General

Optimal
Training • Consulting • Business Solutions

ISO 27001
Certified Lead Implementer

Aladdin Dandis

1

General

Objectives

Provide explanation and guidance on **ISO/IEC 27001** based on **ISO/IEC 27003:2017** for the design and implementation of an Information Security Management System (ISMS).

2

2

General

Who should attend this certification workshop?

Individuals interested in expanding their knowledge of **ISO/IEC 27001** based on **ISO/IEC 27003:2017** for the design and implementation of an Information Security Management System (ISMS).

3

3

General

Agenda

1. Introduction
2. Business Case
3. Diagnostic
4. Context of the Organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

4

4

General

1. Introduction

5

General

Introduction

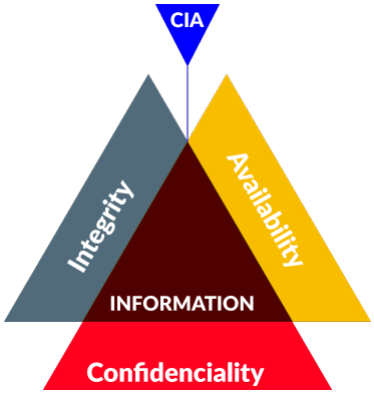
1.1 Information Security
1.2 Information security management system
1.3 ISO/IEC 27001 Structure
1.4 Navigation Path

6

6

General

Information Security



Preserve the **confidentiality, integrity and availability** of information.

7

7

General

Information Security Management System

Part of the overall management system, based on a risk-based approach to a business, to establish, implement, operate, monitor, review, maintain and improve information security.

It includes organizational structure, policies, plans, responsibilities, procedures, processes and resources.

8

8

General

ISO/IEC 27003:2017 Information Technology. Security Techniques

9

9

General

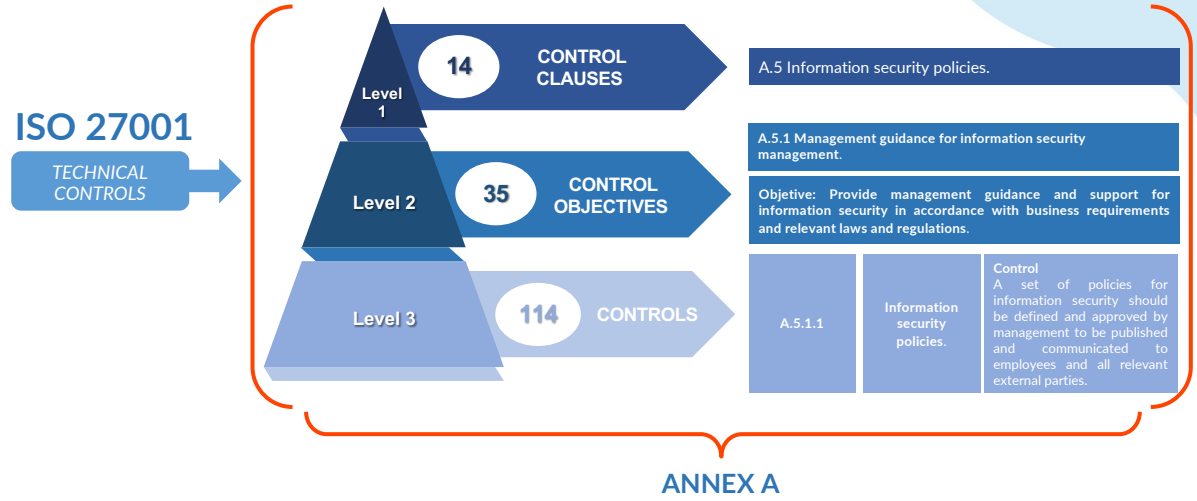
ISO 27001: Administrative

10

10

General

ISO 27001: Technical Controls

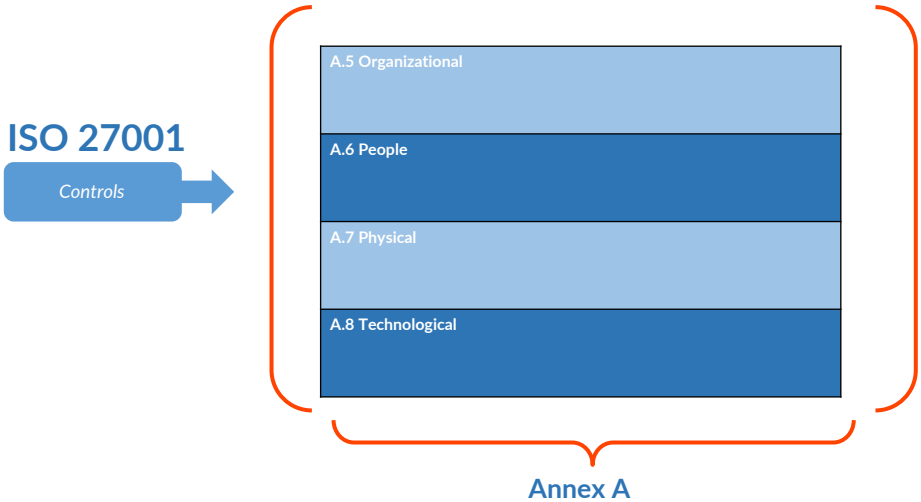


11

11

General

ISO 27001: Controls

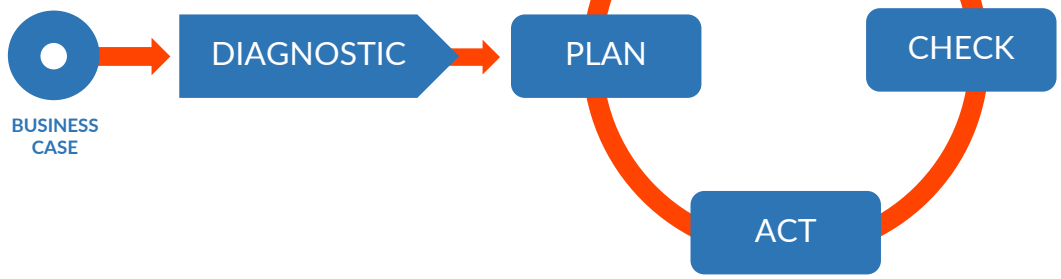


12

12

General

Navegation Path



13

13

General

2. Business Case

14

General

Business Case

2.1 Definition of a Business Case
2.2 Parts of a Business Case
2.3 Description Parts of a Business Case

15

15

General

Business Case

"A document defines the proposal, sets out its objectives, deliverables, estimated cost and effort, and scope."

Tom Mochal

Source: *Tom Mochal, "Select and prioritize projects with a business case", Diciembre 15, 2003. (See: https://www.techrepublic.com/article/select-and-prioritize-projects-with-a-business-case/).*

16

16

General

Business Case

Document that summarizes to Senior Management the main aspects to take into account when implementing an Information Security Management System (ISMS).

17

17

General

Structure of a Business Case

BUSINESS CASE

- Executive Summary
- Opportunity Analysis
- Cost - Benefit Analysis
- Risk and Reward Analysis
- Implementation Plan

18

18

General

Structure of a Business Case

EXECUTIVE SUMMARY	• Description of the business problem the project will solve • How the project will benefit the business • How the project aligns with the strategic needs of the organization
OPPORTUNITY ANALYSIS	• Internal and external organizational context in terms of information systems -IS • Main stakeholder needs • Relevant needs regarding legal issues, according to the sector
COST – BENEFIT ANALYSIS	• Detail the general description of costs and benefits (quantifiable) • Return on investment • Present scenarios
RISK AND REWARD ANALYSIS	• Most relevant external and internal risks in the industry for which an ISMS should be implemented and what is the likely cost if they materialize
IMPLEMENTATION PLAN	• Activities, times, resources, goals (compliance measurements, quality of progress and budget)

19

19

General

3. Gap Assessment

20

General

Gap Assessment

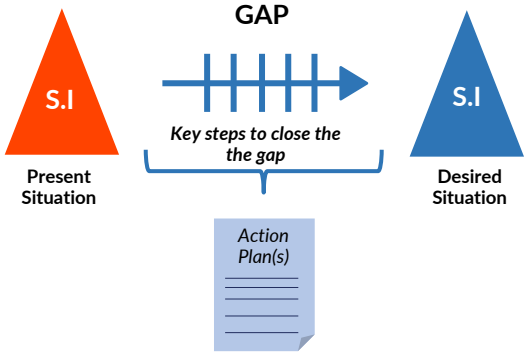
3.1 Definition of GAP Analysis
3.2 Objective of GAP Analysis
3.3 How to Perform a GAP Analysis
3.4 Maturity Models

21

21

General

GAP Analysis



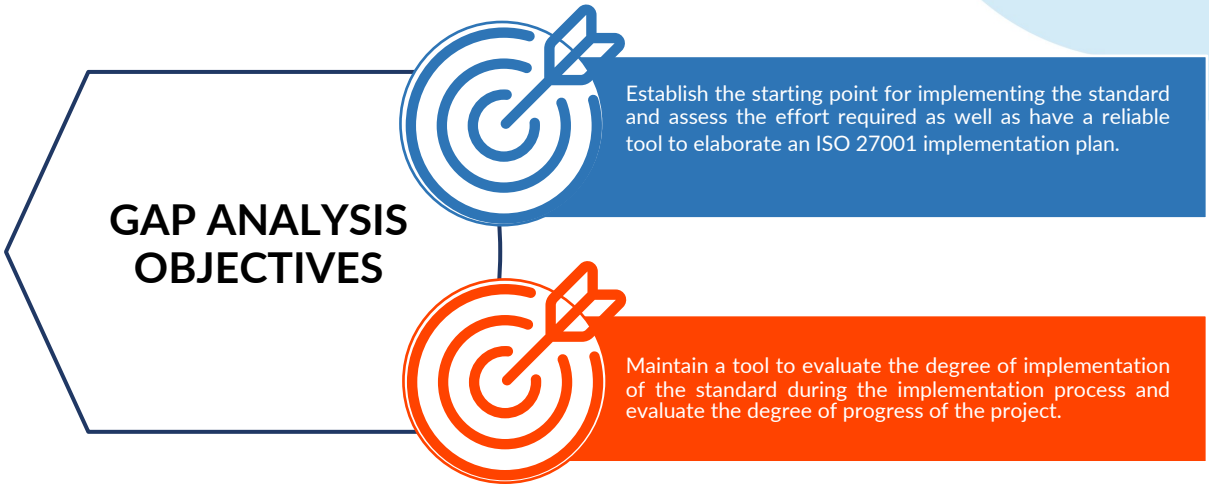
A GAP analysis consists of an analysis of **compliance** with both the **requirements** of ISO/IEC 27001 and its **controls** (Annex A).

