PII)
- **ISO/IEC 27002:** Provides generic information security controls and their implementation guidance
- **ISO/IEC 27003:** Guidance on implementing or setting up an ISMS
- **ISO/IEC 27004:** Guidance on monitoring and measuring information security performance and ISMS effectiveness
- **ISO/IEC 27005:** Guidance on managing information security risks, in accordance with ISO/IEC 27001

ISO/IEC 27001

- The standard specifies requirements for an ISMS (clauses 4 to 10).
- Requirements (clauses) are expressed with the verb “shall.”
- Annex A contains 93 information security controls categorized into 4 groups.
- Organizations can obtain certification against this standard.


INTERNATIONAL STANDARD

ISO/IEC 27001

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ISO/IEC 27002

- The standard provides a list of generic information security controls and their implementation guidance.
- Clauses are expressed with the verb “should.”
- Organizations cannot obtain certification against this standard.

ISO/IEC 27003

- The standard provides guidance on the requirements for an information security management system.
- It serves as a reference document to be used with ISO/IEC 27001 and ISO/IEC 27002 standards.
- It is composed of 10 clauses.
- Organizations cannot obtain certification against this standard.

The Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards which unify the information security programs and policies with regard to credit card information.
- PCI DSS applies to any organization that accepts, transmits, or stores any cardholder data.
- PCI Security Standards Council was founded in 2006 by American Express, Discover, JCB International, MasterCard, and Visa Inc.

Benefits Of ISO 27001 Certification

Value Proposition Of ISO 27001 Certification

Information Security Effectiveness

- Executive Management visibility and support for security
- increase security accountability
- Adequate and effective protection of key Asset
- improved awareness and security minded cutler
- Improved resilience and agility

Compliance

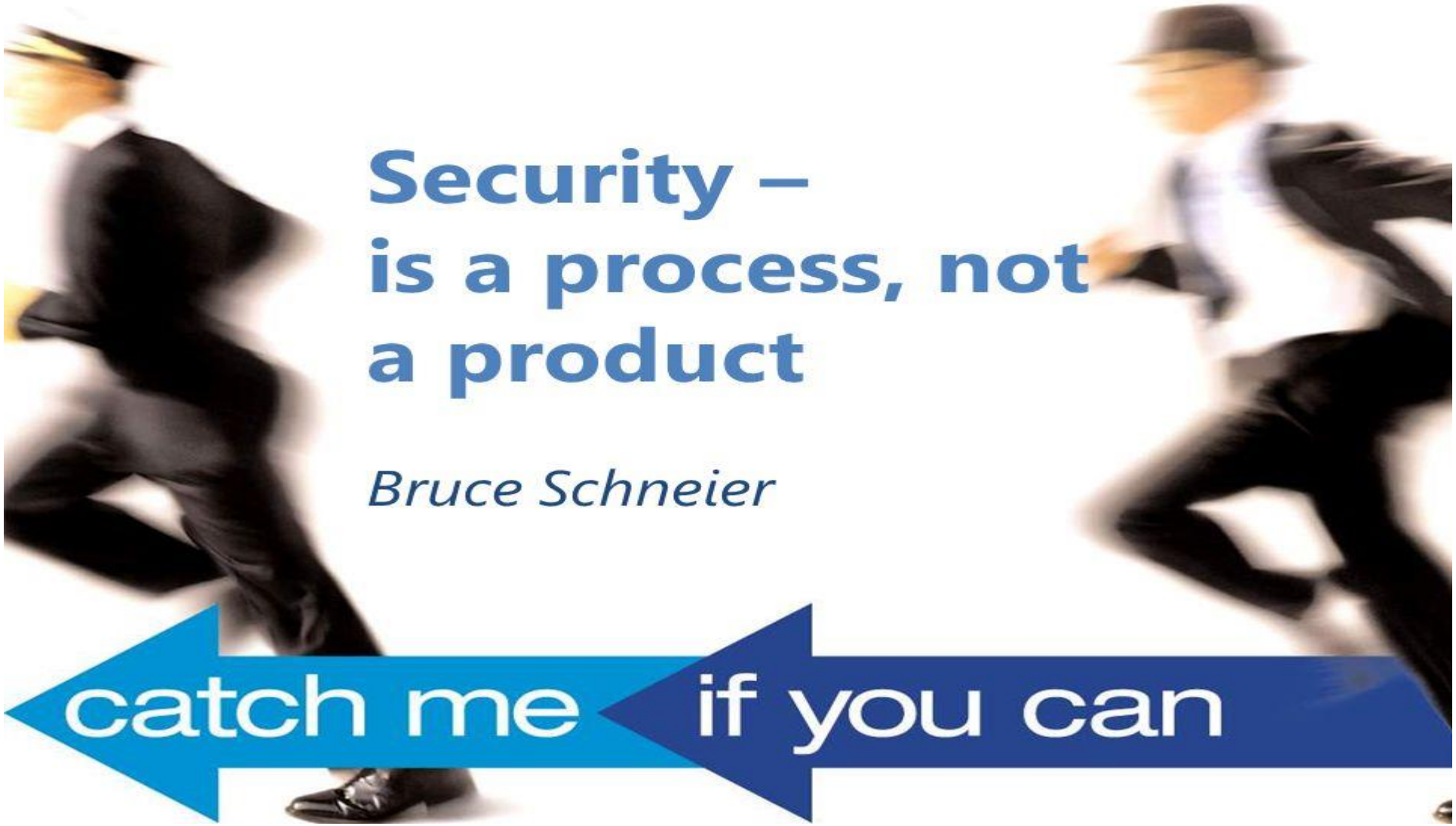
- Compliance with applicable regulations and legislation
- Compliance with government rules and
- Compliance with organizational directives
- Reduction on audit costs and efforts
- Ability to respond efficiently to change on compliance land scape

Building and maintaining trusted relationship

- Market differentiation
- Confidence to stakeholder
- Reputation protection
- Brand enhancement
- Increase in trusted in relationship with third parties.
- Expected financial return

Risk Mitigation

- Risk insight
- Risk prioritization
- Risk avoidance
- Risk mitigation
- Cost avoidance
- Faster , easier recovery from attack.


Security –
is a process, not
a product
Bruce Schneier
catch me
if you can

1. **Which standard below provides requirements for an information security management system (ISMS)?**
    A. ISO/IEC 27001
    B. ISO/IEC 27002
    C. ISO/IEC 27000
2. **Which of the statements below is correct?**
    A. Organizations can obtain certification against ISO/IEC 27001
    B. Organizations can obtain certification against ISO/IEC 27005
    C. Organizations cannot obtain certification against ISO/IEC 27001
3. **Which international standard provides a reference set of information security controls?**
    A. ISO/IEC 27002
    B. ISO/IEC 27701
    C. ISO/IEC 27005

4. **In what areas do ISO/IEC 27001 and the General Data Protection Regulation (GDPR) overlap?**
    A. PII collection and processing and the rights of data subjects
    B. Data confidentiality, availability, and integrity, and risk assessment
    C. Physical security, access control, and continual improvement

Management System Standards

Organizations can get certified to the following primary standards:

ISO 9001

Quality management

ISO 14001

Environmental management

ISO 45001

Occupational health and safety management

ISO/IEC 20000-1

Service management

ISO 22000

Food safety management system

ISO 22301

Business continuity management

ISO/IEC 27001

Information security management system

ISO 28000

Security management

What is Information

ISO 27001 is about Information Security

- Information is an organizational asset, which has a value and needs to be appropriately protected
- Without protections information can:
  - Lose confidentiality
  - Be modified, with or without our knowledge
  - Be deleted or lost irreparably
  - Be made unavailable

Why is information important?

How would you deliver your business services if you lost information?

– Customer information
– Systems documentation and configuration
– Business and marketing plans
– Procedures for key processes
– Financial information

ISO 27001 is about protection of information in support of the business

Information covered by ISO27001

- Internal
  Information that you would not want your competitors to know
- Customer/client/supplier
  Information that they would not wish you to disclose
- Shared
  Information that needs to be shared with other trading partners

