Leadership and project approval

- Business case
- Resource requirements
- ISMS project plan
- ISMS project team
- Management approval

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 5.1

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) *ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;*
b) *ensuring the integration of the information security management system requirements into the organization's processes;*
c) *ensuring that the resources needed for the information security management system are available;*
d) *communicating the importance of effective information security management and of conforming to the information security management system requirements;*
e) *ensuring that the information security management system achieves its intended outcome(s);*
f) *directing and supporting persons to contribute to the effectiveness of the information security management system;*
g) *promoting continual improvement; and*
h) *supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.*

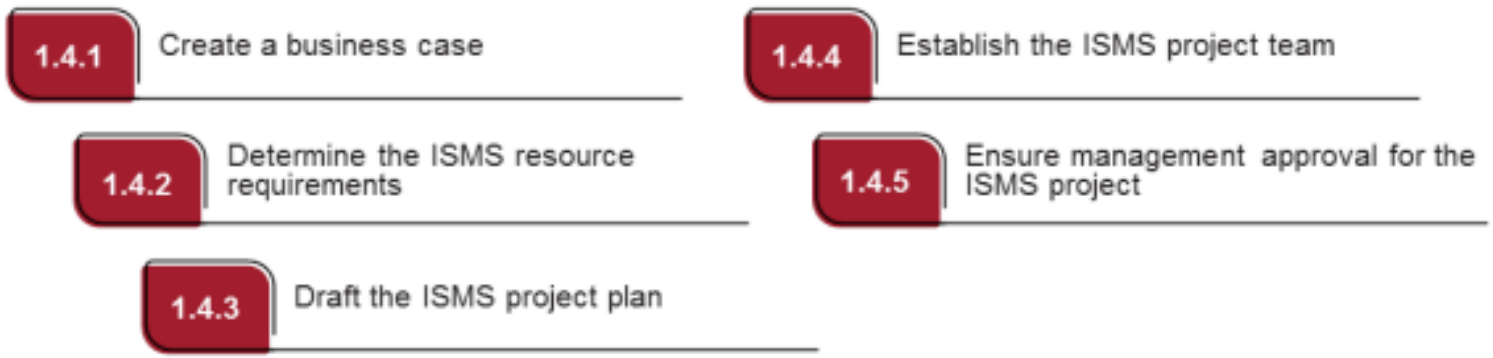
Leadership and Project Approval

ISO/IEC 27021, clause 5.2

ISO/IEC 27001 clause/subclause (if applicable)	***5 Leadership***
Intended outcome	*Directing, motivating and encouraging staff across the organization to deliver information security*
Knowledge required	*— Theories of leadership* *— Negotiation techniques*
Skills required	*— Set and give direction for information security across the organization* *— Provide guidance, set objectives and drive progress within the information security function, team and the business* *— Deliver commitments* *— Deploy responsibilities and authorities at the different levels of the organization*

1.4 Leadership and Project Approval

List of activities



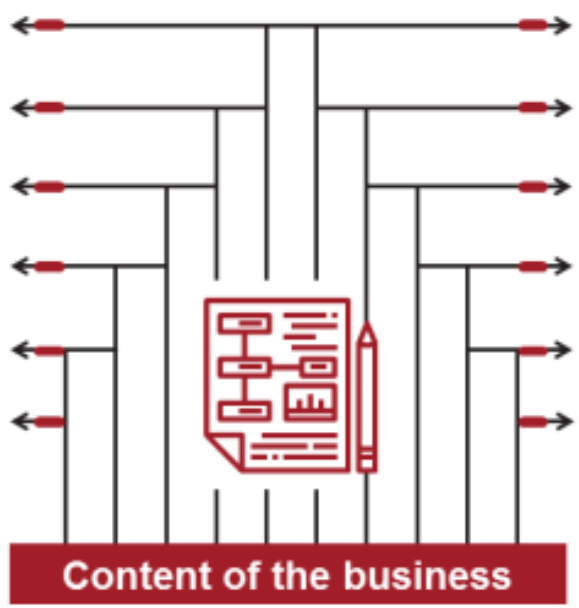
1.4.1 Create a Business Case

A business case is:

1. A tool for decision-making support
2. A document used to promote the ISMS project
3. A way to define clear objectives

The Content of a Business Case

- Environment
- Purpose and objectives
- Project summary
- Expected benefits
- Preliminary scope
- Critical success factors



- Preliminary project plan
- Deadlines and milestones
- Roles and responsibilities
- Necessary resources
- Budget
- Constraints

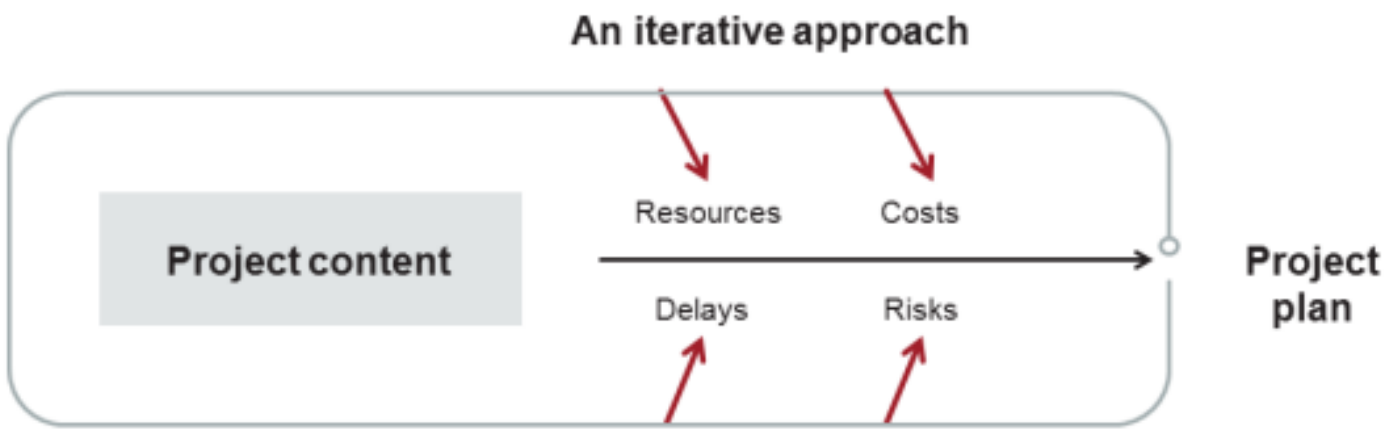
1.4.2 Determine the ISMS Resource Requirements

- In order for the implementation of the ISMS to be carried out successfully, the ISMS project manager must ensure that the necessary resources are identified.
- The resources needed for the project usually include:
  1. People
  2. Information and data
  3. Facilities, equipment, and consumables
  4. Information and communication technology (ICT) systems
  5. Transportation
  6. Finance
  7. Partners and suppliers

1.4.3 Draft the ISMS Project Plan

PMBOK, 5th Edition

The development of a project plan is an iterative process. During the project planning phase, the following are identified: project risks, costs, resources, and potential delays.



The Content of the ISMS Project Plan

A project plan typically includes the following:

- Project charter
- Description of the approach or project management strategy
- Formulation of project content, with project deliverables and objectives
- Work breakdown structure (WBS)
- Estimated costs, projected start date, and assignment of duties
- References, costs, and time performance measurements
- Major milestones with their provisional date
- Key personnel
- Key risks, with the constraints and assumptions and the proposed answers
- Current problems and pending decisions

Review the ISMS Project Plan

PMBOK 5th Edition

- Review the project objectives and success factors
- Review the proposed method
- Highlight the risks and uncertainties inherent in the project
- Estimate the necessary internal resources
- Define the sequence of phases and the planned execution
- Review the deliverables to be provided
- Review the roles and responsibilities
- Review the project documents
- Define the frequency and content of progress meetings

1.4.4 Establish the ISMS Project Team

The ISMS project team:

ISMS Project Manager

Required competences

To be able to carry out the tasks, the ISMS project manager should have:

- Knowledge and skills in project management
- Knowledge of the organization and its context
- Knowledge of basic information security management
- Interpersonal skills (effective communication, negotiation, problem-solving, leadership skills, etc.)

Note:

The ISMS project manager is often the information security manager of the organization.

Steering Committee

Objective	Ensure the planning and monitoring of the ISMS
Missions	1. Plan the ISMS implementation 2. Define the ISMS project in line with the objectives set by the top management 3. Define the roles and responsibilities for the ISMS project 4. Define the roles and responsibilities related to operations and maintenance of the ISMS (after implementation) 5. Select the method of risk analysis and criteria for risk acceptance 6. Manage the resources 7. Perform management reviews
Members	ISMS project manager, security manager, responsible persons for key services involved in the following application domains: IT, audit, legal, finance, HR, physical security department
Meeting frequency	Monthly

1.4.5 Ensure Management Approval for the ISMS Project

Management commitment to the ISMS project can bring several benefits:

- Increased knowledge of applicable laws, regulations, contractual obligations, and standards related to information security
- Adequate allocation of resources dedicated to information security
- Identification and protection of critical assets
- Monitoring and review of information security processes
- Access to reliable information on the organization's level of risk exposure so as to take appropriate decisions

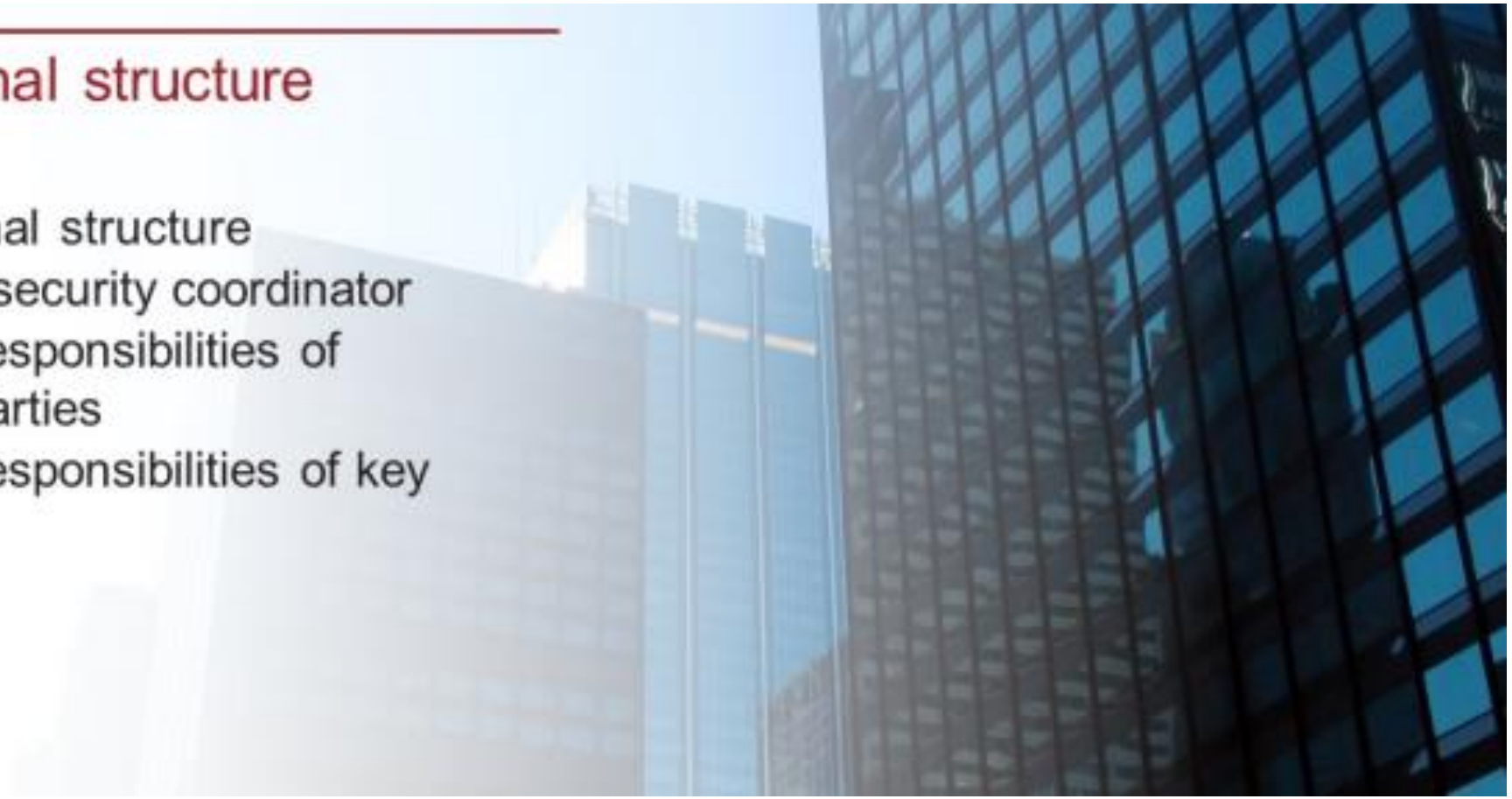
Role of the Top Management in the ISMS Project

Objective	Align the ISMS with the business objectives and strategy
Missions	1. Set the objectives and strategy for the ISMS 2. Validate the roles and responsibilities of key interested parties in the project 3. Validate the security policies of the ISMS 4. Approve the criteria for the acceptance of risk 5. Approve the risk treatment plan and allow the implementation of the ISMS 6. Provide adequate resources for the implementation and maintenance of the ISMS
Members	Top management (CEO, CIO, CFO, etc.)
Meeting frequency	Several meetings when marking the project milestones: risk analysis report, risk treatment planning, Statement of Applicability, management review, etc.