22

22

General

GAP Analysis Objectives

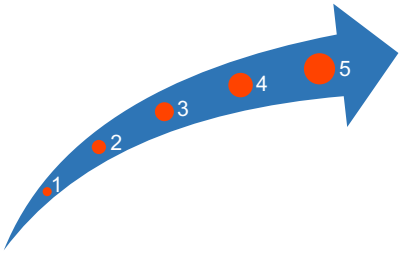


23

23

General

How to Perform a GAP Analysis



In order to perform the GAP analysis, it may be advisable to use a **maturity model** for compliance assessment.

The most common maturity models such as:

- NIST-CSEAT
- CITI-ISEM
- COBIT Maturity Model
- ISM3
- SSE / CMM
- CERT / CSO

24

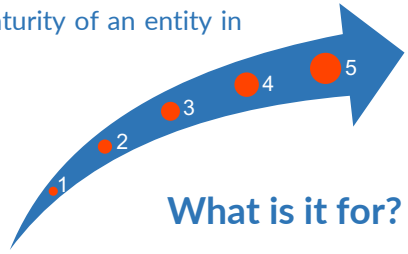
24

General

Maturity Model

What is it?

It is a set and structure of elements that describe the level of maturity of an entity in a given aspect.



What is it for?

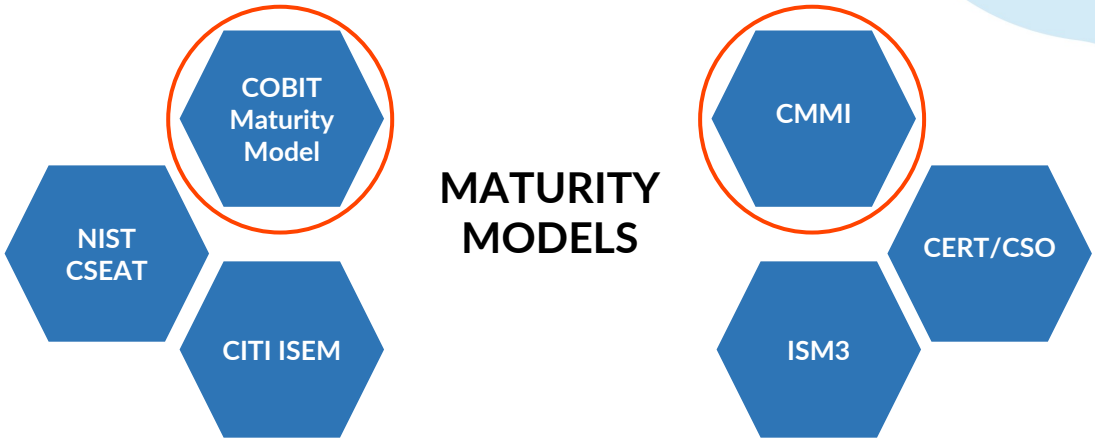
- It allows me to measure: where am I today?
- It allows me to define where I need to be
- It allows me to plan what I need to achieve, to get to where I want to be.
- It allows me to manage my growth and evolution

25

25

General

Maturity Models

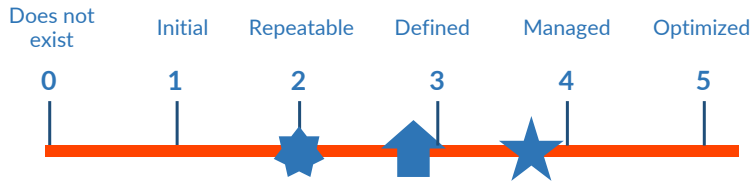


26

26

General

COBIT Maturity Model



This model is perfectly suited to establish an audit model that allows us to measure your current maturity level with respect to the requirements (Numerals) and controls (Annex A) of ISO/IEC 27001.

Symbols Used

- Company's current status
- Industry average
- Company's objective

Qualifiers Used

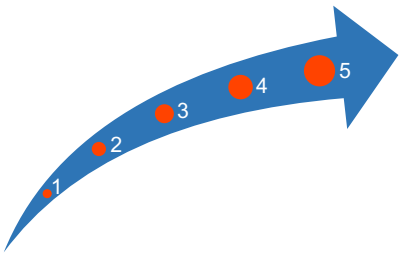
0. Process management is not applied
1. Processes are ad-hoc and disorganized
2. Processes follow a regular pattern
3. Processes are documented and communicated
4. Processes are monitored and measured
5. Good practices are used and automated

27

27

General

How to Perform a GAP Analysis



After choosing the maturity level we use a list of questions to obtain the organization's level of compliance under different scenarios according to the defined maturity levels. This will allow us to establish a maturity level for each of the ISO/IEC 27001 requirements and controls.

The following annexes provide examples of questionnaires for the different requirements and controls of ISO/IEC 27001.

PDF

ISO 27001 COMPLIANCE TEST

PDF

COMPLIANCE TEST ANEX A I27001CLI

28

28

General

4. Context of the Organization

29

General

Organizational Context

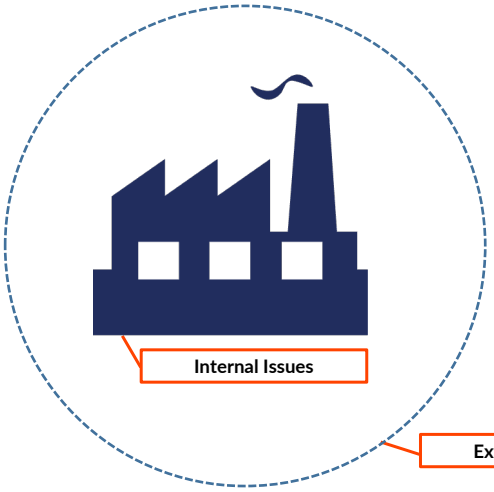
4.1 Understanding the Organization and its Context
4.2 Understanding the Needs and Expectations of Stakeholders
4.3 Determining the Scope of the Information Security Management System

30

30

General

Understanding the Organization and its Context



As an integral function of ISMS, the organization continually analyzes itself and the world around it. This analysis is concerned with **external and internal issues** that affect information security in some way and how information security can be managed, and which are relevant to the organization's objectives.

31

31

General

Understanding the Organization and its Context

Purpose ANALYSIS Internal and External Issues

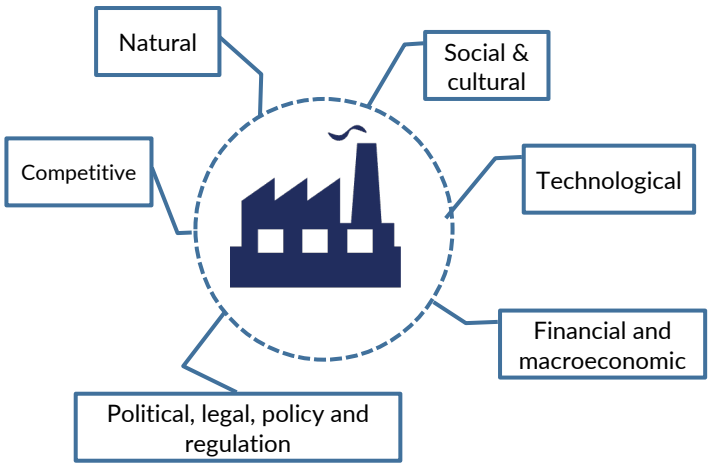
- Understanding the context for deciding the scope of the ISMS.
- Analyze the context to identify risks and opportunities.
- Ensuring that the ISMS is adapted to changing external and internal issues.

32

32

General

External Issues



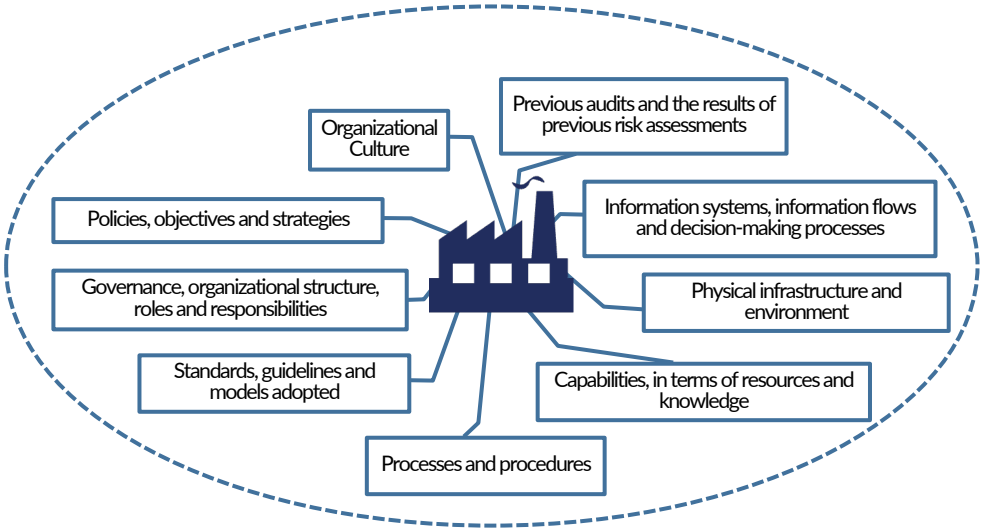
These aspects of the organization's environment continually present issues that affect information security and how information can be managed.