Company strategy

Client NID

Information security

ISO27001 is concerned with the preservation of

- Confidentiality
- Integrity
- Availability

However an organization may also consider

- Authorization
- Non-repudiation
- Accountability

Examples of information

Paper

- Documents
- Ordinary mail

Electronic media

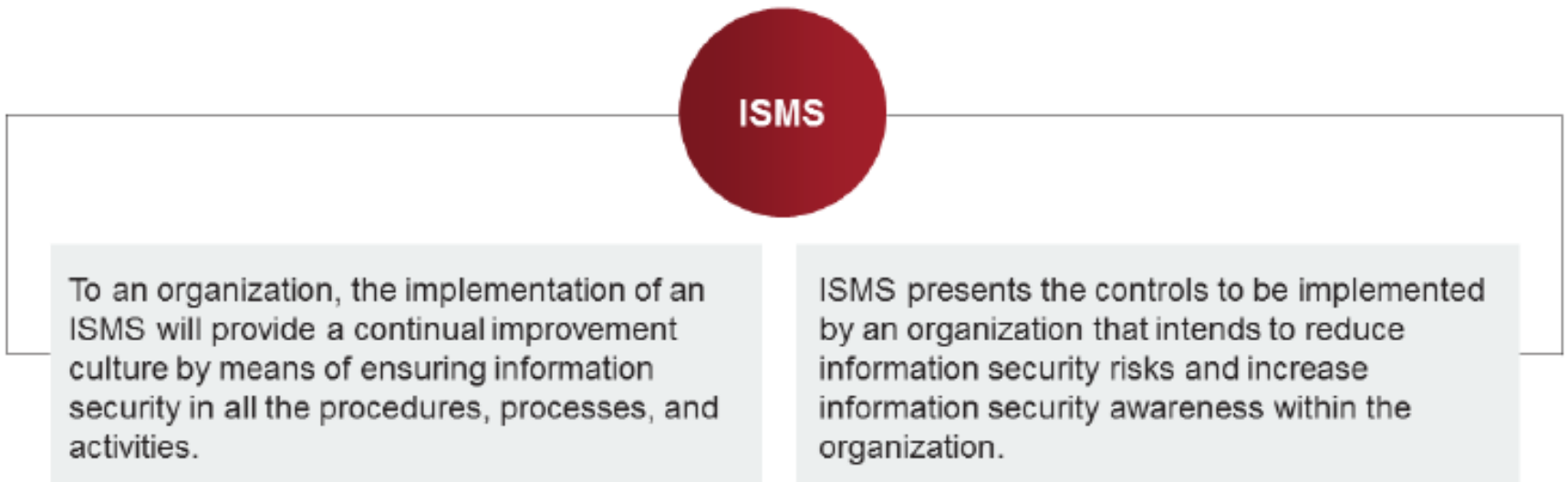
- Database records
- E-mails
- CDROMs DVDs, tapes etc.

Definition of the ISMS

ISO/IEC 27000, clause 4.2.1

- *An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.*
- *An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.*

Definition of an ISMS



What is an ISMS?

- ISMS (Information Security Management System)

- Coordinated set of activities, processes, people and controls aimed at the protection and management of information
- An ISMS is not about technical security alone
- It is a management system!

Managed Information Security

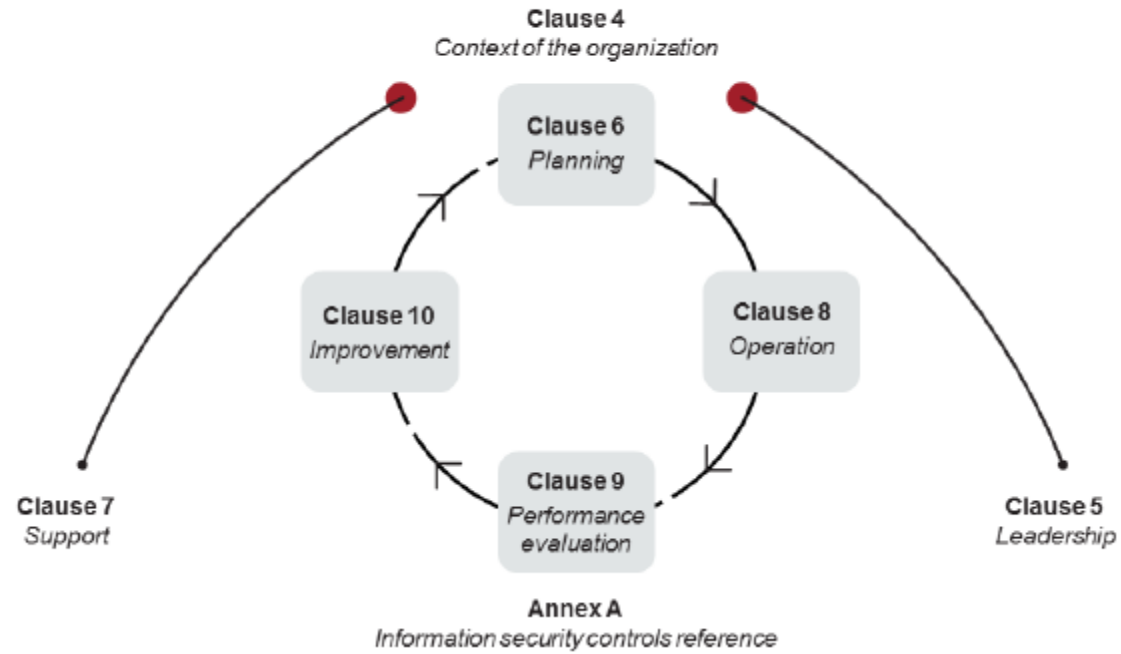
Having a firewall does not mean managing information security

ISO 27001

- Having a firewall administrator who is responsible for its maintenance.
- Having a process for carefully identifying firewall rules and configuration.
- Having a controlled process for approving changes to the firewall.
- Regularly reviewing firewall logs and configuration.
- Taking appropriate corrective and preventive actions.
- Having process for configuration audit.
- Allocating resources for making sure all the above can be sustained over time.

Benefits of the ISMS

Structure of ISO/IEC 27001



Context of the Organization

ISO/IEC 27001, clause 4

4.1 *Understanding the organization and its context*

The organization shall establish the external and internal factors related to the ISMS that can affect the achievement of the ISMS intended outcome(s).

4.2 *Understanding the needs and expectations of interested parties*

The organization shall determine the interested parties and the information security requirements relevant to these interested parties.

4.3 *Determining the scope of the information security management system*

The organization shall establish the ISMS scope by setting its boundaries and applicability. The scope shall be available as documented information.

4.4 *Information security management system*

The organization shall comply with the standard's requirements to establish, implement, maintain, and continually improve an information security management system.

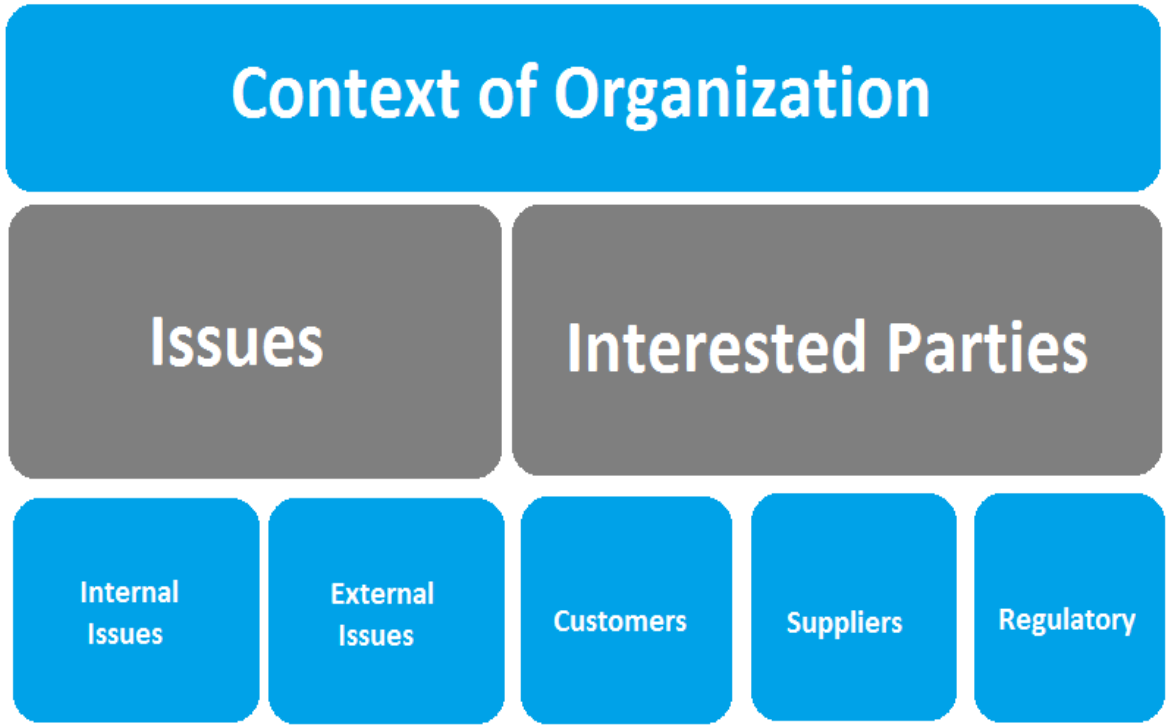
Clause 4 Context of the Organization

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the information security management system