1. **Which of the statements below regarding the definition of a business case is NOT true?**
    A. A tool that promotes ISO/IEC 27001
    B. A way to define clear objectives
    C. A tool for decision-making support
2. **Which resources are necessary for the implementation of an ISMS?**
    A. Cloud, management, and human resources
    B. Technology tools as they surpass the knowledge of employees for information security
    C. People, information, facilities, transportation, finance
3. **Which of the following statements is correct for an ISMS project plan?**
    A. The development of a project plan is a sequential process
    B. The development of a project plan is an iterative process
    C. The development of a project plan is an incremental process
4. **An ISMS project team consists of the project champion, project manager, project management team, project team, and interested parties.**
    A. True
    B. False
5. **Who must approve the ISMS business case and project plan?**
    A. Any of the organization's employees
    B. The organization's management
    C. The head of the IT department

Organizational structure

- Organizational structure
- Information security coordinator
- Roles and responsibilities of interested parties
- Roles and responsibilities of key committees



ISMS Roles and Responsibilities

ISO/IEC 27001, clause 5.3

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.
Top management shall assign the responsibility and authority for:

a) *ensuring that the information security management system conforms to the requirements of this document;*
b) *reporting on the performance of the information security management system to top management.*

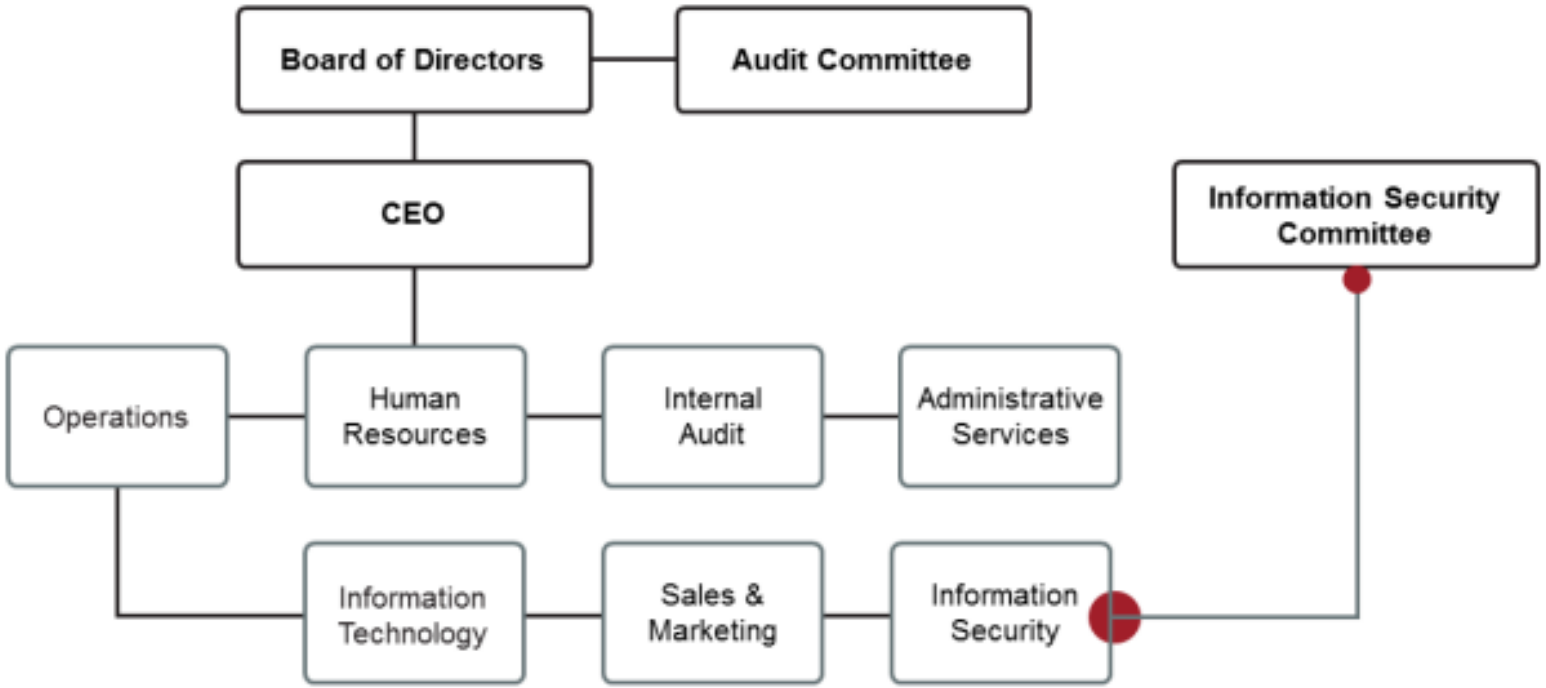
NOTE

Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

1.5 Organizational Structure

List of activities

1.5.1 Define the Organizational Structure for Information Security



1.5.2 Appoint an Information Security Coordinator

- Information security activities are to be coordinated by representatives of different parts of the organization that play relevant roles and job functions within the scope of the ISMS.
- Typically, information security coordination should involve the cooperation of managers, users, administrators, application designers, auditors, and security personnel, as well as experts in areas such as insurance, legal issues, human resources, IT, and risk management.

1.5.3 Assign the Roles and Responsibilities of Interested Parties

Role	Main responsibilities
Head of information security	Coordinate activities related to information security management
Legal counsel	Identify compliance requirements (legal, regulatory, and contractual)
Head of Human Resources	Manage training and awareness programs on information security, consider the security controls in HR processes (recruitment, termination of employment, disciplinary process)
Facilities manager	Implement and manage physical security controls (access control to buildings, protection against fire, electricity maintenance, etc.)
Head of IT	Implement and manage solutions and technical measures in daily operations
Head of service center	Implement and manage services to users and the related controls (access control, incident management, etc.)
Public relations officer	Validate the impact on the organization's reputation, communications with external interested parties
Internal auditor	Validate the ISMS compliance and security controls
Documentation manager	Ensure that the documented information have the qualities of good management of knowledge and information heritage, preservation of evidence, and law enforcement

Key Roles and Responsibilities

What are the missions?	How to implement?	When?
Determine the objectives for the processes/controls	Discuss with the management, the head of information security, and relevant staff members	Once a year
Be a "relay" between the information security responsible personnel and all those involved in the operation of processes/controls	• Communicate and educate on issues related to information security • Encourage the reporting of incidents, malfunctions, suggestions for improvement, etc. • Communicate the decisions of the information security committees and the management reviews	Ongoing
Ensure the proper functioning of the process controls and availability of all related documentation	Verify that the processes and controls are applied every day	Ongoing
Ensure the compliance of documentation with information security requirements (file process, records, procedures, and other related documents)	Take into account the audit results, the reports of the information security committee, and the feedback from interested parties	Ongoing
Ensure the availability of information to monitor and measure the process	Check if the tools to perform a monitoring and review process are available	According to the periodicity of indicators
Follow the treatment of nonconformities and corrective and preventive actions on the process	Verify that the monitoring table notification forms are properly filled out	After each reporting

1.5.4. Define the Roles and Responsibilities of Key Committees

Management Committee

Objective	Ensure the leadership and commitment of the top management related to the information security management system
Level of intervention	Strategic level
Missions	1. Ensure the inclusion of the values of the organization and its business goals in the process of managing information security 2. Set annual objectives and the ISMS strategy 3. Ensure that annual management reviews take place 4. Provide adequate resources for the proper functioning of the ISMS 5. Control the contribution to the ISMS business processes, cost optimization, etc. 6. Approve major projects in information security 7. Validate and approve updates to the risk assessment 8. Communicate with the interested parties
Members	Top management (CEO, CIO, CFO)
Meeting frequency	One to four times a year

Information Security Committee

Objective	Ensure the proper functioning of the ISMS and the security controls
Level of intervention	Tactical level
Missions	1. Ensure the smooth running of the ISMS operations 2. Promote coherence in information security within the organization 3. Maintain the organization's risk assessment 4. Act as the liaison between operations and the management 5. Manage problems of information security and propose solutions to nonconformities 6. Monitor the implementation of action plans and implementation of corrective actions arising from the risk analysis
Members	CISO, ISMS manager, individuals responsible for key services (IT, audit, legal, finance, HR, physical security)
Meeting frequency	Monthly

Operational Committees

Objective	Ensure the effectiveness of corrective actions and the processes of reacting to nonconformities
Level of intervention	Operational level
Missions	1. Ensure the implementation of security controls 2. Manage the ISMS documented information 3. Improve the ISMS and treat the nonconformities
Members	Depends on the specific committee
Meeting frequency	Weekly

1. **Who shall ensure the assignment of ISMS roles and responsibilities according to ISO/IEC 27001?**
   A. The human resources
   B. The top management
   C. The heads of departments
2. **What is one disadvantage of the traditional organizational model in information security governance?**
   A. Strong capacity of influence because the CISO is on the same or lower hierarchical level with IT managers
   B. No real or potential conflicts of interest
   C. Poor consideration to issues related to information security
3. **What does "CISO" stand for in an information security infrastructure?**
   A. Chief information security officer
   B. Corporate information support officer
   C. Champion information security officer
4. **It is advisable for the chief information security officer (CISO) to report directly to the information security committee.**
   A. True
   B. False

5.Which of the following is NOT a key committee in an organization's information security management system implementation project?

A. Information security committee
B. Operational committee
C. A third party committee

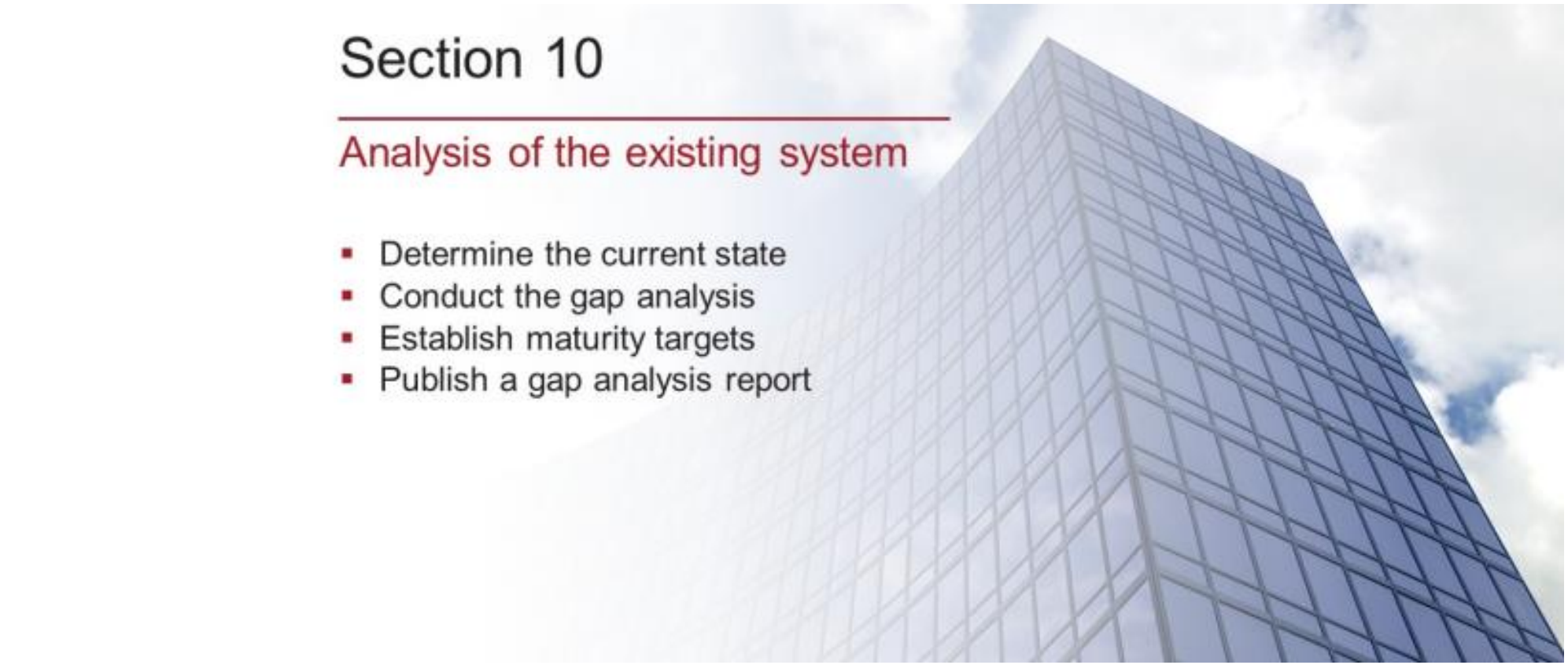
6.The main objective of the _____ is to ensure the proper functioning of the ISMS and security controls.

A. Management committee
B. Information security committee
C. Operational committee

Section 10

Analysis of the existing system

- Determine the current state
- Conduct the gap analysis
- Establish maturity targets
- Publish a gap analysis report



The Gap Analysis Technique

Understanding the gap analysis

Gap analysis is a technique used to determine the steps to move from a current state to a desired future state.

1.6 Analysis of the Existing System

List of activities

1.6.1 Determine the Current State

Information gathering

Observations

Observe the organization's operations, system, and the staff involved in such operations and systems in order to fully understand them

Questionnaires

Send questionnaires to a group of people who represent the interested parties

Interviews

Conduct interviews with key individuals at different hierarchical levels within the organization

Documentation review

Read and analyze the relevant documented information (e.g., internal policies, procedures, previous audit reports, contracts)

Scan tools

Use technical tools to detect technical vulnerabilities and establish a list of assets which have possible impacts on a network, perform a code review, etc.

Conduct Interviews

Recommendations when conducting interviews

- Use open-ended questions and avoid close-ended or guiding questions
- Ensure all the subjects are covered while managing the time available for the interview
- Take notes during the interview
- Ask additional questions to clarify a response or a situation

Individual and Group Interviews

Individual

Individual interviews usually provide more detailed information and allow a more thorough ISMS assessment.

Interviews

Group

Group interviews are more effective in establishing the basic criteria to reach a consensus on the ISMS assessment, discuss treatment options, etc.

Questionnaires

Open-and closed-ended questions

Examples of open-ended questions:

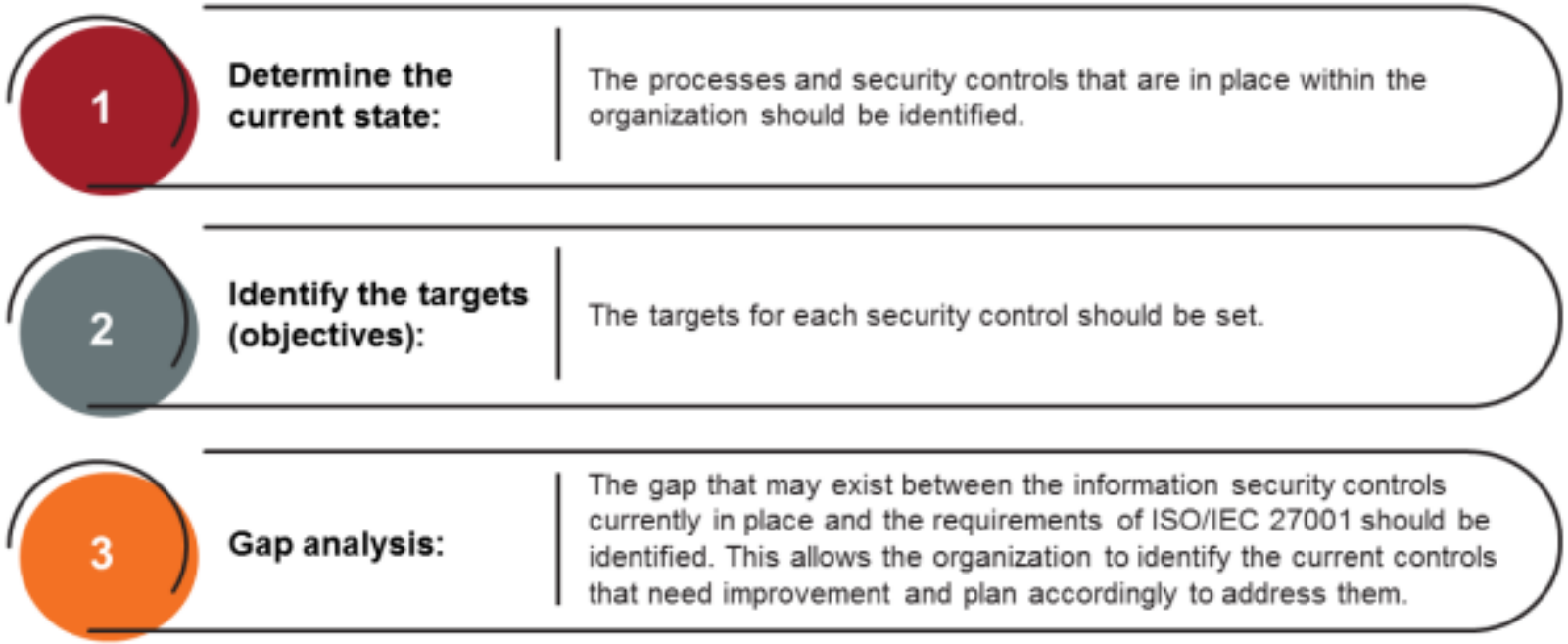
1. How would you improve the implementation of the ISMS?
2. Mention the tools that you used to measure the effectiveness of the ISMS implementation?
3. Could you mention and explain the approach that you took when defining the roles and responsibilities?
4. Mention the points which you focused on when you conducted the training session?

Examples of close-ended questions:

1. Are the processes of the organization controlled?
2. Have all the concerned interested parties been informed about the existing processes?
3. Is there any training session available in the organization?
4. Does the organization document its processes?