33

33

General

Internal Issues

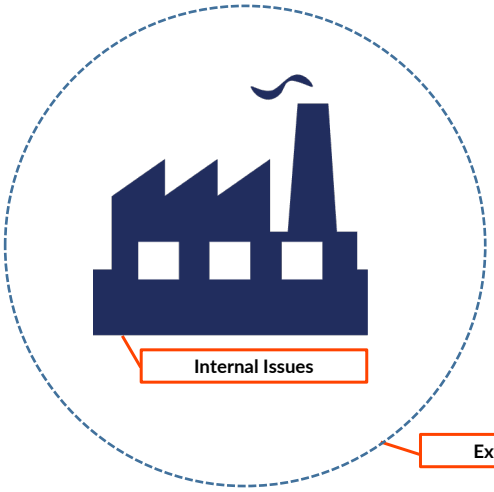


34

34

General

Internal & External Issues



To identify relevant issues, the following question can be asked: How can a certain category of issues affect information security objectives?

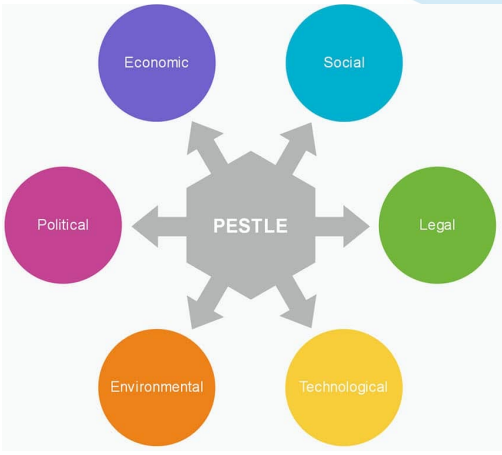
35

35

General

Internal & External Issues

Tools for internal and external analysis.



36

36

General

Understanding Stakeholder Needs and Expectations

Internal Stakeholders

Stakeholder is a term that refers to individuals or organizations that may affect or be affected or perceived to be affected by a decision or activity of the organization.

Stakeholders can be found both inside and outside the organization and may have specific needs, expectations and requirements for the organization's information security.

External Stakeholders

37

37

General

Internal Stakeholders

Internal Stakeholders

- Decision-makers, including senior management
- Process owners, system owners and information owners
- Support functions such as IT or human resources
- Employees and users
- Information security professionals

38

38

General

External Stakeholders

- Regulators and legislators
- Shareholders, including owners and investors
- Suppliers, including subcontractors, consultants and outsourcing partners
- Industry associations
- Competitors
- Customers and consumers
- Activist groups

External Stakeholders

39

39

General

ISMS Scope

- The scope defines where and for what exactly the ISMS is applicable and where and for what it is not applicable
- Setting the scope is a key activity that determines the necessary foundation for all other activities in the implementation of the ISMS

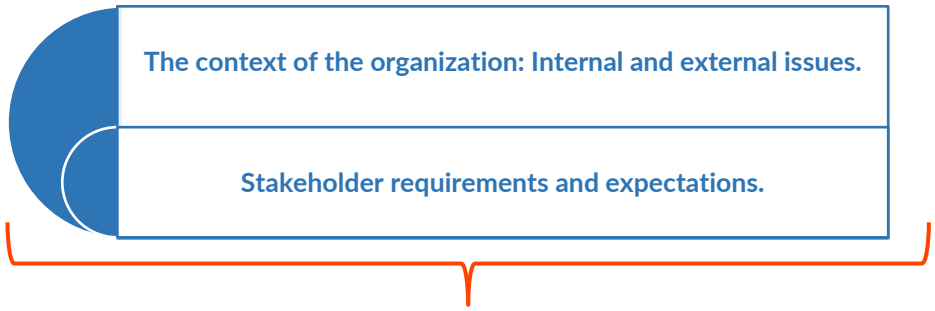
40

40

General

ISMS Scope

Identifying the correct scope of the ISMS is crucial because it will help organizations meet their security requirements and plan the implementation of the ISMS.



The elements that must be taken into account for the definition of the scope are:

41

41

General

ISMS Scope

Considerations before defining the SCOPE of the ISMS

1. Consider the information security requirements that have been identified in 4.1
2. Consider critical services that may cause a major impact on the organization or its customers and stakeholders as a result of loss of confidentiality, integrity or availability.
3. Define the scope and boundaries of the organization.
4. Define the scope and boundaries of the Information Communication Technology (ICT).
5. Define the physical scope and boundaries.
6. Integrate elemental scope and boundaries to obtain the scope and boundaries of the ISMS.
7. Consider the outsourced activities as well as the required interfaces and dependencies.

42

42

General

ISMS Scope

A multi-stage approach can be used to establish the **scope of an ISMS:**

DETERMINE THE PRELIMINARY SCOPE	This activity should be carried out by a small but representative group of management representatives.
DETERMINING THE REFINED SCOPE	Functional units within and outside the preliminary scope should be reviewed, and possibly then some of these functional units should be included or excluded to reduce the number of interfaces along the boundaries.
DETERMINE THE FINAL SCOPE	The refined scope should be evaluated by all management within the refined scope. If necessary, it should be adjusted and then precisely described.
SCOPE APPROVAL	Documented information describing the scope should be formally approved by top management.

43

43

General

5. Leadership

44

General

Leadership

5.1 Leadership and Commitment
5.2 Policy
5.3 Organizational Roles, Responsibilities and Authorities

45

45

General

Leadership & Commitment

- **Top management** is a person or group of persons who directs and controls the ISMS organization at the highest level, i.e. top management has overall responsibility for the ISMS
- **Top management** can delegate authority in the organization and provide resources to actually execute the activities related to information security and the ISMS
- **Top management** also participates in management review and promotes continual improvement

46

46

General

Leadership & Commitment

Top Management should:

- **Ensure** that the information security policy and information security objectives are established and are consistent with the strategic direction of the organization
- **Ensure** that ISMS requirements and controls are integrated into the organization's processes
- **Ensure** the availability of resources for an effective ISMS. Resources required for the ISMS include:
  1. Financial resources
  2. Personnel
  3. Facilities
  4. Technical infrastructure
- **Communicate** the need for information security management in the organization and the need to meet the requirements of the ISMS

47

47

General

Leadership & Commitment

- **Ensure** that the ISMS achieves the intended outcome(s) by supporting the implementation of all information security management processes, and in particular by requesting and reviewing reports on the status and effectiveness of the ISMS
- **Directing and Supporting** the people in the organization who are directly involved with information security and the ISMS
- **Make** an assessment of resource needs during management reviews and set objectives for continual improvement and to follow up on the effectiveness of planned activities
- **Support** individuals who have been assigned roles and responsibilities related to information security management, so that they are motivated and able to lead and support information security activities within their area

48

48

General

Policies

POLICY HIERARCHY

General high-level policies: code of conduct, etc.

Information security policy.

Policies on specific topics, e.g. access control policy, clean desktop and clean screen policy, backup policy, cryptographic control policy, etc.

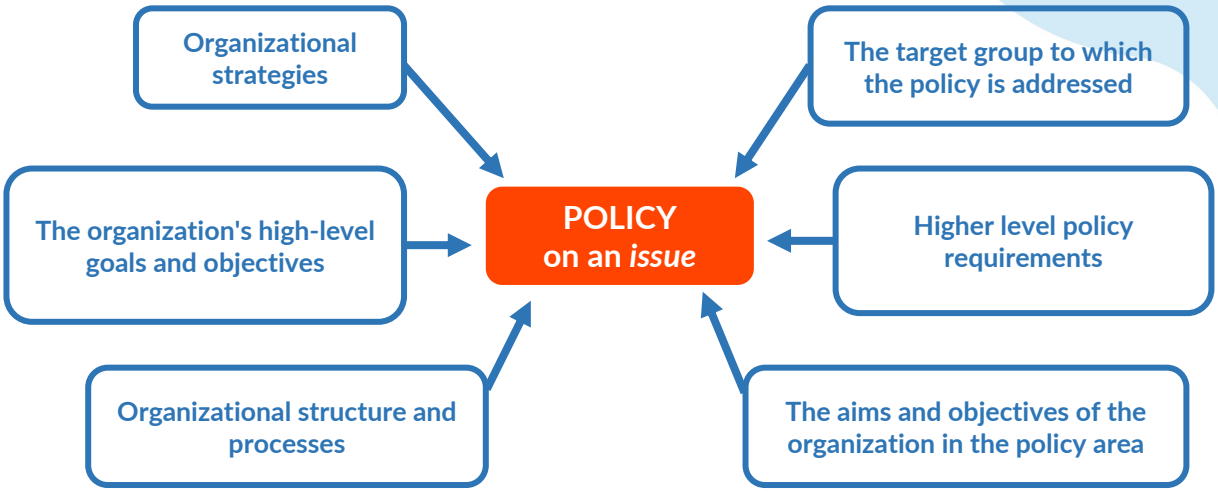
- **A policy** is a statement of an organization's intentions and direction, as formally expressed by top management
- The content of a policy guides actions and decisions about the subject matter of the policy
- An organization may have several policies; one for each area of activity that is of importance to the organization
- Some policies are independent of each other, although other policies have a hierarchical relationship

49

49

General

Content of a Policy



50

50

General

Content of a Policy

STRUCTURE OF A POLICY

Administrative:
Policy name, version, publication/validity dates, history of changes, owner(s) and authorizing person(s), classification, intended audience, etc.

