Version 7.1

Document number: ISMSLID2V7.1

Schedule of the Day

- Section 8 — Leadership and project approval
- Section 9 — Organizational structure
- Section 10 — Analysis of the existing system
- Section 11 — Information security policy
- Section 12 — Risk management
- Section 13 — Statement of Applicability

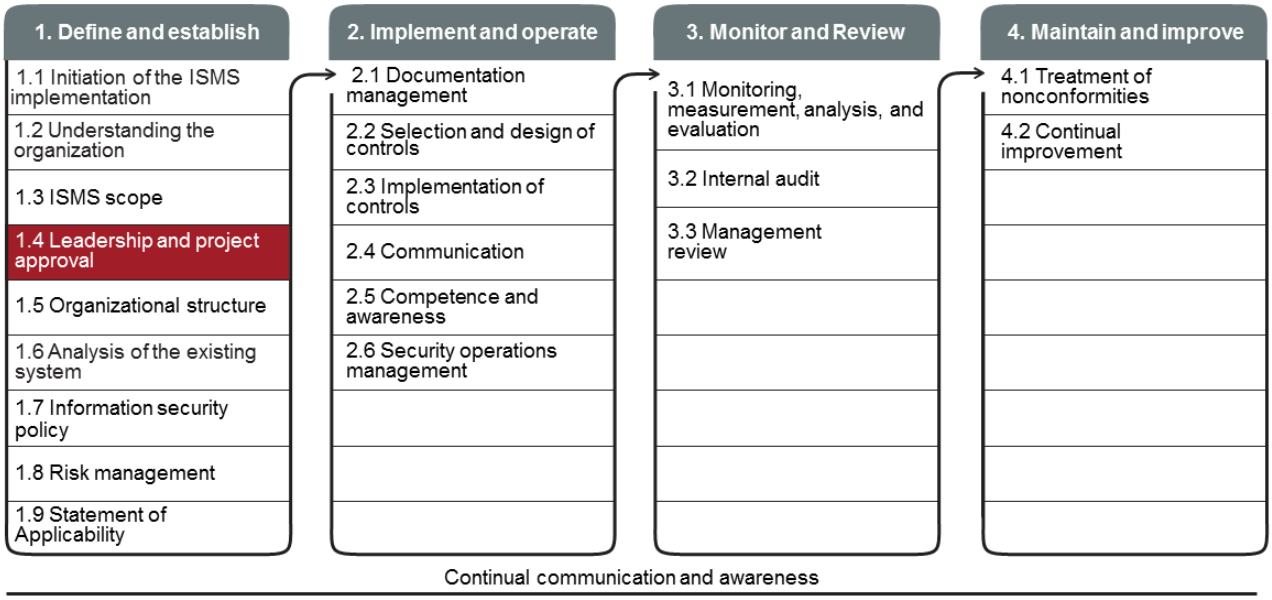
PECB

Learning Objectives of the Day

1. Acquire knowledge on how to create a business case
2. Acquire knowledge on how to create policy models, how to draft information security policies, and how to conduct training and awareness sessions
3. Acquire knowledge on how to establish a risk management process
4. Acquire knowledge on how to define an organizational structure
5. Acquire knowledge on how to review and select the applicable security objectives and controls and how to draft a Statement of Applicability (SoA)

This section provides information that will help the participant gain knowledge on the formalization and approval of the ISMS, which includes the ISMS plan and the project team, requirements for resources, and management approval.

1.4 Leadership and Project 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.

PECB

6

An organization wishing to comply with ISO/IEC 27001 shall at least:

1. Obtain management approval to implement the ISMS
2. Obtain the necessary resources to implement and maintain the ISMS

Leadership and Project Approval

ISO/IEC 27021, clause 5.2

ISO/IEC 27001:2013 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*

PECB

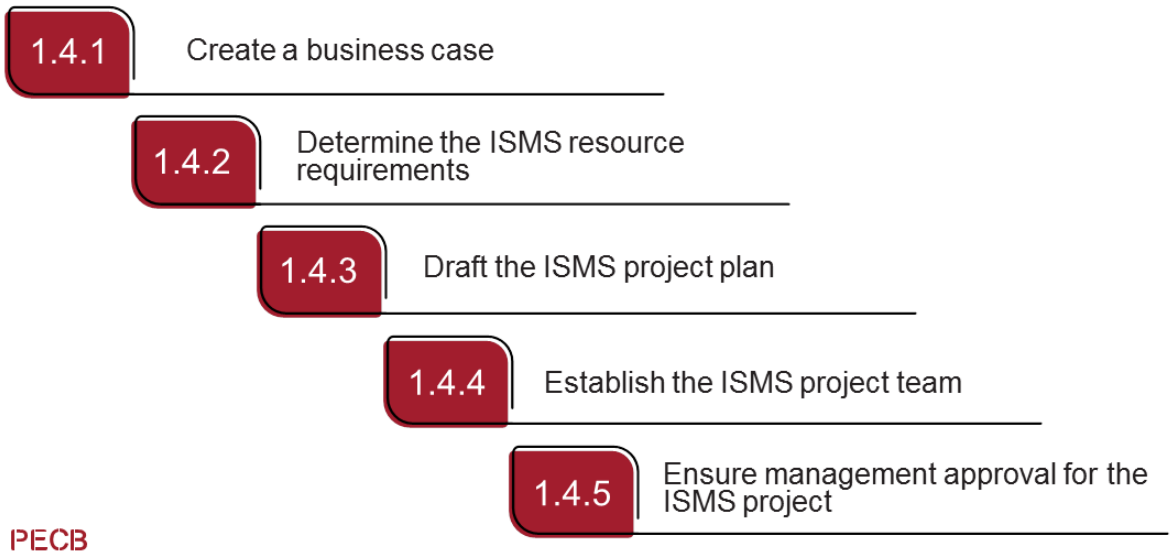
7

Through its leadership and actions, management can create an environment in which all actors are fully involved and in which the management system can operate effectively in synergy with organizational objectives. Management can use the management principles of ISO to define its role, which involves:

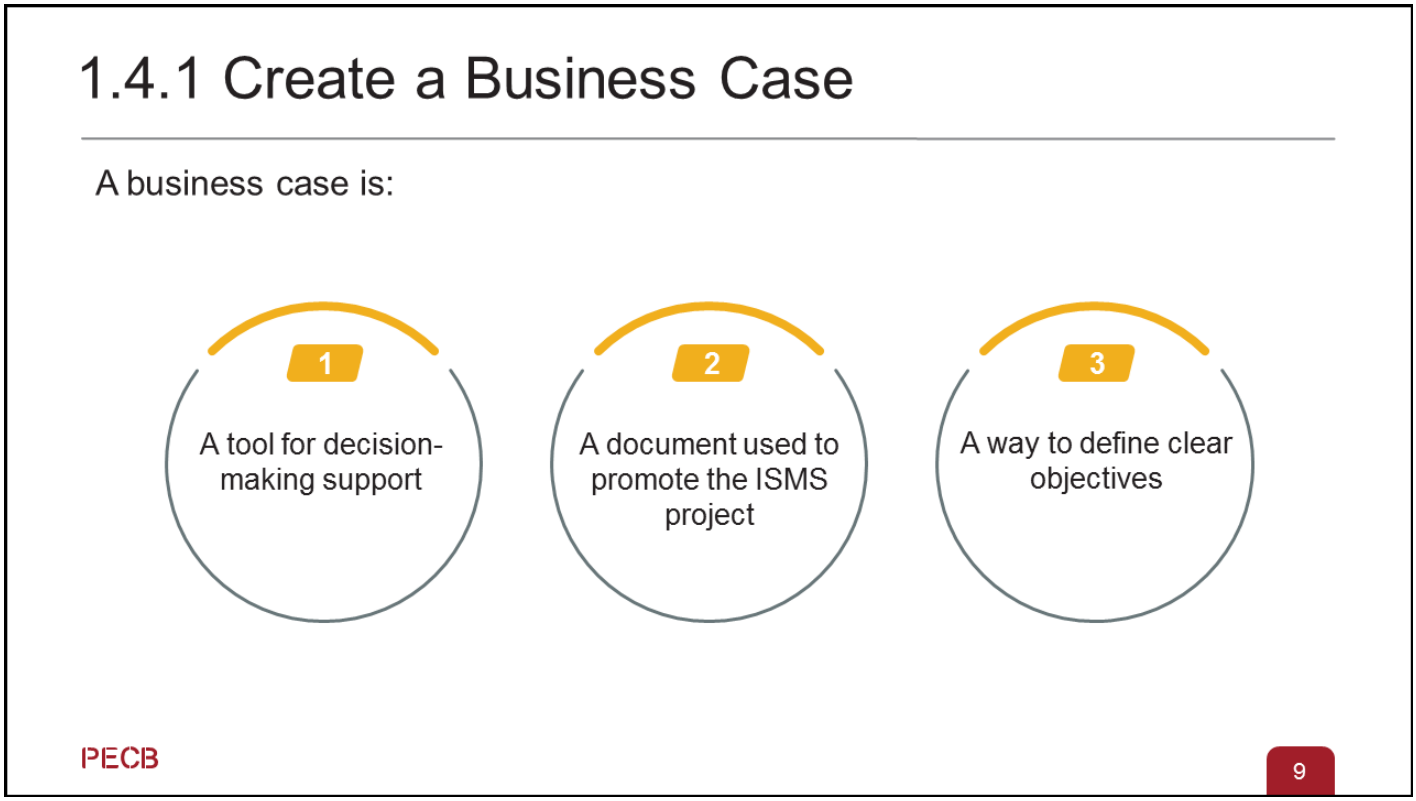
a. Establishing guidelines and the objectives of the organization
b. Promoting policies and objectives at all organizational levels to increase awareness, motivation, and involvement
c. Assuring that the requirements of interested parties (customers, partners, shareholders, legislators, etc.) are a priority at all organizational levels
d. Implementing the appropriate processes and controls to help the compliance of requirements
e. Establishing, implementing, and maintaining an efficient and effective management system
f. Assuring the necessary resources availability
g. Assuring that internal audits are being conducted
h. Establishing management reviews at least once a year
i. Deciding on actions concerning the policy and objectives
j. Deciding on actions to improve the management system

1.4 Leadership and Project Approval

List of activities



PECB



What is a business case?

A business case is a tool that helps planning and decision-making, including decisions regarding the opportunities, choices, and the right time to initiate an action or a sequence of actions. The most common purpose of a business case is to determine the financial consequences of a decision. It should answer the question, “What are the financial consequences if we choose X over Y?”

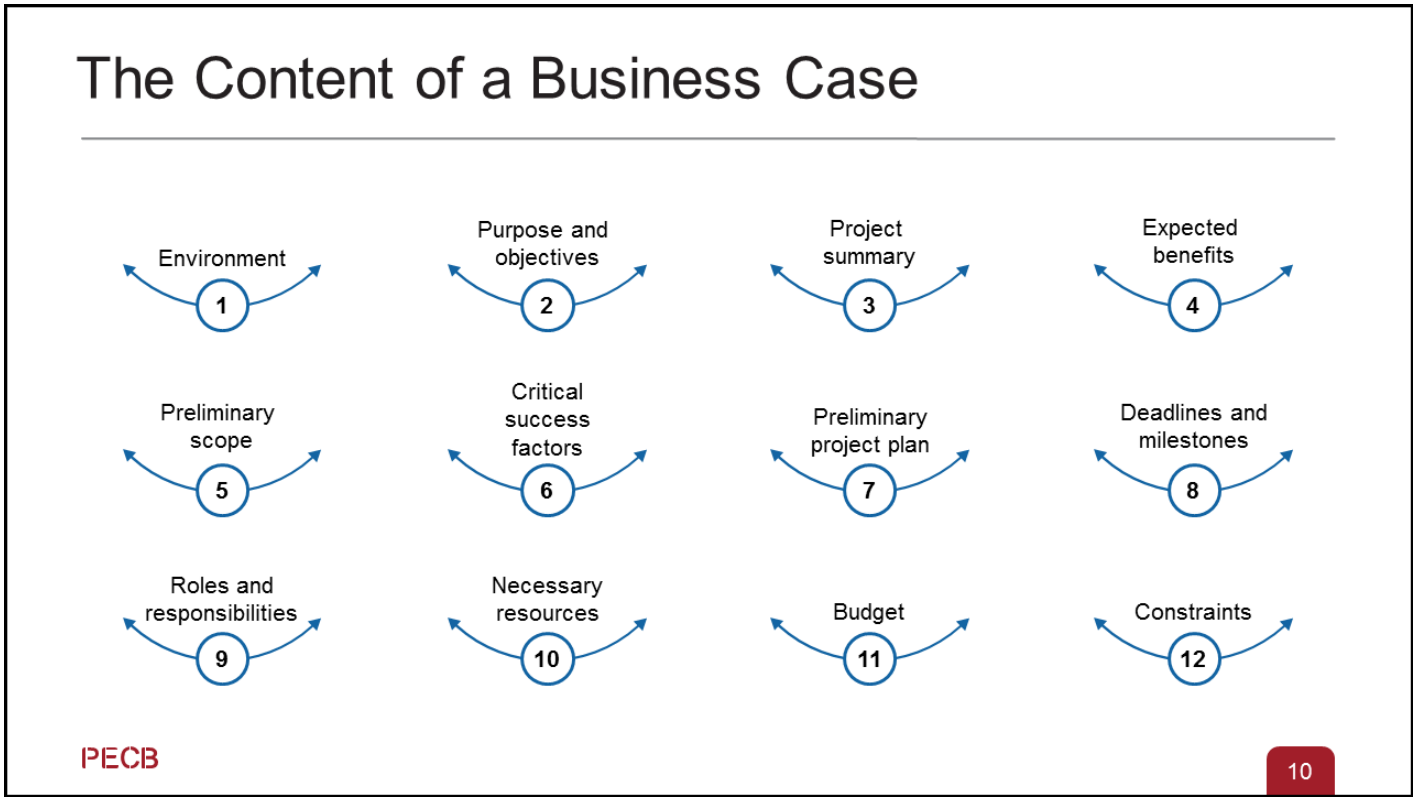
A well-structured business case must indicate what benefits can be expected from a decision on a given period of time. It also includes the methods and the logic used to calculate those benefits. All in all, a business case will be helpful for an organization’s management to have better decisions on the investments of certain resources and achieve positive outcomes.

The business case must describe the overall impact of the implementation in terms easily understood by people who are not specialists in the area. It should address the critical success factors and contingencies. It should also identify significant risks that might occur and cues that would signal any change in the results.

The business case answers questions from interested parties:

- What is the purpose of the project?
- What are the solutions that have been studied?
- Why is this particular solution chosen? What are the risks and constraints?
- How much does it cost? Who is responsible for this project? How to tell if the project is successful?
- How will this project affect my work?

To answer these questions, a business case must have at least five components: the objectives of the project and their alignment with the strategy of the organization, the various options that were considered, the solution chosen, how the project will be implemented, and the resources required for the project.



1. **Environment:** List of factors that justify the existence of the project, the economic, commercial, and competitive environments, the opportunities, etc.
2. **Purpose and objectives:** Project vision, general and strategic objectives, specific and tactical objectives, operational objectives (technical, economic, and temporal)
3. **Project summary:** A summary of the contents of the project in a few words: name/project reference, origin, environment, current status
4. **Expected benefits:** Desired earnings, road map for results, financial benefits (depending on the outcome), value of quantified benefits, financial scenarios, cost/ROI, risks/costs of not acting, project risks (for the project itself, for the profits, and for the business)
5. **Preliminary scope:** Action framework, perimeter, and boundaries, prerequisites
6. **Critical success factors:** Material and human resources, context of the organization
7. **Preliminary project plan:** The project approach, definitions of phases, reports, and deliverables
8. **Deadlines and milestones:** Activities and modifications of project activities, technical distribution, plan and project planning
9. **Roles and responsibilities:** Functions, roles, and resources to cover the workload
10. **Resources:** Resources needed for the project, funds
11. **Budget:** Project controls, financial plans, etc.
12. **Constraints:** Expected problems and solutions, assumptions, identified and assessed options, magnitude, scale, and complexity rating

To these 12 elements of the development plan of the project, the two items below can be added and considered as part of a “facilitation plan” of the project.

13. **Communication:** Operational (media selection, media, public, etc.) or promotional (internal or external)
14. **Project monitoring:** Indicators, dashboards, reporting, project reviews, traceability

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

PECB

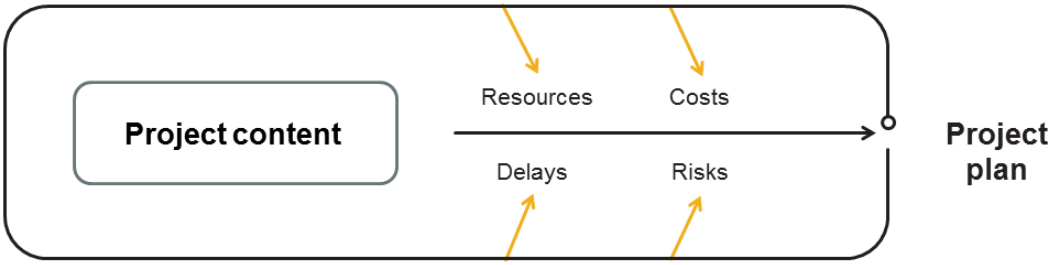
11

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.

An iterative approach



PECB

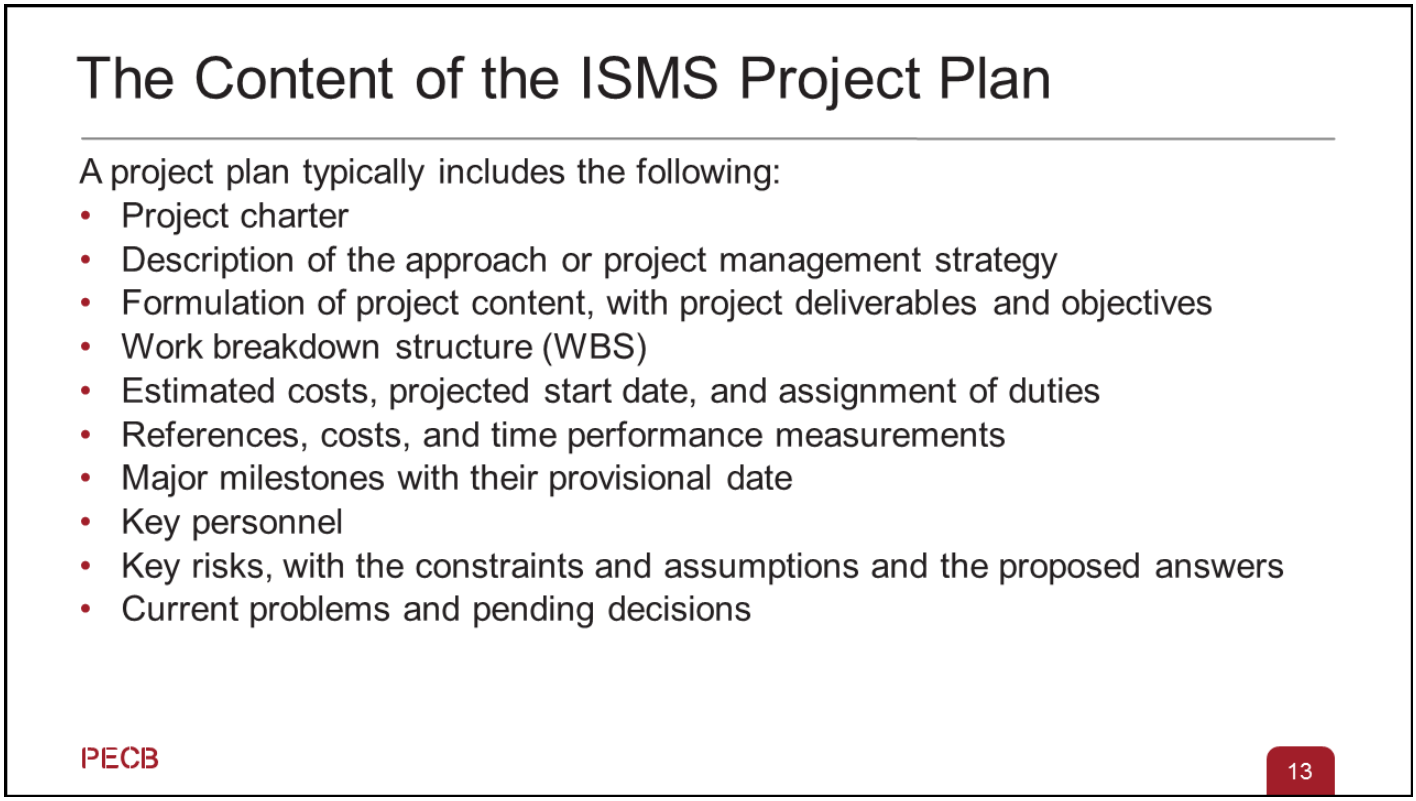
12

The ISMS project plan uses the results of the process of various activities to provide a logical and coherent document that can be used to guide both the realization and the direction of the project.