4.4 Information Security Management System



Clause 4 Context of the Organization

- Make sure all aspects of the ISMS scope are addressed

– Business, information security, legal and regulatory requirements

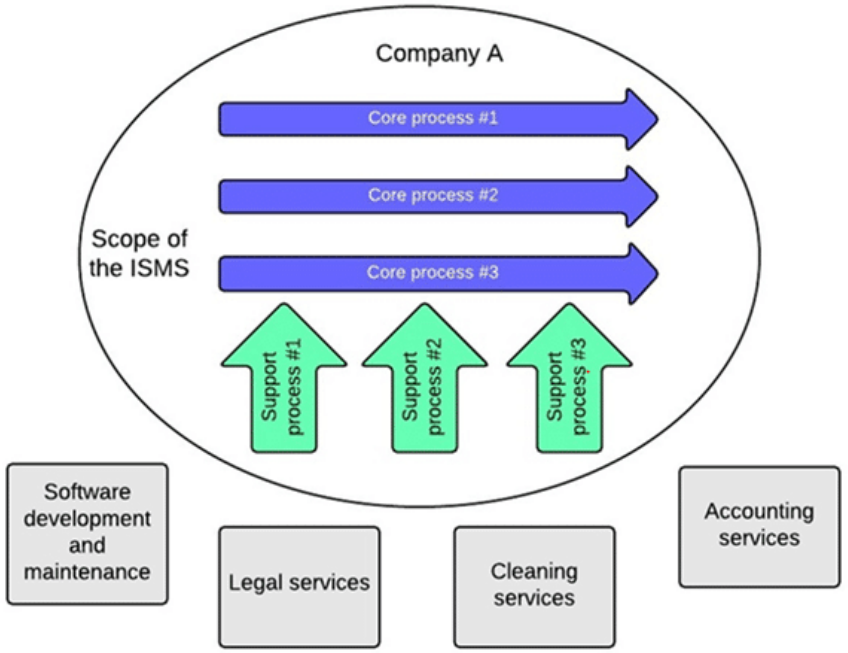
– Must protect information for the purposes of meeting busines legal, regulatory and contractual requirements

- Identification of information security requirements of:

– Applicable legislation

– Contractual obligations

– Regulatory compliance



Organizational principles, objectives and business requirements

- Identify organizational principles, objectives and business requirements to ensure
  - Competitive edge
  - Cash flow/profitability
- Security requirements be documented as part of the risk assessment

Legal, regulatory and contractual requirements

Should not breach any statutory, criminal or civil obligations, or commercial contracts

- Must be identified not just for the organization but also for
  - Trading partners, contractors, service providers
- Example of important requirements to be met:
  - Control of proprietary software copying
  - Safeguarding organization records
  - Data protection
- Reflected in the ISMS Policy

Leadership

ISO/IEC 27001, clause 5

5.1 Leadership and commitment

Top management shall ensure that the ISMS is compatible with the organization's strategic orientation.

Top management shall integrate the ISMS requirements into the organization's business processes, determine the necessary resources for the ISMS, and communicate the importance of an effective information security management.

5.2 Policy

Top management shall create an information security policy that shall be appropriately available and communicated to all interested parties.

The policy shall be aligned with the purpose of the organization and shall include the information security objectives, a commitment to fulfill the information security requirements and a commitment for continual improvement.

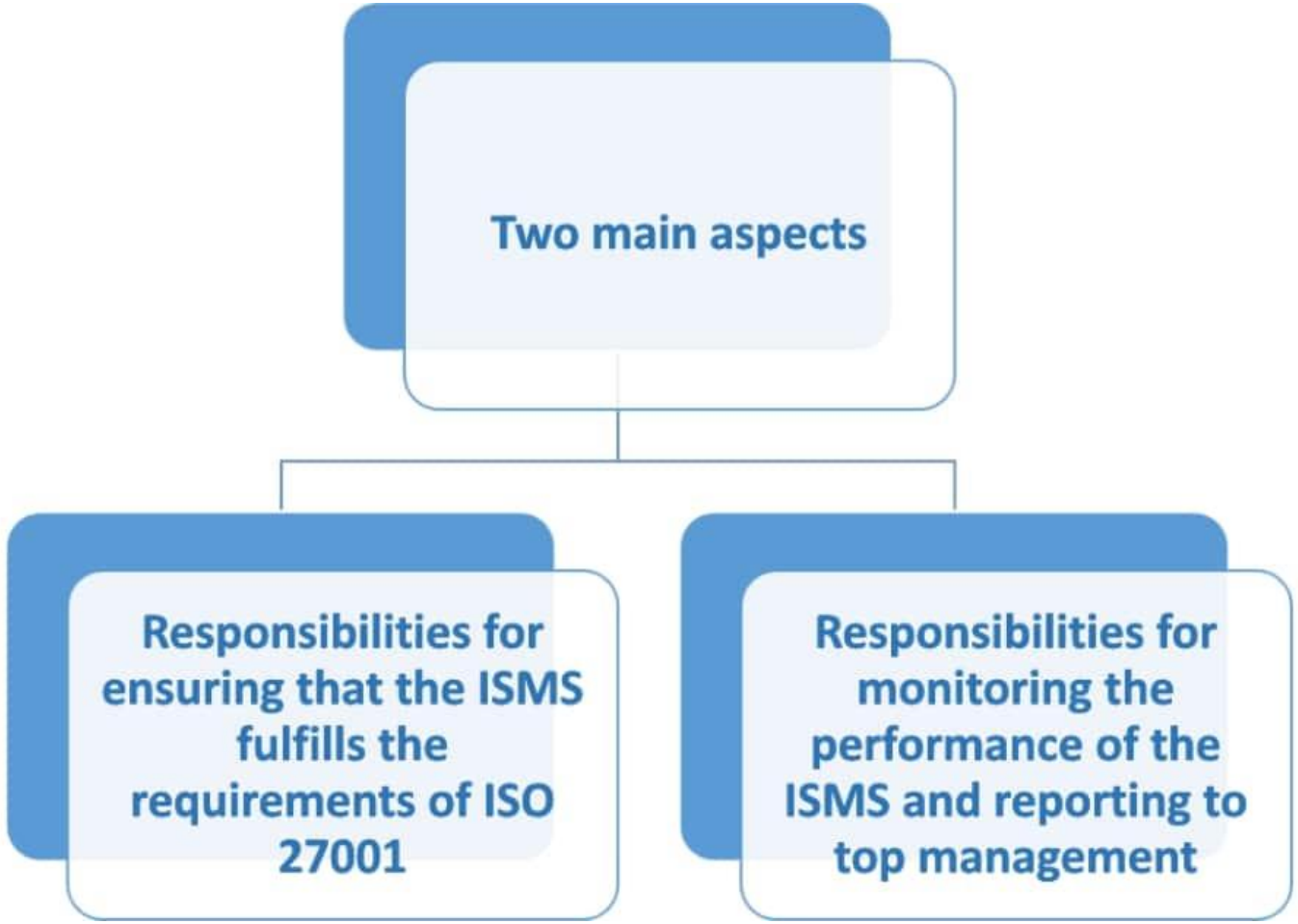
5.3 Organizational roles, responsibilities and authorities

Top management shall assign the appropriate information security roles and responsibilities in order to ensure that the information security management system conforms to the requirements of ISO/IEC 27001.

5.1 Leadership and Commitment

a)Establishing the Information security policy and the Information Security Objectives
b) Ensuring the integration of the information security management system requirements into the organization’s processes
c) Ensuring availability of resources for the ISMS
d) Communicating the importance of effective information security management and of conforming to the information security management system requirements
e) Ensuring that the ISMS achieves its intended outcomes
f) Directing and supporting persons to contribute to the effectiveness of the ISMS
g) Promoting continual improvement
h) Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility

5.3 Organizational Roles, Responsibilities and Authorities



Policies, standards and procedures

Tier 1 Policy Information Security Policy
Tier 2 Policy Backup policy

6.2 Information Security Objectives

The information security objectives shall:

a) be consistent with the information security policy

b) be measurable (if practicable)

c) take into account applicable information security requirements, and results from risk assessment and risk treatment

d) be communicated

e) be updated as appropriate.

When planning how to achieve its information security objectives, the organization shall determine:

a) what will be done;
b) what resources will be required;
c) who will be responsible;
d) when it will be completed; and
e) how the results will be evaluated.

Planning

ISO/IEC 27001, clause 6

6.1 Actions to address risks and opportunities

The organization shall determine the risks and opportunities to achieve the intended outcome(s); prevent or reduce undesired effects; and achieve continual improvement. The organization shall also plan actions to address risks and opportunities, implement those actions, and evaluate their effectiveness.

6.2 Information security objectives and planning to achieve them

The organization's objectives shall be measurable and consistent with the information security policy. They shall also be aligned with the requirements and the results of risk assessment and treatment. The objectives shall be monitored, appropriately communicated, updated, and available as documented information.

6.3 Planning of changes

The organization shall determine the need for changes to the ISMS and implement those changes in a planned manner.

Support

ISO/IEC 27001, clause 7

7.1
Resources

The organization shall determine and provide the necessary resources for the appropriate implementation of the ISMS.

7.2
Competence

The organization shall ensure that it has the competent personnel to perform the tasks related to the ISMS.

7.3
Awareness

The organization shall ensure that its employees are aware of the information security policy, their roles in the ISMS, and the implications of failing to conform to the ISMS requirements.

7.4
Communication

The organization shall establish, implement, and maintain arrangements for communication with relevant external and internal interested parties.

7.5
Documented information

The organization's ISMS shall include documented information required by ISO/IEC 27001 and records to demonstrate the effectiveness of the ISMS.