Policies Summary:
General information written in one or two sentences. (Sometimes it may be merged with the introduction).

Introduction:
A brief explanation of the policy issue.

Scope:
Describes those parts or activities of an organization that are affected by the policy. If applicable, the scope lists the other policies that are supported by the policy.

Objectives:
Describes the intent of the policy.

51

51

General

Content of a Policy

STRUCTURE OF A POLICY

Principles:
Describes the rules concerning actions and decisions to achieve the objectives. In some cases, it may be useful to identify processes.

Responsibilities:
Describes who is responsible for actions to meet the requirements of the policy. In some cases, it may include a description of organizational arrangements.

Key results:
Describes the business results if the objectives are met. In some cases, they can be merged with the objectives.

Related policies:
Describes other policies relevant to the achievement of the objectives, usually providing additional details about specific issues.

Policy requirements:
Describes the detailed policy requirements.

52

52

General

Information Security Policy

- **The information** security policy describes the strategic importance of the ISMS for the organization and is available as documented information
- **The policy** directs the information security activities in the organization
- **The policy** expresses what the information security needs are in the actual context of the organization

53

53

General

I.S. Roles, Responsibilities and Authorities

Top management should regularly ensure that authorities and responsibilities for the ISMS are assigned so that the management system meets the requirements set out in ISO/IEC 27001.

54

54

General

I.S. Roles, Responsibilities and Authorities

Responsibilities and authorities should be assigned to the following information security activities

- Coordinate the establishment, implementation, maintenance, performance reporting and improvement of the ISMS.
- Advise in relation to the assessment and treatment of information security risks.
- Design information security processes and systems.
- Establish standards for the determination, configuration and operation of information security controls.
- Managing information security incidents.
- Review and audit the ISMS.

55

55

General

I.S. Roles, Responsibilities and Authorities

Relevant information security responsibilities and authorities that should be included within other roles.

Example:
Information security responsibilities can be incorporated into the roles of:

- Information owners
- Process owners
- Asset owners (e.g., application or infrastructure owners)
- Risk owners
- The functions or persons who coordinate information security (this particular role is usually a support role in the ISMS)
- Project managers
- Line managers
- Information users

56

56

General

6. Planning

57

General

Planning

6.1 Actions to Address Risks and Opportunities
6.2 Information Security Objectives

58

58

General

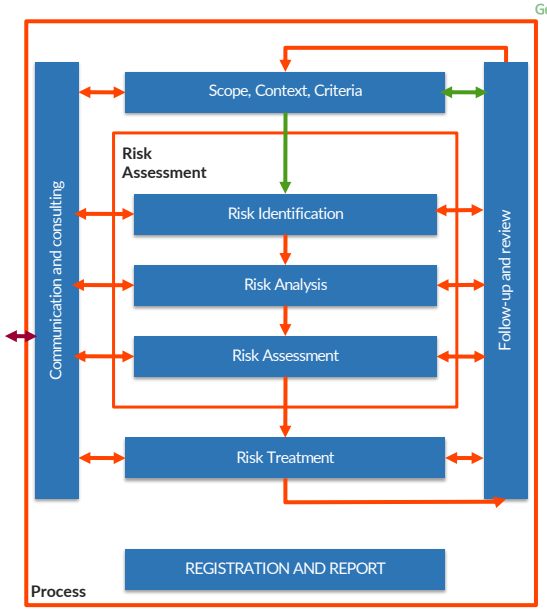
Actions to Address Risks and Opportunities

59

59

General

Actions to Address Risks and Opportunities

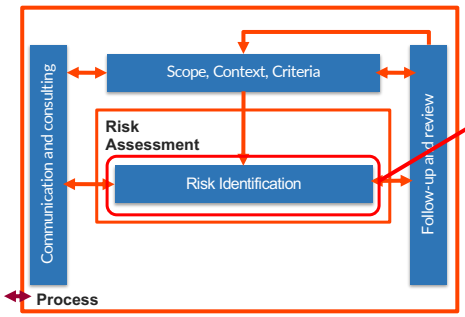


60

60

General

Risk Identification



Risk identification is the process of finding, recognizing and describing risks. It involves the identification of risk sources, events, their causes and their potential consequences.

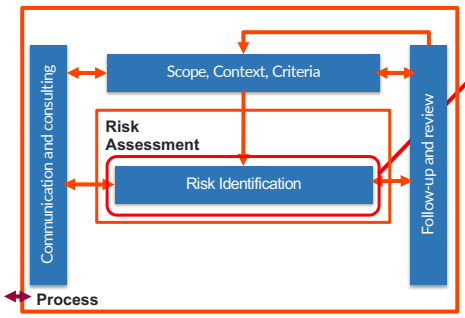
The objective of risk identification is to generate a comprehensive list of risks based on events that could create, enhance, prevent, degrade, accelerate or delay the achievement of information security objectives.

61

61

General

Risk Identification



Two approaches are generally used for the identification of information security risks:

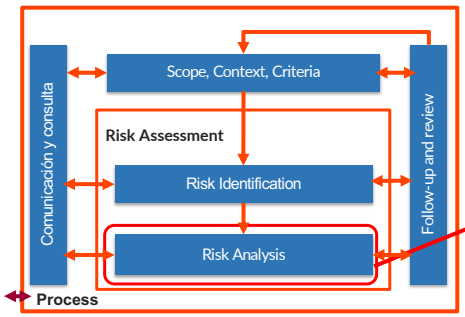
- **Event-based approach:** considers the sources of risk in a generic way. The events considered may have occurred in the past or may be foreseen for the future. In the first case, they may involve historical data, in the second case they may be based on theoretical analysis and expert opinions.
- **Approach based on the identification of assets, hazards and vulnerabilities:** considers two different types of risk sources: assets with their intrinsic vulnerabilities and hazards. The potential events considered here are ways in which threats can take advantage of a given vulnerability of an asset to impact the organization's objectives.

62

62

General

Risk Analysis



Risk analysis aims to determine the level of risk.

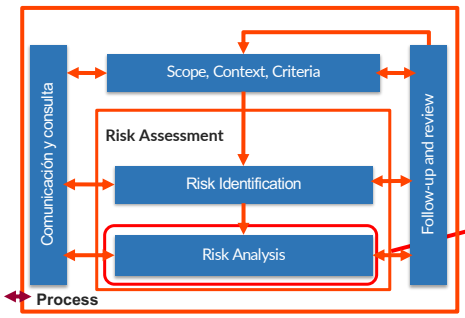
ISO 31000 is referenced in ISO/IEC 27001 as a general model. To determine a risk level, ISO/IEC 27001 requires that for each identified risk the risk analysis is based on the assessment of the consequences resulting from the risk and on the assessment of the probability of these consequences occurring.

63

63

General

Risk Analysis



Techniques for risk analysis based on consequences and probability may include:

1. **Qualitative**, using a scale of rating attributes (e.g., high, medium, low)
2. **Quantitative**, using a scale with numerical values (e.g., monetary cost, frequency or probability of occurrence)
3. **Semi-quantitative**, using qualitative scales with assigned values. Whatever risk analysis technique is used, its level of objectivity should be considered

There are several methods for analyzing risks. The two approaches mentioned above (event-based approach and approach based on the identification of assets, threats and vulnerabilities) may be suitable for information security risk analysis.

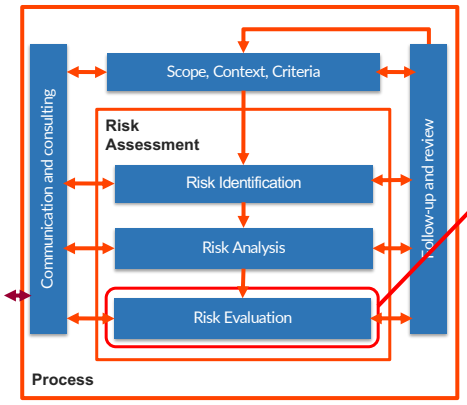
Risk identification and risk analysis processes can be most effective when carried out with the help of experts in the relevant risks being addressed.

64

64

General

Risk Assessment



The assessment of the analyzed risks involves using the organization's decision-making processes **to compare the assessed level of risk for each risk with the predetermined** acceptance criteria to determine risk treatment options.

This final step of the risk assessment verifies whether the risks that have been analyzed in the previous steps can be accepted according to the defined acceptance criteria.

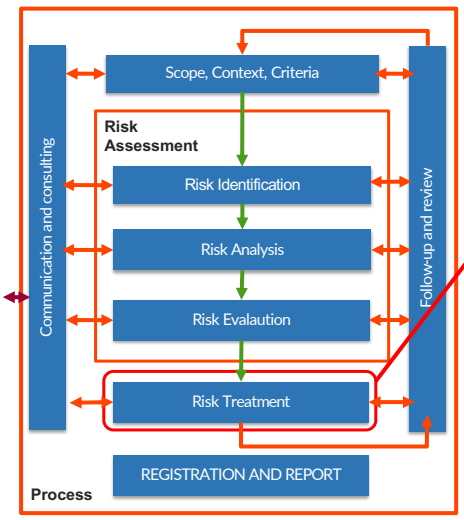
The output of this step should be a list of risks in order of priority..