This process requires several iterations. For example, the first step can describe the activities in general and does not specify the duration of activities, while the final step will detail the specific resources and specify the completion dates.

The project plan is used to:

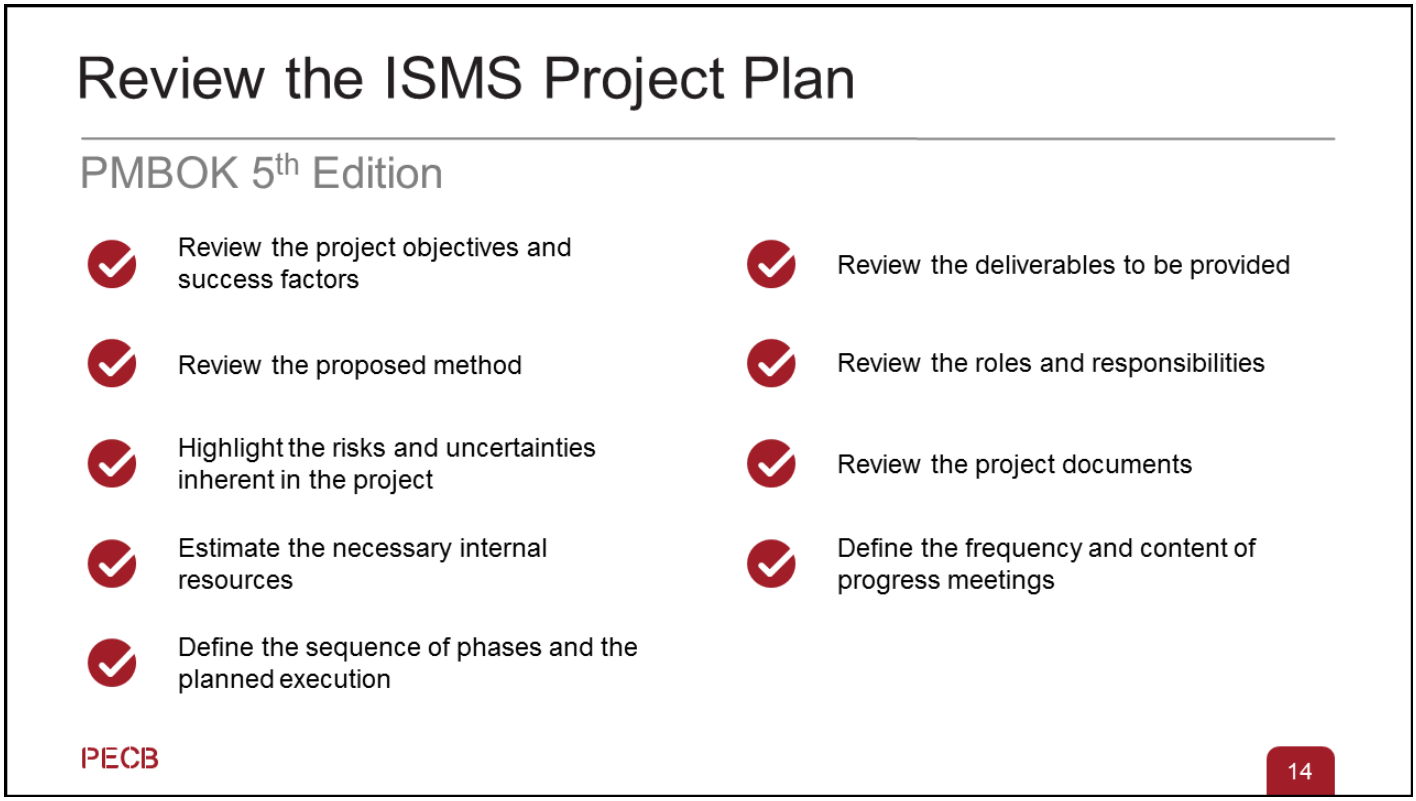
- Guide the project implementation
- Keep a written record of any assumptions made during planning
- Keep track of the decisions made with justifications behind them
- Facilitate communication among interested parties
- Conduct project reviews, including the scope, content, and date
- Provide a benchmark to measure the progress and the control of the project



As part of implementing an ISMS, the integration of the project is a key step to its success, an area of knowledge studied by PMBOK that provides all functions that allow effective coordination of the various elements of the project.

In this regard, the project plan will consist of a summary document, which can be broken down into further different project plans each having a more granular approach related to the specific subprojects. These supplementary plans, in the specific context of the implementation of the ISMS, will identify among others:

- Project charter
- Inputs to other processes
- Organizational chart
- Risk management plan



During the initial phases of the project, the roles and responsibilities of each interested party in the project are clearly defined, as it is of high importance to determine the function of each individual to ensure successful implementation. This phase is relatively short and generally limited to agreeing on a number of key elements that make up the project plan.

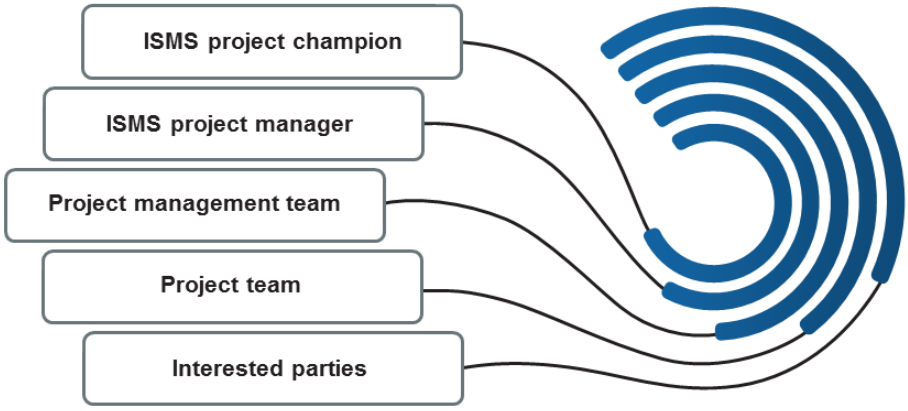
The project plan, defined as a "road map," will then be formally submitted and approved by the management because it encourages the organization in terms of material and human resources and also in financial terms, as already reported previously.

The clarification brought by the completion of the project plan enables the project team to refine and document functional requirements necessary to achieve the objectives of the organization. In other words, the elements listed above allow for the preparation of the following necessary tasks, although those alone would not be sufficient for the initial ISMS:

- Definition of processes and functions to implement the project
- Modeling/documentation of these processes
- Definition of input and output managed by the project
- Identification of organizational impacts that the project would cause
- Identification of reusable elements of previous projects to optimize the current project

1.4.4 Establish the ISMS Project Team

The ISMS project team:

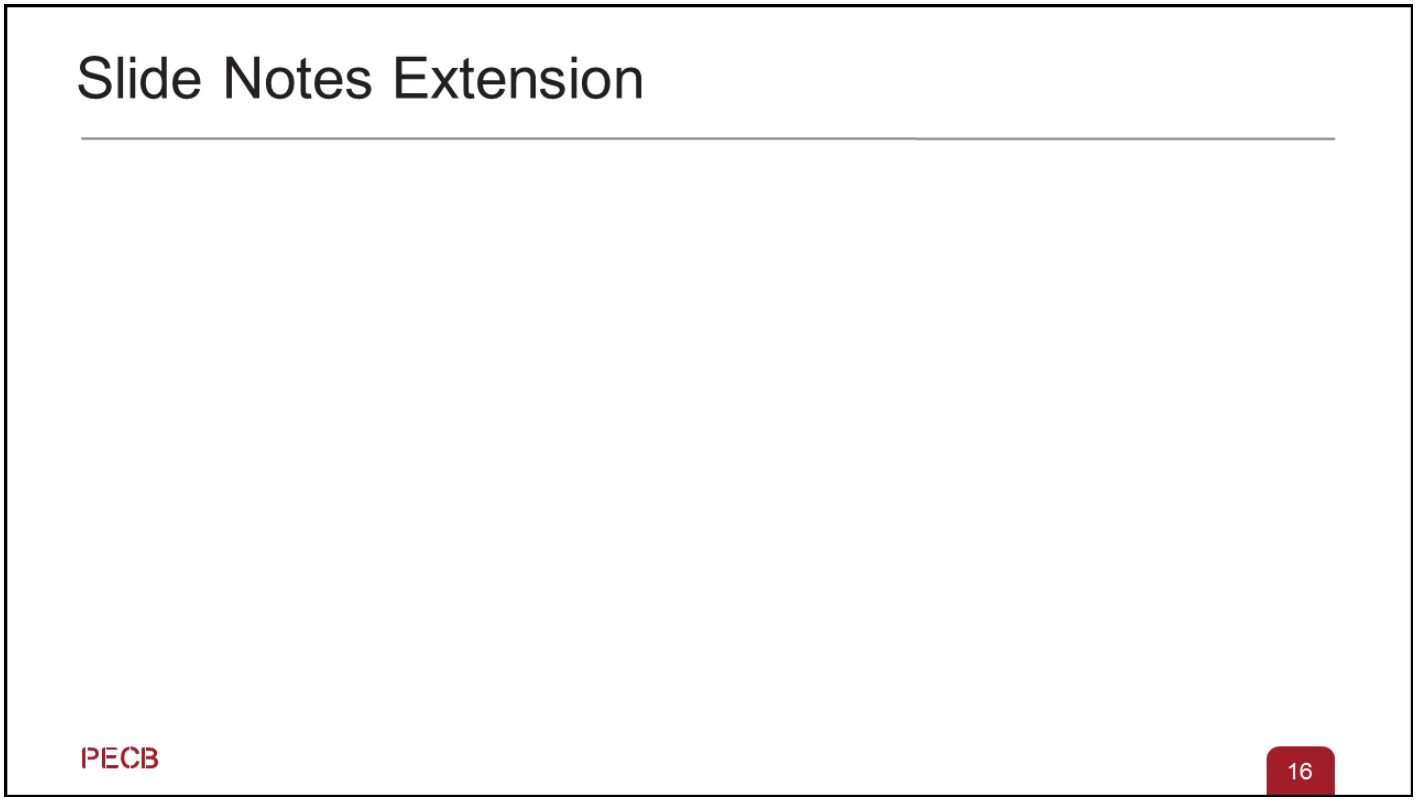


PECB

15

Usually, the ISMS project team consists of the following:

1. **ISMS project champion:** The project champion is the person, usually close to the decision-making level of the organization, who ensures, by using the influence given by their mandate within the organization, that the project can be established and should receive adequate resources. Therefore, they act internally as a kind of project sponsor.
2. **ISMS project manager:** The project manager has a central role in the project on which the success of the project depends heavily. They are responsible for all the activities in the project and for leading the team. The responsibilities of the project manager include:
    - Structuring the project in order to reach the set objectives
    - Encouraging communication with the team members to keep them going and ensure their support for the whole period
    - Working with the project champion to clarify and formalize the objectives and discuss the resources needed for the project
    - Organizing user workshops or involving users early in the project to identify their needs
3. **Project management team:** This team consists of all the persons acting under the control of the project manager that are responsible for assisting in strategic decisions and policies and helping in reaching the objectives set for the project.
4. **Project team:** This team consists of all persons acting under the responsibility of the project manager that are responsible for assisting in the management of project operations.
5. **Interested parties:** Interested parties are individuals or groups of individuals who are affected by the decisions taken in the project or have an interest in its outcome. This approach assumes that the organization meets a certain balance between the interests of these parties, just as the parties are expected to comply with certain interests of the organization.



To improve the performance of the team in charge of the ISMS project, the necessary training, tools, techniques should be provided, and procedures should be in place.

Important note: It is not necessary that all members of the project team are experts in information security. The establishment of a multidisciplinary team should be a priority.

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.

PECB

17

The ISMS project manager is a person who has the responsibility and the authority to lead the project and ensure that the information security management system is established, implemented, and maintained.

Selecting a project manager requires some skill — the gap analysis may reveal a need for technical skills or may suggest that a better understanding of the organization is required. The scope of the ISMS may also dictate who should manage the project and at what level in the organization. While it is typical that the project manager is the CISO, CTO, or CRO in a large organization, such a role may be indifferent to an ISMS being implemented in a "localized" sense. There is no standard answer and project management skills do not necessarily come with technical skills.

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

PECB

18

A steering committee is a committee that provides guidance, direction, and control to a project within an organization. In general, the steering committee of a project involves the organization's key personnel and experts in the field so as to ensure the effectiveness of the project.

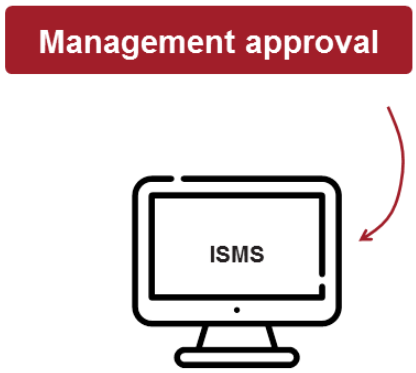
At least the project champion and project manager should be part of the steering committee to inspire and coordinate.

Important note: The steering committee of an ISMS implementation project is often supported by the information security committee of the organization.

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



PECB

19

The commitment and active involvement of the organization's management in the ISMS project is pivotal to the successful implementation and maintenance of the information security management system. The management of the organization helps creating a culture of information security and educating all members of the organization accordingly. The management must approve the business case and project plan of the ISMS. The declarations of support and authorization of the management must be formally documented.

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.

PECB

20

Note: Please note that CISO and CIO are two different terms and cannot be used interchangeably. CISO (Chief Information Security Officer) in most cases reports to the CEO and their main duty is to monitor and analyze potential security risks of the organization. CIO (Chief Information Officer) is responsible for operational IT requirements such as the development of policies, practices, training programs, and the planning of project developments or systems.

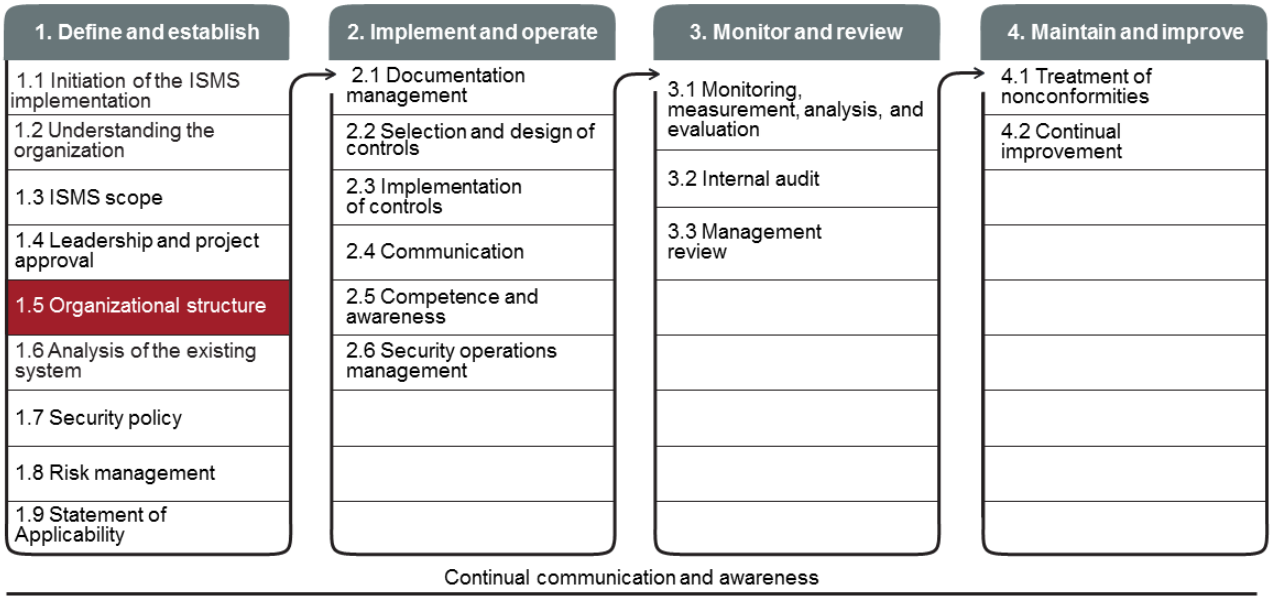
1. **Which of the statements below regarding the definition of a business case is NOT true?**
   A. A tool that promotes ISO/IEC 27001
   B. A way to define clear objectives
   C. A tool for decision-making support
2. **Which resources are necessary for the implementation of an ISMS?**
   A. Cloud, management, 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

Section summary

- A business case is a tool that helps in planning and decision-making, including decisions regarding the opportunities, choices, and the right time to initiate an action or a sequence of actions.
- The ISMS project team includes the following: the project champion, project manager, project management team, project team, and the interested parties.
- A project involves: a project charter, the key personnel, a description of the approach or project management strategy, etc.
- The organization's management must approve the ISMS business case and project plan.

This section provides information that will help the participant gain knowledge on the organizational structure and the roles and responsibilities of interested parties and committees.

1.5 Organizational Structure



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.
Top management shall assign the responsibility and authority for:

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

NOT

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

PECB

25

To comply with the requirements of ISO/IEC 27001, an organization shall at least define the roles and responsibilities of the key interested parties related to the ISMS.

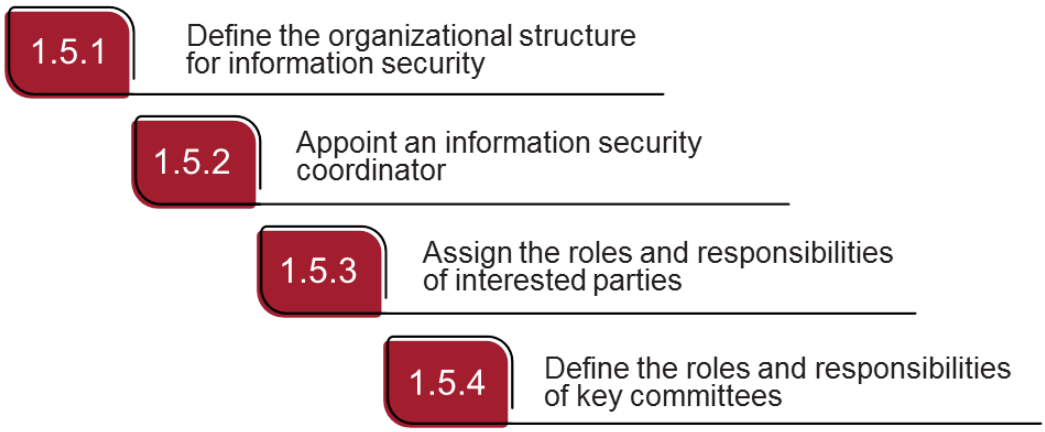
ISO/IEC 27003, clause 5.3 Organizational roles, responsibilities and authorities

Beyond the roles specifically related to information security, relevant information security responsibilities and authorities should be included within other roles. For example, information security responsibilities can be incorporated in the roles of:

g)*information owners;*
h)*process owners;*
i)*asset owners (e.g. application or infrastructure owners);*
j)*risk owners;*
k)*information security coordinating functions or persons (this particular role is normally a supporting role in the ISMS);*
l)*project managers;*
m)*line managers; and*
n)*information users.*