Operation

ISO/IEC 27001, clause 8

8.1 Operational planning and control

The organization shall plan, implement, and control the necessary processes to comply with the standard requirements. The organization shall also implement the plans, keep documented information as evidence of the implementation of planned processes, control and review the planned changes, and determine and control the outsourced processes.

8.2 Information security risk assessment

The organization shall conduct information security risk assessments at planned intervals and shall keep documented information of the risk assessment results.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan and shall keep documented information on risk treatment results.

Performance Evaluation

ISO/IEC 27001, clause 9

9.1

Monitoring, measurement, analysis and evaluation

The organization shall evaluate the performance and effectiveness of the information security management system and keep documented information as evidence of the monitoring and measurement outputs.

9.2

Internal audit

The organization shall perform internal audits at planned intervals in order to validate whether the information security management system is effectively implemented, maintained, and complies with the organization's own requirements as well as the standard's requirements.

9.3

Management review

The top management shall perform reviews of the ISMS at planned intervals in order to ensure its suitability, adequacy and effectiveness. The organization shall keep documented information as evidence of the management review outputs.

Improvement

ISO/IEC 27001, clause 10

The organization shall ensure the continual improvement of the suitability, adequacy, and effectiveness of the information security management system.

The organization shall take the appropriate actions when a nonconformity occurs. It shall evaluate and implement those actions, review their effectiveness and, if necessary, make changes. The organization shall also keep documented information as evidence of the results of corrective actions.

Annex A

- Annex A is part of ISO/IEC 27001 and it contains 93 controls that should be considered when intending to comply with the standard.
- The list of information security controls of Annex A is not exhaustive. The organization may add additional controls from other sources, when needed.
- If a certain control is not applicable, the organization should provide an acceptable justification for its exclusion.

Annex A

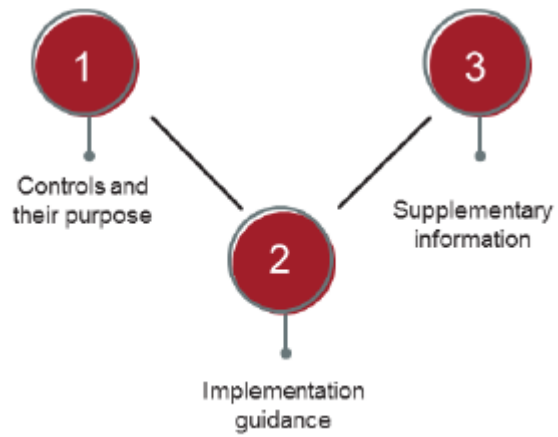
Information security controls

ISO/IEC 27001:2022

Annex A
(List of information security controls)

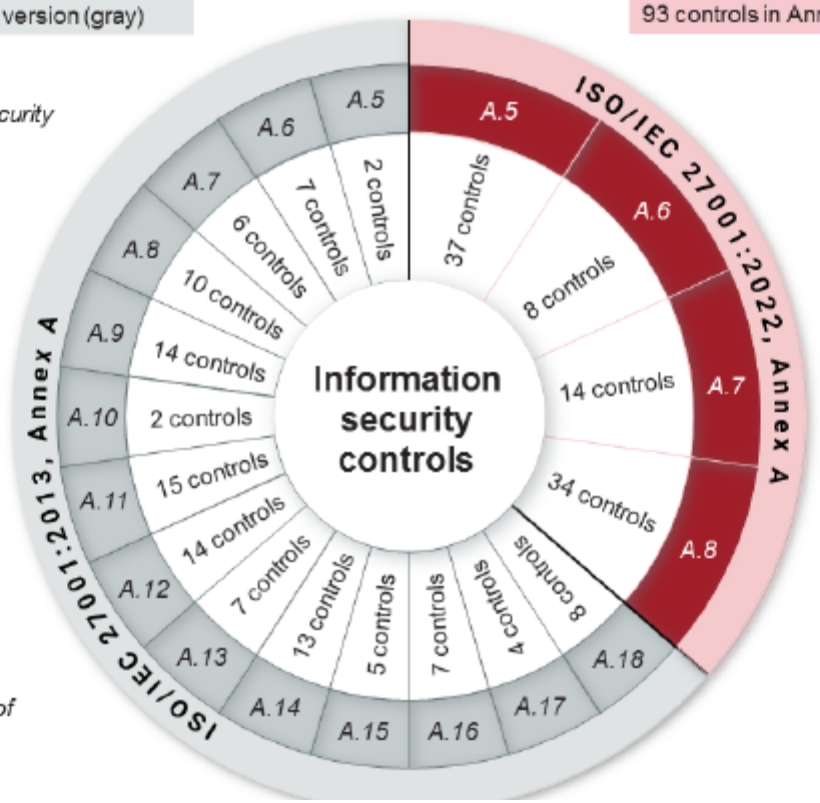
Important note: Since ISO/IEC 27002 is a guideline standard, there is no requirement to follow its recommendations in order to obtain an ISO/IEC 27001 certification.

ISO/IEC 27002:2022



114 controls in Annex A, 2013 version (gray)

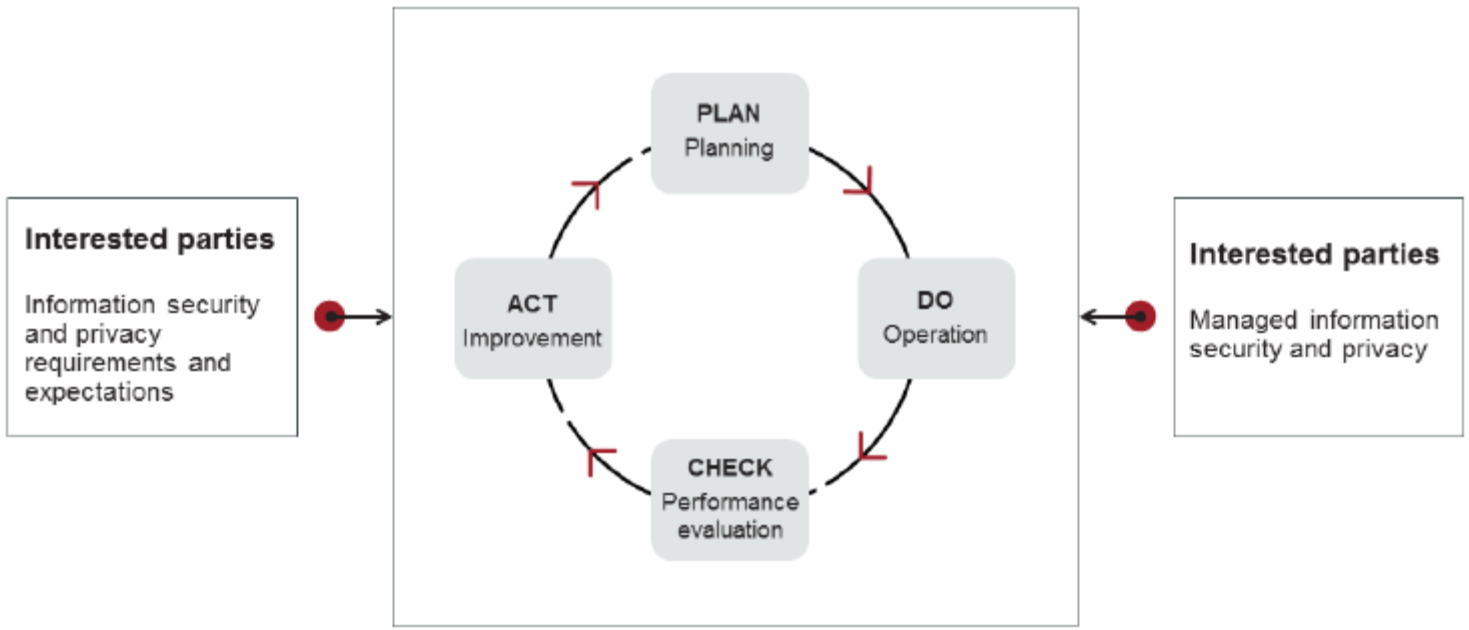
- *A.5 Information security policies*
- *A.6 Organization of information security*
- *A.7 Human resource security*
- *A.8 Asset management*
- *A.9 Access control*
- *A.10 Cryptography*
- *A.11 Physical and environmental security*
- *A.12 Operations security*
- *A.13 Communications security*
- *A.14 System acquisition, development and maintenance*
- *A.15 Supplier relationships*
- *A.16 Information security incident management*
- *A.17 Information security aspects of business continuity management*
- *A.18 Compliance*



93 controls in Annex A, 2022 version (red)

- ***A.5** Organizational controls*
- ***A.6** People controls*
- ***A.7** Physical controls*
- ***A.8** Technological controls*