65

65

General

Risk Management



Information security risk treatment is the overall process of **selecting risk treatment** options, **determining appropriate controls** to implement these options, **formulating a risk treatment** plan, and **obtaining approval** of the risk treatment plan from the risk owner(s).

The risk treatment options are:

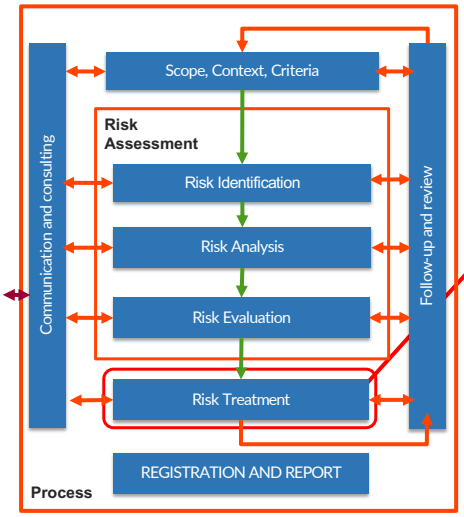
- Avoiding the risk
- Assume the risk
- Modify the risk
- Share the risk
- Retain the risk

66

66

General

Risk Management



To ensure that the treatment of information security risks is effective and efficient, it is important to be able to demonstrate the relationship between the required controls and the results of the risk assessment and treatment processes.

It may be necessary to use multiple controls to achieve the required information security risk treatment. For example, if the option is chosen to change the consequences of a particular event, controls may be required to detect the event early and controls to respond to and recover from the event.

67

67

General

Declaration of Applicability

The statement of applicability contains:

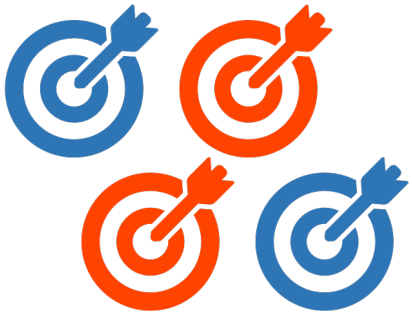
- All necessary controls determined in the previous step and for each control:
  - The justification for the inclusion of the control
  - Whether the control is implemented or not (e.g., fully implemented, in progress, not yet started)
  - The justification for the exclusion of any of the controls from ISO/IEC 27001: 2013, Annex A

68

68

General

Information Security Objectives



- Information security objectives help implement an organization's strategic goals and information security policy
- The objectives of an ISMS are the information security objectives for confidentiality, integrity and availability of information
- Information security objectives also help to specify and measure the performance of information security controls and processes in accordance with the information security policy

69

69

General

Information Security Objectives

Information security objectives should:

- Be consistent with the information security policy.
- Be measurable, if possible; this means that it is important to be able to determine whether or not an objective has been met.
- Be linked to applicable information security requirements and to the results of risk assessment and risk treatment.
- Be communicated.
- Be updated, as appropriate.

70

70

General

Expression of Security Objectives

Information security objectives can be expressed in several ways

- Numerical values with their limits, e.g., "do not exceed a certain level", and "reach level 4"
- Targets for information security performance measurements
- Targets for ISMS effectiveness measurements
- Compliance with ISO/IEC 27001; - Compliance with ISMS procedures
- The need to finalize action and plans; and - The risk criteria to be met.

71

71

General

7. Support

72

General

Support

7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented Information

73

73

General

Resources

Resources are essential to carry out any type of activity. Categories of resources may include:

- People
- Time
- Money
- Information
- Infrastructure

74

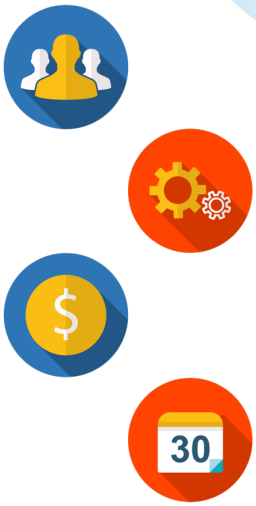
74

General

Resources

The organization should:

- Estimate the resources required for all ISMS-related activities in terms of quantity and quality (potential and capacity)
- Acquire the necessary resources
- Provide the resources
- Maintain the resources across the specific processes and activities of the entire ISMS
- Review the resources provided against the needs of the ISMS and adjust them as required



75

75

General

Competence

What is it?

- It is the ability to apply knowledge and skills for the achievement of intended results, and is influenced by knowledge, experience and wisdom
- Competence relates to the people working under the control of the organization. This means that competence should be managed for the organization's employees and for others, as needed

76

76

General

Competence

The organization should:

- Determine the expected competency for each role within the ISMS
- Assign the roles within the ISMS to people with the required competency by:
  - Identifying people within the organization who have the competency
  - Plan and implement actions for people within the organization to obtain competence
  - Hiring new people who have the competency
- Evaluate the effectiveness of actions
- Verify that people are competent for their roles
- Ensure that competence evolves over time in line with needs and meets expectations

77

77

General

Awareness Raising

The awareness of the people working under the control of the organization refers to their having the necessary understanding and motivation about what is expected of them in relation to information security.

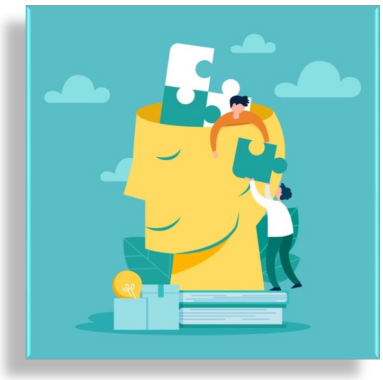
These people need to be aware that there is an information security policy and know where to find information about it.

78

78

General

Awareness Raising



The organization should:

- Develop a program with specific messages targeted to each audience (e.g., internal and external people)
- Include information security needs and expectations within awareness and training materials on other topics, to put information security needs into relevant operational contexts
- Check knowledge and understanding of messages at the end of an awareness session and randomly between sessions
- Check whether people act in accordance with the messages conveyed and use examples of "good" and "bad" behavior to reinforce the message

79

79

General

Communication

- Communication is a key process within an ISMS
- Communication can be between internal stakeholders at all levels of the organization or between the organization and external stakeholders. Communication can be initiated within the organization or by an external stakeholder
- Communication depends on processes, channels and protocols, which should be chosen in a way that ensures that the message communicated is fully received, understood and, where relevant, acted upon appropriately

80

80

General

Communication

Communication can take place on a regular basis or as the need arises. It can be proactive or reactive.

The organization should:

- Determine what content needs to be communicated. For example :
  - Information security policies
  - Objectives
  - Procedures
  - Information security requirements for suppliers
- Determine the preferred or optimal timing for communication activities
- Determine who is involved in communication activities and what the target audience is for each communication effort
- Identify the requirements for communication of relevant issues

81

81

General

Documented Information

The amount of documented information needed is often related to the size of the organization.

It is necessary for:

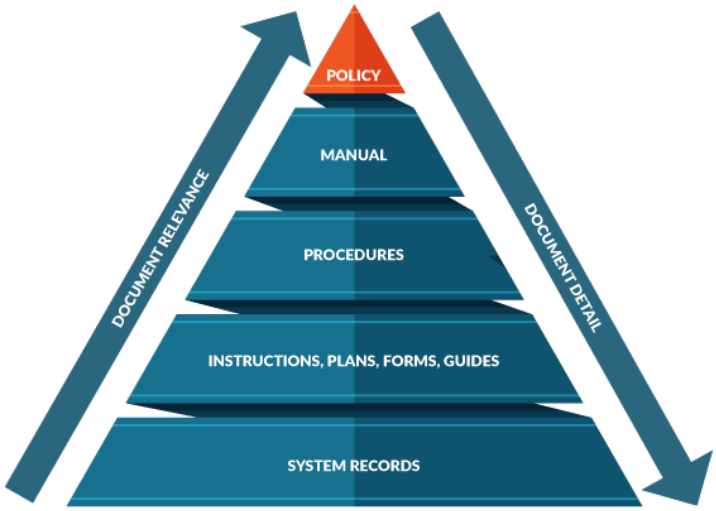
- Define and communicate information security objectives, policy, guidelines, instructions, controls, processes, procedures and which individuals or groups of individuals are expected to do it, and how they are expected to carry it out
- ISMS audits and to maintain a stable ISMS when people in key roles change
- To record the actions, decisions and results of ISMS processes and information security controls

82

82

General

Documented Information



Typical documentation structure

83

83

General

Documented Information

- The results of setting the context.
- Roles, responsibilities and authorities.
- Reports on the different phases of risk management.
- Expected competition.
- The plans and results of awareness-raising activities.
- Plans and results of communication activities.

That the organization can determine how necessary to ensure the **effectiveness of its ISMS**

- Policies, rules and directives to direct and operate information security activities.
- Documented information of external origin that is necessary for the ISMS.
- The process for controlling documented information.
- The processes and procedures used to implement, maintain and improve the ISMS..
- Action plans.
- Evidence of the results of the ISMS processes.

84

84

General

Documented Information

The organization should:

- Create a structured documented information library, linking different pieces of documented information
- Define a documentation approach that includes common attributes of all documents, allowing clear and unique identification. For example:
  - Policy
  - Regulation
  - Guideline
  - Plan
  - Format
  - Process
  - Procedure
- Avoid duplication of information in documented information, and cross-references should be used instead of repeating the same information in different documents

85

85

General

8. Operation

86

General

Operation

8.1 Operational Planning and Control
8.2 Information Security Risk Assessment
8.3 Information Security Risk Management

87

General

Operational Planning and Control

The processes that have been defined as a result of the planning phase should be implemented, operated and verified throughout the organization.