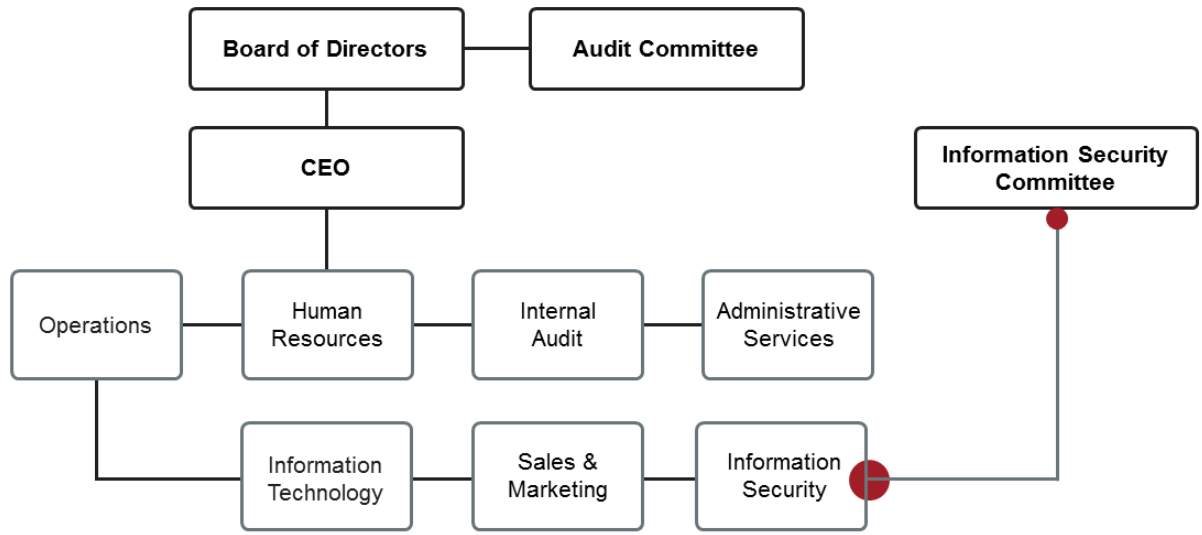
1.5 Organizational Structure

List of activities



PECB

1.5.1 Define the Organizational Structure for Information Security



PECB

27

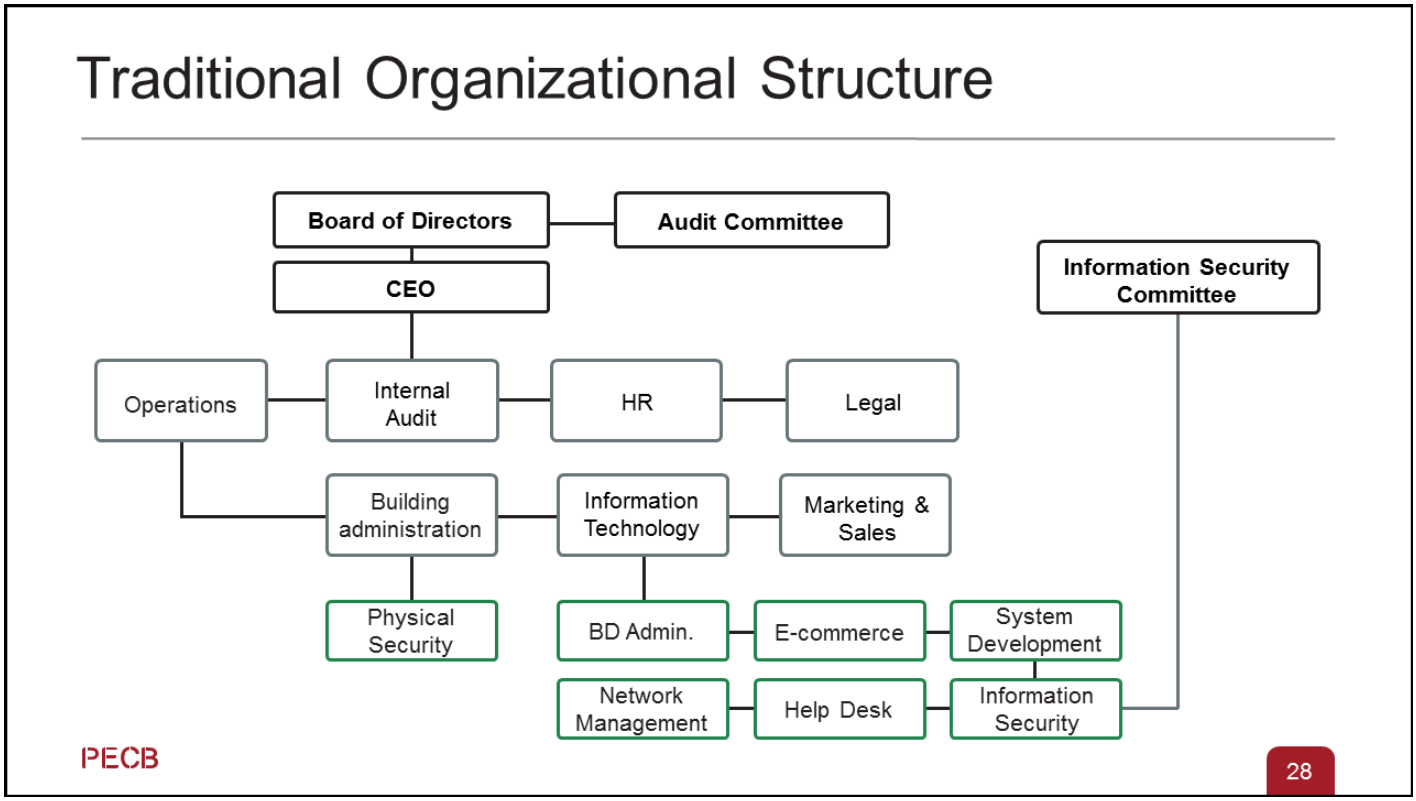
One of the most important elements in defining the information security management and its governance is placing the chief information security officer (CISO) in the organization's hierarchy.

Before defining the structure of information security governance, the organization must consider several factors: the mission, scope, business needs, organizational and functional structure, customers, the degree of centralization or regionalization, and the internal culture.

The organization should develop a governance structure for information security that will meet the following requirements:

- Absence of real and potential conflicts
- Proximity of the decision level
- Strong support from top management
- High influence ability
- Consideration of all security concerns
- Information coverage regardless of the medium of communication

In addition, the activities related to information security should be carried out by a person responsible for information security who establishes the ties of cooperation and collaboration with other branches of the organization.



Traditionally, the information security team is attached to the IT Department of the organization. This is a commonly used model for information security governance. With this model, there is the advantage that the technical security expertise is grouped in the same department.

However, there are several disadvantages of this model:

1. No independence in the functions of information security related to IT systems
2. Weak capacity of influence because the CISO is on the same or lower hierarchical level with IT managers
3. Real or potential conflicts of interest
4. Poor consideration of issues related to information security
5. Issues mainly focus on operational security and technology

This type of structure does not allow the CISO to properly exercise the mandate. Sometimes, the Information Resources Management (IRM) could be in a position of real or potential conflicts of interest. The presence of an additional hierarchical level between the CISO and top management slows the process of information exchanging and decision-making with respect to information security. There is also a risk of interference by IRM in communications and reports that the CISO forwards to the top management. To manage this risk of interference, it is advisable for the CISO to send the reports directly to the information security committee rather than to the information resources management.

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.

PECB

29

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

PECB

30

The roles and responsibilities of the interested parties, who have a function or tasks directly related to the ISMS, should be clearly defined. The description of the duties of responsibilities can be documented in several ways: information security manual, functions form, employment contract, terms of security policy, etc.

The person responsible for a task can delegate tasks to others, but not the responsibilities.

In the case of asset management, an owner may appoint a "custodian" who shall by delegation ensure the security of the assets under their responsibility. Thus, the person will:

1. Authorize and respond to the utilization of assets
2. Ensure that appropriate security controls are in place, implemented, and verified periodically
3. Master risk analysis and ensure the management of residual risks after the approval of the owner
4. Ensure user awareness

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

PECB

31

When drafting the Statement of Applicability, a person responsible for each of the selected security controls should be appointed.

The individuals responsible for processes or security controls will be involved in various stages of implementation of the ISMS, such as:

1. When formulating the objectives of information security
2. When drafting the Statement of Applicability
3. When designing security controls and drafting specific policies and procedures
4. During the transfer of the ISMS project to ISMS operations
5. When setting indicators
6. When following up on nonconformities

1.5.4. Define the Roles and Responsibilities of Key Committees

PECB

32

It is important to have in mind that creating these committees is not a necessity. As such, it is common to reuse existing committees by expanding their scope. The promotion of a multidisciplinary approach to information security in the conduct of committees that consist of members with diverse skills and from different units of the organization is considered to be vital.

In addition to committees, it is necessary to establish links with experts outside the organization to develop contacts, including contacts with the relevant authorities, to monitor trends and issues related to information security.

The extent to which committees are productive in small-scoped organizations needs to be carefully gaged.

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

PECB

33

The executive committee is the body of guidance, control, validation, decision-making, and arbitration for the ISMS. It is composed of representatives of the Board of Directors of the organization.

This committee determines the development strategy of the ISMS. It decides the allocation of necessary resources to achieve the goals and plays a monitoring role. It arbitrates any disputes and guards the respect for the values of the organization.

It is the only committee that is a requirement of ISO/IEC 27001 and its minimum meeting frequency should be once a year. It is very rare that an organization establishes a specific executive committee for information security. Most often, this is a point in the agenda of the executive committee which is responsible for the overall conduct of the organization's activities.

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

PECB

34

This committee consists of representatives from various divisions within the organization, usually chaired by the CISO. The representatives of different units are often a "liaison officer" to the problems related to information security. The role of this committee is to ensure coordination and cooperation of information security within the organization.

Specifically, the information security committee promotes coherence in information security within the organization and monitors the strategic direction and priorities for actions agreed by the management. This committee is responsible for daily operations but also ensures the smooth running of operations of the ISMS and the implementation of action plans and also the implementation of corrective actions arising from risk analysis.

In order to avoid the proliferation of committees within the organization, the information security committee may, in the event of a major incident, play the role of the emergency committee.

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

PECB

35

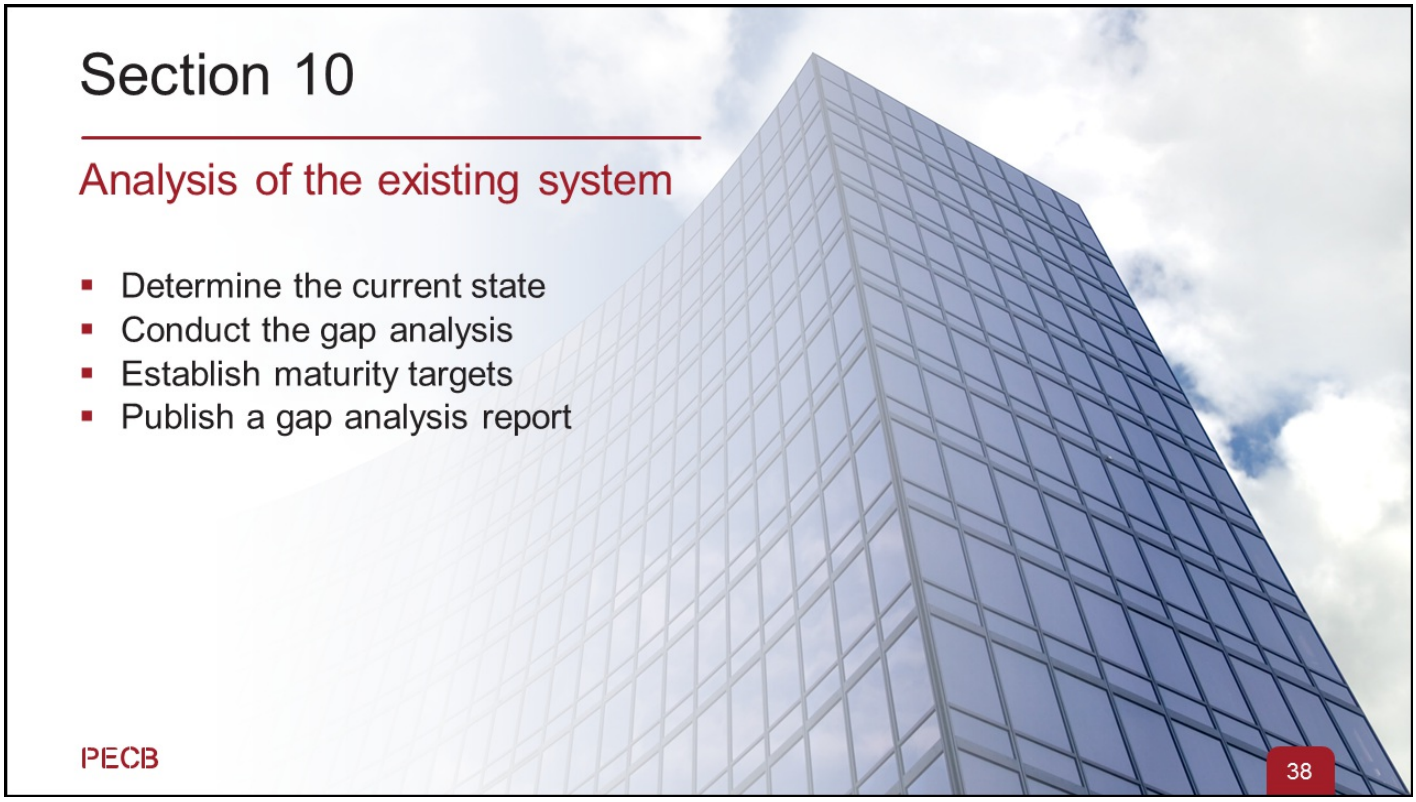
Depending on the size of the organization and its culture, certain responsibilities in information security should be entrusted to operational committees. The duplication of committees should be avoided and the responsibilities should be integrated with the structures already in place as the change management committee, the human resources management committee, quality assurance committee, etc.

It is appropriate for the CISO to participate in various committees as a member or be represented by an information security liaison officer.

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

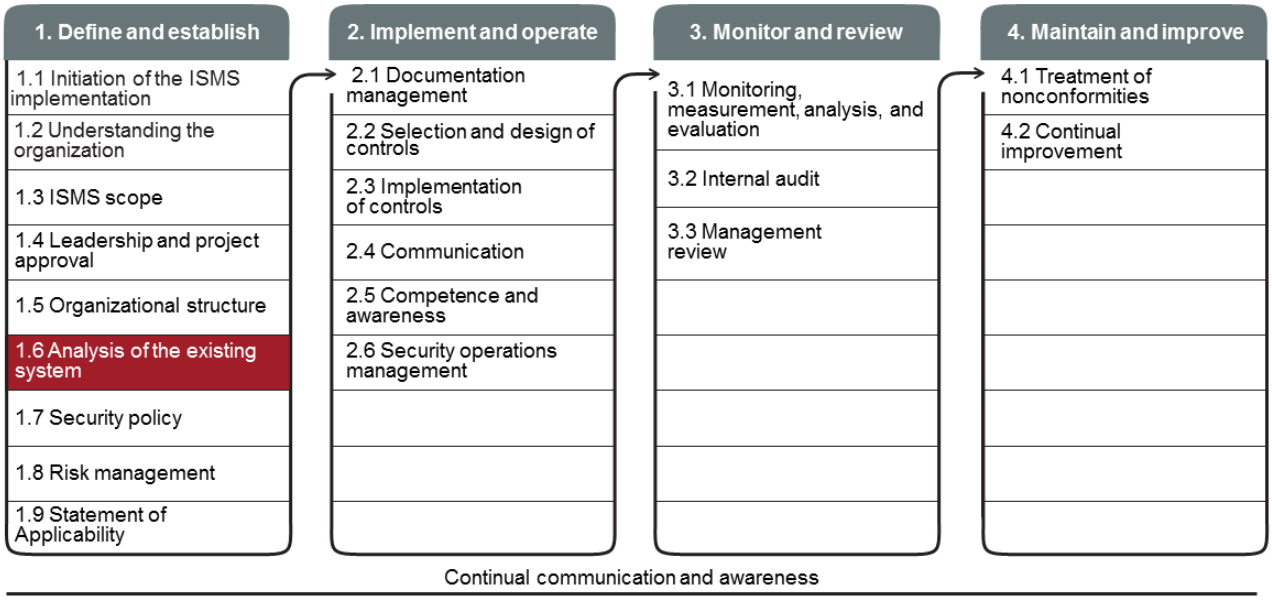
Section summary

- According to 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.
- 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.



This section provides information that will help the participant understand the process of conducting a gap analysis and establishing maturity targets.

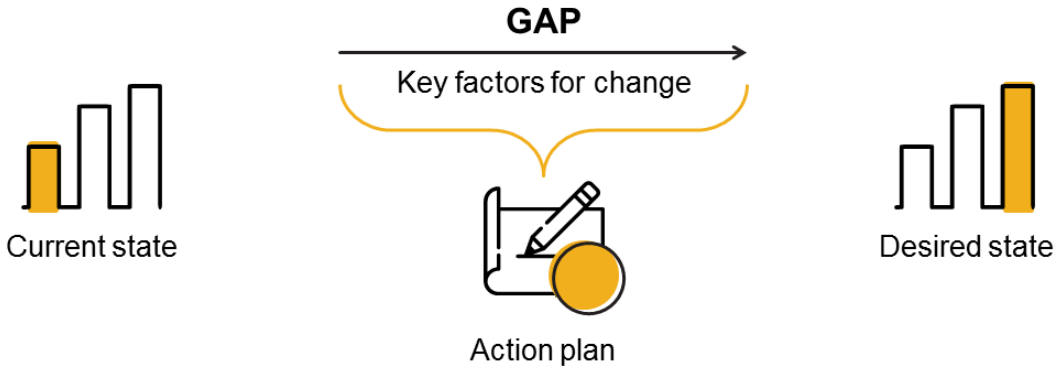
1.6 Analysis of the Existing System



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.



PECB

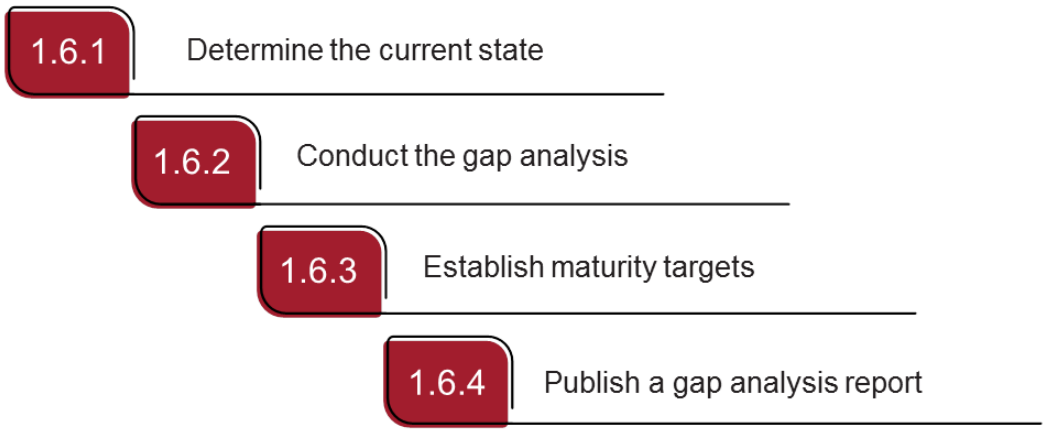
40

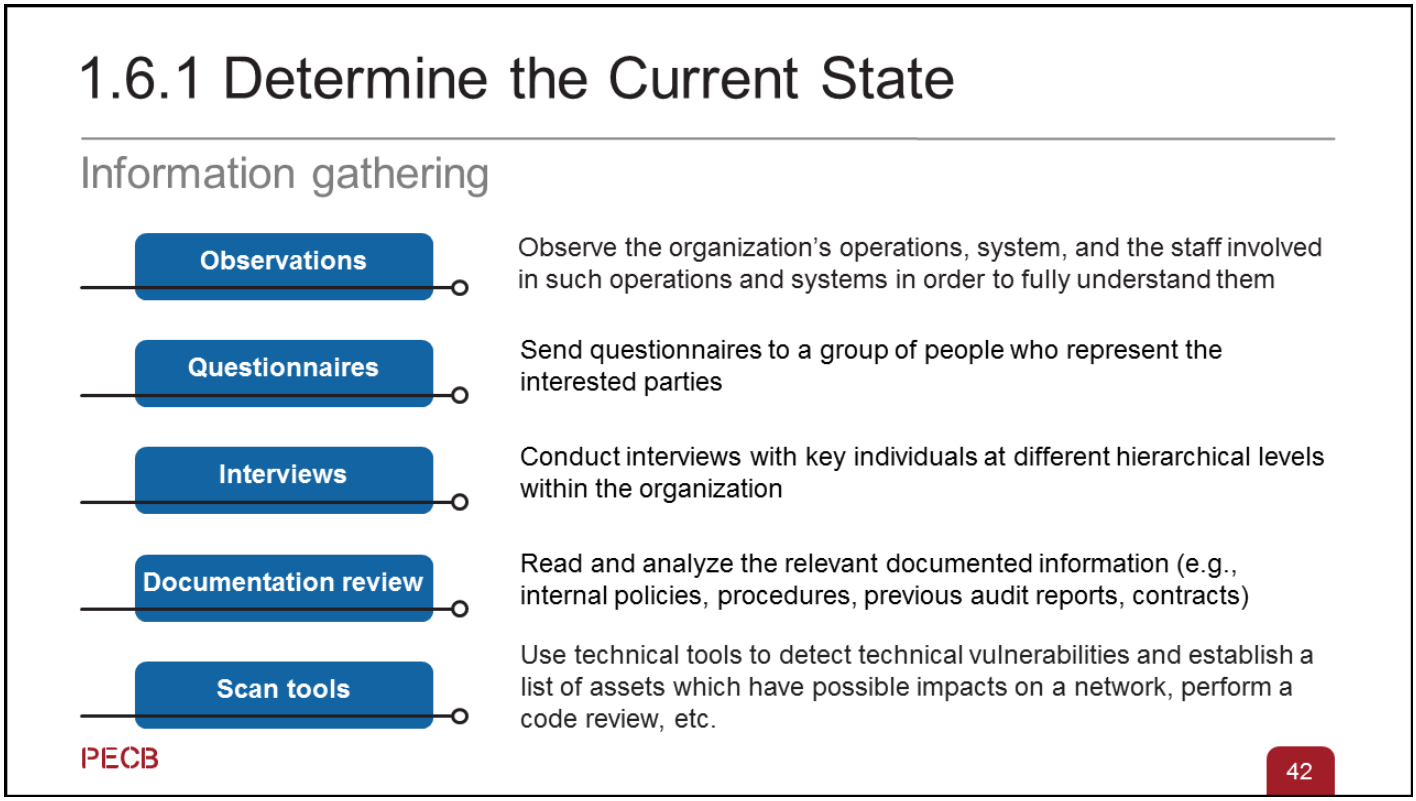
The gap analysis addresses the following questions:

- What is our current state?
- What is our desired state (objective)?
- What is the difference between our current and desired state (objective)?