1.6.2 Conduct the Gap Analysis

A gap analysis is performed as follows:



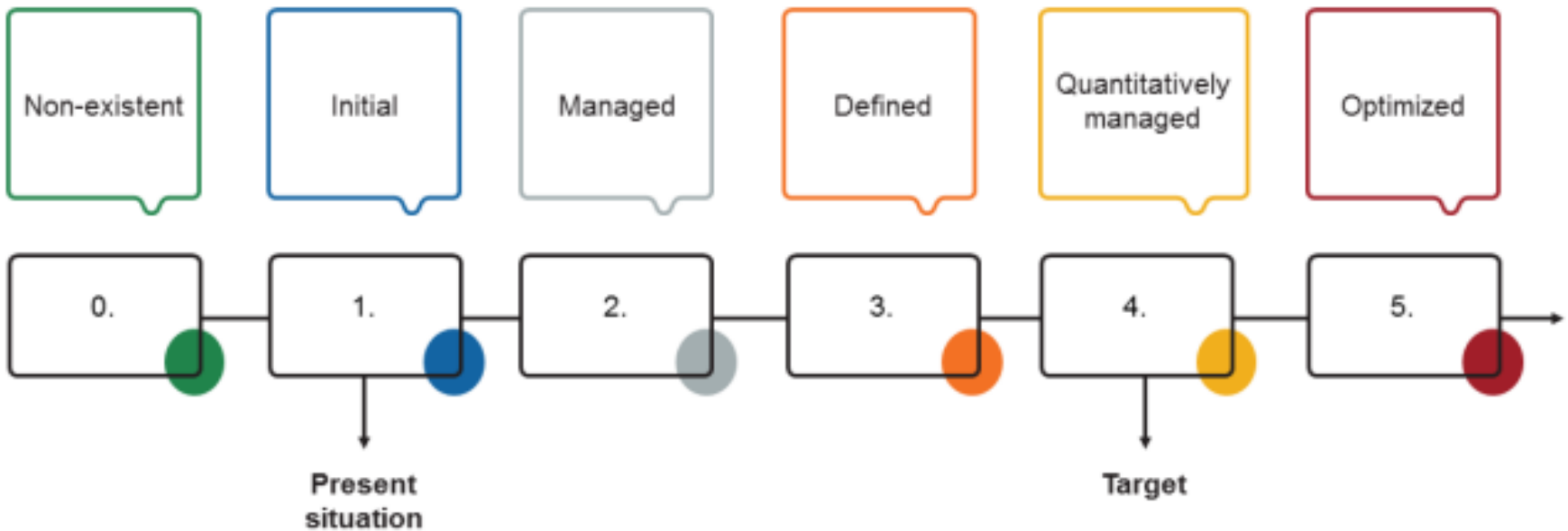
ISO/IEC 21827 and CMM

Assessment matrix of maturity levels

ISO/IEC 21827 seeks the improvement of the software development process based on the CMM (Capability Maturity Model) which is:

- An evaluation model and evolution of capabilities on a grid of maturity in five hierarchical levels
- A model largely reproduced by experts to conduct a gap analysis with ISO/IEC 27001 and ISO/IEC 27002

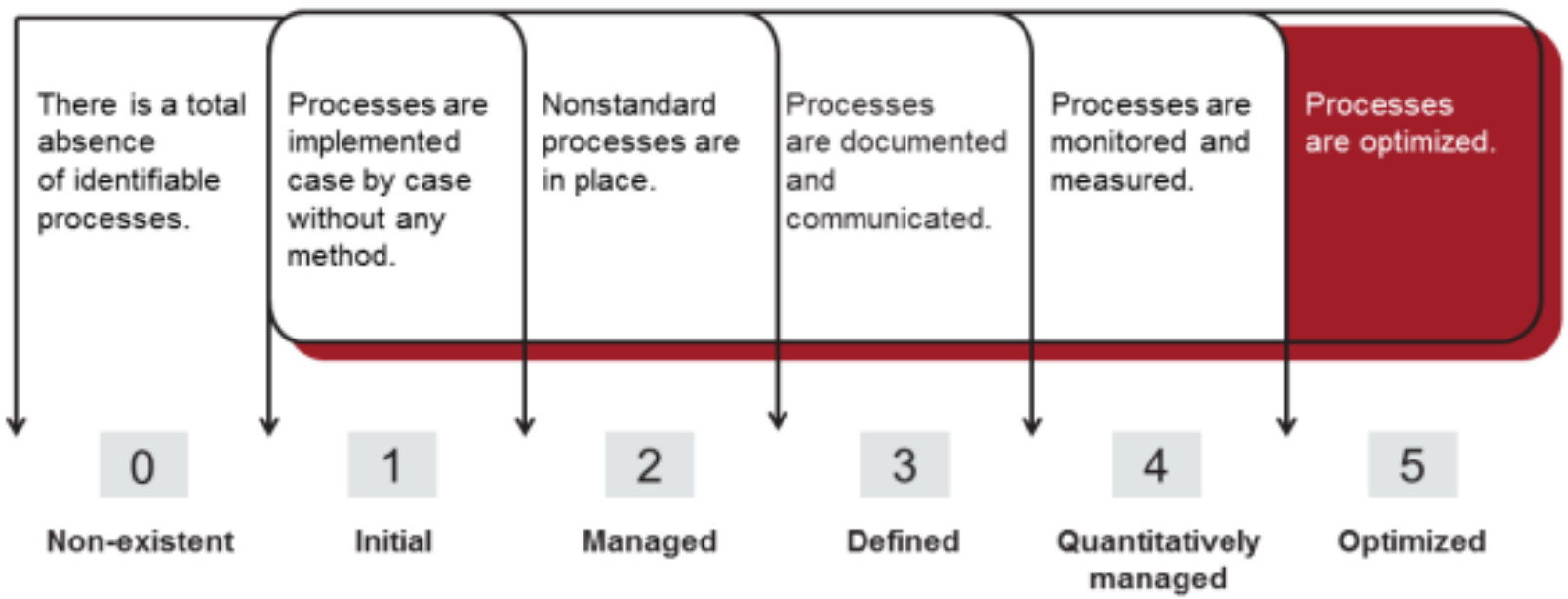
1.6.3 Establish Maturity Targets



Establish Maturity Targets

Gap analysis and the level of maturity

You can set targets for processes and information security controls based on target maturity levels:



Establish Maturity Targets and Analysis

Example 1: Gap analysis in the context of ISO/IEC 27001

Clause	Requirement	Description of the actual situation	Current maturity	Target maturity	Gap analysis	Responsible
Annex A 5.1 *Policies for information security*	*Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.*	An information security policy does exist and has been signed by the top management, but the document has never been disseminated to all employees. Only the persons involved in the implementation of the ISMS are aware of the policy. The document is also not easy to find on the organization's intranet.	3	4	The policy was not communicated properly.	Robert Johnson, CISO

Establish Maturity Targets and Analysis

Example 2: Gap analysis in the context of ISO/IEC 27001

Clause	Requirement	Description of the actual situation	Current maturity	Target maturity	Gap analysis	Responsible
Annex A 5.18 *Access rights*	*Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.*	The organization has procedures in place for the provision and revocation of physical and logical access rights based on the organization's access control rules. However, the organization has not established a procedure for ensuring regular reviews of access rights.	2	5	The physical and logical access rights are not reviewed periodically. The access rights review procedure should be established and should consider the current responsibilities of users and authorizations for privileged access rights.	Robert Johnson, CISO

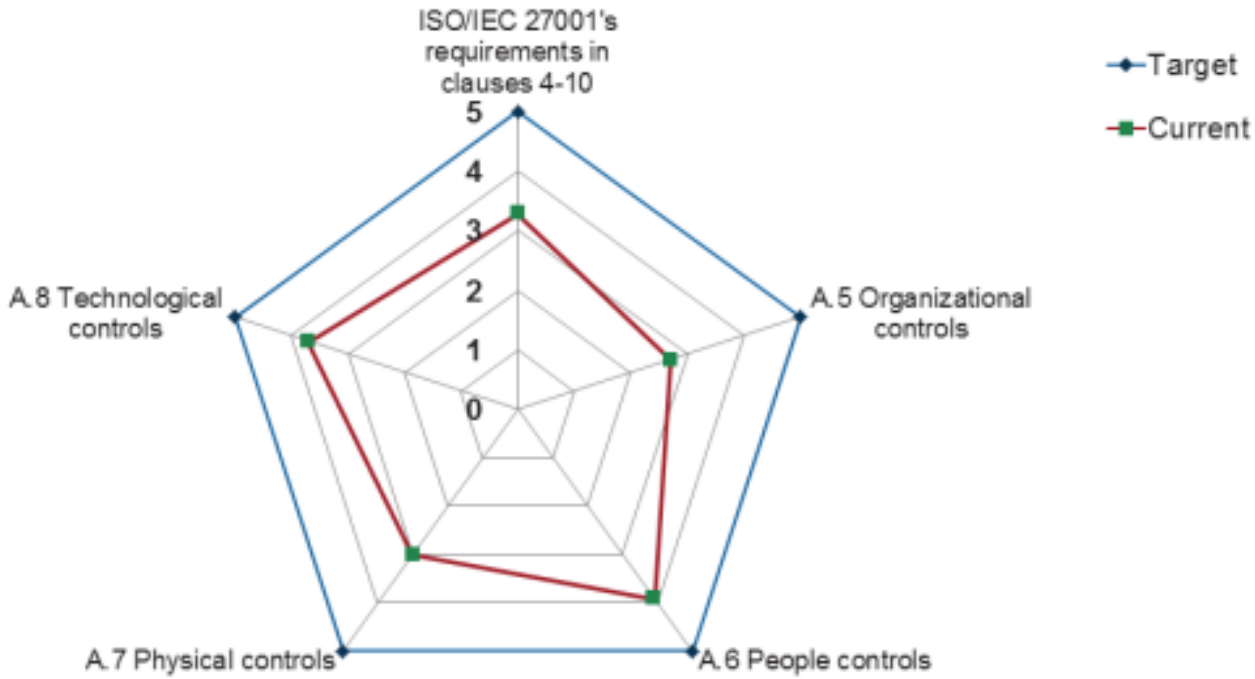
1.6.4 Publish a Gap Analysis Report

Example — Content of a gap analysis report

- Introduction
  - Report objective
  - Methodology
- Baseline of the current information security controls
  - Available tools and processes
  - Challenges with the available tools, processes, and resources
- Information security-focused decision-making framework
  - Identify and select a project
  - Predict the outcomes of the ISMS project
  - Implement the ISMS project
- Identification and analysis of gap(s)
- Suggested bridging options
- Summary and next steps to be taken

Publish a Gap Analysis Report

Example of a graphical representation



1. **What is a gap analysis?**
    A. A technique used to determine the steps to move from a current state to a desired future state
    B. A technique used to determine the ways in which a process might potentially fail, with the objective of eliminating the likelihood of such a failure
    C. A technique used to evaluate the organization against its competitors and produce a comprehensive long-term planning
2. **An organization has reported that its processes have reached the level of best practices. What level of maturity is this?**
    A. Quantitatively managed
    B. Optimized
    C. Initial
3. **Which of the following is NOT a level of maturity?**
    A. Quantitatively managed level
    B. Non-existent level
    C. Objective-based level
4. **Which type of interviews prevents the "bandwagon effect"?**
    A. Individual interviews
    B. Group interviews
    C. Questionnaires

5.An organization has concluded that its processes are standardized, documented, and communicated. What level of maturity is this?

A. Level 2: Managed
B. Level 3: Defined
C. Level 4: Quantitatively managed

6.Which of the following is an effective visual tool to present the gap analysis results?

A. Radar chart
B. Ichikawa diagram
C. Cause-and-effect diagram

Section 11

Information security policy

- Types of policies
- Policy models
- Information security policy
- Specific security policies
- Management policy approval
- Publication and dissemination
- Training and awareness sessions
- Control, evaluation, and review

ISO/IEC 27001 Requirements

ISO/IEC 27001, clauses 5.1 and 5.2

5.2. Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;
b) includes information security objectives or provides the framework for setting information security objectives;
c) includes a commitment to satisfy applicable requirements related to information security;
d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;
f) be communicated within the organization;
g) be available to interested parties, as appropriate.

5.1. Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

Policy — Guideline

Policy

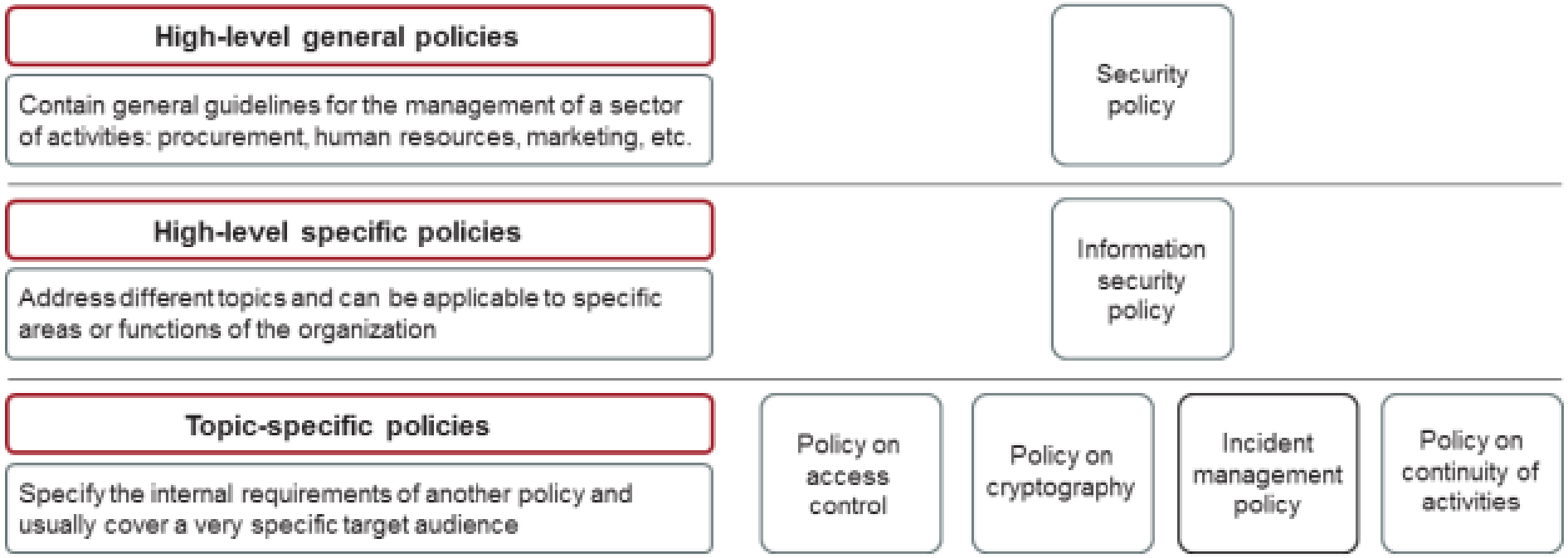
Clause 3.53 of ISO/IEC 27000 defines a policy as “intentions and direction of an organization, as formally expressed by its top management.”

Guideline

A guideline is a document stating a general rule, principle, or information on how something should be done.