They should be considered and implemented:

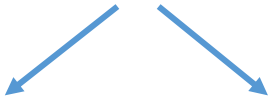
- The processes that are specific to information security management
  - Risk management
  - Incident management
  - Continuity management
  - Internal audits
  - Management reviews
- The processes arising from the information security controls in the information security risk treatment plan
- The reporting structures within the information security area, e.g., incident reports, reports on measurement of compliance with information security objectives, reports on activities performed

88

General

Operational Planning and Control

The processes that an organization uses to meet its control requirements are planned and, once implemented, monitored, particularly when changes are required.



Planned **Not foreseen**

89

89

General

Operational Planning and Control

Planned Changes

The organization should:

- **Plan** its implementation and assign tasks, responsibilities, deadlines and resources
- **Implement** changes according to the plan
- **Track** their implementation to confirm that they have been implemented according to the plan
- **Collect and retain** documented information on the execution of changes as evidence that they have been carried out as planned (e.g., with responsibilities, deadlines, effectiveness assessments)

90

90

General

Operational Planning and Control

Unplanned Changes

The organization should:

- **Examine** its consequences
- **Determine** whether any adverse effects have already occurred or may occur in the future
- **Plan and implement** actions to mitigate any adverse effects, according to need
- **Collect and retain** documented information on unanticipated changes and actions taken to mitigate adverse effects

91

91

General

Operational Planning and Control

Processes or Functions Controlled with External Suppliers

The organization should:

- **Determine** all outsourcing relationships
- **Establish** appropriate interfaces with suppliers
- **Addressing** information security issues in vendor agreements
- **Monitor and review** vendor services to ensure that they operate as intended and that the associated information security risks meet the organization's risk acceptance criteria
- **Manage** changes to supplier services, as required

92

92

General

Information Security Risk Assessment

When conducting information security risk assessments, the organization executes the risk assessment process established in the Planning phase.

The organization should:

- Have a plan in **place to carry out scheduled information security risk assessments**. When significant changes to the ISMS (or its context) or information security incidents occur
- Determine which of these changes or incidents require an additional information security risk assessment
- Determine how these assessments are triggered
- Gradually refine the level of detail of risk identification in subsequent iterations of the information security risk assessment in the context of continuous improvement of the ISMS
- Conduct an information security risk assessment at least once a year

93

93

General

Information Security Risk Management

To address information security risks, the organization needs to carry out the information security risk treatment process established in the Planning phase.

The organization should:

- Carry out the risk treatment process after each repetition of the information security risk assessment process or when the implementation of the risk treatment plan or part of it fails

94

94

General

9. Performance Evaluation

95

General

Performance Evaluation

9.1 Monitoring, Measurement, Analysis and Evaluation
9.2 Internal Audit
9.3 Management Review

96

96

General

Monitoring, Measurement, Analysis and Evaluation

MONITORING AND MEASUREMENT

Objetive

To assist the organization in judging whether the intended outcome of information security activities, including risk assessment and treatment, have been achieved as planned.

The Organization Establishes

- What to track and what to measure
- Who does the monitoring, who measures and when they do it
- The methods for obtaining valid (i.e., comparable and reproducible) results

97

97

General

Monitoring, Measurement, Analysis and Evaluation

ANALYSIS AND EVALUATION

The Organization Establishes

- Who establishes and evaluates the results of monitoring and measurement, and when
- The methods for producing valid results. There are two aspects of evaluation

Performance

To determine whether the organization is performing as expected, which includes determining the extent to which the processes within the ISMS meet its specifications.

ISMS Effectiveness

To determine whether the organization is doing things the right way, including determining the extent to which information security objectives are being met.

98

98

General

Monitoring, Measurement, Analysis and Evaluation

ASPECTS TO BE MEASURED

- Project progress Implementation
- Decrease in the value of the risk from one period to another
- Coverage of allocated budget
- Improved stakeholder perception of security
- Awareness of the policy
- Decrease in security incidents in confidentiality, integrity or availability
- Incident attention
- Effectiveness of corrective actions
- Lessons learned implemented
- Evaluation of personnel
- Decrease in nonconformities identified by process
- Verification of teleworking security conditions
- Time delay in the withdrawal of privileges
- Efficiency in equipment maintenance
- Incidents due to passwords assignment and management.
- Equipment leaving and entering the organization
- Controlled removable media
- Backup recoveries
- Effectiveness in complying with evacuations and drills
- Threats detected by antivirus
- Decrease in technical vulnerabilities identified from one period to the next

99

99

General

Internal Auditing

- An audit is characterized by several principles:
  - Integrity
  - Fair presentation
  - Due professional care
  - Confidentiality
  - Independence
  - Evidence-based approach
- Internal audits provide information about whether the ISMS meets the organization's own requirements for its ISMS as well as those of ISO/IEC 27001

100

100

General

Internal Auditing

AUDIT PROGRAM — Describes the general framework for a group of audits planned for specific times and directed towards specific purposes.

AUDIT PLAN — Describes activities and arrangements for a specific audit.

AUDIT CRITERIA — They are a set of policies, procedures or requirements used as a reference against which audit evidence is compared, i.e. audit criteria describe what auditors expect to find.

101

101

General

Management Review

Ensuring: continued suitability, adequacy and effectiveness of the ISMS.

INPUT

- Results of previous reviews
- Stakeholder feedback
- External and internal changes
- Process performance
- Non-conformities and corrective actions
- Tracking and measurement results
- Audit results
- Achievement of objectives
- Risk assessment results and treatment plan status
- Opportunities for improvement

OUTPUT

Continuous Improvement decisions and any change decisions.

RECORDS

Development, analysis, conclusions, action plans.

102

102

10. Improvement

103

Improvement

10.1 Non-conformity and Corrective Action
10.2 Continuous Improvement

104

104

General

Nonconformity and Corrective Action

NONCONFORMITY

It is the non-compliance with an ISMS requirement. Requirements are needs or expectations that are established, implicit or mandatory.

Types

- Non-compliance with an ISO/IEC 27001 requirement (in whole or in part) in the ISMS
- Non-implementation or non-compliance with a requirement, regulation or control established in the ISMS
- Partial or total non-compliance with legal, contractual or customer agreed requirements

105

105

General

Nonconformity and Corrective Action

Examples of NON-CONFORMITIES

- Individuals whose behavior is not in accordance with procedures and policies.
- Suppliers that do not supply the agreed products or services.
- Projects that do not produce the expected results.
- Controls not operating according to design.

106

106

General

Nonconformity and Corrective Action

CORRECTIVE ACTIONS

They are aimed at eliminating the cause of a nonconformity and preventing its recurrence. Corrective actions can occur after corrections or in parallel with them.

The following process steps should be undertaken:

1. Decide whether corrective action is necessary according to the established criteria
2. Review the nonconformity considering whether similar nonconformities have been recorded, all the consequences and their secondary effects caused, and the corrections made
3. Conduct a thorough analysis of the cause of the nonconformity

107

107

General

Nonconformity and Corrective Action

4. Conduct an analysis of the potential consequences on the ISMS
5. Determine the actions needed to correct the cause, assessing whether they are proportional to the consequences and impact of the nonconformity
6. Plan the corrective actions giving priority, if possible, to the areas with the highest probability of recurrence and to the most significant consequences of the nonconformity
7. Implement the corrective actions according to the plan
8. Make an assessment of the corrective actions to determine whether they have actually addressed the cause of the nonconformity and whether related nonconformities have been prevented from occurring

108

108

General

Continuous Improvement

- Continuous improvement of the ISMS should imply that the ISMS itself and all its elements were assessed considering internal and external issues (4.1), stakeholder requirements (4.2) and performance assessment results (clause 9)
- The assessment may also include an analysis of the efficiency of the ISMS and its elements, considering whether its use of resources is appropriate, whether there is a risk that lack of efficiency may lead to loss of effectiveness or whether there are opportunities to improve efficiency
- Opportunities for improvement can also be identified when managing nonconformities and corrective actions

109

109

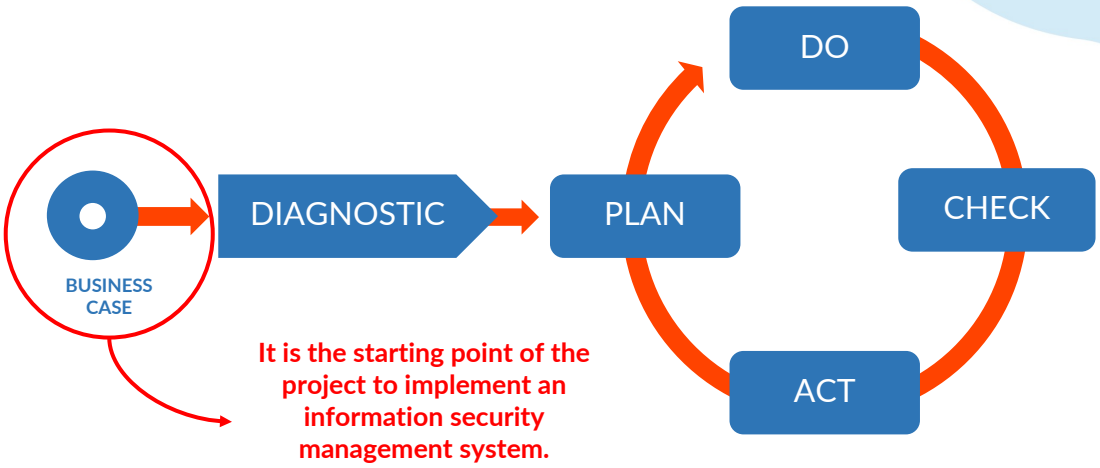
General

Structure: Business Case

110

General

Business Case Creation



It is the starting point of the project to implement an information security management system.