Process Approach – PDCA Cycle



1. **A management system is a system that allows organizations to establish policies and objectives and to subsequently implement them.**
    A. True
    B. False
2. **What is an integrated management system (IMS)?**
    A. A management system that integrates all the guidelines and best practices so as to enable the achievement of its purpose and mission
    B. A management system that integrates all the components of a business into a coherent system so as to enable the achievement of its purpose and mission
    C. A management system that integrates all frameworks and resources so as to enable the achievement of its purpose and mission
3. **Which of the options below is a benefit of an effective ISMS?**
    A. Reducing information security risks and minimizing exposure to information security breaches
    B. Processing and removing redundant information
    C. Exposing the confidentiality of information
4. **Annex A of ISO/IEC 27001 consists of 114 controls that organizations have to consider when intending to comply with the standard.**
    A. True
    B. False
5. **Which process model does ISO/IEC 27001 adopt?**
    A. Plan, improve, operate, and act
    B. Plan, manage, check, and act
    C. Plan, do, check, and act

Information and Asset

ISO 9000, clause 3.8.2 and ISO 55000, clause 3.2.1

Information: *meaningful data*

Asset: *item, thing or entity that has potential or actual value to an organization*

There are many types of assets, including:

- Information
- Software, such as computer programs
- Physical assets, such as computers
- Services
- People and their qualifications and skills
- Intangibles, such as reputation and image

Information Security

- Information security determines what information needs to be protected, the reason why it should be protected, how to protect it, and what to protect it from.
- By protecting the organization against threats and vulnerabilities, information security reduces the risks and the impact of such risks to its assets.
- Information security covers information of all kinds, such as printed or handwritten, transmitted by email or website, mentioned during conversations, etc.

Confidentiality

ISO/IEC 27000, clause 3.10

Confidentiality 

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

- Confidentiality requires that only authorized users have access to protected and sensitive data.
- Some of the practices employed to address confidentiality are:
  - An authentication process that requires a user identification and password when addressing confidential data
  - Security methods to ensure viewer authorization
  - Access controls that provide restrictions on the network access based on the employee's roles and responsibilities

Integrity

ISO/IEC 27000, clause 3.36

Integrity 

Property of accuracy and completeness

- Integrity ensures that:
  - Information is not modified when in storage or in transit
  - Only authorized modifications are made
  - Data is accurate, authentic, and safe from unauthorized access in order for users to be able to rely on the correctness of information when processing it

Availability

ISO/IEC 27000, clause 3.7

Availability 

Property of being accessible and usable on demand by an authorized entity

- Information availability is crucial for modern information security.
- Information availability means that the information is accessible:
  - As required
  - When required
  - Where required
  - To the person(s) requiring
- Information security managers usually face three challenges:
  - Denial of service (DoS) as a result of intentional attacks (e.g., a programmer is not aware of a defect that could harm the software due to a specific and unexpected input)
  - Losing protection capacities of information systems due to natural disasters or human activities
  - Equipment failures

Vulnerability

ISO/IEC 27000, clause 3.77

Vulnerability

Weakness of an asset or control that can be exploited by one or more threats

- Vulnerabilities that do not have corresponding threats may not require controls, but should be recognized and monitored for changes.
- Controls that get implemented incorrectly or malfunction could become vulnerabilities.

Examples of Vulnerabilities

ISO/IEC 27005, Table A.11 (excerpt)

Category	Examples of vulnerabilities
Hardware	Insufficient maintenance/faulty installation of storage media
	Insufficient periodic replacement schemes for equipment
Software	No or insufficient software testing
	Complicated user interface
Network	Unprotected communication lines
	Single point of failure
Personnel	Insufficient security training
	Unsupervised work by outside or cleaning staff
Site	Unstable power grid
	Location in an area susceptible to flood
Organization	Improper allocation of information security responsibilities
	Information security responsibilities are not present in job descriptions

Threats

ISO/IEC 27005, clauses 3.1.9 and 7.2.1

Threat: *Potential cause of an information security incident that can result in damage to a system or harm to an organization*

A threat exploits a vulnerability of an asset to compromise the confidentially, integrity and/or availability of corresponding information.

Examples of Threats

ISO/IEC 27005, Table A.10 (excerpt)

Category	Threat description
Physical threats	*Fire* *Water*
Natural threats	*Volcanic phenomenon* *Flood*
Infrastructure failures	*Failure of a supply system* *Loss of power supply* *Electromagnetic radiation* *Thermal radiation*
Technical failures	*Failure of device or system* *Saturation of the information system*
Human actions	*Tampering with hardware* *Theft of media or documents*
Compromise of functions or services	*Denial of actions* *Forging of rights or permissions*
Organizational threats	*Lack of resources* *Violation of laws or regulations*

Relationship Between Vulnerability and Threat

Examples

Vulnerabilities	Threats
Warehouse unprotected and without surveillance	Theft
Complicated data processing procedures	Data input error by personnel
No segregation of duties	Fraud, unauthorized use of a system
Unencrypted data	Information theft
Use of pirated software	Lawsuit, virus
No review of access rights	Unauthorized access by persons who have left the organization
No backup procedures	Accidental power interruption

Impact


Examples of impacts on availability
Performance degradation
Service interruption
Unavailability of services
Disruption of operations
Examples of impacts on confidentiality
Invasion of the privacy of users or customers
Invasion of the privacy of employees
Leak of confidential information
Examples of impacts on integrity
Accidental change
Deliberate change
Incorrect results
Incomplete results
Loss of data

The following is a list of potential impacts that can affect availability, integrity, or confidentiality, or a combination of them:

1. Financial losses
2. Loss of assets or their value
3. Loss of customers and suppliers
4. Lawsuits and penalties
5. Loss of competitive advantage
6. Loss of technological advantage
7. Loss of efficiency or effectiveness
8. Violation of the privacy of users or customers
9. Service interruption
10. Inability to provide service
11. Loss of branding or reputation
12. Disruption of operations
13. Disruption of third party operations (suppliers, customers)
14. Inability to fulfill legal obligations
15. Inability to fulfill contractual obligations
16. Endangering safety of staff and users

Information Security Risk

ISO/IEC 27000, clause 3.61

- *Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" of occurrence.*
- *Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.*
- *Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.*

Classification of Security Controls

Classification by type

Technical control

Controls related to the use of technical measures or technologies, such as firewalls, alarm systems, surveillance cameras, etc.

Legal control

Controls related to the application of a legislation, regulatory requirements, or contractual obligations

Administrative control

Controls related to organizational structure, such as segregation of duties, job rotations, job descriptions, approval processes, etc.

Managerial controls

Controls related to the management of personnel, including training of employees, management reviews, internal audits, etc.

Classification of Security Controls

Classification by function

Preventive control

Controls to avoid or prevent the occurrence of incidents

Detective control

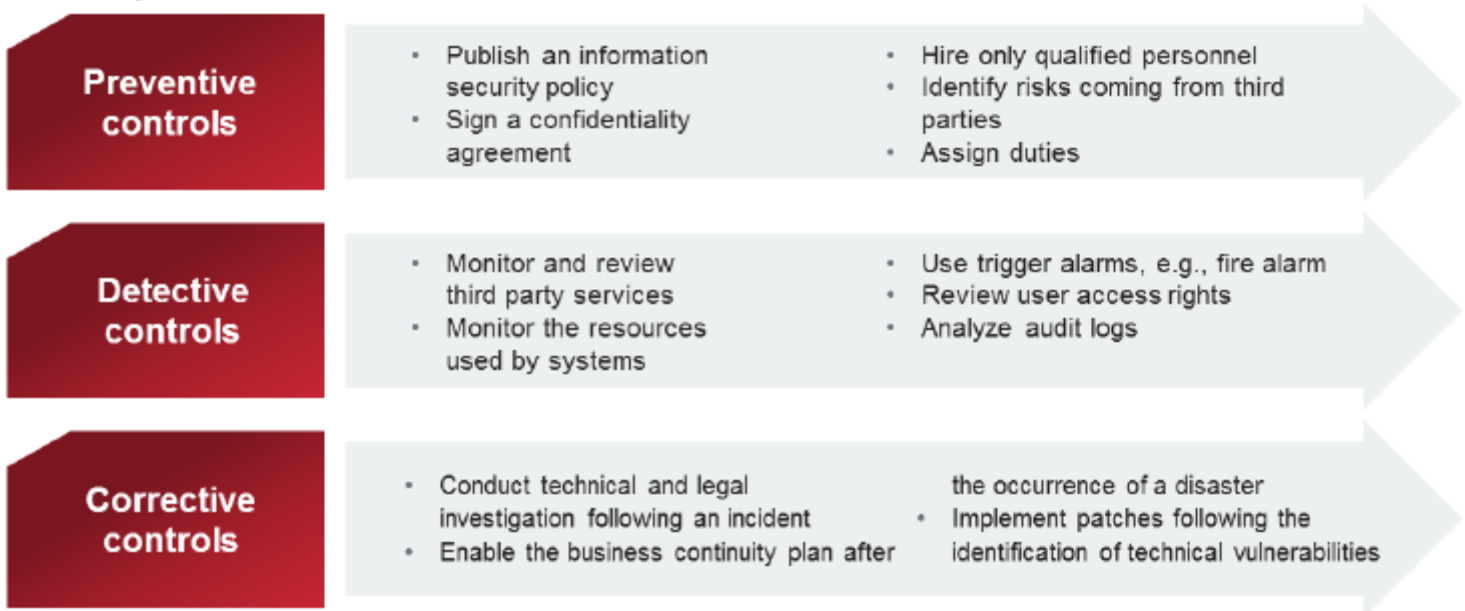
Controls to search for, detect, and identify incidents