Types of Policies

ISO/IEC 27003, Annex A

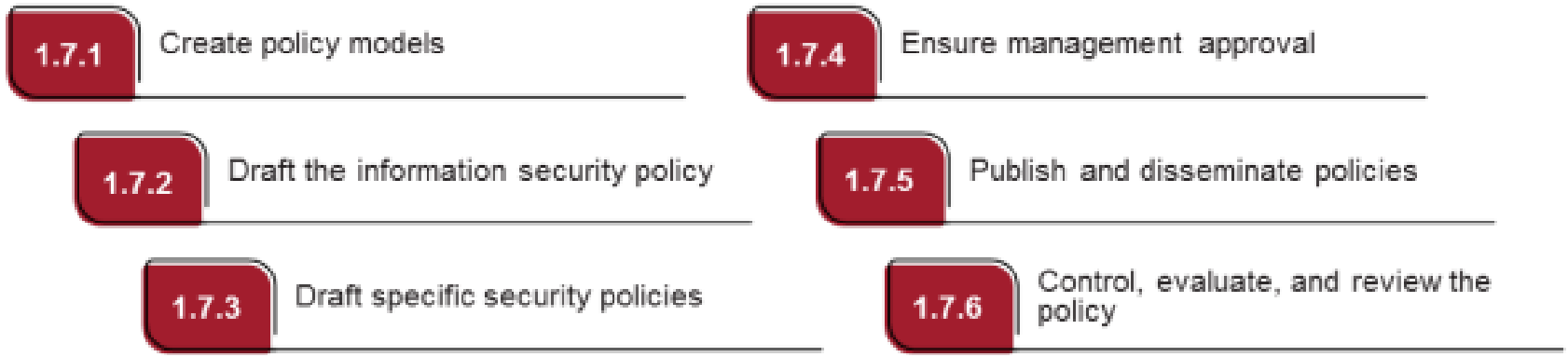


Information Security Policies

Information security policy development life cycle

1.7 Security Policy

List of activities



1.7.1 Create Policy Models

ISO/IEC 27003, Annex A

Policies can have the following structure:

- **a)** *Administrative*
- **b)** *Policy summary*
- **c)** *Introduction*
- **d)** *Scope*
- **e)** *Objectives*
- **f)** *Principles*
- **g)** *Responsibilities*
- **h)** *Key outcomes*
- **i)** *Related policies*
- **j)** *Policy requirements*

Policy Drafting Process

General process

Note: It is important to ensure the support and understanding of a policy before its publication.

1.7.2 Draft the Information Security Policy

Model (extract)

Summary of the information security policy	The information security policy aims to ensure an adequate level of information assets of the organization against all threats. The ISMS establishes, implements, operates, monitors, reviews, maintains, and improves processes and controls related to information security based on a risk approach.
Introduction	The organization should ensure that the integrity, confidentiality, and availability of information generated within the scope of the ISMS is respected. The organization shall ensure the protection of its information assets against internal or external and accidental or deliberate threats.
ISMS scope	This policy applies to all activities of the organization included in the ISMS scope.
ISMS objectives	The objectives are to: ensure continuity of critical business activities; ensure that all information processed, stored, traded, or released by the organization is of absolute integrity; ensure that all information will be monitored and stored according to the procedures for maintaining confidentiality; provide choice of appropriate security controls to protect the assets and give confidence to interested parties; and ensure effective management and efficient information security management.
Principles of the information security policy	The organization shall establish, implement, operate, monitor, review, maintain, and improve the ISMS based on a documented approach to risk activity and compliance with the requirements of ISO/IEC 27001. The organization should take into account all legal, regulatory, and contractual requirements in its ISMS. The legal and regulatory requirements will be met in priority, even if they are inconsistent with the policy described here. The organization shall establish and implement a risk management program documented in accordance with the requirements of ISO/IEC 27001. The criteria for evaluation and acceptance of risk must be established, formalized, and approved by the management. This policy has been approved by the management and is subject to an annual review.

Draft the Information Security Policy (Cont'd)

Model (extract)

Responsibilities	The management is responsible for ensuring that the objectives and plans for the ISMS are established and reviewed annually in management review meetings, the roles and responsibilities regarding information security are defined, awareness programs are conducted, an internal audit is conducted at least once a year, and the necessary resources to maintain and improve the ISMS are provided. The CISO is responsible for intervening on all aspects of the organization's information security. The CISO decides on, in general, all the requirements for the effective operation of the ISMS by means of administrative directives, previously submitted to the top management. Each executive has the responsibility of ensuring that persons working under their control will protect information in accordance with the policies of the organization. All users (management, employees, contractors, and third party users) should be aware of the risks to information security, their responsibilities, and the need to respect the policies to ensure the adequate protection of information.
Expected results	Appropriate and proportionate information security controls will be implemented to protect assets and give confidence to interested parties. Decisions on matters of information security will be based on an evaluation of risks faced by the organization. The legal, regulatory, and contractual requirements related to information security will be met.
Related policies	The security policy, the human resource management policy, the policy on training and skills development of personnel

1.7.3 Draft Specific Security Policies

Example of a policy on email use

Policy summary	The email system is a resource belonging to the organization and is available to users for business purposes. The occasional and not abusive emails for personal use are tolerated if they are made during the free time of the user and only if they do not impair the performance of their work.
Introduction	All outgoing emails are part of an organization's public image; therefore, managing these emails is crucial in order to avoid the potential reputational risk that may result from the inappropriate delivery of such emails. The aim of this policy is to regulate the use of emails by all users.
Scope	This policy covers the appropriate use of any email sent from the organization's email account. This policy applies to all employees, members of management, and contracted personnel using a corporate email account provided by the organization.
Information security objectives	The objective is to prevent the public image of the organization from being damaged by the improper use of corporate email addresses, to prevent the risks of junk email (spam) arising from improper use of email, both internally, and by third parties related to the organization.

Draft Specific Security Policies (Cont'd)

Information security principles	• **Prohibited use:** The corporate email account will not be used and it shall not be offensive or racist. Any user who finds this type of use in the hands of one of their colleagues should immediately report the case. • **Personal:** It is forbidden to pass on chain emails or jokes. This prohibition also applies to relay emails that were received from colleagues. • **Monitoring:** The organization will monitor the messages circulating on its infrastructure without prior notification. • **Penalties:** Any user who violates this policy may be subject to disciplinary action including dismissal or final termination of contract.
Responsibilities	It is the responsibility of the ISMS team, in cooperation with human resources, to ensure compliance with this policy and take steps to enforce it. Each user must know this policy and shall respect it.
Key outcomes	The outcomes are: decrease of the problems related to spam, better usage of the email by users, better protection of the organization's image
Related policies	Information security policy, the public relations and use of trademarks, privacy policy

1.7.4 Ensure Management Approval

The information security policy shall:

- Demonstrate the commitment of the management
- Be approved by the management

The policy must be signed by an individual (often the CEO) but the approval process may belong to a committee:

- Board of Directors
- Management Board
- Security Governance Committee

1.7.5 Publish and Disseminate Policies

Main modes of communication

Intranet

Meeting

Distribution of hard copies

New employee orientation session

1.7.6 Control, Evaluate, and Review the Policy

Review

Maintain conformity

Control

Ensure conformity

Evaluation

Measure the
degree of conformity

1. **Who shall establish the information security policy according to ISO/IEC 27001?**
    A. The top management
    B. External interested parties
    C. The information security manager
2. **What is the difference between a policy and a guideline?**
    A. A policy states the intentions and direction of an organization, whereas a guideline states how something should be done
    B. A policy is a type of a guideline that provides guidance for different topics
    C. A policy is a document stating how something should be done, whereas a guideline is an explanation of procedures
3. **Which type of policy specifies the internal requirements of another policy and covers a very specific target audience?**
    A. High-level general policies
    B. High-level specific policies
    C. Topic-specific policies
4. **Which of the options below is a high-level specific policy?**
    A. Incident management policy
    B. Information security policy
    C. Policy on cryptography

5.What is the first phase of the information security policy development life cycle?

A. Policy construction
B. Policy monitoring and maintenance
C. Risk assessment

6.Who shall communicate the information security policy to the relevant interested parties?

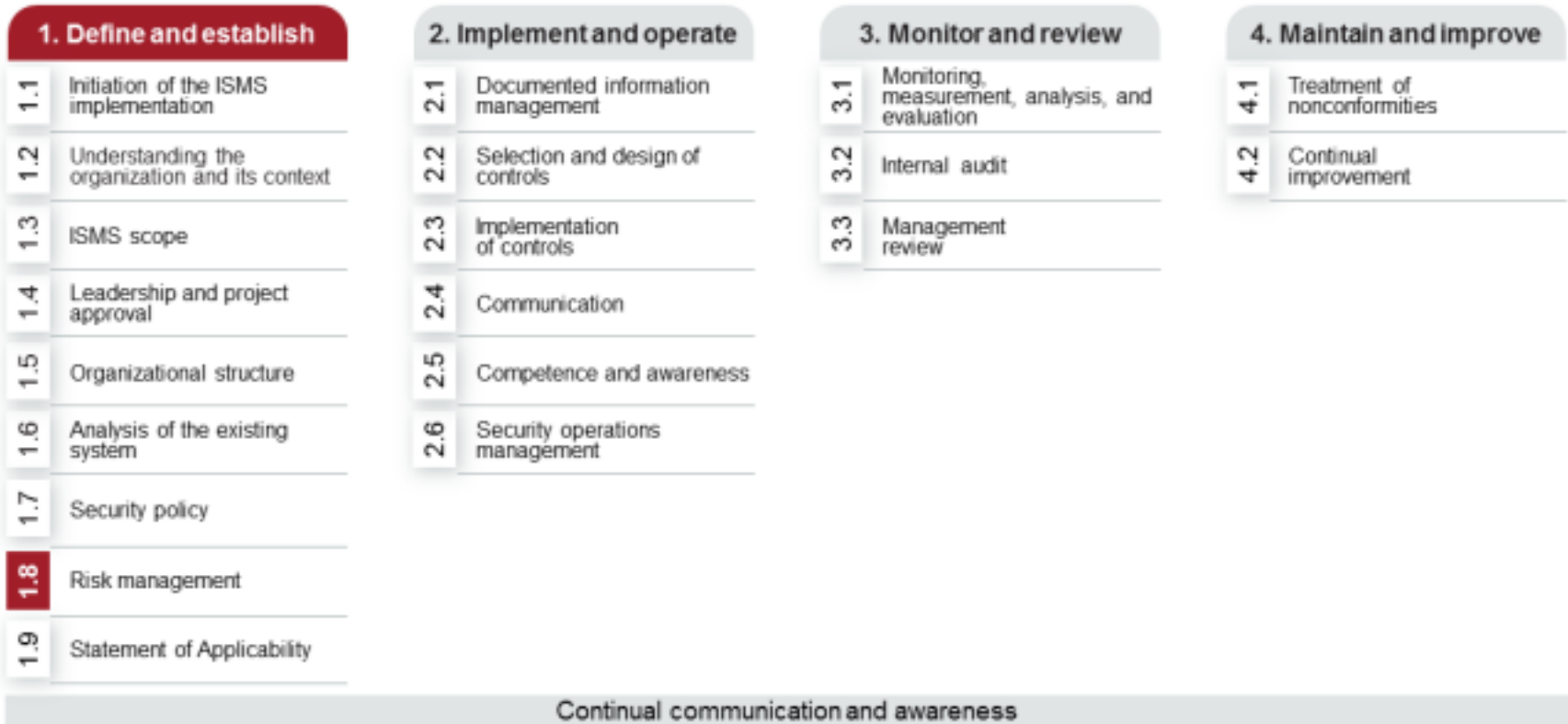
A. The ISMS coordinator
B. The information security manager
C. The top management

Section 12

Risk management

- ISO 31000
- ISO/IEC 27005
- Context establishment
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Communication and consultation
- Recording and reporting
- Monitoring and review

1.8 Risk Management



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 6.1.1

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) *ensure the information security management system can achieve its intended outcome(s);*

b) *prevent, or reduce, undesired effects;*

c) *achieve continual improvement.*

The organization shall plan:

d) *actions to address these risks and opportunities; and*

e) *how to*

   1) *integrate and implement the actions into its information security management system processes; and*

   2) *evaluate the effectiveness of these actions.*

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 6.1.3

The organization shall define and apply an information security risk treatment process to:

a) *select appropriate information security risk treatment options, taking account of the risk assessment results;*

b) *determine all controls that are necessary to implement the information security risk treatment option(s) chosen;*

c) *compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;*

d) *produce a Statement of Applicability;*

e) *formulate an information security risk treatment plan; and*

f) *obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.*

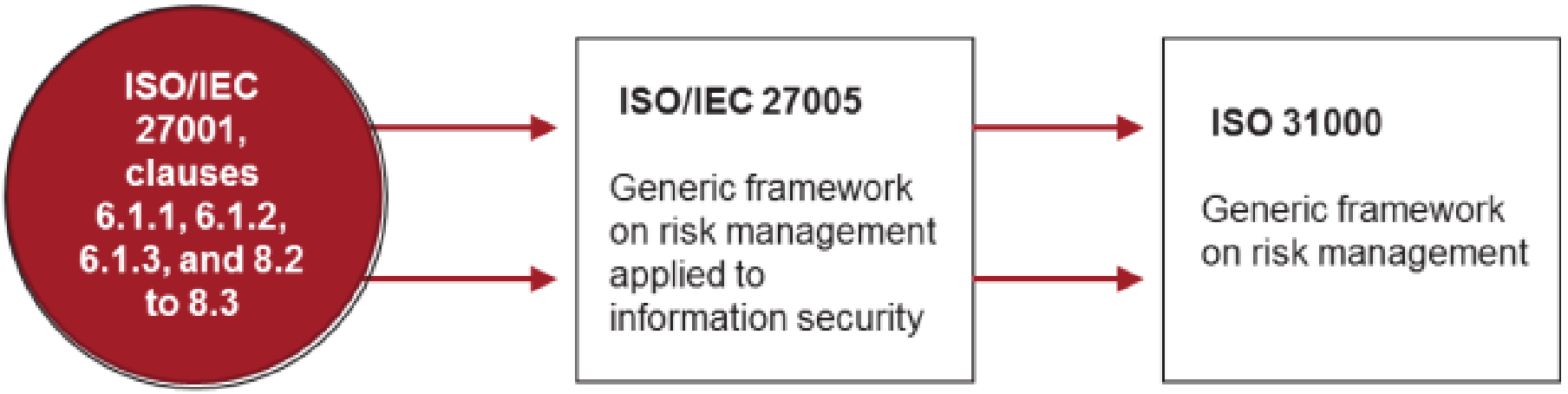
ISO 31000: Risk Management — Guidelines

- ISO 31000 provides a common approach for risk management.
- It can be applicable to any type of risk, regardless of its nature or consequences.
- It is not intended for certification purposes.