1.6 Analysis of the Existing System

List of activities





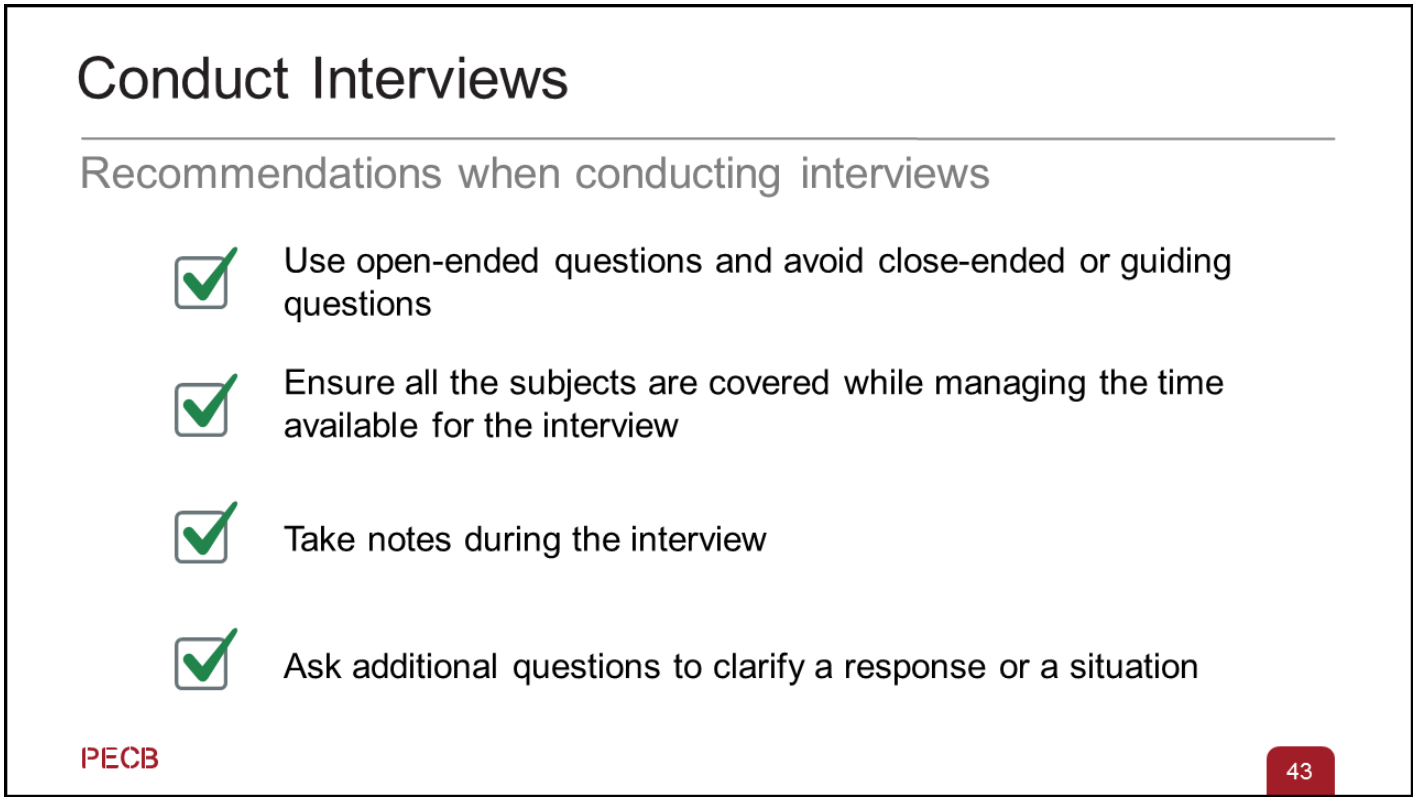
The project team should gain a detailed knowledge of the existing management system by collecting information from multiple interested parties.

To determine a given state based on a situation at a given time, the choice of the data collection method often depends on the type of data to be collected, the individuals to be interviewed, the skills and knowledge of the interviewers, as well as the availability of resources (time, budget, etc.).

To gather the appropriate information in an organization, it may be useful to conduct the following actions:

- Observe the on-site physical security controls
- Conduct interviews with the individuals responsible for information security management and those responsible for the daily operations of ISMS
- Examine the documented information on information security management processes, procedures, description of security controls, reports, etc.
- Review the internal audit results

Important note: Although some employees may claim that there is no system in place in an organization, this is by no means true. Even if a system is disorganized and informal, there will always be a series of information security controls in place which are to some degree effectively managed.



Experience shows that the more you prepare for an interview, the more productive it will be. An effective strategy that can be used to conduct interviews is to draw up a checklist that ensures the interviews are systematically conducted and that relevant evidence is obtained. The checklist can include a list of definitions to ensure the uniformity of responses. The checklist should have a section for answers, comments, and observations to be made. The items of the checklist should also include the reference to the related standard. The interviewee can receive the checklist prior to the interview in order to be adequately prepared for the interview.

During the interview, it may be useful to clarify the specialized terminology related to information security, such as “threats” and “vulnerabilities” in a language that is more comprehensible for the unexperienced interested parties. One can, for example, use the following construction of a question: “What are you trying to avoid?” or “What do you fear may happen with this particular resource?”

The interview can be recorded only if the interviewee agrees to it. However, the most common practice is to simply take notes. Recording the interview can be intimidating to the interviewee and could have a negative impact on the outcomes of the interview.

The interview notes should contain the following:

Function of the interviewee and date (due to the principle of confidentiality, the name of the interviewee is not included in the interview notes, unless the interview is a member of the management)

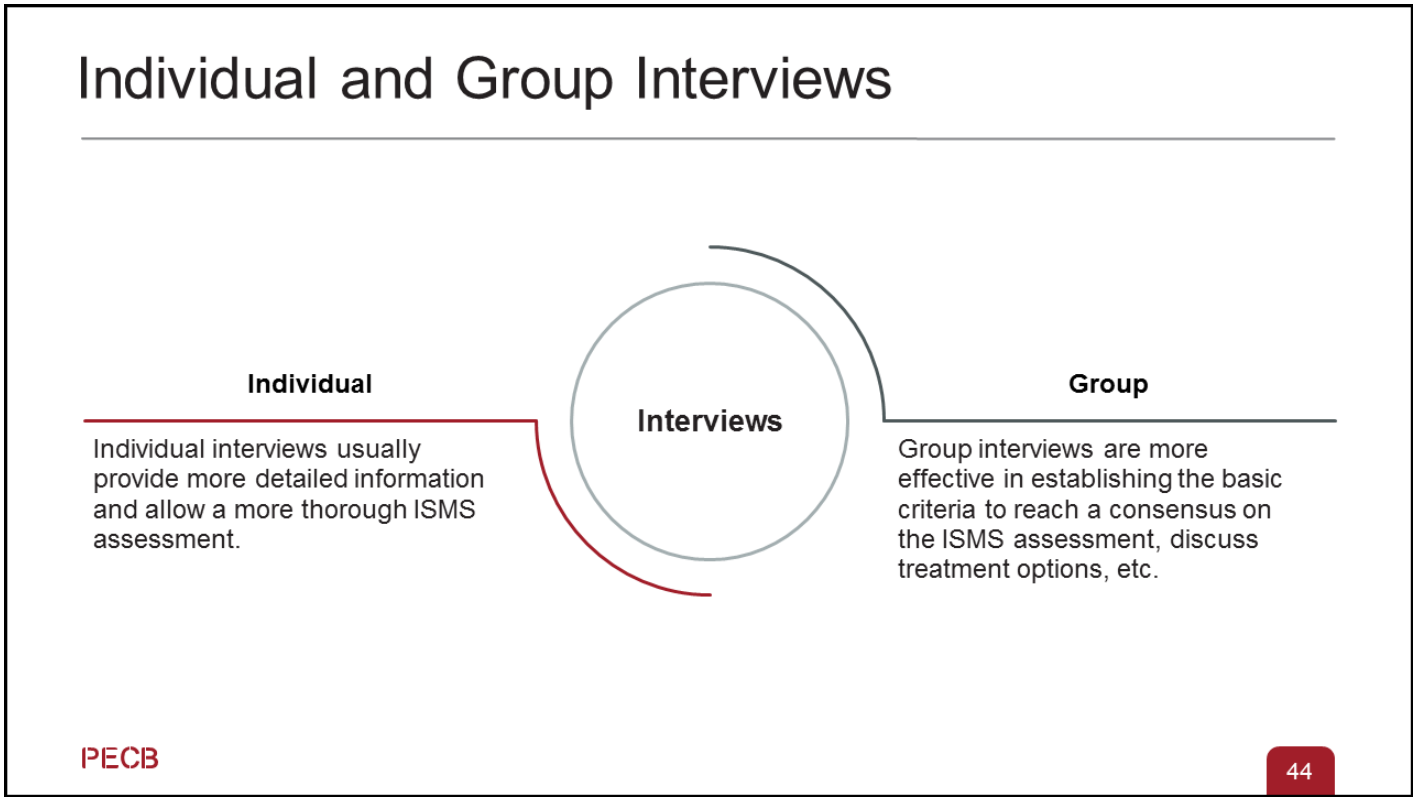
Example: Discussion with an employee from the IT Department, September 3rd, 2019

Interview objectives

Example: Validating if the organization is adequately following the established training plan or not

Summary of the collected evidence

The documented information must be gathered in a clear, concise, and accurate language. We should only include facts, not judgments. In addition, we should identify weaknesses. Then, the identified weaknesses will be reported in the gap analysis. The exact reference to the related standard should be listed with the clause number.



Some people might question the value of the detailed ISMS questions addressed to people without professional experience on matters of information security risks. However, research shows that it is essential to ascertain the views of interested parties (whether they are experts or not) on their exposure to the activities they manage or the tasks they perform. Individuals responsible for business processes will provide a much more "business" oriented view on risks, e.g., the public relations officer will indicate concerns about a risk in the organization's reputation.

Individual interviews:

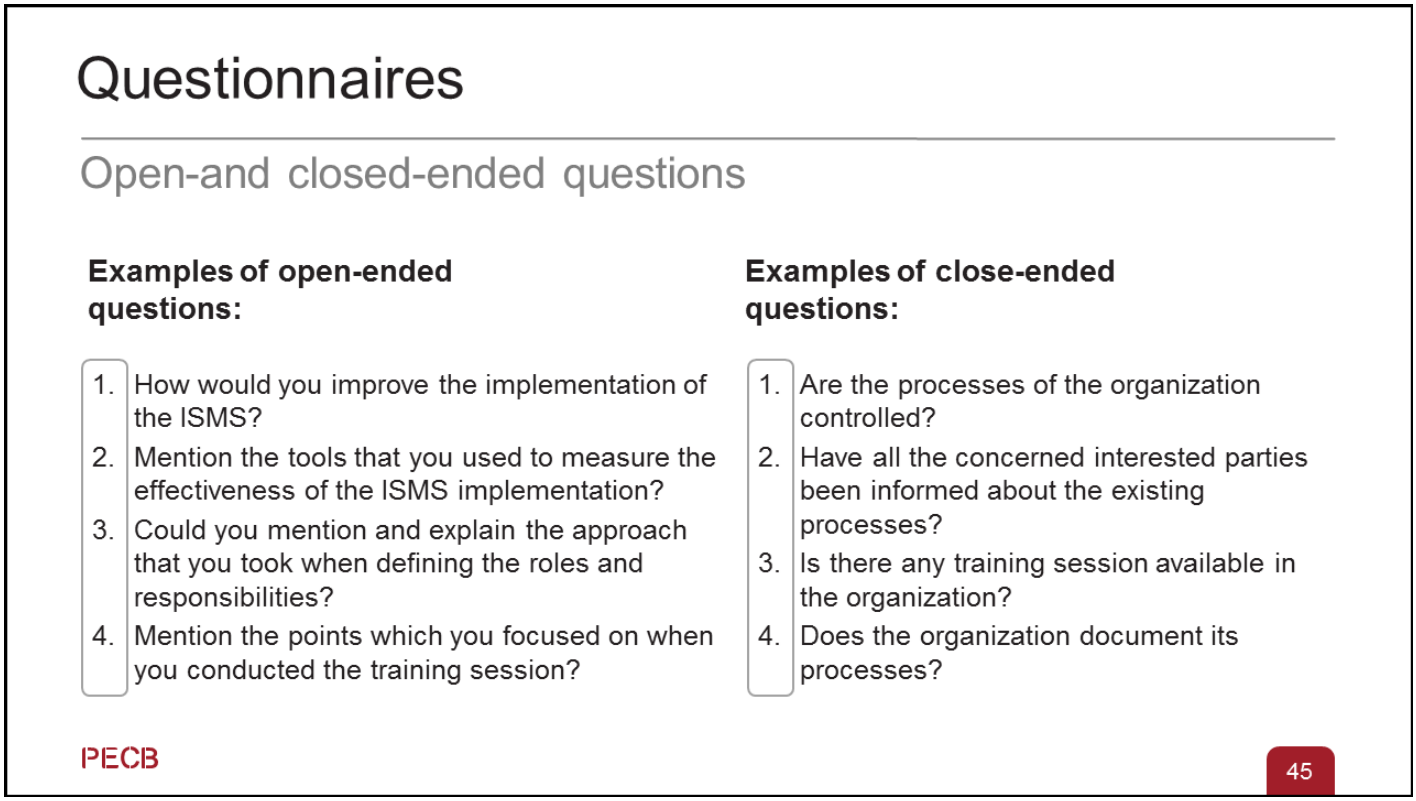
In individual interviews, the interviewer can focus on a single person and generally obtain more detailed information about the ISMS. Individual interviews prevent any dominant member of the group from influencing the response of others, which is otherwise known as the *"bandwagon effect."* Therefore, it is preferable to conduct this type of interview.

Individual interviews enable the interviewer to:

- Read the body language of the interviewee
- Identify the sensitive elements of the discussion
- Ensure the confidentiality of discussions with the interviewee
- Adjust the follow-up questions

Group interviews:

The practice of conducting group interviews must be limited, unless the interviewer wants to check the interaction and dynamics between the various members of the group. In group interviews, members of the group gives their summarized opinion on the ISMS.



The determination of the current state of the implemented information security controls can be undertaken by the project team or outsourced to external consultants. The advantage of entrusting the analysis to external parties is that, theoretically, one will receive neutral reports. The collection of data during the analysis phase requires the responsible team to be highly knowledgeable about the current situation. In most cases, much of this analysis will be produced on the basis of responses to structured and semi-structured questionnaires that will, depending on one's choice or context, be sent in writing (or electronically).

When using questionnaires, questions can be:

Open-ended: The interviewee has complete freedom of response and, consequently, the interviewer will be able to obtain more detailed information.

Note: With open-ended questions, interviewers can collect more valuable and complete information. However, these responses often are more difficult to analyze because they generate important content for "content analysis." The response rate to these questions is often less important but more suitable for the analysis of opinions and attitudes.

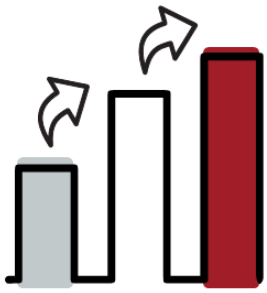
Closed-ended: The interviewee is limited and does not have the freedom to further clarify the answer to the interviewer.

Note: Closed-ended questions have the potential to generate answers that are not as spontaneous. They especially are useful for the study of behavior (nature, frequency, etc.). Opinion scales represent a particular format for closed-ended questions. They provide information on the degree of support for a proposal; people must position themselves on an "agreement/disagreement" scale of several levels.

1.6.2 Conduct the Gap Analysis

A gap analysis is performed as follows:

- **Determine the current state:** The processes and security controls that are in place within the organization should be identified.
- **Identify the targets (objectives):** The targets for each security control should be set.
- **Gap analysis:** The gap that may exist between the information security controls currently in place and the requirements of ISO/IEC 27001 should be identified. This allows the organization to identify the current controls that need improvement and plan accordingly to address them.



PECB

46

The main use of a gap analysis is to provide a basis for identifying and measuring the necessary investments in time, money, human, and other resources to effectively implement the proposed ISMS.

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

PECB

47

ISO/IEC 21827 allows an organization to measure its level of maturity and ability to develop its software development. This standard is based on the CMM ® (Capability Maturity Model), originally developed by the Software Engineering Institute at Carnegie Mellon University. The CMM was designed to measure the quality of services provided by software vendors of the Department of Defense of the United States. In March 2016, ISACA (Information Systems Audit and Control Association) acquired the CMMI Institute. This evaluation and development capacity model is based on a hierarchical grid of five maturity levels (see next slide).

The model proposed by ISO/IEC 21827 is now widely used by R&D companies, computer services, and software vendors to evaluate and improve their own product development. Subsequently. this model has been adapted to sectors outside software engineering, including:

- CMMI (Capability Maturity Model Integration), which determines the practical development and maintenance of systems and applications
- CMM-TSP (Team Software Process), which specifies standardized practices of a team project
- CMM-PSP (Personal Software Process), which specifies standardized practices of an individual resource development
- SSE-CMM (Systems Security Engineering Capability Maturity Model) that determines the safety practices related to information systems

Several other models and frameworks have adopted the maturity scale CMM. The best known is COBIT, issued by ISACA.

Slide Notes Extension

PECB

48

To measure, in a precise way, the progress of the ISMS during its entire life cycle, it is advisable to lean on methodologies such as CMMI. This model allows to achieve a proactive status for security activities. It is, however, still insufficient in itself because it must take into account the culture of the organization and allow a considerable time for the organization to reach the necessary maturity.

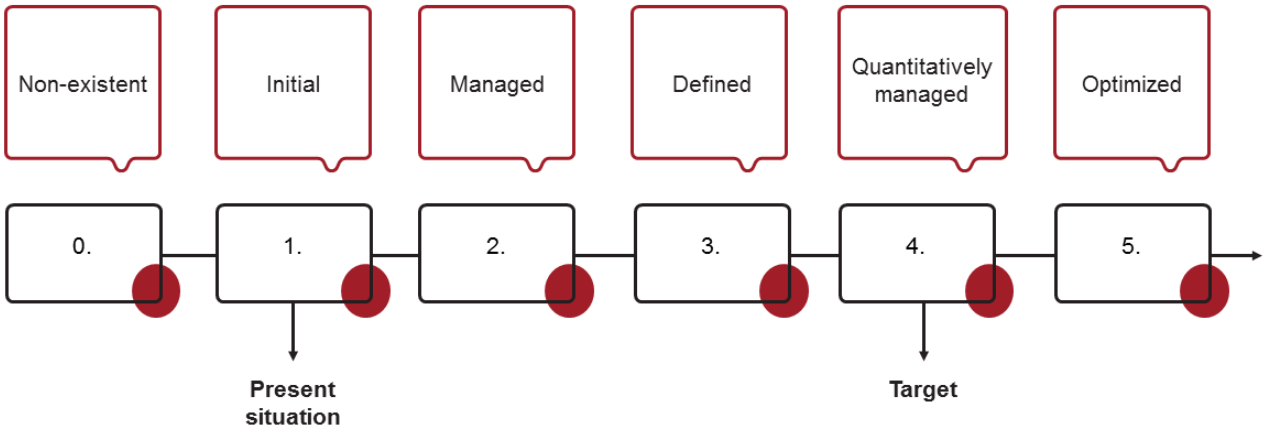
Mapping ISO/IEC 27001 with other best practices:

Many organizations have recently taken steps to implement references for IT governance — the most frequently cited ones are CMMI, COBIT, and ITIL. These different standards can complement and enable economies of scale. For example, the implementation of CMMI and ITIL processes facilitates the implementation of controls of ISO/IEC 27002. COBIT, with its approach to risk management, is also a possible alternative that helps the implementation of ISO/IEC 27001.

More types of risks are considered other than those in ISO/IEC 27001 (risks affecting the efficiency, reliability, and efficiency of information systems, in addition to the criteria oriented toward security such as confidentiality, integrity, availability, or compliance) but the approaches are fundamentally similar.

Generally, we can consider that the ISO/IEC 27000 series are deepening on the subject of information security and risk management. It is also worth noting that ISO/IEC 20000-1 and ITIL now point directly to ISO/IEC 27001 with regard to the information security management process.