Corrective control

Controls to solve the identified incidents and prevent their recurrence

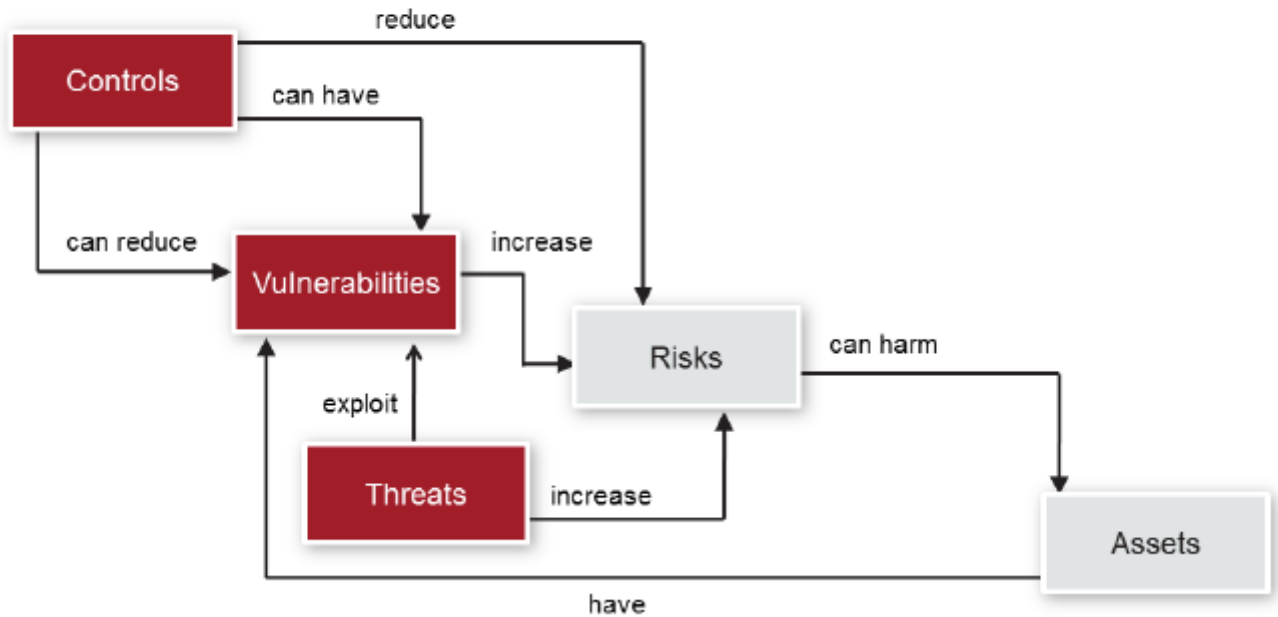
Classification of Security Controls

Examples



Relationships Between Information Security Elements

Overview



1. **What are information, software, services, and people considered as?**
    A. Inventories
    B. Assets
    C. Information
2. **Which of the following statements regarding information security is correct?**
    A. Information security protects the confidentiality, integrity, and availability of information regardless of its type and form
    B. Information security protects the confidentiality, integrity, and availability of information only in an electronic form
    C. Information security protects the organization against threats by only identifying the threat source
3. **What does confidentiality ensure?**
    A. That the information is accessible to the authorized individuals
    B. That the information is accurate and complete
    C. That the information is available
4. **Which of the following is NOT an example of a threat?**
    A. Theft of media or documents
    B. Complicated user interface
    C. Unauthorized use of equipment
5. **Performance degradation can have an impact on the _____ of information.**
    A. Availability
    B. Confidentiality
    C. Integrity

6.Vulnerability is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.

A. True
B. False

7.What type of controls are the segregation of duties, job rotations, and approval processes?

A. Technical controls
B. Managerial controls
C. Administrative controls

8.What type of control is the separation of development, testing, and operating environment?

A. Preventive control
B. Detective control
C. Corrective control

9.An organization has installed a fire alarm in its premises. What type of control is this?

A. Preventive and administrative
B. Corrective and managerial
C. Detective and technical

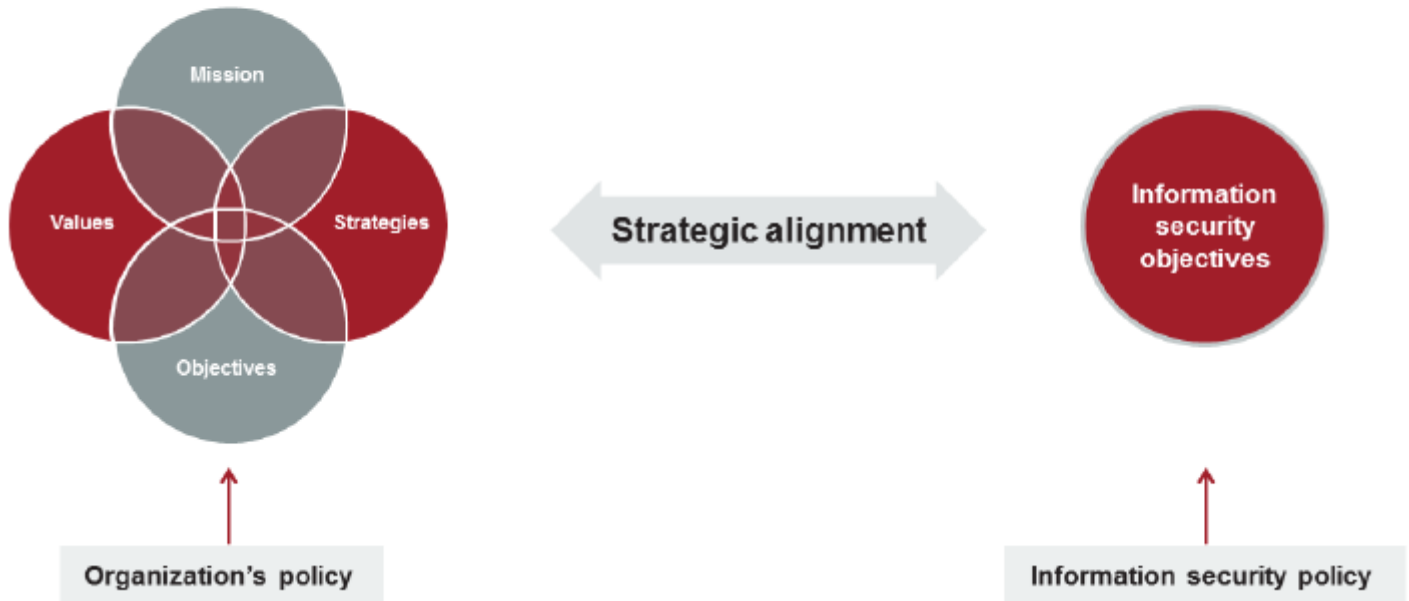
10.Assets and controls can present _____ that can be exploited by _____.

A. Threats, vulnerabilities
B. Vulnerabilities, threats
C. Threats, risks

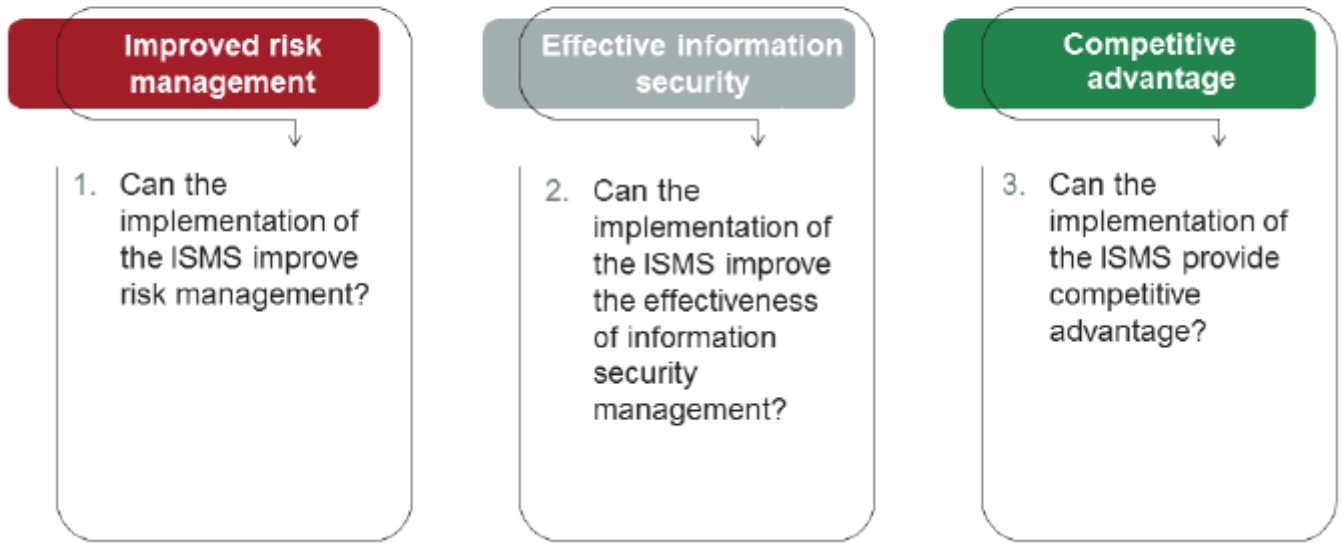
1.2 Understanding the Organization and its Context