ISO/IEC 27005: Guidance on Managing Information Security Risks

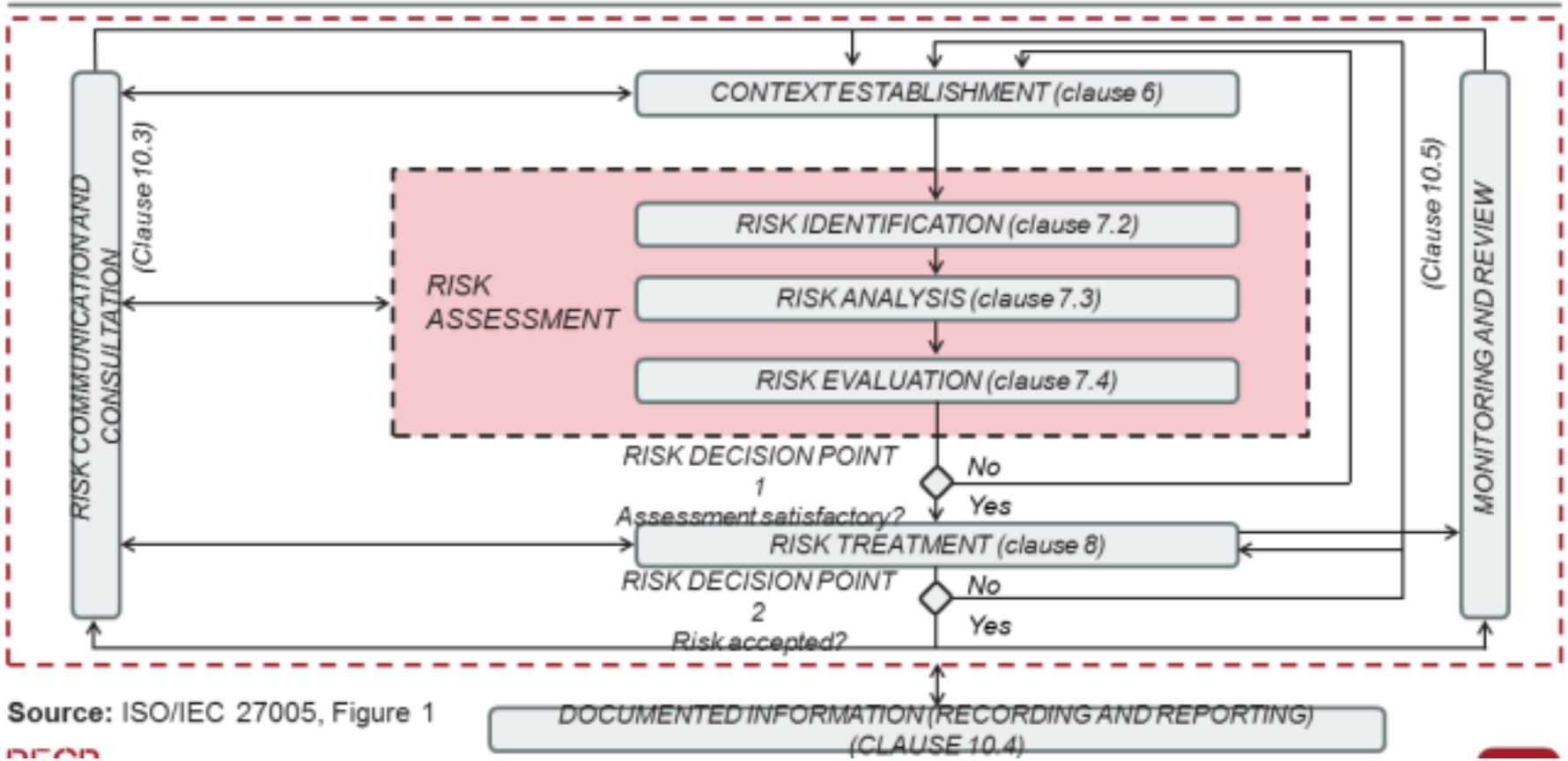
- ISO/IEC 27005 provides guidelines for organizations in meeting the requirements of ISO/IEC 27001 for information security risk management.
- It is applicable to any organization that intends to manage risks that may compromise its information security.
- Organizations cannot obtain certification against this standard.

The Relation between ISO/IEC 27001, ISO/IEC 27005, and ISO 31000



Important note: It is not required to apply the risk management process provided in ISO/IEC 27005 and ISO 31000 to get certified against ISO/IEC 27001.

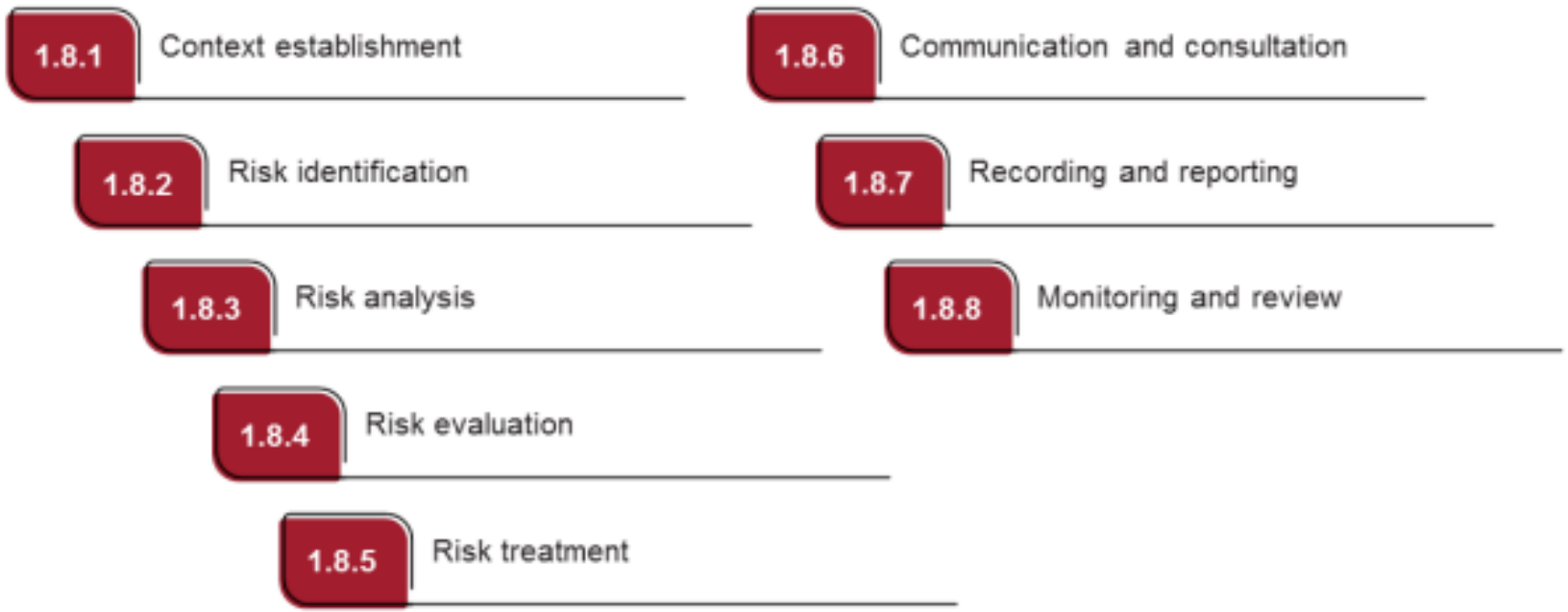
The Risk Management Process



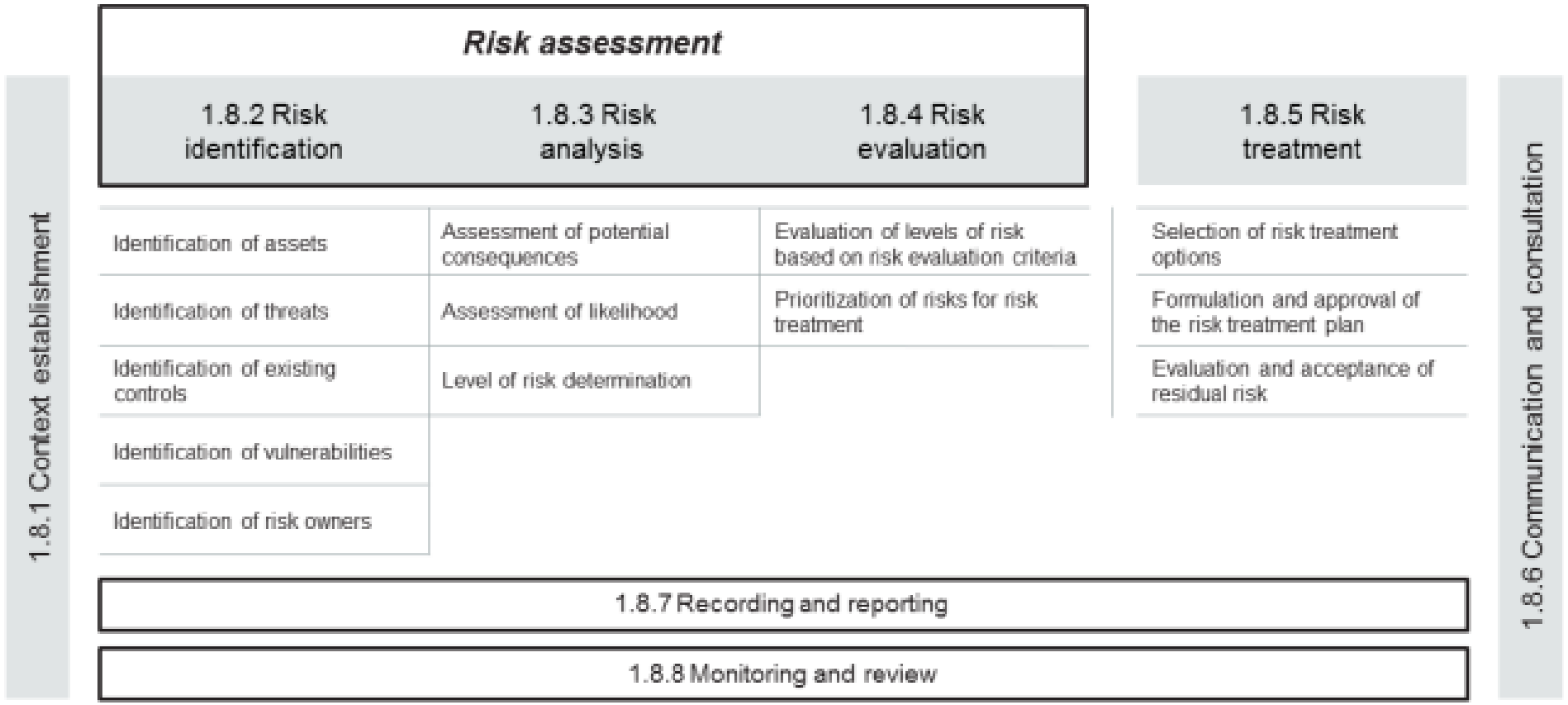
Source: ISO/IEC 27005, Figure 1

1.8 Risk Management

List of activities



PECB Risk Management Process



1.8.1 Context Establishment

ISO/TR 31004, clause 3.3.3.1

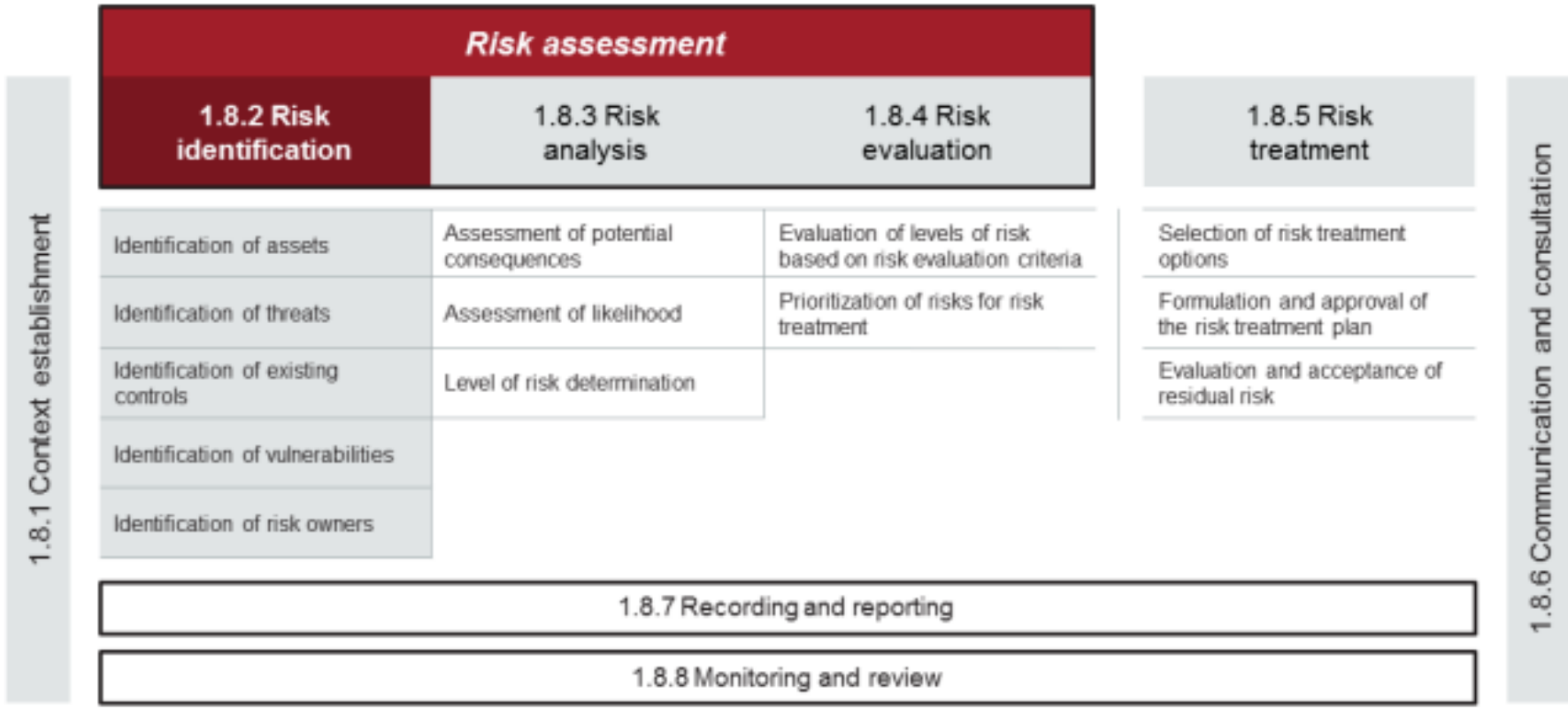
Existing approaches to risk management in the current organization should be evaluated, including context and culture.

a) *It is important to consider any legal, regulatory or customer obligations and certification requirements that arise from any management systems and standards that the organization has chosen to adopt. The purpose of this step is to permit careful tailoring of the design of the risk management framework and the implementation plan itself, and to permit alignment with the structure, culture and general system of management of the organization.*

b) *It is important to consider both the process used to manage risks and the aspects of the existing risk management framework that enable this process to be applied.*

c) *Appropriate risk criteria should be established. Risk criteria need to be consistent with the objectives of the organization and aligned with its risk attitude. If the objectives change, the risk criteria need to be adjusted accordingly. It is important for effective risk management that the risk criteria are developed to reflect the organization's risk attitude and objectives.*

1.8.2 Risk Identification



Approaches for Risk Identification

ISO/IEC 27005, clause 7.2.1

There are two approaches commonly used to perform risk identification.

a)

Event-based approach: identify strategic scenarios through a consideration of risk sources, and how they use or impact interested parties to reach those risk's desired objective.

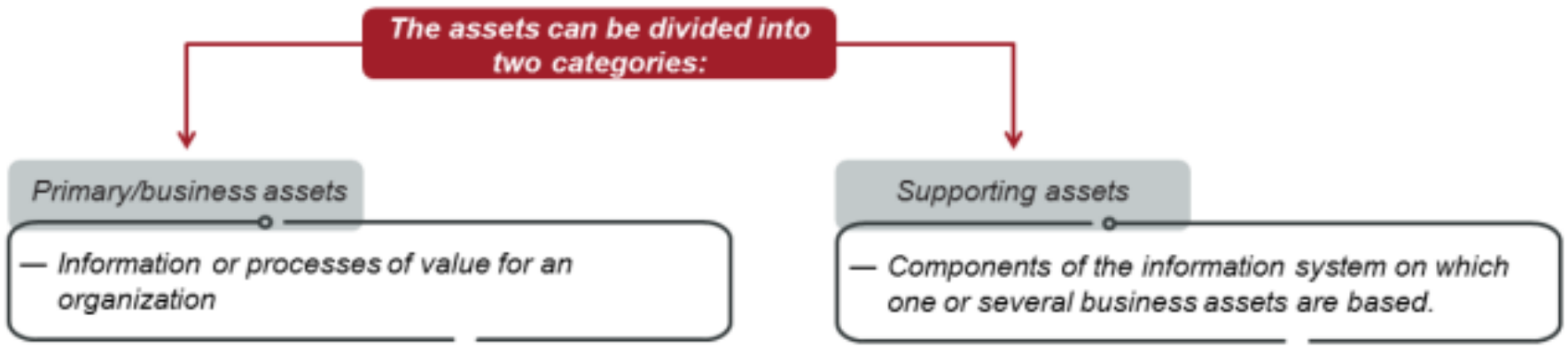
b)

Asset-based approach: identify operational scenarios, which are detailed in terms of assets, threats and vulnerabilities.