111

111

General

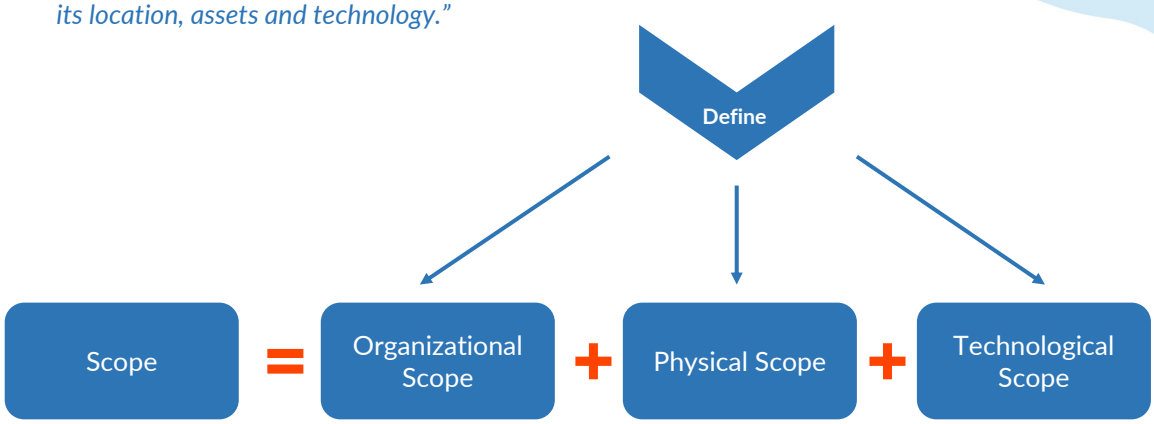
Methodology: ISMS Scope and Boundary

112

General

Define

"Define the scope of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology."



113

113

General

ISMS Scope Definition Steps

1 **Organizational Scope** — Based on the description of the organization's processes and structure.

2 **Physical Scope** — Considering the different locations and the physical distribution of the different areas of the organization.

3 **Technological Scope** — Based on the diagrams and descriptions of the technology infrastructure.

4 **Integration** — The 3 dimensions and provide a rationale for any exclusions to the scope of the ISMS.

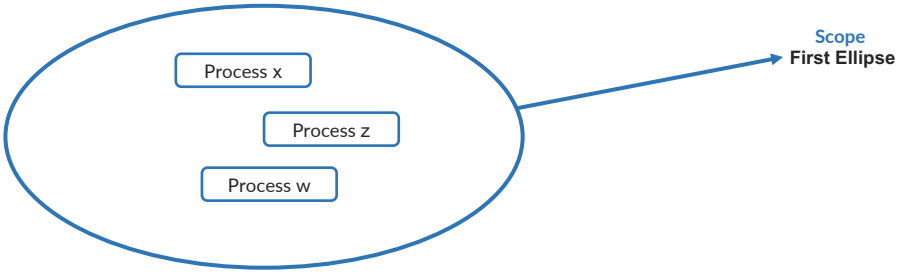
114

114

General

Ellipse Method

1 Locate the most relevant processes within the scope ellipse.



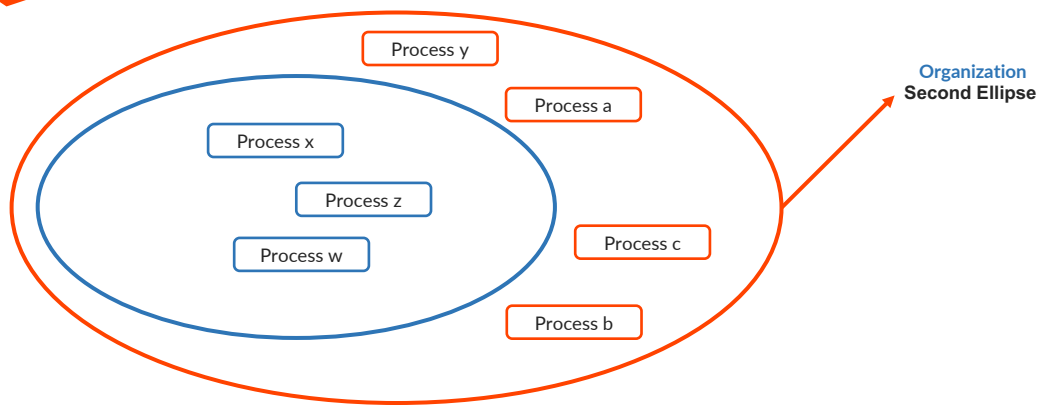
115

115

General

Ellipse Method

2 Locate the other processes according to the characteristics of the organization.



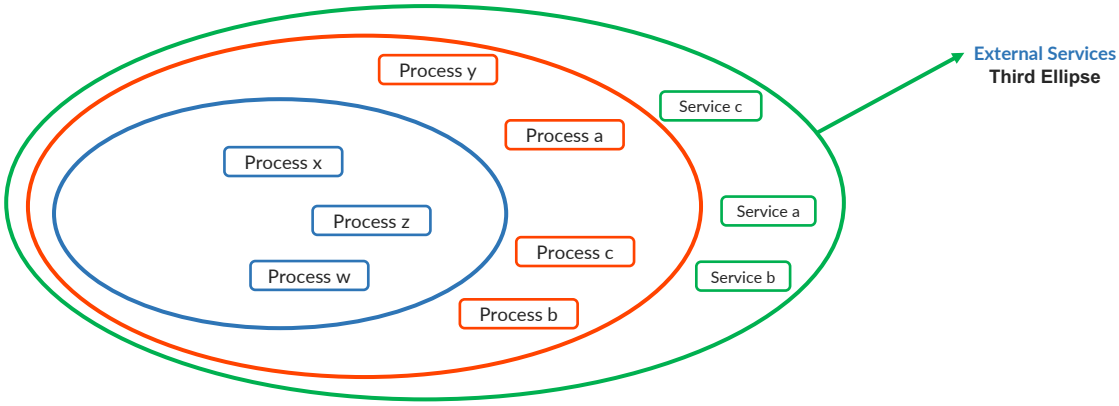
116

116

General

Ellipse Method

3 Locate those external services that have interaction with the scope processes.



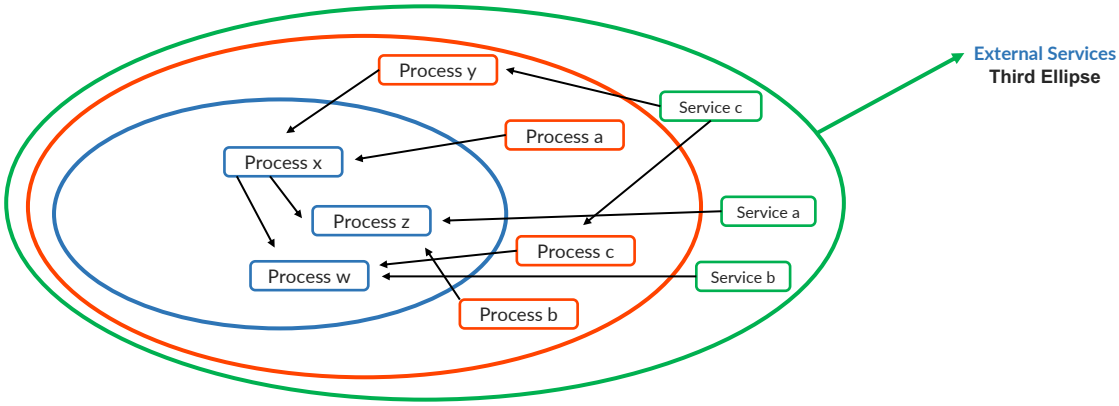
117

117

General

Ellipse Method

4 Trace the interrelationships between the processes according to the description of the interactions and interrelationships between them.



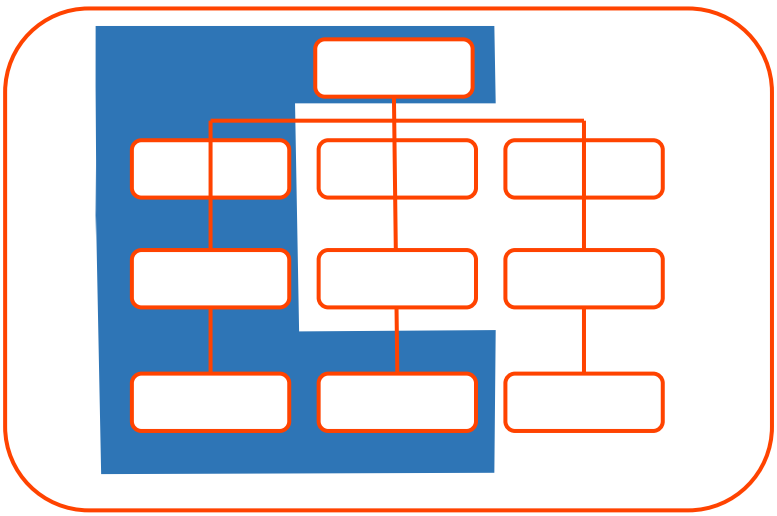
118

118

General

Functional Structure Diagram

- Draw a diagram of the functional structure of the organization
- Identify the areas included in the proposed scope
- Highlight lines of command and other safety-relevant information