1.6.3 Establish Maturity Targets



PECB

49

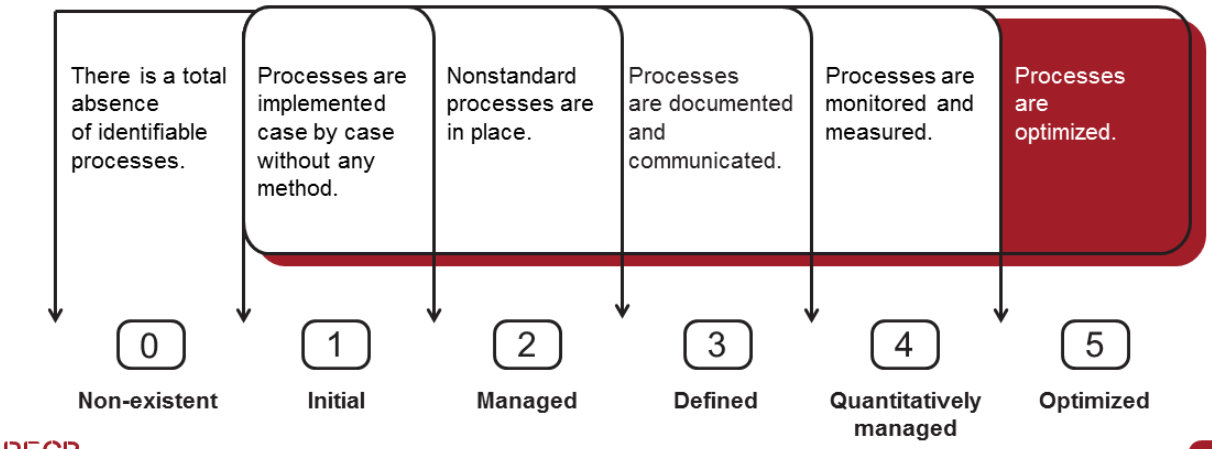
The gap analysis report should include at least:

1. A summary description of the observed existing situation
2. The objective of the project
3. The description of the differences between the existing situation and the objective to be achieved
4. Various recommendations on how to get there

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:



PECB

50

0.Nonexistent: The organization is not aware that there is a total absence of the identifiable processes and that this is a problem to be considered.

1.Initial: The organization is aware of the problem and the need to investigate it; however, there is no standardized process to do this. There is no general approach agreed by the management.

2.Managed: Processes have been developed to a stage where different people performing the same task are using the same procedures. There is no formal training or communication of standard procedures and the responsibility is left to certain individuals. It relies heavily on personal knowledge, where the probability of error exists.

3.Defined: Procedures have been standardized, documented, and communicated through training sessions. However, their use is left to individual initiative and it is likely that failures can be detected.

4.Quantitatively managed: It is possible to monitor and measure compliance with procedures and take action when some processes may fail to function properly. At this stage, the processes are constantly improved and correspond to good practice. Automation and the use of tools, however, are limited or partial.

5.Optimized: The process has reached the level of best practice, following a steady improvement in comparison with other organizations (maturity model). The computer is used as a way to automate integrated workflow, providing tools that improve quality and efficiency and make the organization adapt quickly.

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
A.5.1.1 *Policies for information security*	*A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.*	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

PECB

51

For the identification of existing and planned information security controls in an organization, the list of information security controls of ISO/IEC 27002 (or of ISO/IEC 27001, Annex A) can be used. This helps to get an overview of the existing status in relation to security best practices.

This document summarizes the gap analysis that was made within an organization by highlighting the actions to be taken first. Its short-term objective is to promote the implementation of corrective or preventive measures for assets with a high risk potential. In the long term, the reporting template keeps track of planned measures and the different analysis carried out, emphasizing the continual improvement of the ISMS.

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
A.5.1.2 *Review of the policies for information security*	*The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.*	The policy has existed for more than six months but it has not been formally reviewed by the management yet. Currently, there is no scheduled review. However, it is clear that no major change has occurred in the organization that would require a revision of the document.	2	5	The policy is not reviewed periodically and if no major change occurs, it is not reviewed at all. However, the management is responsible for reviewing the policy if a major change occurred in the organization.	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

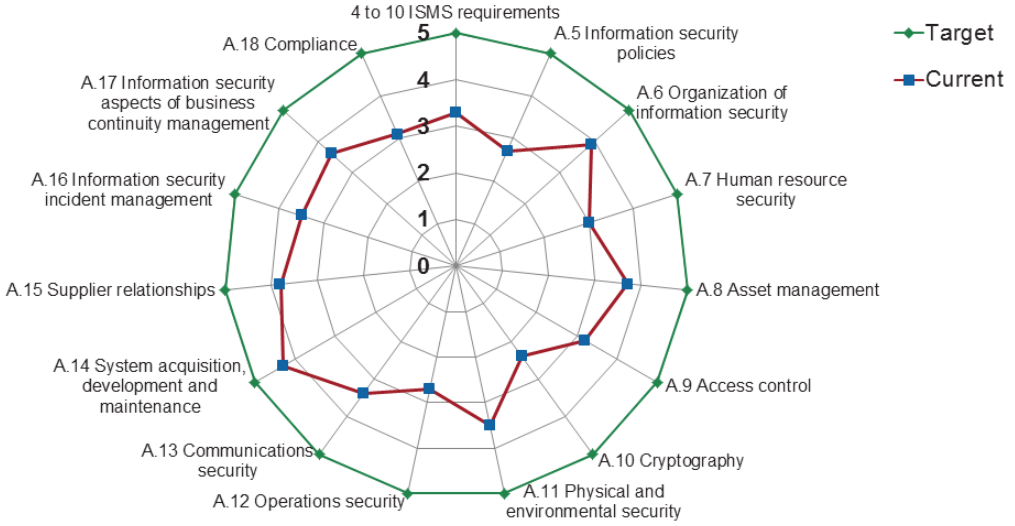
PECB

53

The example shown on the slide represents a potential gap analysis report.

Publish a Gap Analysis Report

Example of a graphical representation



PECB

54

In order to present the differences that have been examined, it is favorable to choose an effective visual tool. The data that produce numerical values based on qualitative scales should be presented so that one can immediately notice the positive elements and those elements that need improvement.

The slide shows a “Radar” chart (also known as the “spider chart”) where there are as many axes as there are categories.

The categories representing the elements of the information security management system (the ISO/IEC 27001 standard), leave all the central point in a classical time sequence. They are shown around the chart (X axis). The values of the series (in this case, the values assigned by the analysis of process maturity) are displayed within the canvas (Y axis) on a scale of zero to five.

The presentation in concentric circles may vary depending on whether line segments (lines) connect the data series, forming a “spider web” whose form will vary depending on the number of sets and assigned values to each category of the chart.

The advantages of this representation include:

- There may be several series in a single graph.
- It is used in various domains to compare a series against another, as superimposed “spider webs” give a good overview of a situation.

Exercise 5: Gap analysis

By referring to the case study, rate the maturity level of the process of accessing customer data stored in the blockchain. In addition, provide recommendations for the improvement of the process, so that the company fulfills the requirements of control A.9 of ISO/IEC 27001 on access control.

Duration of the exercise: 30 minutes

Comments: 15 minutes

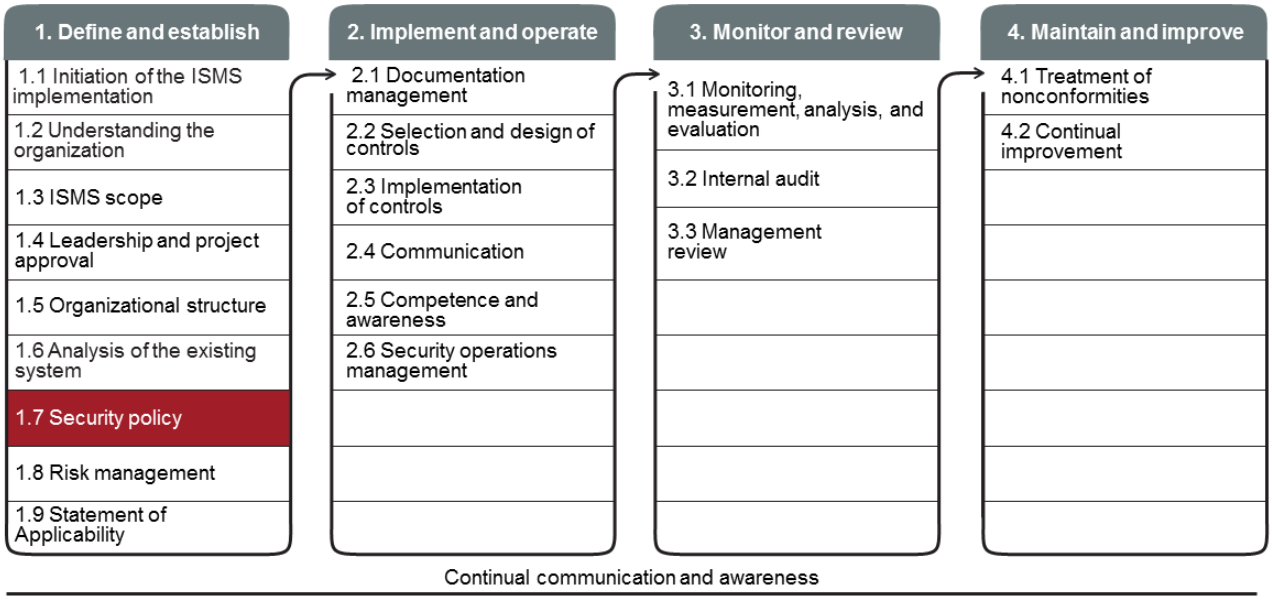
1. **What is a gap analysis?**
   A. A technique used to determine the steps to move from a current state to a desired future state
   B. A technique used to determine the ways in which a process might potentially fail, with the objective of eliminating the likelihood of such a failure
   C. A technique 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

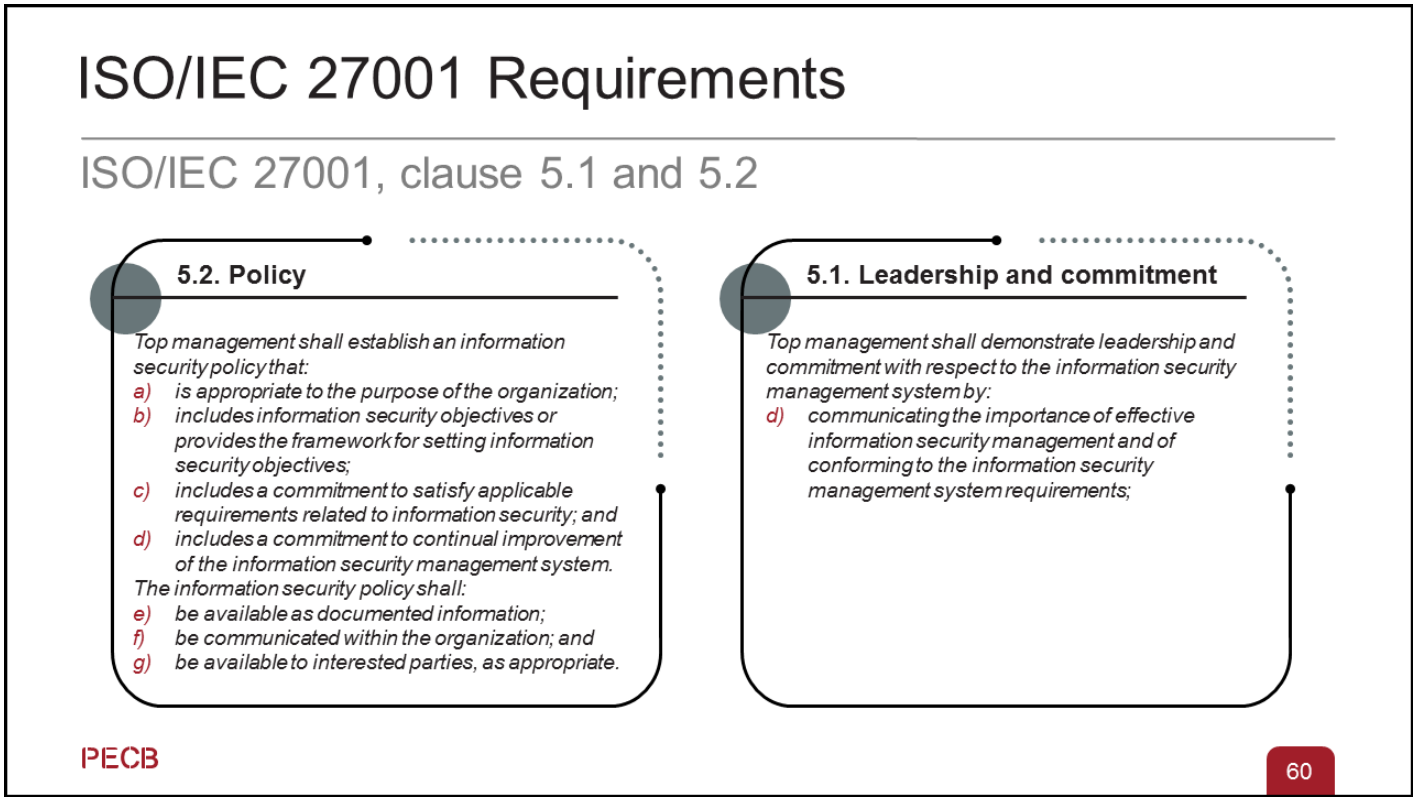
Section summary

1. In order to define the steps to move from a current state to a desired future state, the gap analysis is conducted.
2. The most commonly used information gathering procedures are: observation, questionnaires, interviews, documented information review, and scan tools.
3. ISO/IEC 21827 aims to improve the software development process based on the CMM (Capability Maturity Model).
4. There are six maturity levels that are helpful in setting targets for processes and security controls: nonexistent, initial, managed, defined, quantitatively managed, and optimized.

This section provides information that will help the participant gain knowledge on the information security policies, which include types of policies, creation of policy models, management approval, publication and dissemination, training, communication and awareness, control, evaluation, and review.

1.7 Security Policy





In order to comply with the requirements of ISO/IEC 27001, the organization should:

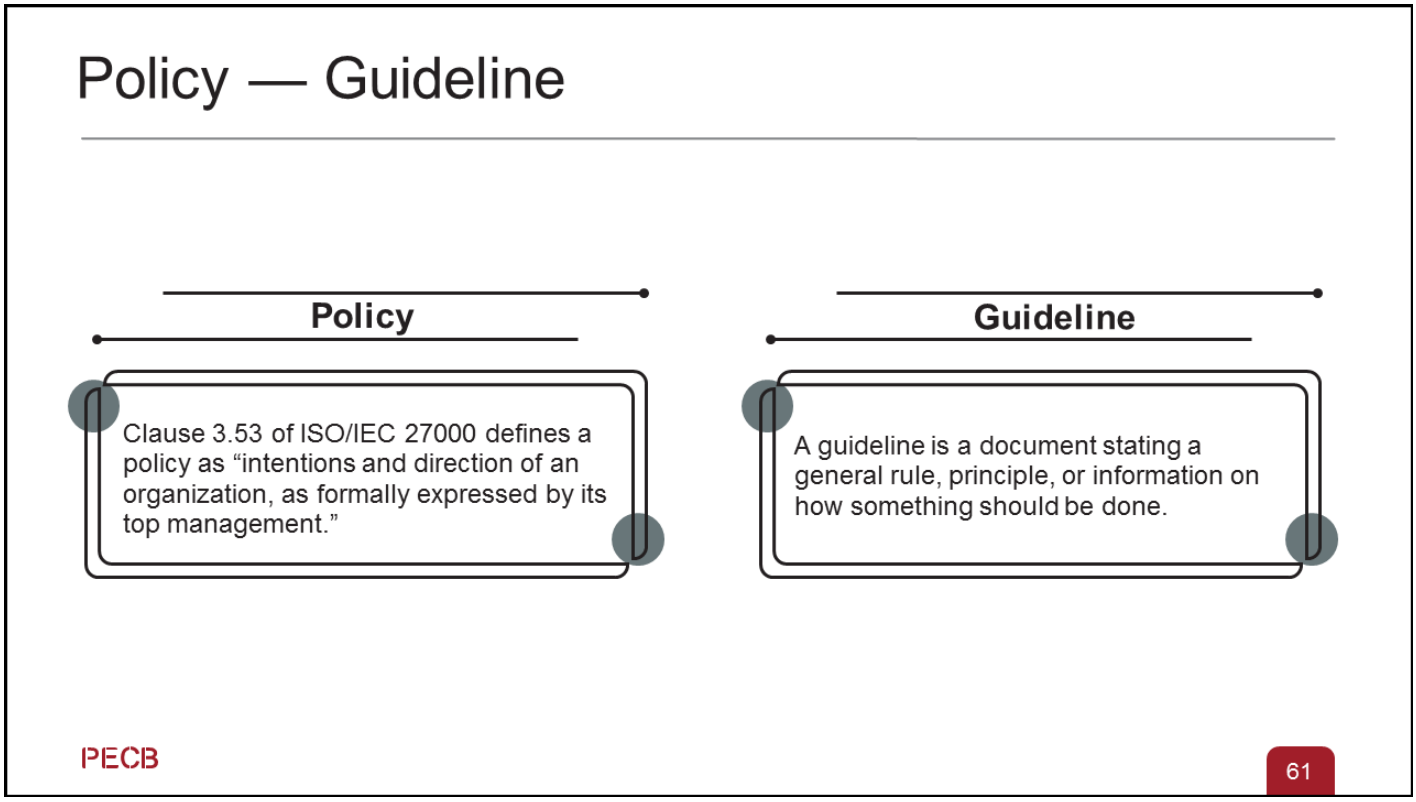
1. Publish the information security policy
2. Communicate the policy to the relevant interested parties

ISO/IEC 27003, clause 5.2 Policy (cont'd)

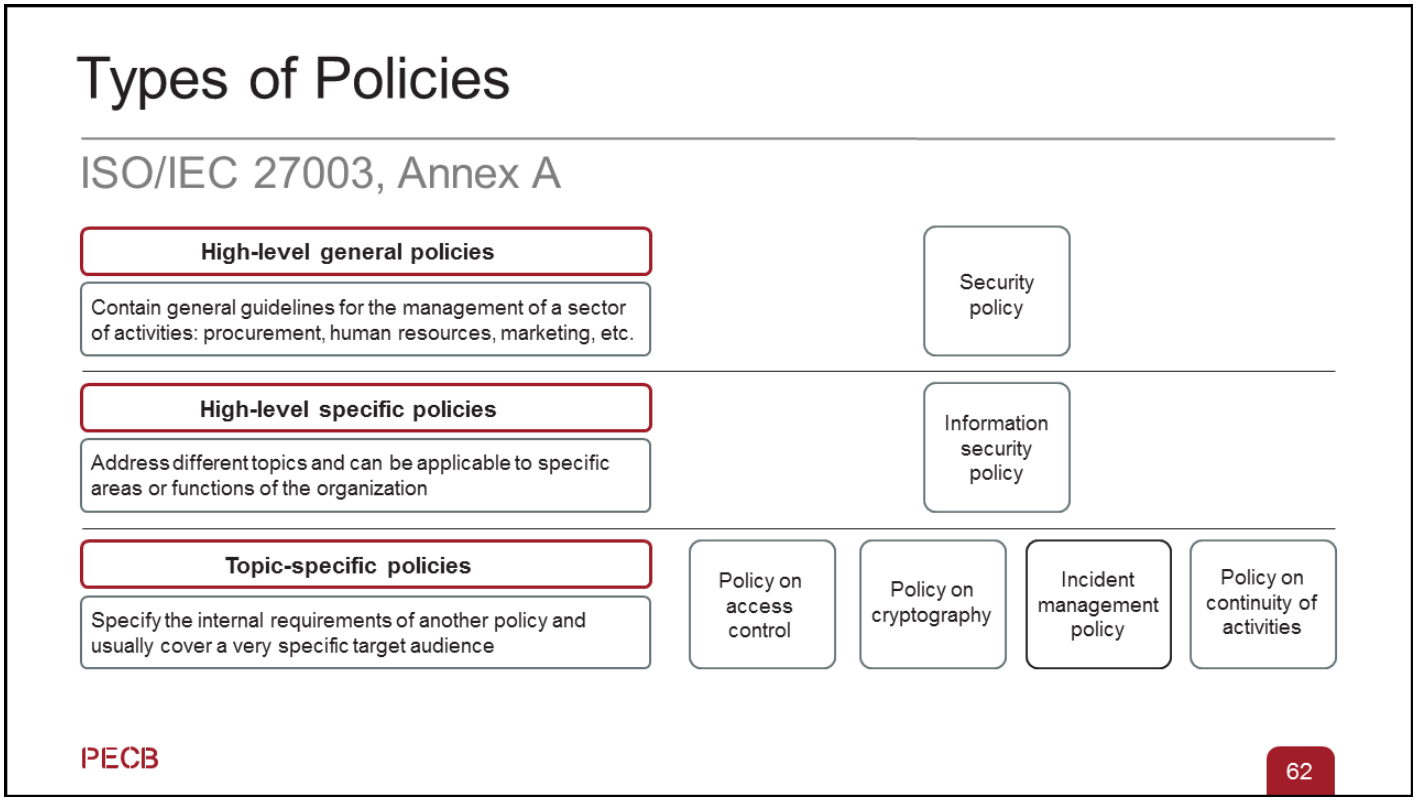
The information security policy should reflect the organization's business situation, culture, issues and concerns relating to information security. The extent of the information security policy should be in accordance with the purpose and culture of the organization and should seek a balance between ease of reading and completeness. It is important that users of the policy can identify themselves with the strategic direction of the policy.