List of activities

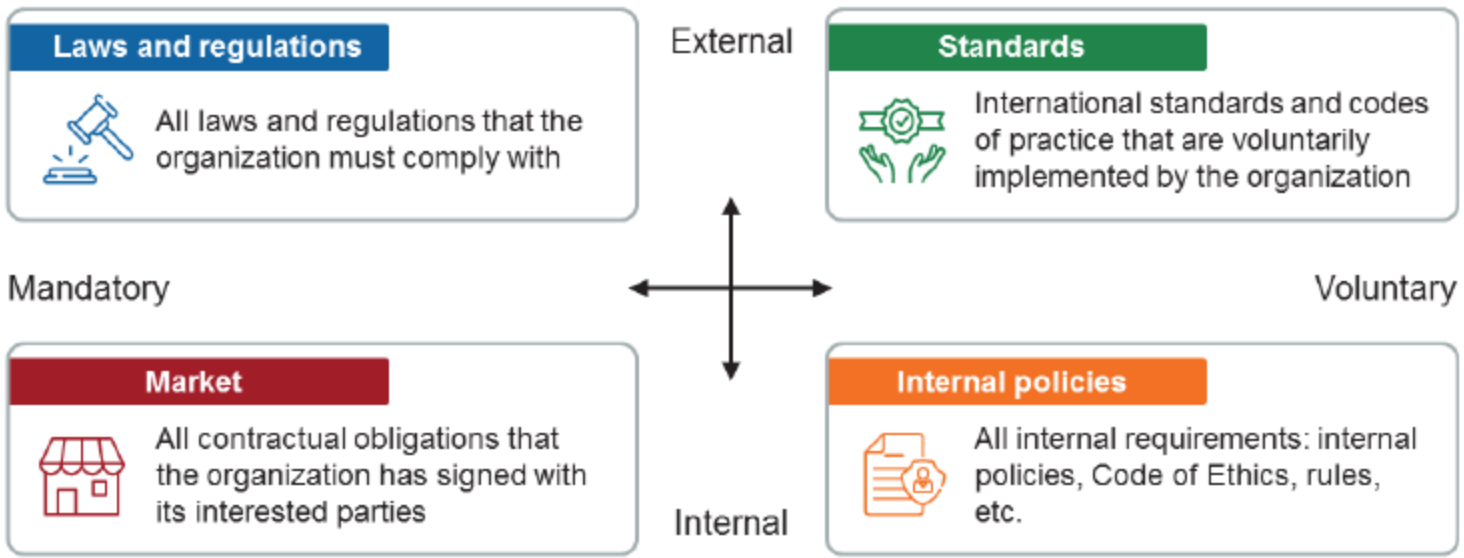
1.2.1 Understand the Mission, Objectives, Values, and Strategies



1.2.2 Determine the ISMS Objectives



1.2.3 Identify and Analyze the Business Requirements



1.2.4 Determine the Preliminary Scope

ISO/IEC 27003, clause 4.3

The organization determines the boundaries and applicability of the ISMS to establish its scope.

The following factors can affect the determination of the scope:

a) the external and internal issues described in 4.1;

b) the interested parties and their requirements that are determined according to ISO/IEC 27001, 4.2;

c) the readiness of the business activities to be included as part of ISMS coverage;

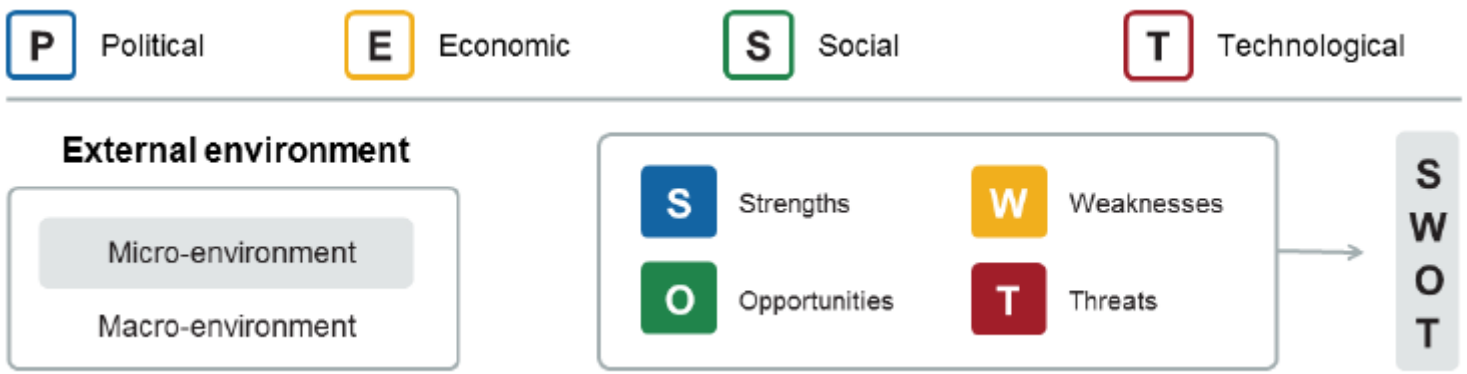
d) all support functions, i.e. functions that are necessary to support these business activities (e.g. human resources management; IT services and software applications; facility management of buildings, physical zones, essential services and utilities); and

e) all functions that are outsourced either to other parts within the organization or to independent suppliers.

1.2.5 Analyze the Internal and External Environment

Practical advice

- Considering that ISO/IEC 27001 does not offer any practical approach to analyze the context of an organization, the organization is free to choose the tools it deems most appropriate.
- Several methodologies that help in understanding how an organization functions exist.
- The important thing is to identify the characteristics of internal and external factors that will influence risk management: mission, main activities, interested parties, etc.



1.2.6 Identify the Key Processes and Activities

Assets

What are the key assets of the organization?

Organization's activities

What are the goods and services produced by the organization?

Business processes

What are the key processes that enable the organization to achieve its mission?

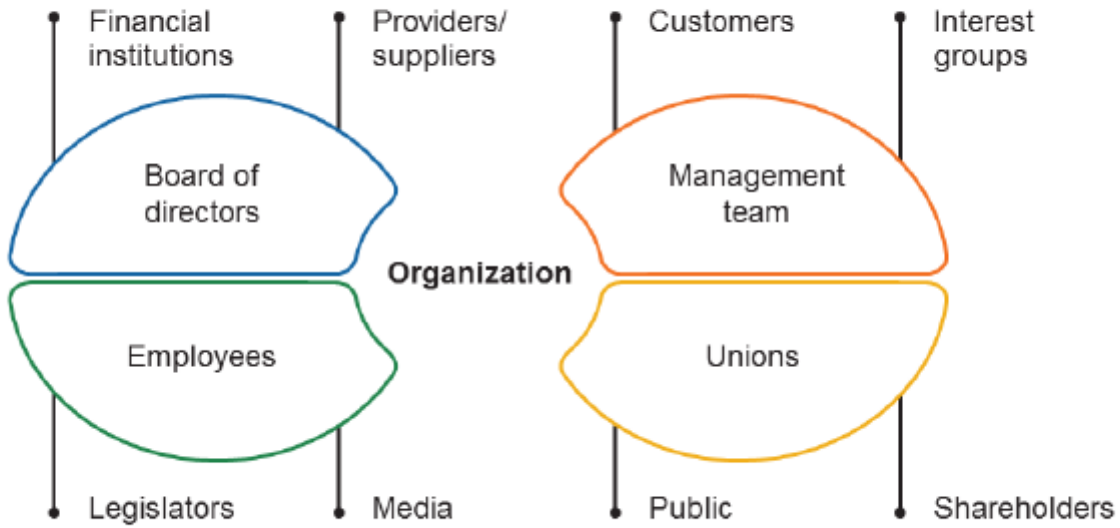
Note:

At this stage, there is no need to completely map out the processes, only to establish a general list.

Identification of Infrastructure

Category	Definition	Examples
Hardware	Physical components that support the process	Server, laptop, printer, CD-ROM, etc.
Software	Programs that contribute to data processing	Operating system, word processer, accounting software, etc.
Networks	Telecommunications equipment used to physically connect the elements in an information system	Router, firewall, network cable, switch, bridge, etc.
Sites	Physical locations where operations take place	Office, server room, employees residence, secure area, air conditioning system, etc.
Third party supplier	Organization that provides a product not supplied by the main organization	Telephone company, marketing agency, etc.