Identification of Assets

ISO/IEC 27005, clause 7.2.1 and Annex A.2.2

An asset is anything that has value to the organization and therefore requires protection. Assets should be identified, taking into account that an information system consists of activities, processes and information to be protected. The assets can be identified as the primary and the supporting assets according to their type and priority, highlighting their dependencies, as well as their interactions with their risk sources and the organization's interested parties.



Identification of Primary Assets

Information assets to be considered:

- Vital assets that enable the achievement of the organization's mission
- Assets that contain information which has economic, administrative, or legal value for the organization
- Assets subject to costs associated with collection, acquisition, or storage

Examples of information assets that can be frequently identified as important to the organization include:

- Employee files
- Customer lists
- Organization's strategic plan
- Network setup
- Patents
- Accounting data

Identification of Supporting Assets

Categories

Category	Definition	Examples
Hardware	All the physical elements that support processes	Server, laptop, printer, disk drive, etc.
Software	All the programs that contribute to data processing	Operating system, word processing software , accounting software, etc.
Networks	All telecommunications devices used to interconnect several physically remote computers or elements of an information system	Router, firewall, network cable, switch, bridge, etc.
Personnel	All people involved in the information system	Owner, user, developer, trustee, client, decision-maker, etc.
Sites	Physical places where operations take place	Desktop, server room, staff residence, secure area, air conditioning system, etc.
Organizational structure	Organizational framework, assigned to perform the activities	Headquarters, division, department, project teams, subcontractors, suppliers, etc.

Identification of Threats

ISO/IEC 27005, clause 7.2.1

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

Identification of threats enables organizations to make better decisions related to risk treatment options and activities.

The list of threats is not exhaustive. New threats may appear instantaneously due to trends in technology and the evolving capabilities of threat agents.

Identification of Existing Controls

- To ensure the identification of existing and planned security controls, a comparison against the set of controls established in Annex A of ISO/IEC 27001 can be performed. This helps establishing the existing status in relation to information security best practices.
- The identification of existing security controls should be made to avoid unnecessary work or costs, e.g., the duplication of controls or the implementation of unnecessary ones.
- Moreover, while identifying the existing security controls, an analysis of these should be conducted to ensure that these controls are working properly. Management reviews, dashboards, and audit reports can also provide information on the effectiveness of existing security controls.

Identification of Vulnerabilities

ISO/IEC 27005, Annex A.2.5.3

Proactive methods such as information system testing can be used to identify vulnerabilities depending on the criticality of the Information and Communications Technology (ICT) system and available resources (e.g. allocated funds, available technology, persons with the expertise to conduct the test).

Test methods include:

- *automated vulnerability scanning tool;*
- *security testing and evaluation;*
- *penetration testing;*
- *code review.*

Identification of Risk Owners

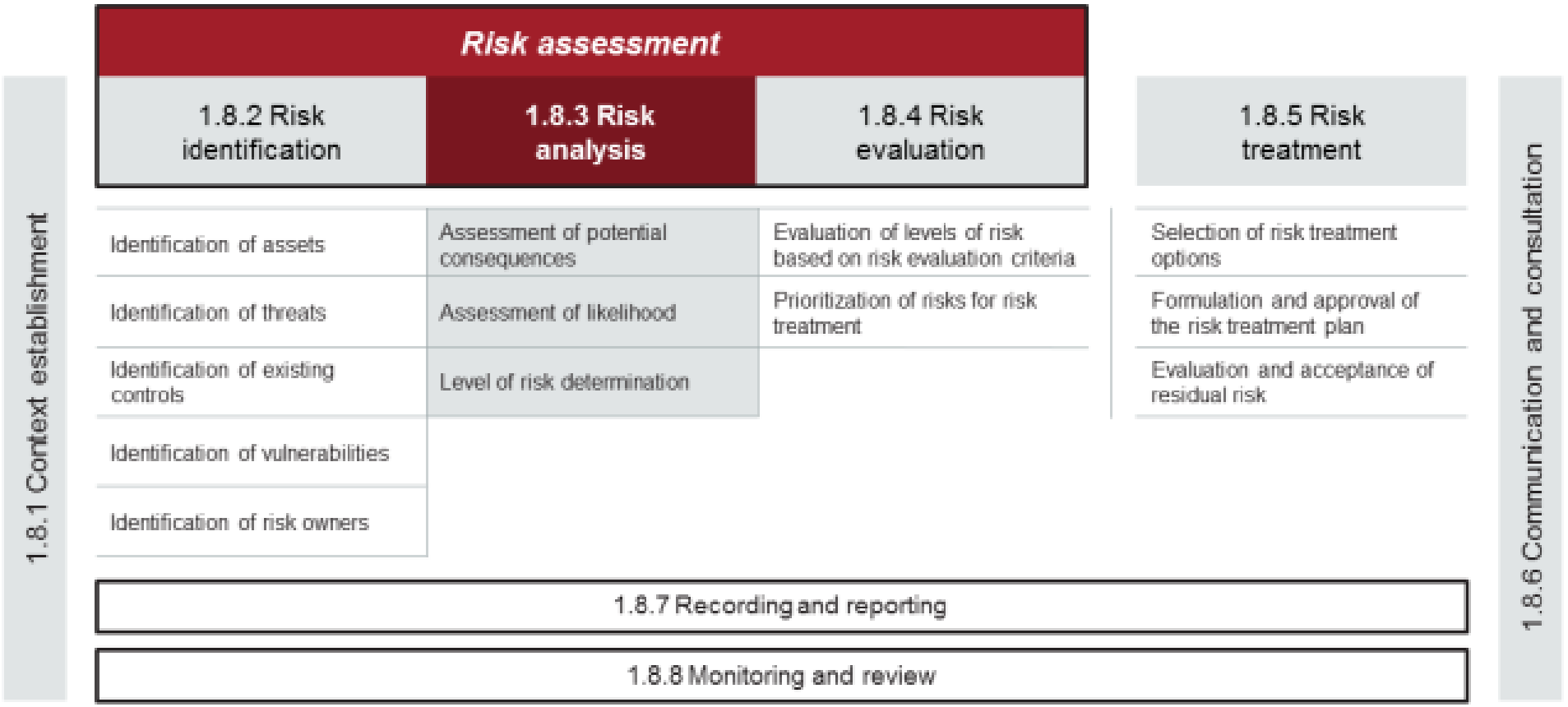
ISO/IEC 27005, clause 7.2.2

Top management, the security committee, process owners, functional owners, department managers and asset owners can be the risk owners.

An organization should use the organizational risk assessment process (if established) regarding identifying risk owners, otherwise it should define criteria for identifying risk owners. Such criteria should take into consideration that risk owners:

- *are accountable and have the authority for managing the risks they own, i.e. they should have a position in the organization that allows them to actually exercise this authority;*
- *understand the issues at hand, and are in a position to make informed decisions (e.g. regarding how to treat the risks).*

1.8.3 Risk Analysis



Assessment of Potential Consequences

ISO/IEC 27005, clause 7.3.2

- *Failure to adequately preserve the security of information can lead to loss of its confidentiality, integrity or availability. Loss of confidentiality, integrity or availability can have further consequences for the organization and its objectives. Consequence analysis can be performed bottom up from the information security consequences by considering what can happen if there is a loss of confidentiality, integrity or availability of the information in question. Typically, the risk owner can estimate the consequence if the event occurs.*
- *The following elements should be taken into consideration:*
  - *— estimation (or measure based on experience) of the losses (time or data) due to the event as result of interrupting or disturbing operations;*
  - *— estimation/perception of severity of the consequence (e.g. expressed in money);*
  - *— recovery costs depending on whether recovery can be done internally (by the risk owner team), or there is a need to call an external entity.*

Example of a Consequence Scale

ISO/IEC 27005, Table A.1

Consequences	Description
5 - Catastrophic	***Sector or regulatory consequences beyond the organization*** *Substantially impacted sector ecosystem(s), with consequences that can be long lasting.* *And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance.* *And/or: critical consequences on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.).*
4 - Critical	***Disastrous consequences for the organization*** *Incapacity for the organization to ensure all or a portion of its activity, with possible serious consequences on the safety of persons and property. The organization will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences.*
3 - Serious	***Substantial consequences for the organization*** *High degradation in the performance of the activity, with possible significant consequences on the safety of persons and property. The organization will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact.*
2 - Significant	***Significant but limited consequences for the organization*** *Degradation in the performance of the activity with no consequences on the safety of persons and property. The organization will overcome the situation despite a few difficulties (operation in degraded mode).*
1 - Minor	***Negligible consequences for the organization*** *No consequences on operations or the performance of the activity or on the safety of persons and property. The organization will overcome the situation without too much difficulty (margins will be consumed).*

Exercise 2: Identification of threats and vulnerabilities, and assessment of consequences

Determine the threats and vulnerabilities associated with the following scenarios and indicate the potential consequences if the identified vulnerabilities are exploited by the identified threats. Then, indicate if the consequences would affect the confidentiality, integrity, or availability of the company's information.

1. Internal audit results have disclosed that the user credentials of a former employee were still being used.
2. An employee made a wrong input value into the command line interface of the development server, bringing down the entire server.
3. The beta version of the application was lost when an array of hard-disks installed in developer machines were proven to be faulty and failed.

Complete the risk matrix and prepare to discuss your answers.

Risk scenarios	Threat	Vulnerability	Consequences	C	I	A
1. Internal audit results have disclosed that the user credentials of a former employee were still being used.		• Access to the blockchain data given to many people • Weak authentication system • System accessible via the internet • No review of access control rights • Data not encrypted				
1. An employee made a wrong input value into the command line interface of the development server, bringing down the entire server.		• Lack of control when entering data into the development server • Lack of a validation process				
1. The beta version of the application was lost when an array of hard-disks installed in developer machines were proven to be faulty and failed.		Lack of an automated backup process for accounting data				

- Employee incompetence
- Former employee Hacker
- Employees who do not follow internal procedures for backup

- Disclosure of sensitive data Loss of confidential data to a competitor
- Loss of data
- Corruption of the development database

Assessment of Likelihood

ISO/IEC 27005, clause 7.3.3

- *After identifying the risk scenarios, it is necessary to analyse the likelihood of each scenario and consequence occurring, using qualitative or quantitative analysis techniques. Assessing the likelihood is not always easy and should be expressed in different ways. This should take into account how often the risk sources occur or how easily some of them (e.g. vulnerabilities) can be exploited, considering:*
  - *experience and applicable statistics for risk source likelihood;*
  - *for deliberate risk sources: the degree of motivation [e.g. the viability (cost/benefit) of the attack] and capabilities (e.g. the level of the skill of possible attackers), which change over time, resources available to possible attackers, and influences on possible attackers such as serious crime, terrorist organizations or foreign intelligence, as well as the perception of attractiveness and vulnerability of information for a possible attacker;*
  - *for accidental risk sources: geographical factors (e.g. proximity to dangerous facilities or activities), the possibility of natural disasters such as extreme weather, volcanic activity, earthquakes, flooding, tsunami and factors that can influence human errors and equipment malfunction;*
  - *known weaknesses and any compensating controls, both individually and in aggregation;*
  - *existing controls and how effectively they reduce known weaknesses.*

Example of a Qualitative Likelihood Scale

Level	Qualitative scale	Likelihood
0	Very rare	Less than once every 50 years
1	Rare	Once every 10 years (on average)
2	Possible	Once every three years (on average)
3	Very possible	Once per year (on average)
4	Likely	Several times a year
5	Almost common	Several times a month
6	Common	Several times a week
7	Very common	Several times a day

Example of a Quantitative Likelihood Scale

1. Last year, 730 incidents related to password reset were reported in the organization.
2. 730 incidents/365 days = Two defects/day
3. The likelihood of the incident scenario related to password reset in this organization is:

Two incidents a day

Level of Risk Determination

ISO/IEC 27005, clause 7.3.4

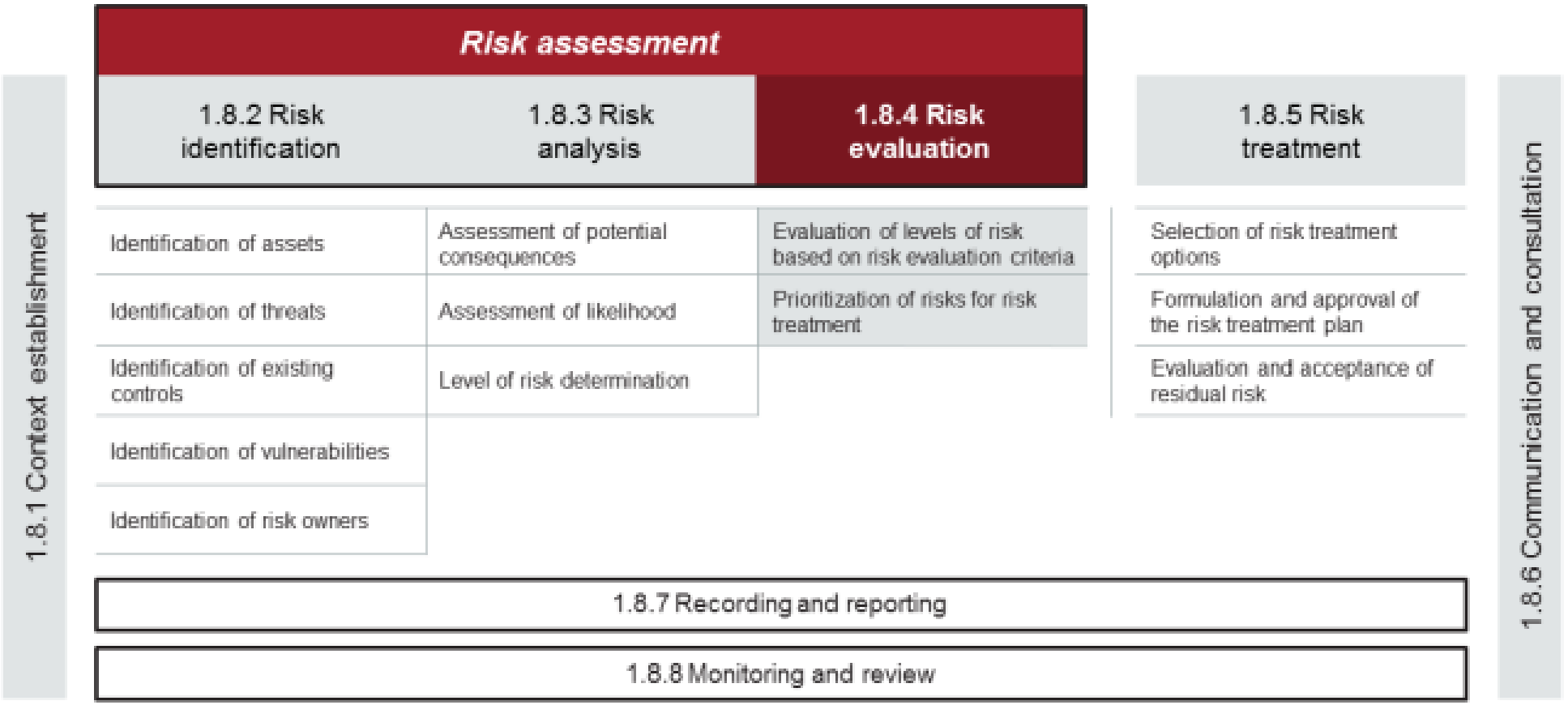
- *The level of risk can be determined in many possible ways.*
- *It is commonly determined as a combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios.*
- *Alternative calculations can include an asset value as well as likelihood and consequence.*
- *In addition, the calculation is not necessarily linear, e.g. it can be likelihood squared combined with consequence.*
- *In any case the level of risk should be determined using the criteria established as described in 6.4.3.4.*

Example of a Qualitative Approach for Level of Risk Determination

ISO/IEC 27005, Table A.3

Likelihood	***Consequence***				
	Catastrophic	***Critical***	***Serious***	***Significant***	***Minor***
Almost certain	*Very high*	*Very high*	*High*	*High*	*Medium*
Very likely	*Very high*	*High*	*High*	*Medium*	*Low*
Likely	*High*	*High*	*Medium*	*Low*	*Low*
Rather unlikely	*Medium*	*Medium*	*Low*	*Low*	*Very low*
Unlikely	*Low*	*Low*	*Low*	*Very low*	*Very low*

1.8.4 Risk Evaluation



Evaluation of Levels of Risk Based on Risk Evaluation Criteria

ISO 31000, clause 6.4.4

The purpose of risk evaluation is to support decisions.

Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.

Prioritization of Risks for Risk Treatment

The organization needs to prioritize risks in order to focus the treatment efforts into risks that have both higher impact and likelihood.

1. **What does ISO/IEC 27005 provide?**
    A. Requirements for information security risk management
    B. Practical methods for the management of all risks
    C. Guidelines for information security risk management
2. **What criteria should be considered when selecting a risk assessment methodology?**
    A. New technologies
    B. Personnel competence and training
    C. Risk treatment plan
3. **What type of asset is information categorized as?**
    A. Supporting asset
    B. Secondary asset
    C. Primary asset
4. **Which phase of risk assessment aims to find, recognize, and describe risks?**
    A. Risk identification
    B. Risk evaluation
    C. Risk analysis

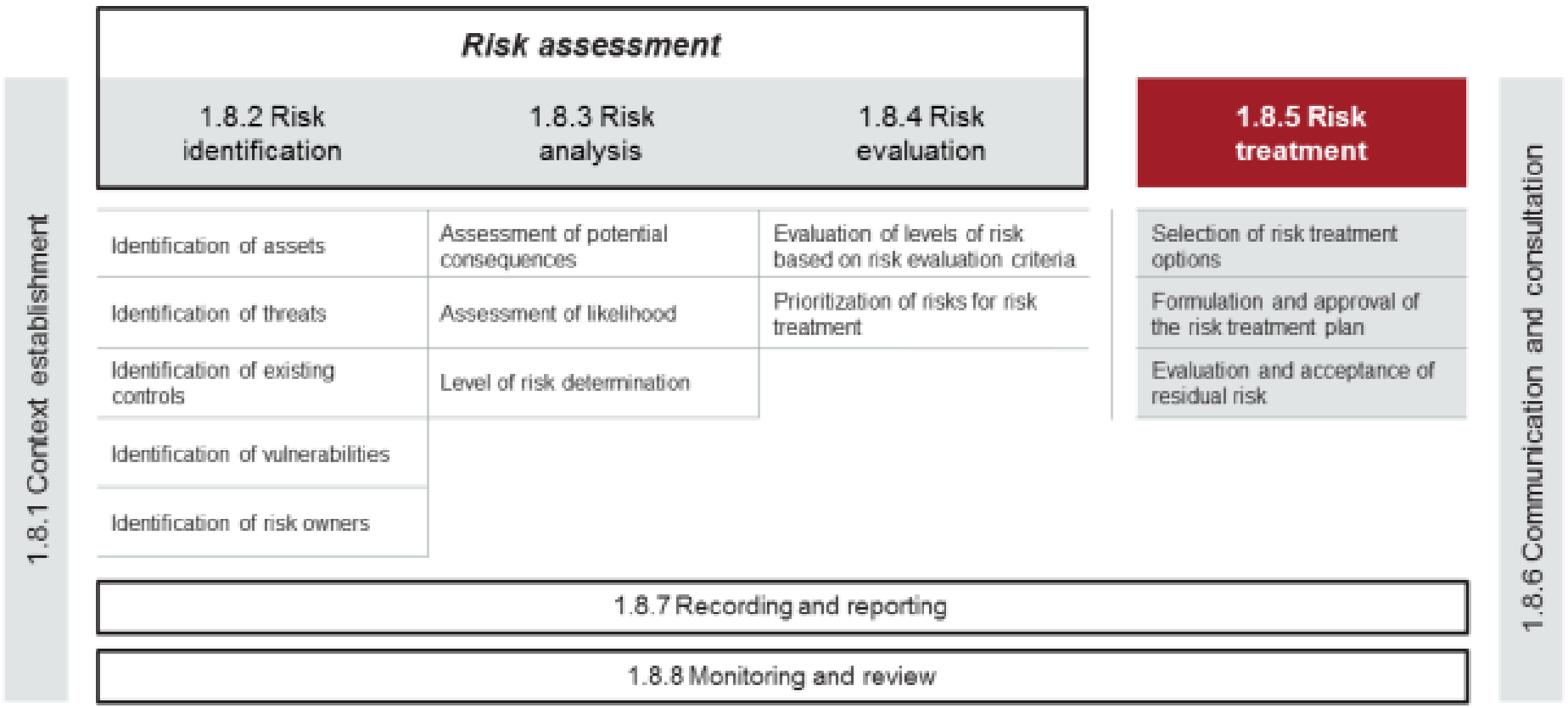
5.Which phase of risk management takes into consideration the source, likelihood, and consequences of risk?

A. Risk treatment
B. Risk analysis
C. Risk evaluation

6._____ is the process of comparing the results of risk analysis with the risk criteria to determine whether the risk is acceptable.

A. Risk treatment
B. Risk evaluation
C. Risk acceptance

1.8.5 Risk Treatment

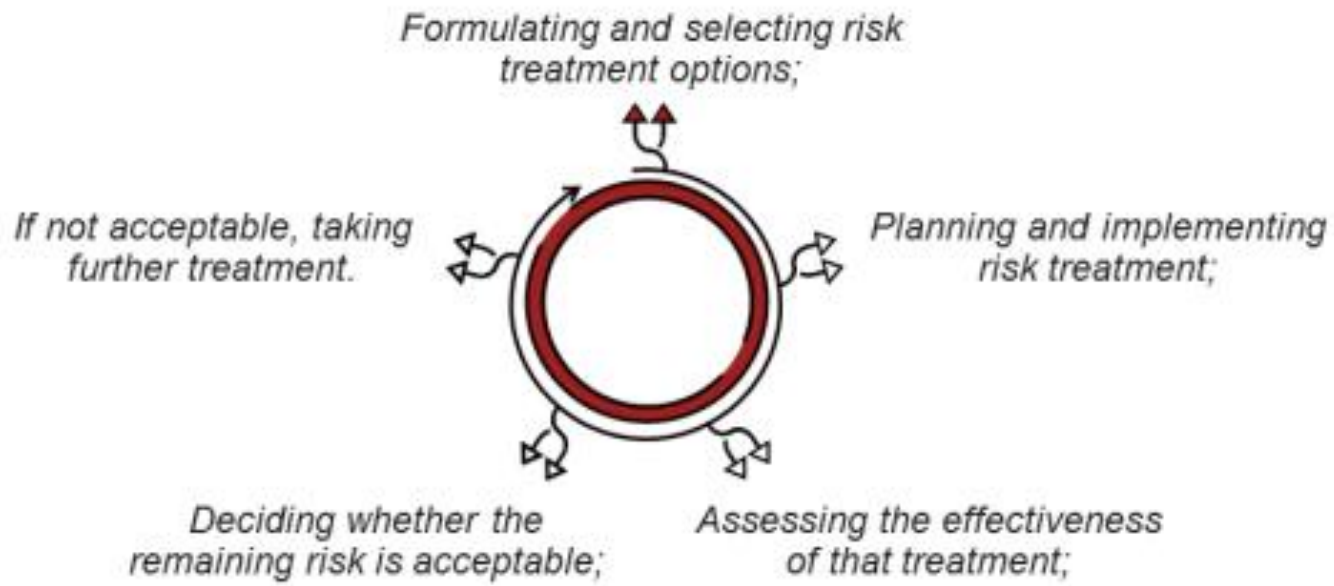


Risk Treatment

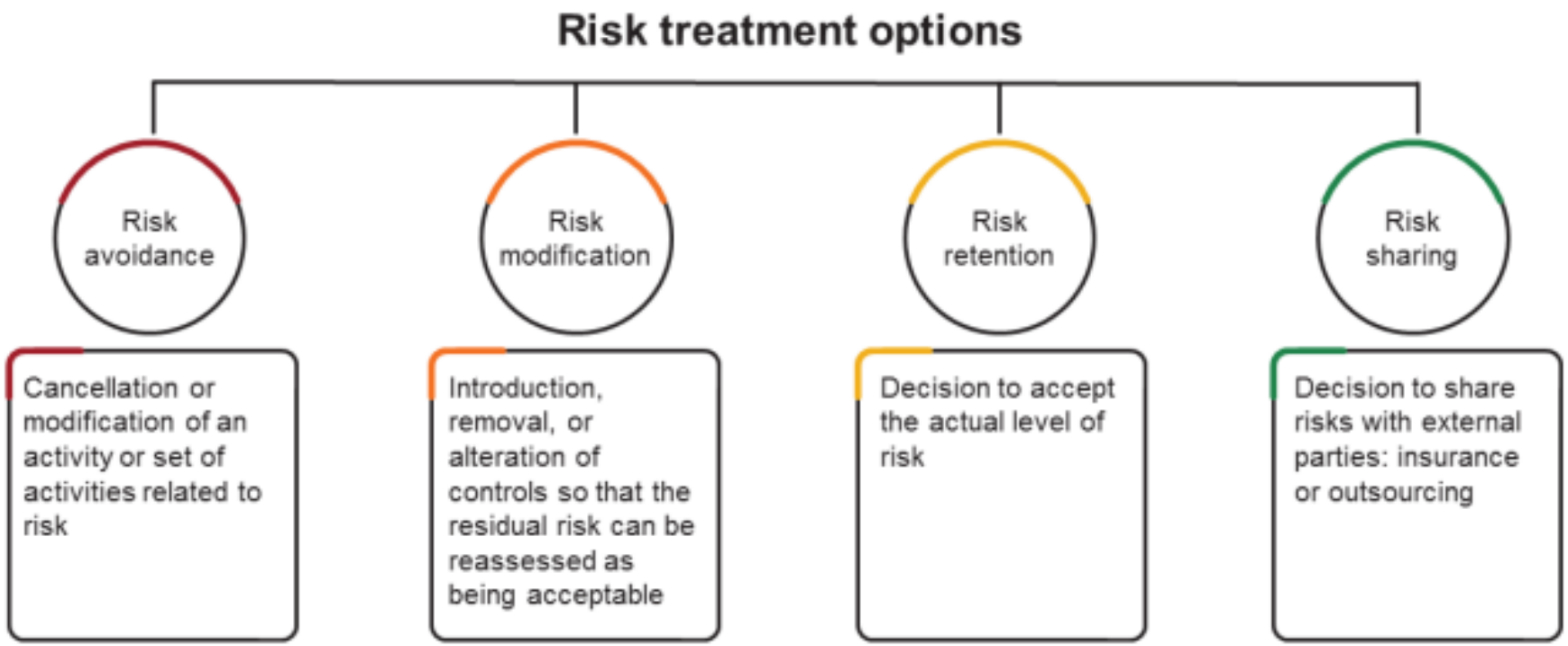
ISO 31000, clause 6.5.1

The purpose of risk treatment is to select and implement options for addressing risk.

Risk treatment involves an iterative process of:



Selection of Risk Treatment Options



Formulation and Approval of the Risk Treatment Plan

ISO/IEC 27005, clause 8.6.1

A risk treatment plan is a plan to modify risk such that it meets the organization's risk acceptance criteria.

- Once the organization chooses the relevant risk treatment option, it must plan and implement it accordingly.
- The activities to be taken to implement the risk treatment option should be classified by order of priority.
- The organization should allocate the necessary resources to ensure the effective implementation of the chosen risk treatment option.
- The risk treatment plan should be approved by the risk owners.

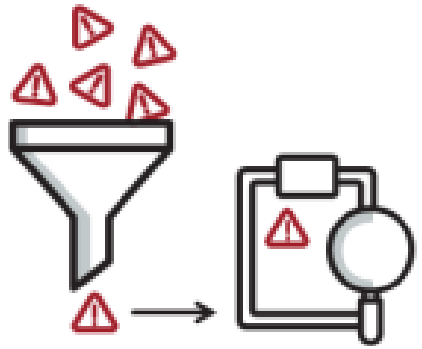
Example of a Risk Treatment Plan

Risk (vulnerability/threat):	Unauthorized users can log on via the extranet to SharePoint and search for files of the organization with the requested ID.
Risk level:	Six
Priority:	High
Treatment option:	Avoid
Measuring details:	Make SharePoint inaccessible
Resources required:	10 hours to reconfigure and test the system
Responsible	David Smith, SharePoint administrator and John McGee, Firewall administrator
Start and end date:	2019-08-20 to 2019-08-21
Maintenance required/comments:	Conduct periodic security reviews of the system to ensure that adequate security is provided for SharePoint

Evaluation of Residual Risk

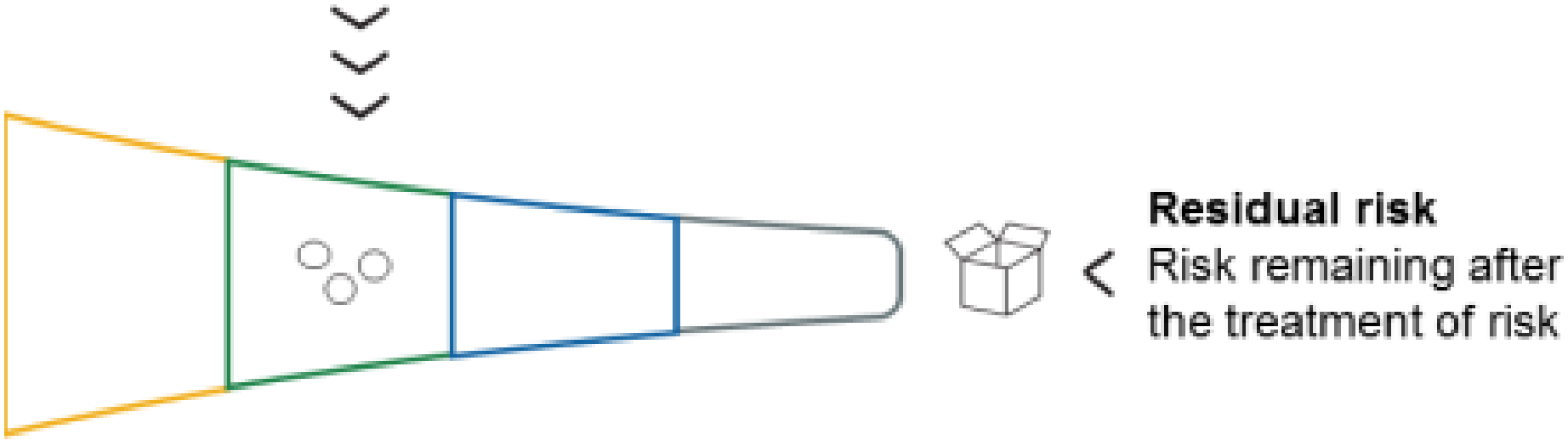
ISO 31000, clause 6.5.2

- *Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment.*
- *The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.*



Treated risk

Risk treated with controls



Residual risk

Risk remaining after the treatment of risk

1.8.6 Communication and Consultation

ISO/IEC 27005, clause 10.3

The communication and consultation activity aims to achieve agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners and other relevant interested parties. The information includes, but is not limited to, the existence, nature, form, likelihood, consequence, significance, treatment and acceptance of risks.