Top management should decide to which interested parties the policy should be communicated. The information security policy can be written in such a way that it is possible to communicate it to relevant external interested parties outside of the organization. Examples of such external interested parties are customers, suppliers, contractors, subcontractors and regulators. If the information security policy is made available to external interested parties, it should not include confidential information.

The information security policy should be available as documented information. The requirements in ISO/IEC 27001 do not imply any specific form for this documented information, and therefore is up to the organization to decide what form is most appropriate. If the organization has a standard template for policies, the form of the information security policy should use this template.



Note on terminology:
It is important to not confuse “policy” with a direction, procedure, guideline, or other types of documented information. The main goal of a policy is to provide guidance on a particular topic. A detailed explanation on the drafting of other documented information is provided in several sections of Day 3 of this training course.

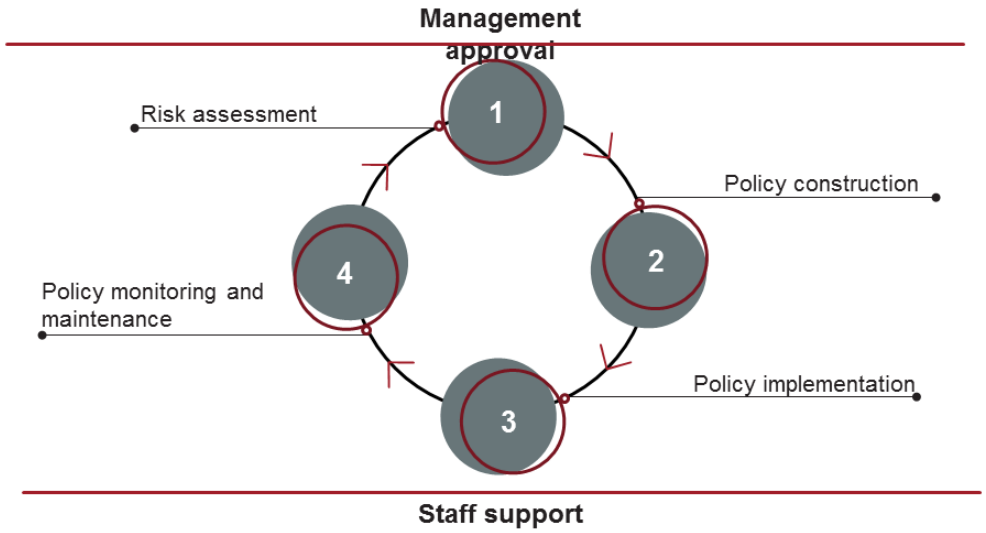


There are generally three levels of policies within an organization:

1. **High-level general policies** define a general framework within which the information security will be provided and the general objectives to ensure business continuity and to limit or prevent the potential damage of assets to an acceptable level and consequently limit the potential consequences of security incidents.
2. **High-level specific policies** define a subset of rules and practices still fairly general but that are related to a specific area. They are mostly subordinate to the high-level general policies.
    - **Note:** Both types of policies are usually subject to a review process because of their sensitive nature with regard to the functional strategy of the organization they are supposed to support.
3. **Topic-specific policies** are policies that support the information security policy (i.e., high-level specific policy). These policies determine how to proceed in order to ensure information security in specific application areas. Examples include the following policies: security policy for access rights to information and technology infrastructure, policy on internet use, policy on archiving and destruction of documents, etc.
    - **Note:** Some of these topic-specific policies are independent, while others are attached to and dependent on another policy. For example, an organization may have a (general) security policy which is complemented by a (topic-specific) policy on physical security and another on information security. In turn, the information security policy may be a reference for the publication of specific policies as the policy on access control.

Information Security Policies

Information security policy development life cycle



PECB

63

The policy development life cycle is an iterative process. The information security policy development life cycle usually comprises four phases: risk assessment, policy construction, policy implementation, and policy monitoring and maintenance. The management's approval and staff support are needed throughout the entire life cycle.

It is the responsibility of the top management to approve the policies and communicate them to the relevant interested parties.

Phase 1: Risk assessment

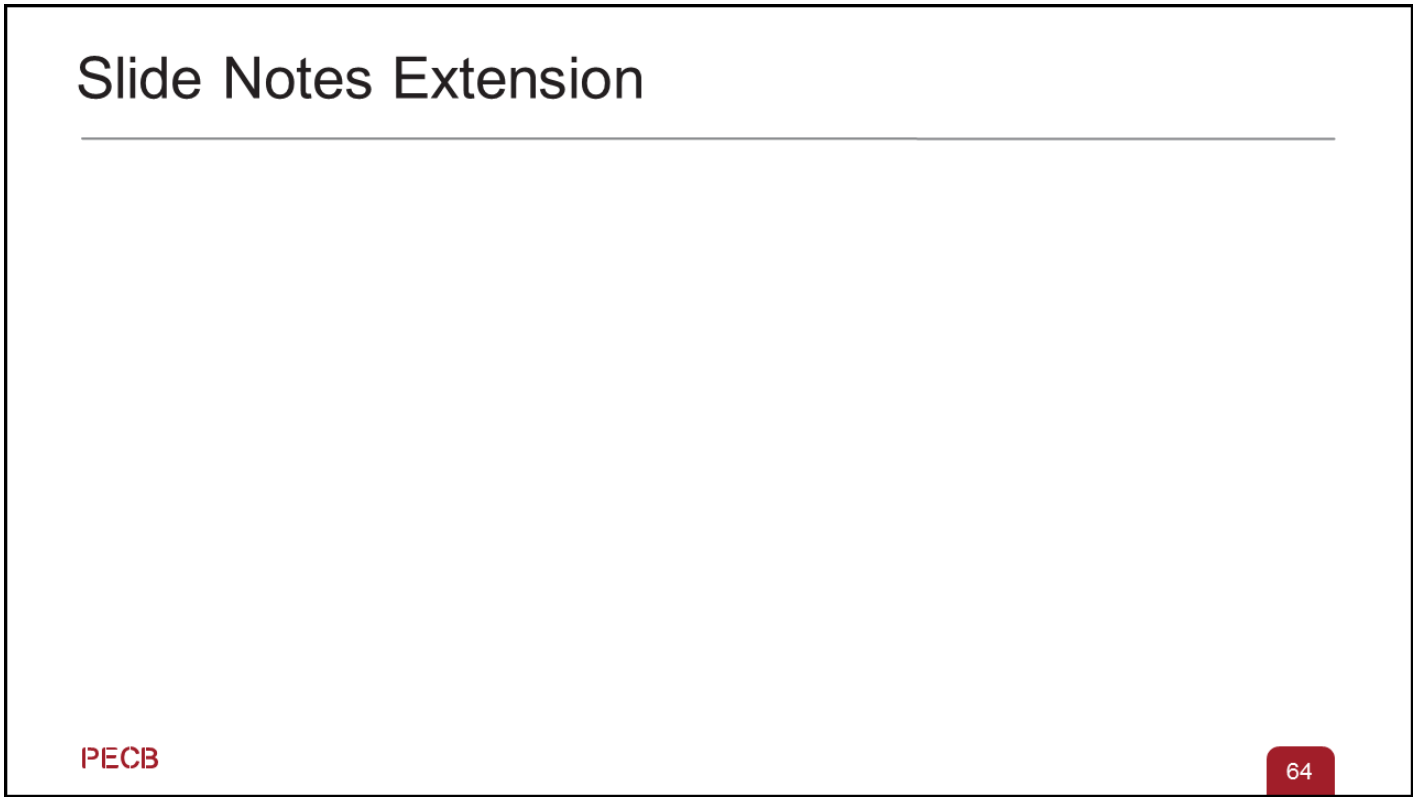
In this phase, the assets that should be protected and the potential threats and vulnerabilities to these assets are identified. The results will enable the top management to evaluate the costs and benefits of implementing controls to reduce risks to an acceptance level. If the expenses are within the budget, the organization initiates the policy construction; otherwise, risk mitigation strategies need to be reviewed or the budget should be increased.

Phase 2: Policy construction

In this phase, the information security policy is developed based on the findings and recommendations of the risk assessment phase, business strategies of the organization, and the applicable legal requirements. Drafting the information security policy involves selecting control objectives to be achieved in the organization. The policy should then be reviewed and approved by the top management. A communication plan is needed during the policy construction phase in order to inform and receive feedback from relevant employees.

Phase 3: Policy implementation

This phase requires a detailed implementation plan on how to define security and control requirements, how to assign security responsibilities, how to perform tests, and how to conduct training and awareness sessions. The top management should ensure that the information security policy is available and accessible by all employees.

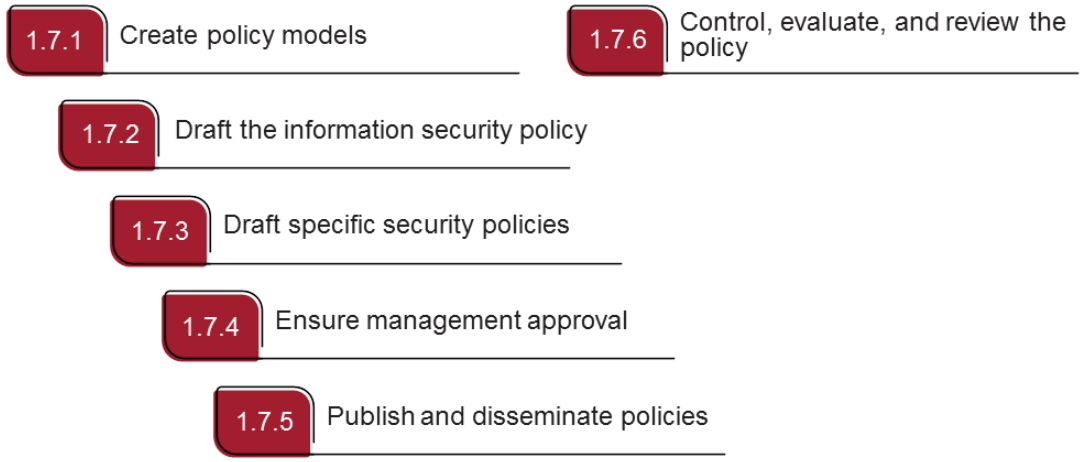


Phase 4: Policy monitoring and maintenance
The two main activities of this phase are monitoring and maintenance. Monitoring mechanisms should be put in place to ensure that the information security policy is enforced in the organization and all employees comply with its requirements. Maintenance is concerned with the review of security incidents, business strategies, legal requirements, and any request for policy changes.

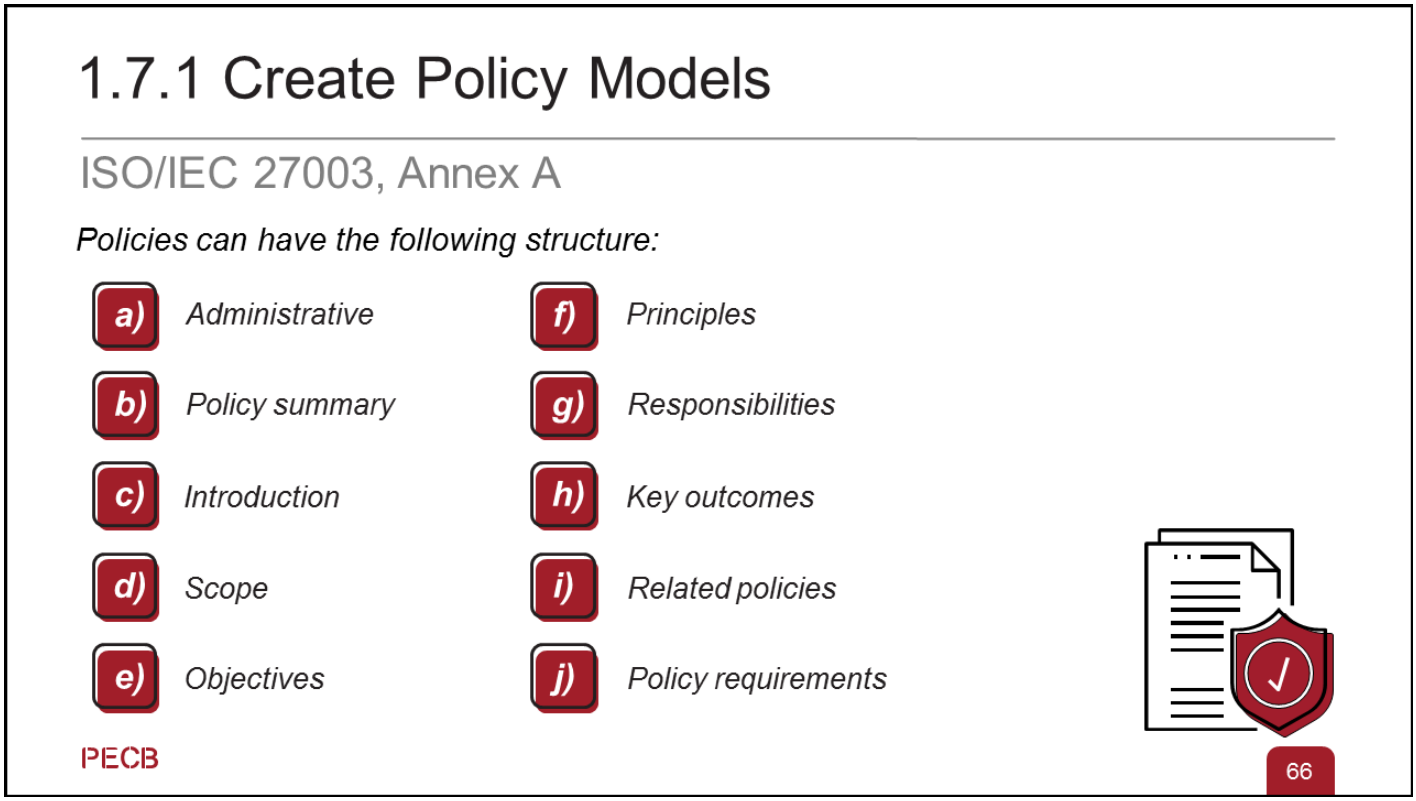
Source: Tuyikeze, Tite, and Dalenca Pottas. "An Information Security Policy Development Life Cycle." *SAISMC 2010.*

1.7 Security Policy

List of activities



PECB



ISO/IEC 27003, Annex A Policy framework (cont'd)

Policies can have the following structure:

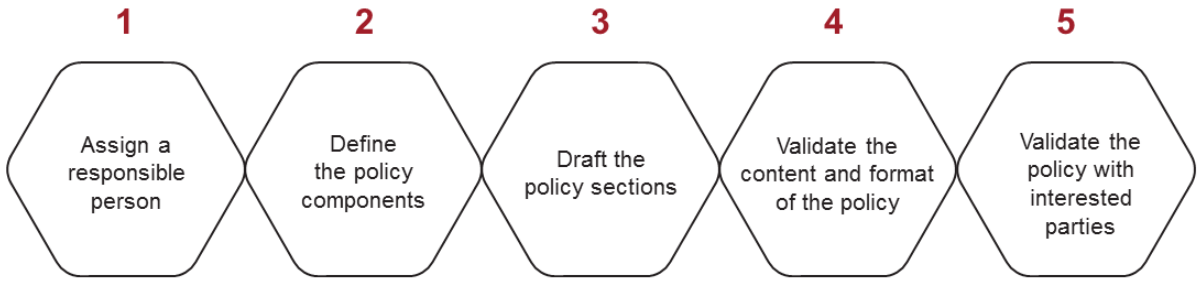
a. *Administrative – policy title, version, publication/validity dates, change history, owner(s) and approver(s), classification, intended audience etc.;*
b. *Policy summary – a one or two sentence overview. (This can sometimes be merged with the introduction.);*
c. *Introduction – a brief explanation of the topic of the policy;*
d. *Scope – describes those parts or activities of an organization that are affected by the policy. If relevant, the scope clause lists other policies that are supported by the policy;*
e. *Objectives – describes the intent of the policy;*
f. *Principles – describes the rules concerning actions and decisions for achieving the objectives. In some cases, it can be useful to identify the key processes associated with the topic of the policy and then the rules for operating the processes;*
g. *Responsibilities – describes who is responsible for actions to meet the requirements of the policy. In some cases, this can include a description of organizational arrangements as well as the responsibilities and authority of persons with designated roles;*
h. *Key outcomes – describes the business outcomes if the objectives are met. In some cases, this can be merged with the objectives;*
i. *Related policies – describes other policies relevant to the achievement of the objectives, usually by providing additional detail concerning specific topics; and*
j. *Policy requirements – describes the detailed requirements of the policy.*

Other subjects may be added to the model of the policy of an organization. The following are some of them:

- **Definitions** contains a list of terms and definitions used in the policy that may be unclear to the reader.
- **Penalties** contains a description of the list of possible sanctions if a user violates a policy (e.g., any user who violates this policy is subject to disciplinary action up to and including dismissal, including criminal prosecution).

Policy Drafting Process

General process



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

PECB

67

The typical steps of the process of drafting a policy are as follows:

1. **Assign a responsible person:** A person should be assigned as responsible for developing, reviewing, and evaluating the policy. Usually, the chief information security officer (CISO) is given the responsibility of managing and monitoring the information security policy and detailed policies directly related to a theme of security. On the other hand, many of the policies that can be included in the ISMS are usually the responsibility of other managers, e.g., the policy of purchasing IT equipment, the physical security policy.
2. **Define the policy components:** The person responsible for drafting the policy provides a list of all topics to be addressed in the policy. As a minimum, the policy must cover the requirements of ISO/IEC 27001 clause 5.2 Policy.
3. **Draft the policy sections:** The person responsible for drafting the policy writes the different sections of the policy. The statements must be written in simple but accurate language so that the policy is understood by all the parties affected by its publication. Furthermore, the inclusion of operational specifications or references to specific products must be avoided in the policy. The policy should address the “Why” and especially the “What,” not the “How.” The latter will be detailed in the procedures.
4. **Validate the content and format of the policy:** The person responsible for drafting the policy has to validate the contents so as to ensure that the policy complies with the requirements of ISO/IEC 27001 and other policies of the organization. For example, it would be contradictory to publish a policy permitting the monitoring and screening of all employee communication if an organizational policy, with respect to privacy provisions, prohibits this. In terms of format, the person must assure that the policy meets the requirements of clause 7.5.3 Control of documented information of ISO/IEC 27001.

Slide Notes Extension

PECB

68

5.Validate the policy with interested parties: To ensure the support and understanding of the policy, it is good practice to collect comments from employees, managers, and other parties concerned with the policy or affected by it in one way or another. Experience shows that the validation stage of a policy can be long depending on the size of the organization, the organizational structure, and diversity of the involved parties. The inclusion of these elements has a direct impact on the validation time that may sometimes take longer than the development of the policy itself.

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.

PECB

69

The information security policy is usually defined by the scope of the ISMS itself.

This policy includes:

- A framework that allows to define objectives and establish a direction and policy guidelines for the management of information security
- A consideration of legal and regulatory obligations imposed on the organization as well as other commitments
- Alignment of the information security risk management with the strategic objectives of the organization
- A list of criteria to evaluate information security risks
- Formal approval by the management for the abovementioned measures

Although the information security policy model presented in the slide is applicable to most organizations, it should, however, be adapted to the specific conditions of each organization.

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

PECB

73

ISO/IEC 27002, clause 5.1.1 Policies for information security

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

1.7.5 Publish and Disseminate Policies

Main modes of communication

Intranet

Meeting

Distribution of hard copies

New employee orientation session

PECB

74

During the initial publication of the security policy of the organization, it is good practice (but not required) to have the security policy signed by all employees of the organization including the management team. The original signed form should be kept by the Human Resources Department staff or any other body that is responsible.

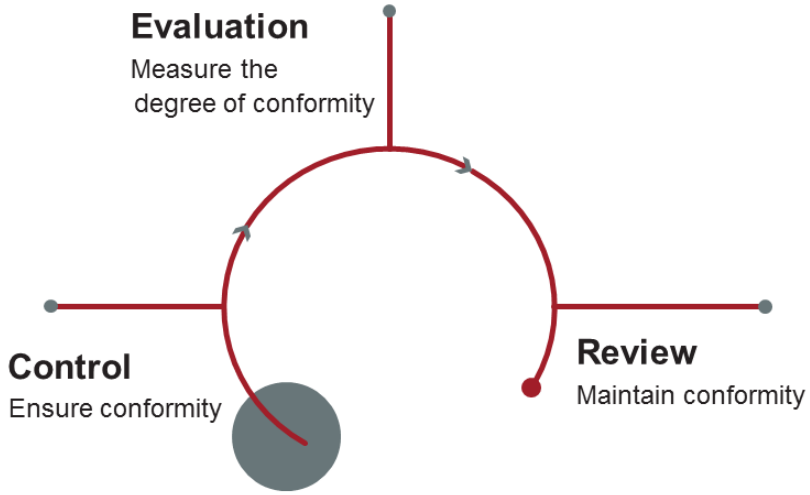
If the signing of the policy is not done, the organization should be sure to be able to demonstrate that members of the organization understand and respect the policy. For example, this can be achieved by participating in a training session.