1.2.7 Identify and Analyze the Interested Parties



Note: The term "interested party" is synonymous with the term "stakeholder." Therefore, these terms are used interchangeably.

1. **Why is it important to understand the mission, objectives, values, and strategies of an organization?**
   A. To facilitate the internal audit process
   B. To create a map of all the processes
   C. To understand the information security challenges the organization faces
2. **Which of the options below represents an ISMS objective?**
   A. Integration of new technologies
   B. Protection of critical assets
   C. Improvement of the information security incidents
3. **Which of the following statements is correct?**
   A. Standards take precedence over laws
   B. The implementation of an ISO standard is not a legal requirement
   C. Compliance with the ISO/IEC 27001 ensures compliance with data protection laws and regulations
4. **Do outsourcing activities of an organization impact its ISMS?**
   A. No, because outsourcing activities should not be included in the ISMS scope
   B. Yes, because outsourcing activities do not directly support the business activities
   C. Yes, because outsourcing activities can affect the determination of the ISMS scope
5. **What can be included when analyzing the internal environment of an organization?**
   A. Information systems, information flow, and decision-making processes
   B. Information systems boundaries and physical boundaries
   C. Trends having impact on the objectives of the organization

1.3 Scope


1. Define and establish
1.1 Initiation of the ISMS implementation
1.2 Understanding the organization and its context
1.3 ISMS scope
1.4 Leadership and project approval
1.5 Organizational structure
1.6 Analysis of the existing system
1.7 Security policy
1.8 Risk management
1.9 Statement of Applicability
2. Implement and operate
2.1 Documented information management
2.2 Selection and design of controls
2.3 Implementation of controls
2.4 Communication
2.5 Competence and awareness
2.6 Security operations management
3. Monitor and review
3.1 Monitoring, measurement, analysis, and evaluation
3.2 Internal audit
3.3 Management review
4. Maintain and improve
4.1 Treatment of nonconformities
4.2 Continual improvement
Continual communication and awareness

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 4.3

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

Scope

Importance

A clear definition of the scope focusing on the key activities of the organization is an important success factor for the ISMS implementation. This will make it easier to:

- Obtain the management's support
- Mobilize the interested parties for the project
- Justify added value to the interested parties

Important note:

The size of the scope is the first factor influencing the amount of effort required for the project.

1.3 Scope

List of activities

Boundary of the ISMS

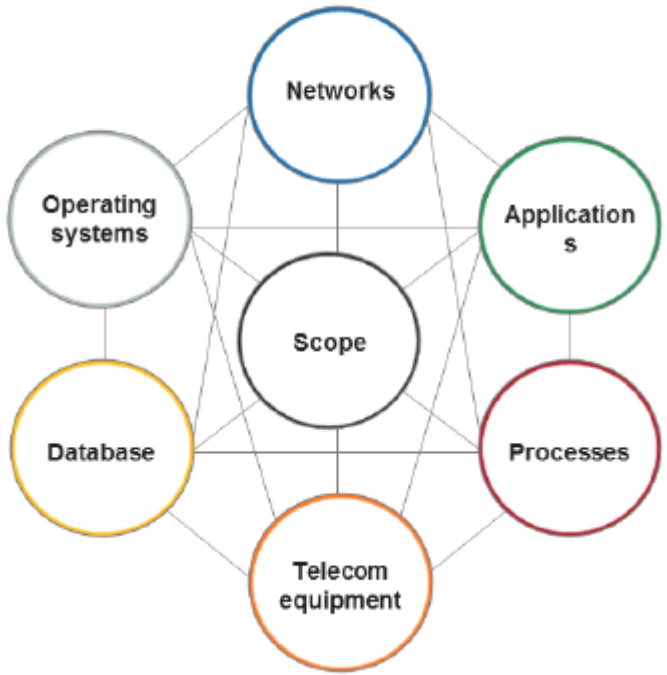
Three dimensions to consider:

1.3.1 Define the Organizational Boundaries of the Scope

1.3.2 Define the Information Security Boundaries

All system components are to be taken into account; the focus is not to be limited to hardware components only.

Note: In theory, the lack of technical infrastructure does not prevent an organization from obtaining an ISO/IEC 27001 certification.



1.3.3 Define the Physical Boundaries

- All physical locations, both internal and external, included in the ISMS should be taken into account.
- The sites include all locations within the scope or within part of the scope and the physical means required for them to work.
- In the case of outsourced physical sites, the interfaces with the ISMS and the applicable service agreements have to be considered.

1.3.4 Define the ISMS Scope

The scope should include:

1. Key characteristics of the organization
2. Organizational processes
3. Descriptions of the roles and responsibilities related to the ISMS
4. List of information assets
5. List of information systems
6. Maps of geographic locations
7. Details and reasons for exclusions

Scope Statement

Examples

The scope statement is public and, in general, is available from the certification organization that has issued the certificate.

This summary statement will be written on the certificate. It should be:

1. As simple as possible
2. Understandable by external parties
3. Precise enough to show what is covered by the certification

Example

.

Editing and web hosting services

AAD Co., Ltd (Japan): Printing and planning, producing and designing related thereof. Planning for websites and implementation thereof. Statement of Applicability, issued on 19/Jul/2011, Version 3 Other location(s): Kawaguchi Plant.

Define the ISMS scope

Most important step of the implementation process

- The scope must be clearly defined
- Identifying key departments/people involved
- Involves business aware/responsible staff
- Linked to business objectives
- Iterative process

Defined in terms of
– Characteristics of the business
– The organization
– Location
– Assets
– Technology
- Include details for any exclusions from the scope

Writing the Scope

- Scope format not prescribed by the standard
- ISMS scope document (clause 4.3)
- CB makes sure that the scope meets the requirements of the standard and that it is clear and unambiguous
- A scope statement will appear on the ISO27001 certificate issued by the Certification Body (CB)
- Also linked to the Statement of Applicability (SOA)
- Best practice Scope Document
- Scope statement → Appears on the ISO27001 Certificate
- Detailed description

Scope

- **Scope Statement**

The following statement, known as the ISMS Scope Statement, provides a summary description of the overall ISMS Scope and is also reported on the xxxx ISO27001 Certificate of Compliance issued by the Certification body.

"The scope of the information security management system of xxxx to the delivery of the yyyy services of bill payment, money transfer, in accordance with the statement of applicability {CLI-REC-002_v1.0}."

Scope How to

- Top down approach
– Identify key business services (senior management)
– Draw a pictorial map of the organization
– Identify departments and processes in support of those services
- Scope Boundaries
– Identify which departments and processes we have direct control over
– Identify dependencies
– Internal
– External

Business Services

Business services in the scope of the ISMS are <insert business services in scope>. A thorough description of these processes is maintained within the ISMS Asset Registry (CLI-REC-001_ISMS Asset Registry_v1.0).

Organization and Staff

The scope applies to the following departments and associated members of staff:

Business Units in Scope

Division/ Department/ Unit	Process	# People
Commercial Division		
ICT		

Support Services in scope

Division/ Department/ Unit	Process	# People
HR	Recruitment, Disciplinary, Training and Termination	
Facilities and Estate management/ Facilities and Administration	Physical Security and Asset management	

Scope and boundaries

- Identify interfaces with:
  - Supporting departments
  - Third parties and external organizations
  - Suppliers
- Controlling dependencies
  - SLAs, OLAs, MOUs, contracts
  - Outsourcing arrangements

The following table summarizes the interdependencies of business systems within the defined scope

business Service	System Dependency	

External dependencies

The below tables depicts the external dependencies and critical system dependencies at the back end support level and the customer facing support level receptively of the systems in scope:

Service	Third Parties	Dependency

Example: scope of ISMS

“The provision of financial services such as loans and leases by the head office in Asia which has branches throughout Europe. It also includes the provision of support services like supervision, rescheduling of the repayment and the collection of payments. The main asset of the company is its manpower and the use of the IT hardware and software to support the business.”

1. **What should an organization do when establishing its ISMS scope?**
    A. Determine the amount of effort required for the ISMS implementation
    B. Determine the internal and external information security risks
    C. Determine the boundaries and applicability of the ISMS
2. **Which of the following is considered an ISMS boundary?**
    A. Information systems boundaries
    B. Critical assets boundaries
    C. Information security incident boundaries
3. **In which of the ISMS boundaries below should the evaluation of the responsibilities of decision-makers and their areas of influence in the organization be done?**
    A. Organizational
    B. Physical
    C. Information systems
4. **Which of the following is included in the ISMS scope?**
    A. The description of the changes in the external environment
    B. The description of the information security risks related to the ISMS
    C. The description of the roles and responsibilities related to the ISMS
5. **Which of the following statements regarding the ISMS scope is correct?**
    A. The ISMS scope should be categorized as confidential information
    B. The ISMS scope should not consider the information systems
    C. The ISMS scope should be available as documented information
6. **When can an organization make a change in the ISMS scope?**
    A. When the organization is applying for certification
    B. When new risk scenarios are to be considered
    C. When the list of information assets has been modified