119

119

General

Physical Plant Diagram

- Represent, in a diagram, the physical plant of the organization
- Identify the areas included in the proposed scope
- Highlight access points, physical barriers, facilities and other security-relevant information

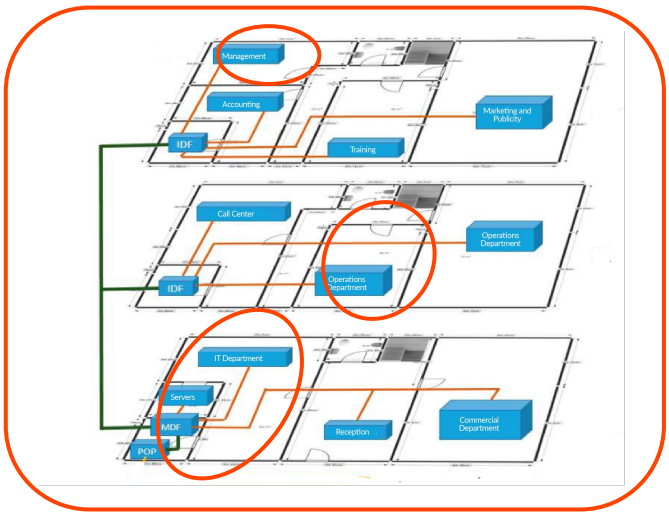
120

120

General

Logical Plant Diagram

- Represent in a diagram the logical organization of the organization's network and IT services
- Identify the areas included in the proposed scope
- Highlight gateways, routers, firewalls, active equipment, services, actors, facilities and other security-relevant information



121

121

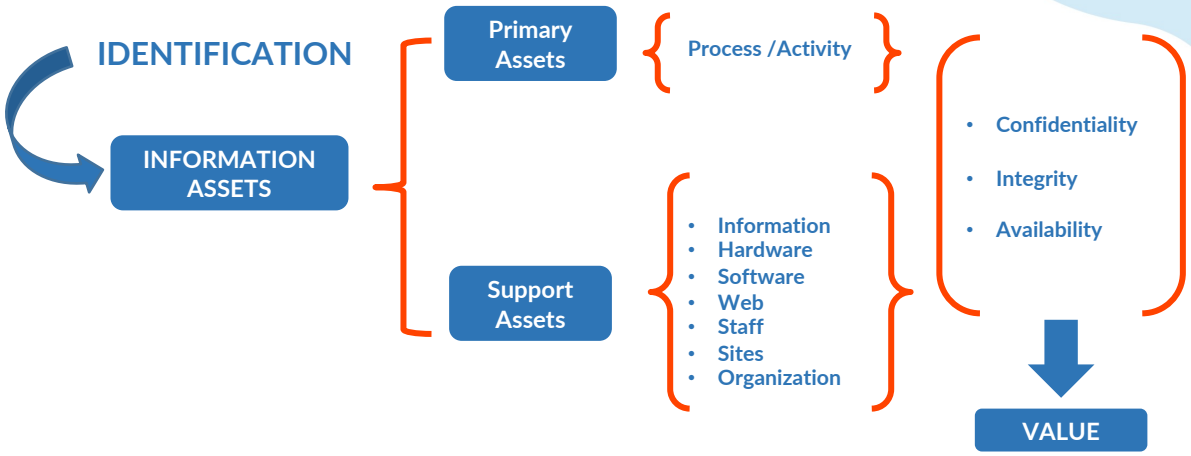
General

Methodology: Asset Management

122

General

Identification



123

123

General

Classification and Valuation

CLASSIFICATION AND VALUATION → INFORMATION ASSETS

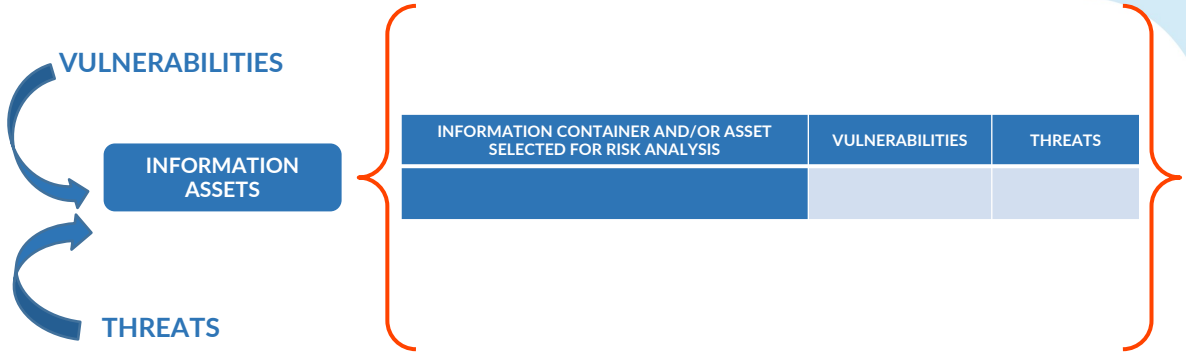
INFORMATION ASSET IDENTIFICATION		CONFIDENCIALITY			INTEGRITY			AVAILABILITY			CONSOLIDATED VALUATION			TOTAL
ASSET N.	ASSEST NAME	FINANCIAL	LEGAL	IMAGE	FINANCIAL	LEGAL	IMAGEN	FINANCIAL	LEGAL	IMAGE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	
1	ASSET 1													

124

124

General

Analyze Information Assets



125

125

General

Methodology: Risk Management

126

	RATE										
ASSETS	Confidentiality	Integrity	Availability	Total	Threats	Possibility/ Occurreace	Vulnerability	Potential Vulerability Exploitability	Active Value	Potential Occurreace	Total
1) Customer Data	H	H	H	H	Plagiarism Counterfeiting Alteration Privacy	L L L A	Organizational deficiency Difficulty in shipping Unauthorized access Document control	L H H M	H	M	M
2) Invoice as Document	H	H	H	H	Loss of document Delayed delivery Ilegitimacy of data Incorrect Charges	H H L L	Incomplete documents Lack of knowledge of routes Printing deficiency Processing errors	H H L H	H	M	M
3) Rates	H	H	H	H	Incorrect Alteration Ignorance of changes Offers	L M H	Unauthorized access Poor training Lack of communication	M L M	H	L	L
4) Services provided	L	H	H	H	Misinterpretation Little detail Unsolicited service	M H M	Unqualified personnel, Cost reduction, Typing error	M H M	H	M	M
5) Invoicing software	H	H	H	H	Code errors Malicious code Technical flaws User Errors Lack of security	M H M L H	Unqualified personnel Access controls Electric power Poor training Lack of policies	L M H L H	H	H	H
6) Means of communication and/or delivery	H	H	H	H	Functioning faults Lack of security Lack of personnel	H H L	Electric power Configuration error Low availability	H M L	H	H	H
Legend	High Medium Low	H M L									

127

General

Methodology: ISMS Policy

General

ISMS Policy Creation Steps

129

129

General

Internal Requirements

Identify internal requirements

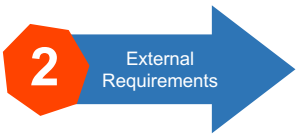
INTERNAL REQUIREMENTS LIST	
TOP MANAGEMENT	
SHAREHOLDERS	
EMPLOYEES	

130

130

General

External Requirements



Identify external requirements

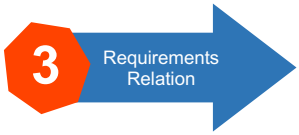
EXTERNAL REQUIREMENTS LIST	
27001 REQUIREMENTS	
STANDARDS / LEGISLATION	
MARKET FORCES	

131

131

General

Requirements Relation



Establish the degree of relationship that each one of them has, valuing it on a scale of 1 to 5 (5 being the highest value), then add them up and the most representative values will correspond to guidelines or phrases that should make up the Policy

REQUIREMENTS	27001 REQUIREMENTS	STANDARDS / LEGISLATION	MARKET FORCES
TOP MANAGEMENT			
SHAREHOLDERS			
EMPLOYEES			
FURTHER GUIDELINES			

132

132

General

Revision & Delivery

4 Revision & Delivery

Then review vision, mission and other guidelines and determine if there are any guidelines regarding information security that have not been taken into account, in order to include them in the policy

Mission

Vision

Values

133

133

General

Policy Writing

5 Policy Writing

Recommendations for drafting an information security policy

- The policy should have as part of its text the statement indicating what is to be done, what regulates the policy, what is the guideline to be followed by employees, contractors and/or third parties, all aligned with the organization's strategy
- Align with the scope of the ISMS
- It must be specified to whom the policy is addressed, it must be easily identified who must comply with the policy
- In case the policy applies, it must indicate the exceptions to the policy and to whom the exception applies

134

134

General

Policy Writing

Recommendations for drafting an information security policy

- Where applicable, reference is made to the regulation by which the policy is supported
- Details of the persons or roles in the entity that can provide information on the policy
- Name, role or person responsible for authorizing the policy
- Describe the steps and procedures for making adjustments to the policy
- Explanation of the consequences in the event that a staff member, contractor or third party fails to comply with the policy
- Effective date of the policy

135

135

General

Policy Writing

It is important to clarify that a policy:

- Is **NOT** a standard
- It should **NOT** indicate how any work or control will be executed in a specific way
- It does **NOT** indicate specific technology of use

They are very general and high-level statements that embody an objective to be met by the organization.

136

136

General

ISO 27001
CERTIFIED LEAD IMPLEMENTER

137

Optimal
Training • Consulting • Business Solutions

ISO 27001
Certified Lead Implementer

Thanks for your participation

138