ISO/IEC 27002, clause 5.1.1. Policies for information security

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme".

Training and awareness plans will be discussed in the section 19 of Day 3 of this training course.

1.7.6 Control, Evaluate, and Review the Policy



PECB

75

The control, evaluation, and review of the information security policy facilitate the initiation of a continual improvement process. By regularly reviewing the information security policy, the organization ensures consistency with business requirements and legal constraints.

Control: The management must ensure that the information security policy is respected in day-to-day operations in the organization. In addition, the management must provide a formal disciplinary process for employees who violate the policy. The formal disciplinary process ensures a correct and fair treatment of employees suspected of violating the policy. The formal disciplinary process should provide for a gradual response that takes into consideration factors such as the nature and severity of the breach and its impact on the business (ISO/IEC 27002, clause 7.2.3 *Disciplinary process*).

Evaluation: The organization must implement mechanisms for evaluating the effectiveness and enforcement of its information security policy.

Review: To ensure the relevance, adequacy, and effectiveness of the information security policy, the policy should be reviewed at predetermined intervals or when major changes occur. The emergence of new threats and vulnerabilities and the constantly changing technological environment are non-exhaustive examples of events that may affect, partly or in all, the operational nature of a security policy.

Exercise 6: Drafting a security policy

Following some recent information security incidents in the company, *e-Scooter* has decided to establish a policy to control the use of all communication devices (e.g., smartphones, tablets, and other forms of portable communication devices) in the workplace.

You are assigned the task of drafting a smartphone usage policy. In order to accomplish this, complete the provided template.

Duration of the exercise: 20 minutes

Comments: 15 minutes

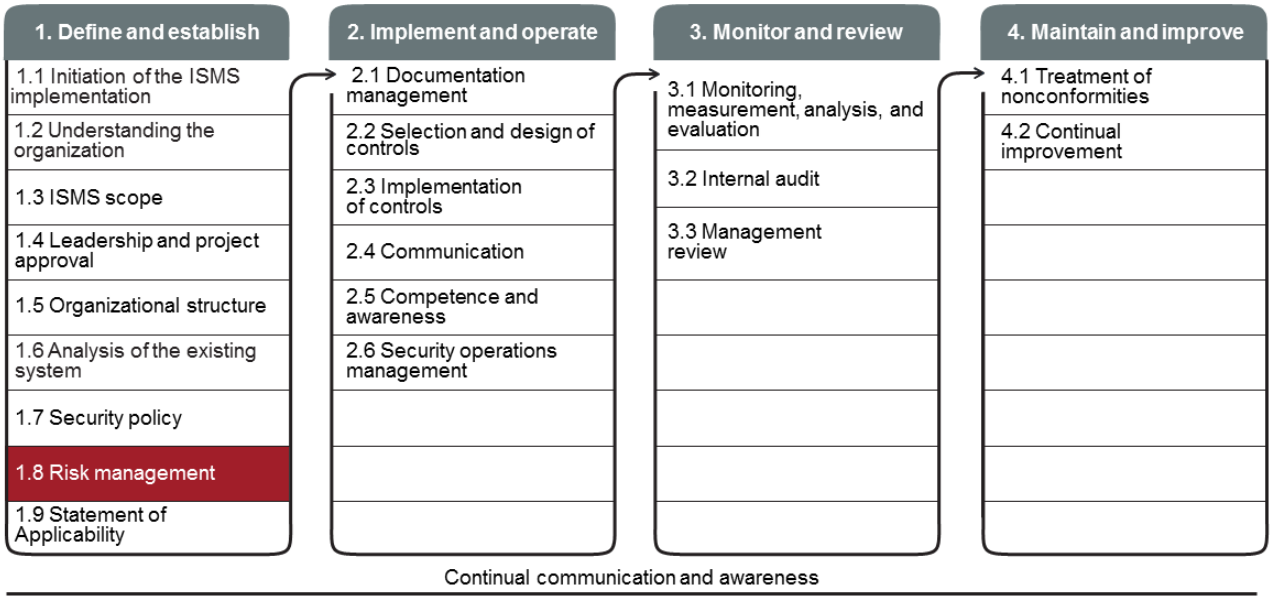
1. **Who shall establish the information security policy according to ISO/IEC 27001?**
   A. The top management
   B. External interested parties
   C. The information security manager
2. **What is the difference between a policy and a guideline?**
   A. A policy states the intentions and direction of 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

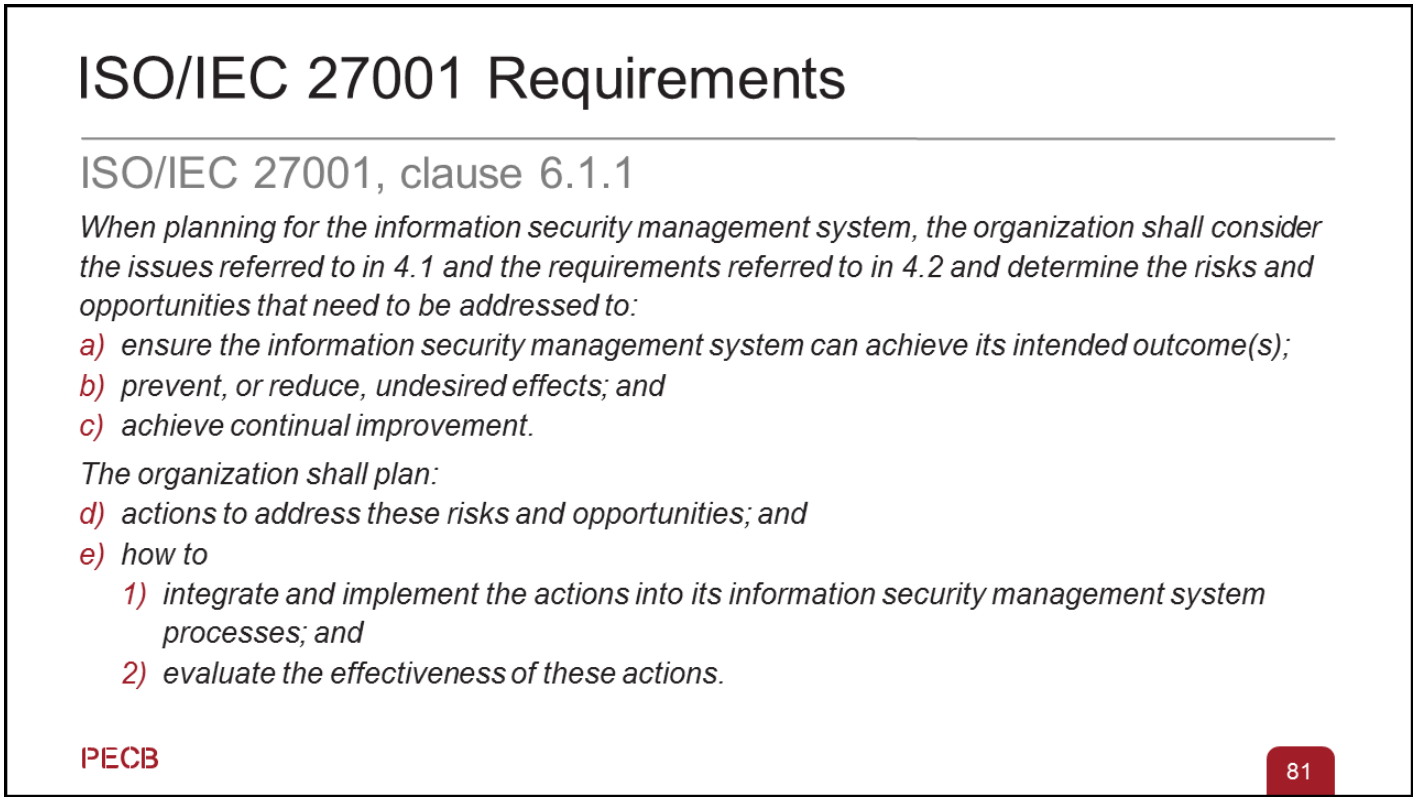
Section summary

- There are generally three levels of policies within an organization: high–level general policies, high–level topic–specific policies, and detailed policies.
- The drafting process of a policy consists of the following steps: assigning a responsible person, deciding on the policy components, drafting the policy sections, and validating the contents and the format of the policy.
- By frequently reviewing the information security policy, the organization guarantees consistency in business requirements and legal constraints.

This section provides information that will help the participant gain knowledge on the risk management process, which includes risk identification, risk estimation, risk evaluation, and risk treatment.

1.8 Risk Management Process





An organization wishing to comply with ISO/IEC 27001 shall at least:

1. Select and define a risk assessment methodology
2. Demonstrate that the selected methodology will provide comparable and reproducible results
3. Define criteria for accepting risks and identify acceptable levels of risk

ISO/IEC 27003, clause 6.1.1 General

The subdivision of requirements for addressing risks can be explained as follows:

- *it encourages compatibility with other management systems standards for those organizations that have integrated management systems for different aspects like quality, environment and information security;*
- *it requires that the organization defines and applies complete and detailed processes for information security risk assessment and treatment; and*
- *it emphasizes that information security risk management is the core element of an ISMS.*

NOTE The term "risk" is defined as the "effect of uncertainty on objectives".

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 6.1.2

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks;

d) analyses the information security risks;

e) evaluates the information security risks.

PECB

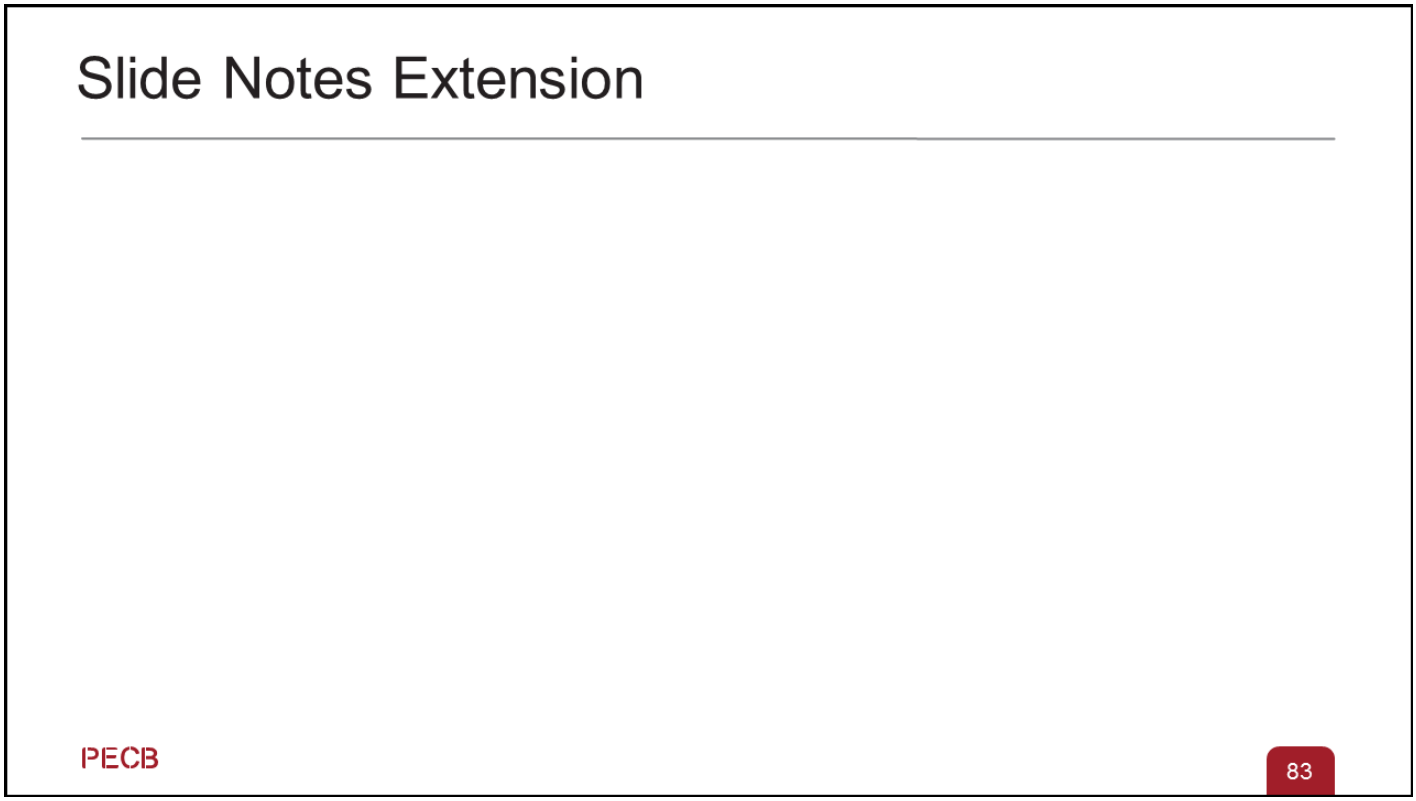
82

ISO/IEC 27001, clause 6.1.2 Information security risk assessment (cont'd)

The organization shall define and apply an information security risk assessment process that:

a. *establishes and maintains information security risk criteria that include:*
    1. *the risk acceptance criteria; and*
    2. *criteria for performing information security risk assessments;*
b. *ensures that repeated information security risk assessments produce consistent, valid and comparable results;*
c. *identifies the information security risks:*
    1. *apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and*
    2. *identify the risk owners;*
d. *analyses the information security risks:*
    1. *assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;*
    2. *assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and*
    3. *determine the levels of risk;*
e. *evaluates the information security risks:*
    1. *compare the results of risk analysis with the risk criteria established in 6.1.2 a); and*
    2. *prioritize the analysed risks for risk treatment.*

The organization shall retain documented information about the information security risk assessment process.



ISO/IEC 27003, clause 6.1.2 Information security risk assessment

Guidance on establishing risk criteria (6.1.2 a))

The information security risk criteria should be established considering the context of the organization and requirements of interested parties and should be defined in accordance with top management's risk preferences and risk perceptions on one hand and should allow for a feasible and appropriate risk management process on the other hand.

After establishing criteria for assessing consequences and likelihoods of information security risks, the organization should also establish a method for combining them in order to determine a level of risk. Consequences and likelihoods may be expressed in a qualitative, quantitative or semi-quantitative manner.

Risk acceptance criteria relates to risk assessment (in its evaluation phase, when the organization should understand if a risk is acceptable or not), and risk treatment activities (when the organization should understand if the proposed risk treatment is sufficient to reach an acceptable level of risk).

Guidance on producing consistent, valid and comparable assessment results (6.1.2 b))

The risk assessment process should be based on methods and tools designed in sufficient detail so that it leads to consistent, valid and comparable results.

Whatever the chosen method, the information security risk assessment process should ensure that:

- *all risks, at the needed level of detail, are considered;*
- *its results are consistent and reproducible (i.e. the identification of risks, their analysis and their evaluation can be understood by a third party and results are the same when different persons assess the risks in the same context); and*
- *the results of repeated risk assessments are comparable (i.e. it is possible to understand if the levels of risk are increased or decreased).*

Guidance on identification of information security risks (6.1.2 c))

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

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

Guidance on analysis of the information security risks (6.1.2 d))

Risk analysis has the objective to determine the level of the risk.

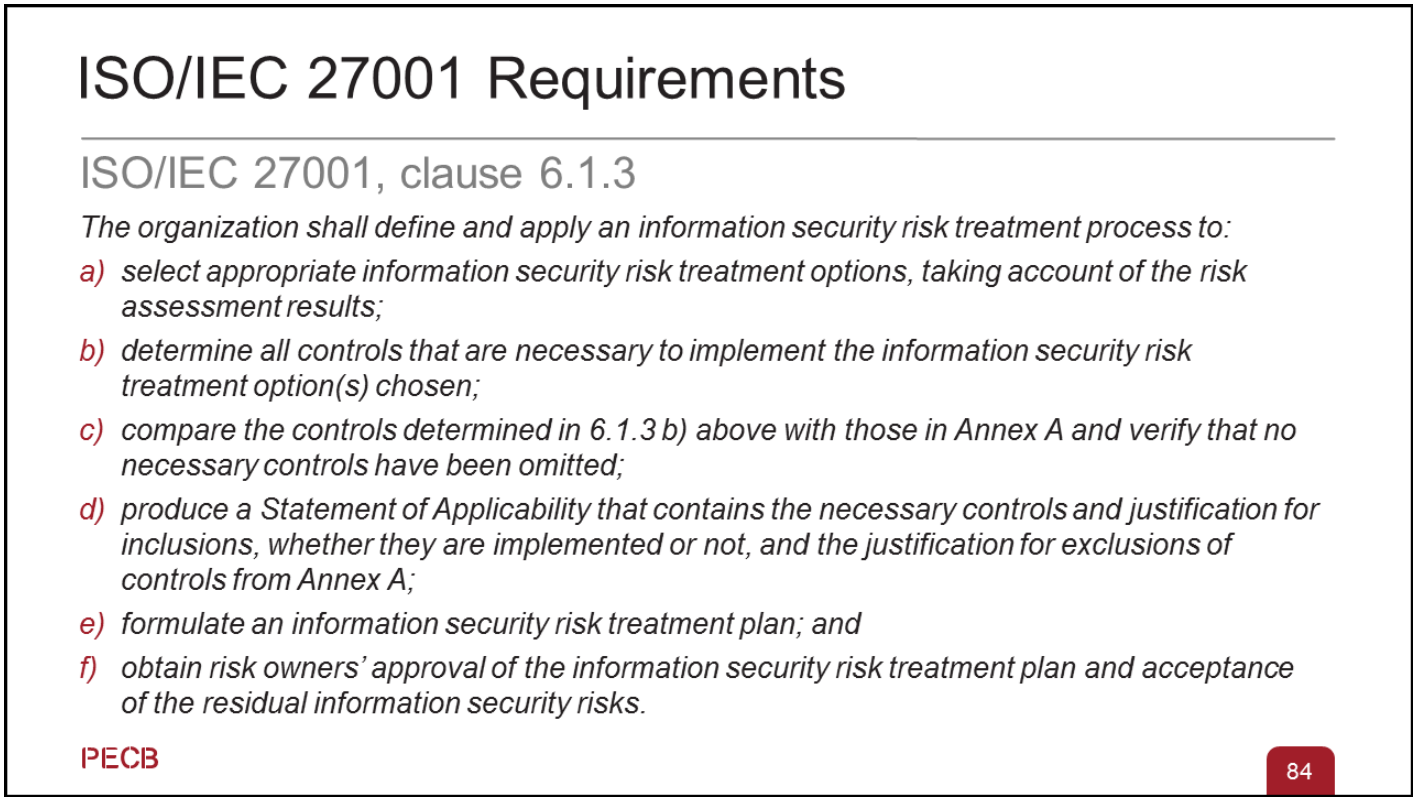
ISO 31000 is referenced in ISO/IEC 27001 as a general model. ISO/IEC 27001 requires that for each identified risk the risk analysis is based on assessing the consequences resulting from the risk and assessing the likelihood of those consequences occurring to determine a level of risk.

Techniques for risk analysis based on consequences and likelihood can be:

1. *qualitative, using a scale of qualifying attributes (e.g. high, medium, low);*
2. *quantitative, using a scale with numerical values (e.g. monetary cost, frequency or probability of occurrence); or*
3. *semi-quantitative, using qualitative scales with assigned values.*

Guidance on evaluation of the information security risks (6.1.2 e))

Evaluation of analysed risks involves using the organization's decision making processes to compare the assessed level of risk for each risk with the pre-determined acceptance criteria in order to determine the risk treatment options.



ISO/IEC 27003, clause 6.1.3 Information security risk treatment

Guidance on information security risk treatment options (6.1.3 a))

Risk treatment options are:

a. *avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk or by removing the risk source (e.g. closing an e-commerce portal);*
b. *taking additional risk or increasing risk in order to pursue a business opportunity (e.g. opening an e-commerce portal);*
c. *modifying the risk by changing the likelihood (e.g. reducing vulnerabilities) or the consequences (e.g. diversifying assets) or both;*
d. *sharing the risk with other parties by insurance, sub-contracting or risk financing; and*
e. *retaining the risk based on the risk acceptance criteria or by informed decision (e.g. maintaining the existing e-commerce portal as it is).*

Guidance on determining necessary controls (6.1.3 b))

Special attention should be given to the determination of the necessary information security controls. Any control should be determined based on information security risks previously assessed. If an organization has a poor information security risk assessment, it has a poor foundation for its choice of information security controls.

Guidance on comparing controls with those in ISO/IEC 27001:2013, Annex A (6.1.3 c))

ISO/IEC 27001:2013, Annex A contains a comprehensive list of control objectives and controls. Users of this document are directed to the generic representation of controls in ISO/IEC 27001:2013, Annex A to ensure that no necessary controls are overlooked.