Risk communication should be carried out in order to:

- *provide assurance of the outcome of the organization's risk management;*
- *collect risk information;*
- *share the results from the risk assessment and present the risk treatment plan;*
- *avoid or reduce both the occurrence and consequence of information security breaches due to the lack of mutual understanding among risk owners and interested parties;*
- *support risk owners;*
- *obtain new information security knowledge;*
- *coordinate with other parties and plan responses to reduce the consequences of any incident;*
- *give a sense of responsibility to risk owners and other parties with a legitimate interest at risk;*
- *improve awareness.*

1.8.7 Recording and Reporting

ISO 31000, clause 6.7

- *The risk management process and its outcomes should be documented and reported through appropriate mechanisms.*
- *Recording and reporting aims to:*
  - *communicate risk management activities and outcomes across the organization;*
  - *provide information for decision-making;*
  - *improve risk management activities;*
  - *assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.*
- *Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to: their use, information sensitivity and the external and internal context.*

1.8.8 Monitoring and Review

ISO/IEC 27005, clause 10.5.1

- *The organization's monitoring process should encompass all aspects of the risk assessment and risk treatment processes for the purposes of:*
  - *a) ensuring that the risk treatments are effective, efficient and economical in both design and operation;*
  - *b) obtaining information to improve future risk assessments;*
  - *c) analysing and learning lessons from incidents (including near misses), changes, trends, successes and failures;*
  - *d) detecting changes in the internal and external context, including changes to risk criteria and the risks themselves, which can require revision of risk treatments and priorities;*
  - *e) identifying emerging risks.*

1. **Which phase of risk management is used to modify risk?**
    A. Risk evaluation
    B. Risk identification
    C. Risk treatment
2. **Upon an analysis of risk, an organization found out that around 0.4% of its electronic transactions are fraudulent. The organization has decided to outsource the payment process to an external organization in order to reduce the risk. What risk treatment option is this?**
    A. Risk retention
    B. Risk sharing
    C. Risk modification
3. **The risk that remains after risk treatment is known as:**
    A. Inherent risk
    B. Treated risk
    C. Residual risk
4. **What is the aim of the communication and consultation activity?**
    A. To achieve agreement on how to manage risks
    B. To review and approve risk treatment plans
    C. To determine whether a residual risk falls above or below the threshold

5.An organization has decided to move its information processing facilities to a place where the risk of flooding is low. Which risk treatment option has the organization chosen?

A. Risk avoidance
B. Risk evaluation
C. Risk sharing

6.Which of the following is NOT a risk treatment option?

A. Share the risk
B. Modify the risk
C. Trade the risk

7.Which of the following is an example of risk sharing?

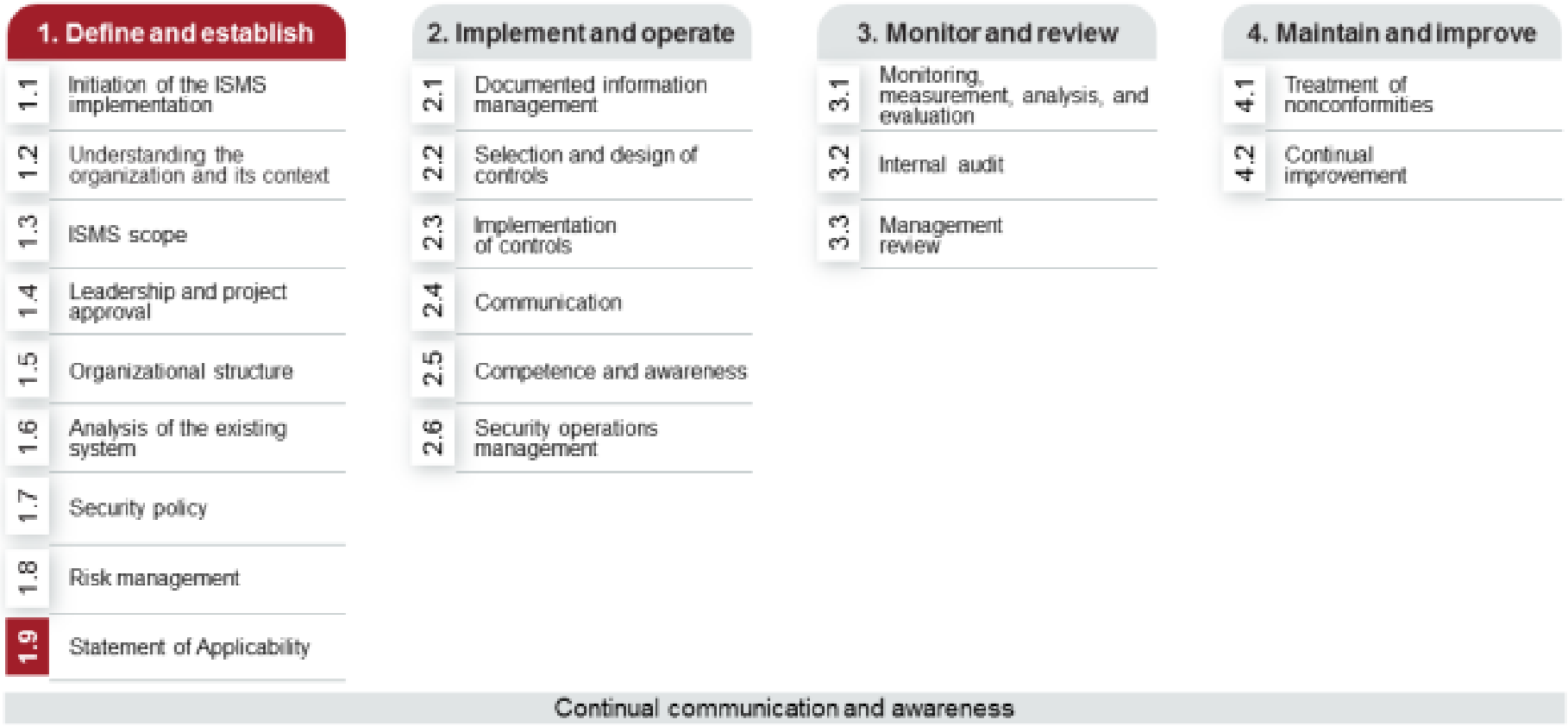
A. Removing the assets from an area at risk
B. Retaining the current risk
C. Distributing risk to another party

Section 13

Statement of Applicability

- Drafting the Statement of Applicability
- Management approval
- Review and selection of the applicable information security controls
- Justification of selected controls
- Justification of excluded controls

1.9 Statement of Applicability



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 6.1.3d

Produce a Statement of Applicability that contains:

- *the necessary controls;*
- *justification for their inclusion;*
- *whether the necessary controls are implemented or not; and*
- *the justification for excluding any of the Annex A controls.*

NOTE

ISO/IEC 27001 does not require that the organization selects its controls only from Annex A.

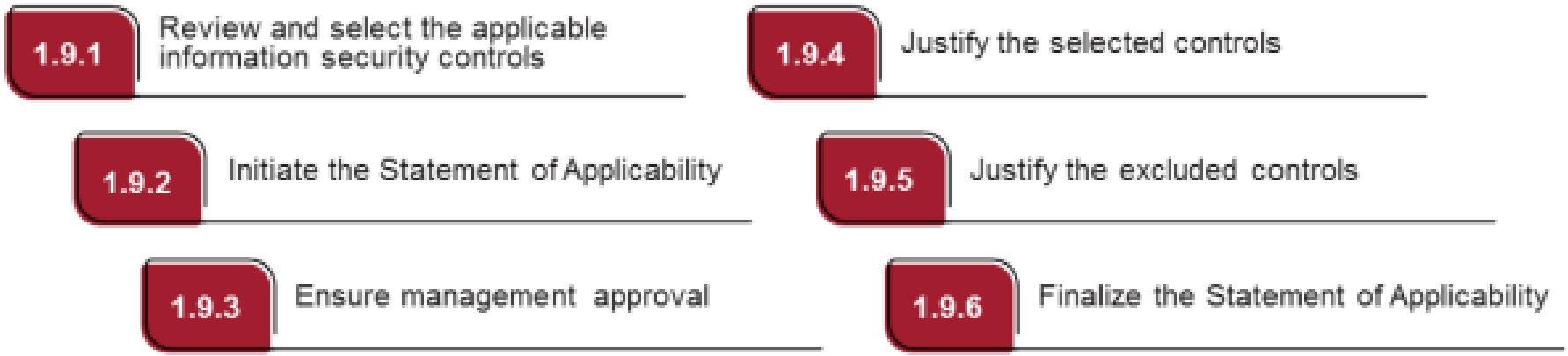
Statement of Applicability

Definition

- A Statement of Applicability (SoA) is a documented statement listing the controls that are relevant and applicable to the organization's information security management system.
- Not only does the SoA contain the organization's justifications for including certain controls of Annex A, it also contains justifications for the exclusion of other controls.

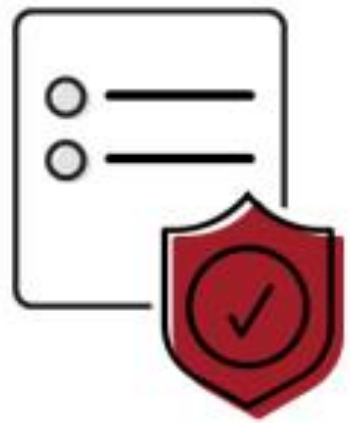
1.9 Statement of Applicability

List of activities



1.9.1 Review and Select the Applicable Information Security Controls

- The organization must review the 93 information security controls in Annex A in order to identify those that are applicable and those that are not applicable to its context.
- Most organizations report to have more than 80 security controls.



1.9.2 Initiate the Statement of Applicability

- The Statement of Applicability is one of the key documents that links risk assessment and risk treatment with the implementation of the ISMS.
- ISO/IEC 27001 does not specify the form of the Statement of Applicability. It requires, however, that it includes a list of information security controls, the justification for inclusions, and actions taken to implement the selected controls.
- It is advisable to state, in the Statement of Applicability, the functions of persons responsible for each control, as well as the list of documents or records related to the control. The SoA model proposed by PECB has the following structure:
  - Information security control
  - Applicability
  - Brief description
  - Justification
  - Documented information
  - Responsibility

1.9.3 Ensure Management Approval

Possible evidence of management authorization:

- Resolution from the Board of Directors or steering committee
- Official letters
- Management review meeting minutes

1.9.4 Justify the Selected Controls

- The organization should justify the selection of each security control included in the ISMS.
- This answers the “Why?” question for each control.

Addressing information security within supplier agreements (ISO/IEC 27001, Annex A 5.20):

Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.

Justification for the selection: Ensuring the security of the organization’s information that is processed by its suppliers

1.9.5 Justify the Excluded Controls

- The organization should justify the exclusion of each security control presented in Annex A of ISO/IEC 27001.
- The reasons for exclusion most often cited are:
  - This would lead to the violation of a legal, statutory, or contractual requirement, e.g., ISO/IEC 27001, Annex A 6.1 *Screening*.
  - No activity related to this control is present in the organization, e.g., ISO/IEC 27001, Annex A 6.7 *Remote working*.

1.9.6 Finalize the Statement of Applicability

Example

Control	Applicable	Description	Justification	Documentation	Responsible
ISO/IEC 27001, Annex A 5.1 *Policies for information security*	Yes	The information security policy, approved by the management, is effective as of December 21, 2018. A copy of this policy was sent to all employees and other relevant interested parties. The official version is available on the intranet.	To provide guidance on information security To ensure that the information security practices comply with business requirements, laws, and regulations	Security-policy-3213PO	Information security manager

Finalize the Statement of Applicability (Cont'd)

Example

Control	Applicable	Description	Justification	Documentation	Responsible
ISO/IEC 27001 Annex A 5.1 *Policies for information security*	Yes	The information security policy is reviewed annually in the management review meeting and the formal resolution is extended for another year. In case of major changes, a review may take place during the year at the request the top management.	Ensure that the information security policy is kept up to date and remains aligned with the objectives of the organization	1. Management-review-procedure-312PR 2. Security-policy-3213PO 3. Management review proceedings 2017	Information security manager
ISO/IEC 27001 Annex A 6.7 *Remote working*	No	----------	Our organization has no activities related to remote working.	N/A	IT manager

1. **Which statement regarding the Statement of Applicability (SoA) is correct?**
   A. SoA is a tool for decision-making support
   B. SoA is a document that is specific to ISO/IEC 27001
   C. SoA is a key process of the ISMS
2. **How does an organization select the security controls of ISO/IEC 27001, Annex A?**
   A. Based on the risk assessment results
   B. Based on the top management's decision
   C. Based on the internal audit report
3. **Why should an organization create a Statement of Applicability?**
   A. To document the justifications for inclusion and exclusion of Annex A controls
   B. To ensure that the ISMS is aligned with the mission of the organization
   C. To ensure compliance with the industry best practices
4. **ISO/IEC 27001 requires that the organization select its security controls only from Annex A.**
   A. True
   B. False
5. **An organization has drafted its Statement of Applicability (SoA) which comprises of the list of applicable and inapplicable information security controls of Annex A along with the justification for the exclusion of the inapplicable controls. Does this SoA comply with the ISO/IEC 27001 requirements?**
   A. Yes, because it has included the list of selected controls from Annex A and the reasoning of their selection
   B. No, because it does not justify the selection of information security controls of Annex A
   C. No, because it does not include the list of any controls from Annex A determined as inapplicable

Scenario-based quiz 2: Sections 8-13

Research Metric is a research development company, highly dependent on the protection of its development and research data and the availability of its IT systems. They have recently decided to implement an information security management system (ISMS) and, as such, the top management assigned the role of the ISMS project manager to Melanie based on her outstanding knowledge and skills in project and information security management. In addition, they decided to include only the key processes in the ISMS scope and stop collecting and processing sensitive information of their customers until the ISMS becomes fully operational.
Since the company had a security policy in place, the ISMS project team decided to adopt it by renaming it to “Information security policy.” Following the conduct of a risk assessment, *Research Metric* prepared a document containing a list of all information security controls deemed applicable to their ISMS.

Answer the following questions by referring to the above-mentioned scenario:

- **In addition to establishing the ISMS project and managing it throughout its operational life, Melanie is responsible for:**

A. Formalizing the ISMS objectives
B. Providing adequate resources for the ISMS implementation
C. Approving the risk acceptance criteria

- **Which ISMS scope boundary has Research Metric defined?**

A. Organizational boundaries
B. Physical boundaries
C. Information systems boundaries

- **Why should the security policy be updated instead of only being renamed to “Information security policy”?**

A. To address the information security risks
B. To provide an overview of information assets
C. To reflect the information security objectives

- **Which risk treatment option has *Research Metric* utilized when it decided to stop collecting and processing sensitive information of their customers until the ISMS was fully operational?**

A. Risk avoidance
B. Risk sharing
C. Risk retention

- ***Research Metric* has prepared a document containing a list of all information security controls deemed applicable to their ISMS. This document is known as:**

A. Statement of Applicability
B. Risk assessment report
C. Information security strategy