Slide Notes Extension

PECB

85

ISO/IEC 27003, clause 6.1.3 Information security risk treatment (cont'd)

Guidance on producing a Statement of Applicability (SoA) (6.1.3 d))

The SoA contains:

- *all necessary controls and, for each control:*
  - *the justification for the control's inclusion; and*
  - *whether the control is implemented or not (e.g. fully implemented, in progress, not yet started); and*
- *the justification for excluding any of the controls in ISO/IEC 27001: 2013, Annex A.*

Guidance on formulating an information security risk treatment plan (6.1.3 e))

ISO/IEC 27001 does not specify a structure or content for the information security risk treatment plan. However, the plan should be formulated from the outputs of 6.1.3 a) to c). Thus the plan should document for each treated risk:

- *selected treatment option(s);*
- *necessary control(s); and*
- *implementation status.*

Other useful content can include:

- *risk owner(s); and*
- *expected residual risk after the implementation of actions.*

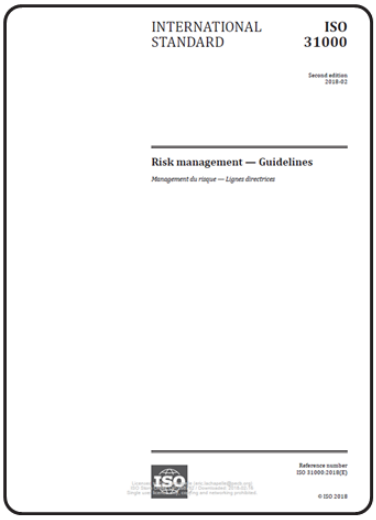
Guidance on obtaining risk owners' approval (6.1.3 f))

When the information security risk treatment plan is formulated, the organization should obtain the authorization from the risk owners. Such authorization should be based on defined risk acceptance criteria or justified concession if there is any deviance from them.

Through its management processes the organization should record the risk owner's acceptance of the residual risk and management approval of the plan.

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.



PECB

86

ISO 31000, clause 1 Scope

This document provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

This document provides a common approach to managing any type of risk and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

Given that ISO/IEC 27001 does not provide any specific method for risk management in the context of the ISMS, it is up to each organization to identify and select one that matches their context, business activities, and management and operational practices.

ISO/IEC 27005: Information Security Risk Management

- It is an adaptation of the ISO 31000 framework to information security.
- It is aligned with the requirements of ISO/IEC 27001.
- Each organization must choose a methodology for risk management that is appropriate to its context.

PECB

87

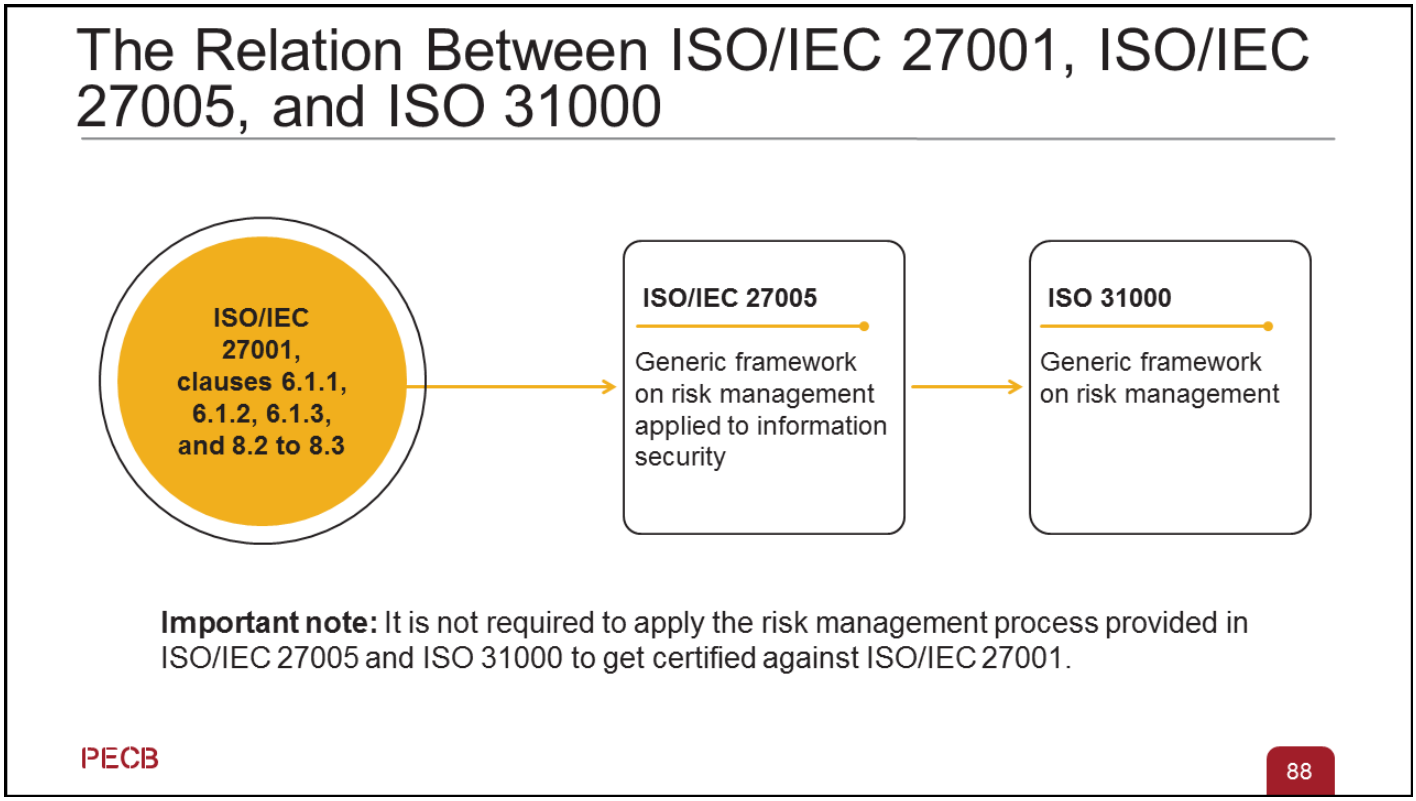
ISO/IEC 27005, clause 1 Scope

This document provides guidelines for information security risk management.

This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document.

This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.



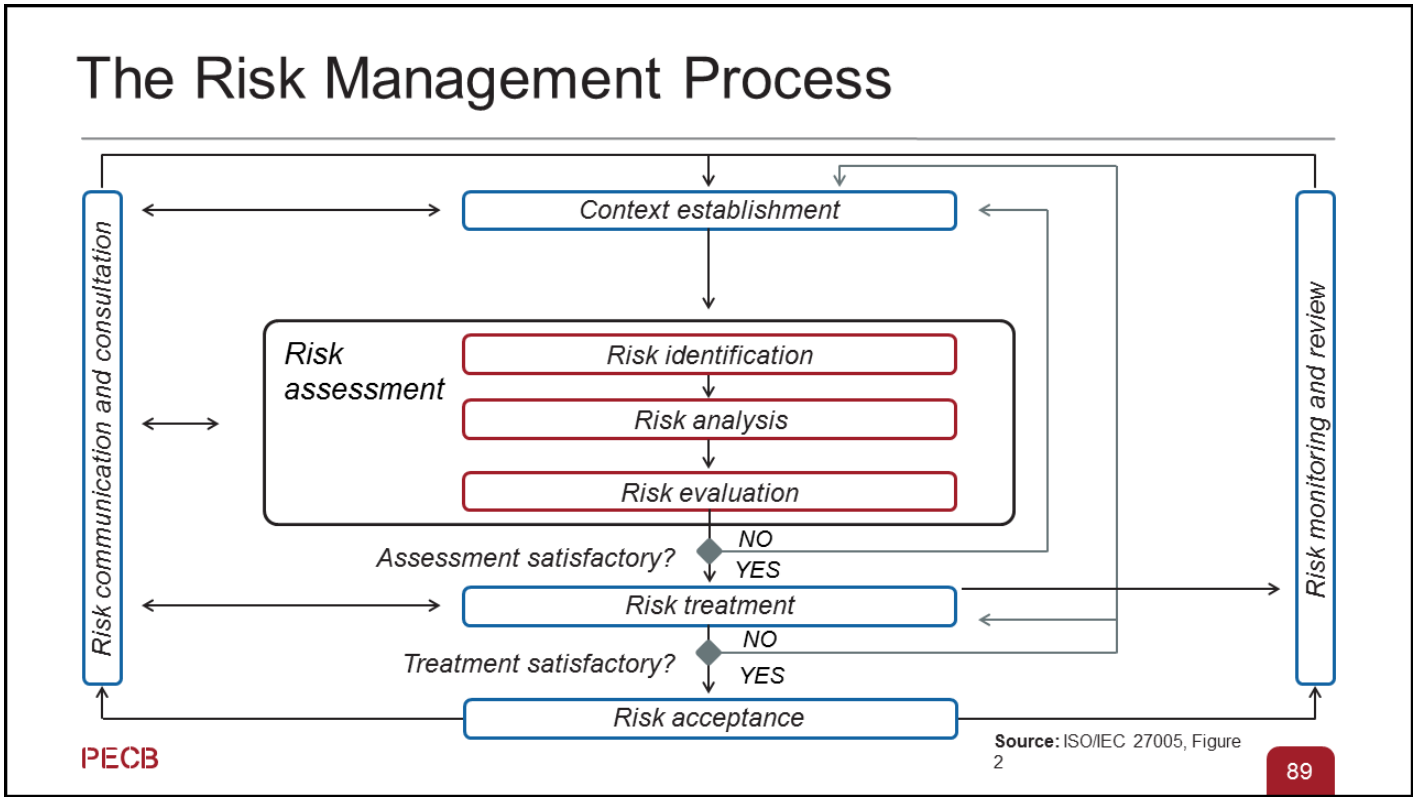
Based on the ISO 31000 framework, the ISO/IEC 27005 standard explains in detail how to conduct risk assessment and risk treatment in the context of information security. This is the implementation of the PDCA cycle (Plan, Do, Check, Act) for risk management as it is used in all standards of management systems. In this case, it can be easily connected to the corresponding clauses of ISO/IEC 27001 on risk management (clauses 6.1.2 and 6.1.3), ultimately leading to the certification of the organization.

ISO/IEC 27005, Introduction

This document provides guidelines for information security risk management in an organization. However, this document does not provide any specific method for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of an information security management system (ISMS), context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this document to implement the requirements of an ISMS. This document is based on the asset, threat and vulnerability risk identification method that is no longer required by ISO/IEC 27001. There are some other approaches that can be used.

This document does not contain direct guidance on the implementation of the ISMS requirements given in ISO/IEC 27001.

This document is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.



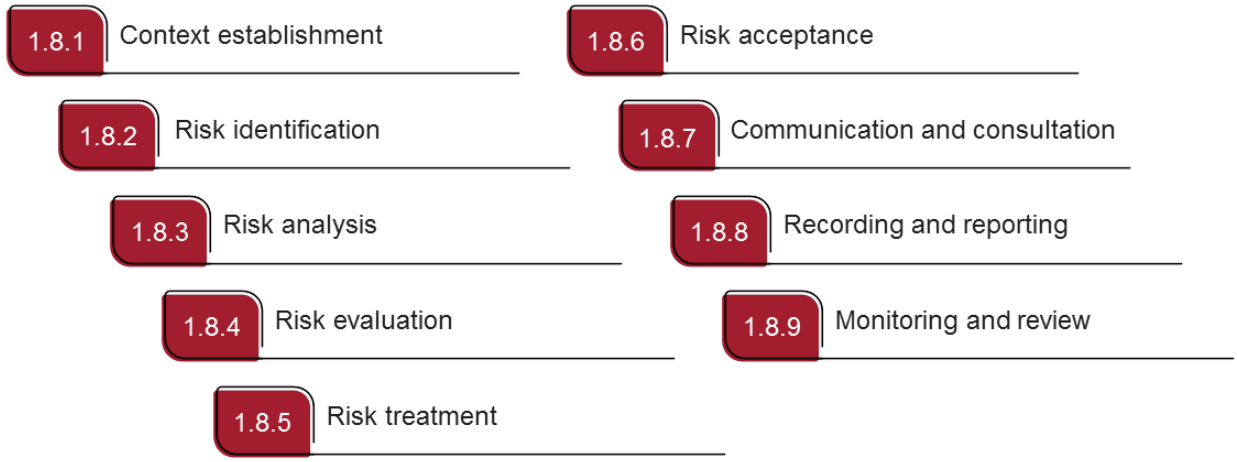
As illustrated in the figure, the risk management process should be iterative for risk assessment and risk treatment activities. If the risk assessment activities have provided sufficient evidence that the determined actions will reduce the risk to an acceptable level, the next step is to implement risk treatment options. However, if there is insufficient evidence to determine the risk level and if the risk treatment process appears to be unacceptable, a new iteration of risk assessment will be conducted on some or all the items of the application domain. If the risk treatment option is not satisfactory, but the context establishment and risk assessment are correct, a new iteration of risk treatment will be conducted; otherwise, a new iteration of context establishment will also have to be applied.

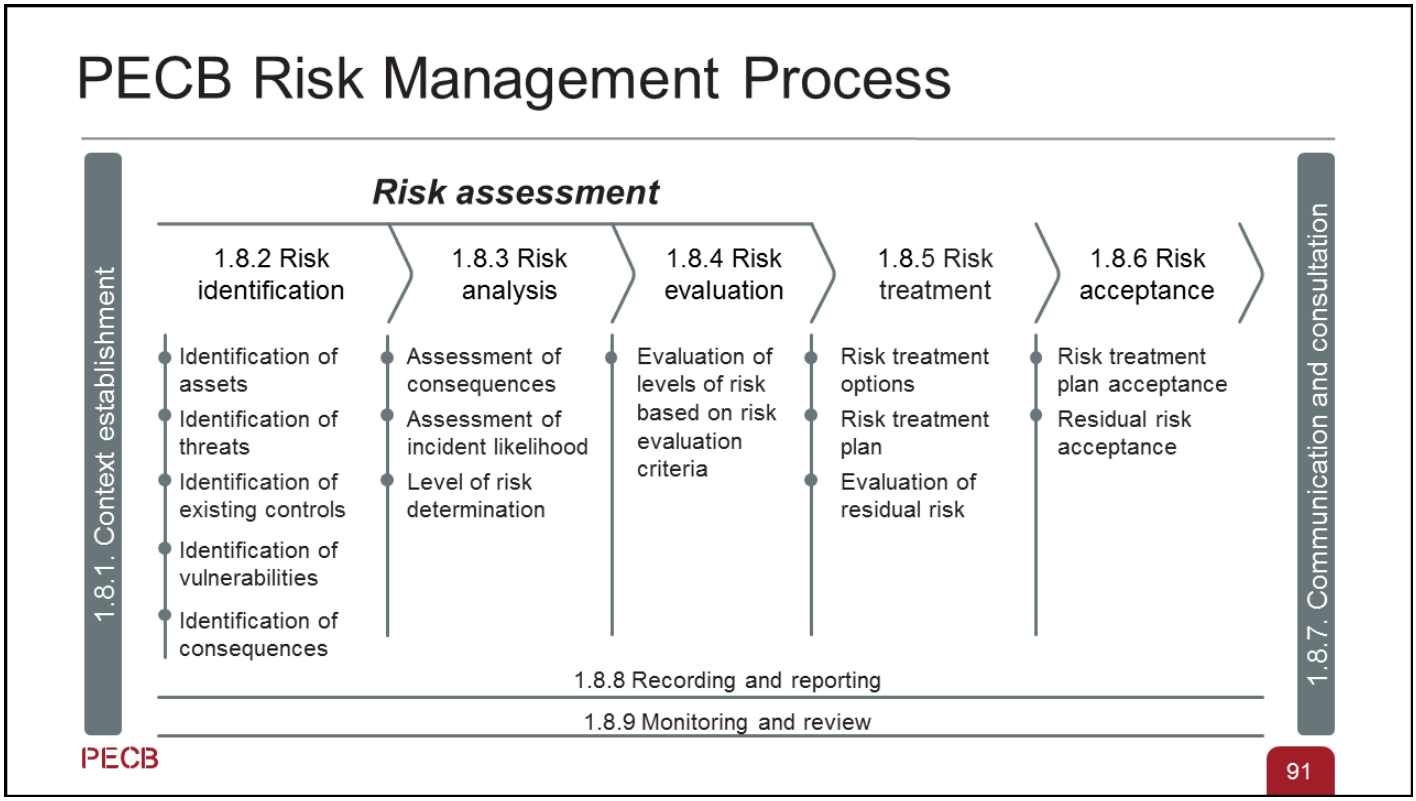
Whether the risk treatment is effective depends on the outcomes of the risk assessment. It is possible that risk treatment may not directly lead to an acceptable level of residual risk and, if that is the case, a new iteration of risk assessment should be undertaken.

Risk communication to the organization's interested parties and risk monitoring are ongoing activities.

1.8 Risk Management

List of activities





Important note: The risk management process is not an independent operating process (as could be understood by the diagram on the slide). ISO 31000 underlines the importance of integrating the risk management process into the organization's processes, activities, or systems.

To obtain more in-depth knowledge of the implementation and the management of an information security risk management program, it is recommended to take the PECB Certified ISO/IEC 27005 Risk Manager training course.

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.*

PECB

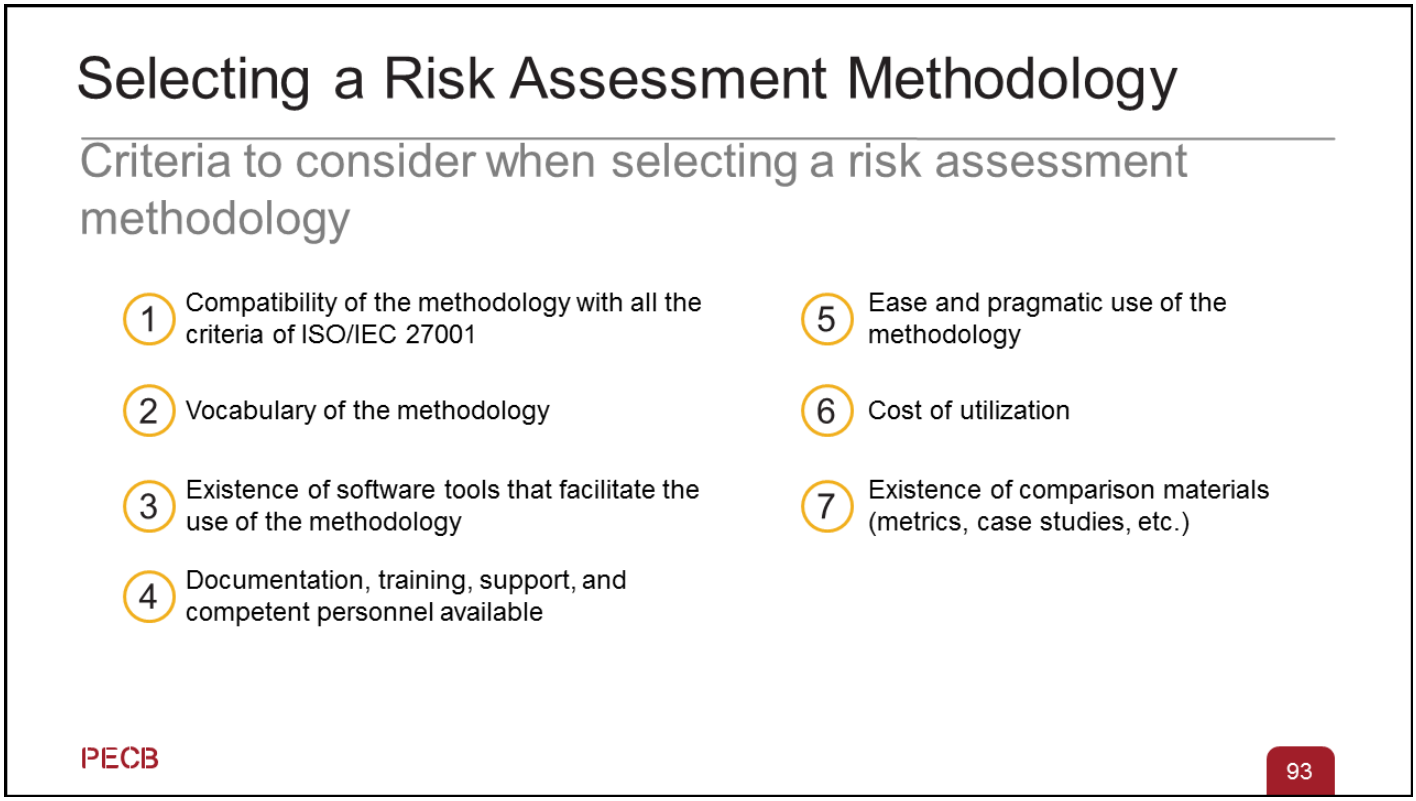
92

ISO/TR 31004, clause 3.3.3.2

On the basis of the evaluations described in 3.3.3.1, the organization should decide which aspects of the current risk management approach:

a. *could continue to be used in future (possibly extended to other types of decision making);*
b. *need amendment or enhancement;*
c. *no longer add value and should be discontinued.*

The organization should develop, document and communicate how it will be managing risk. The scale and content of the organization's internal standards, guidelines and models related to risk management should reflect organizational culture and context.

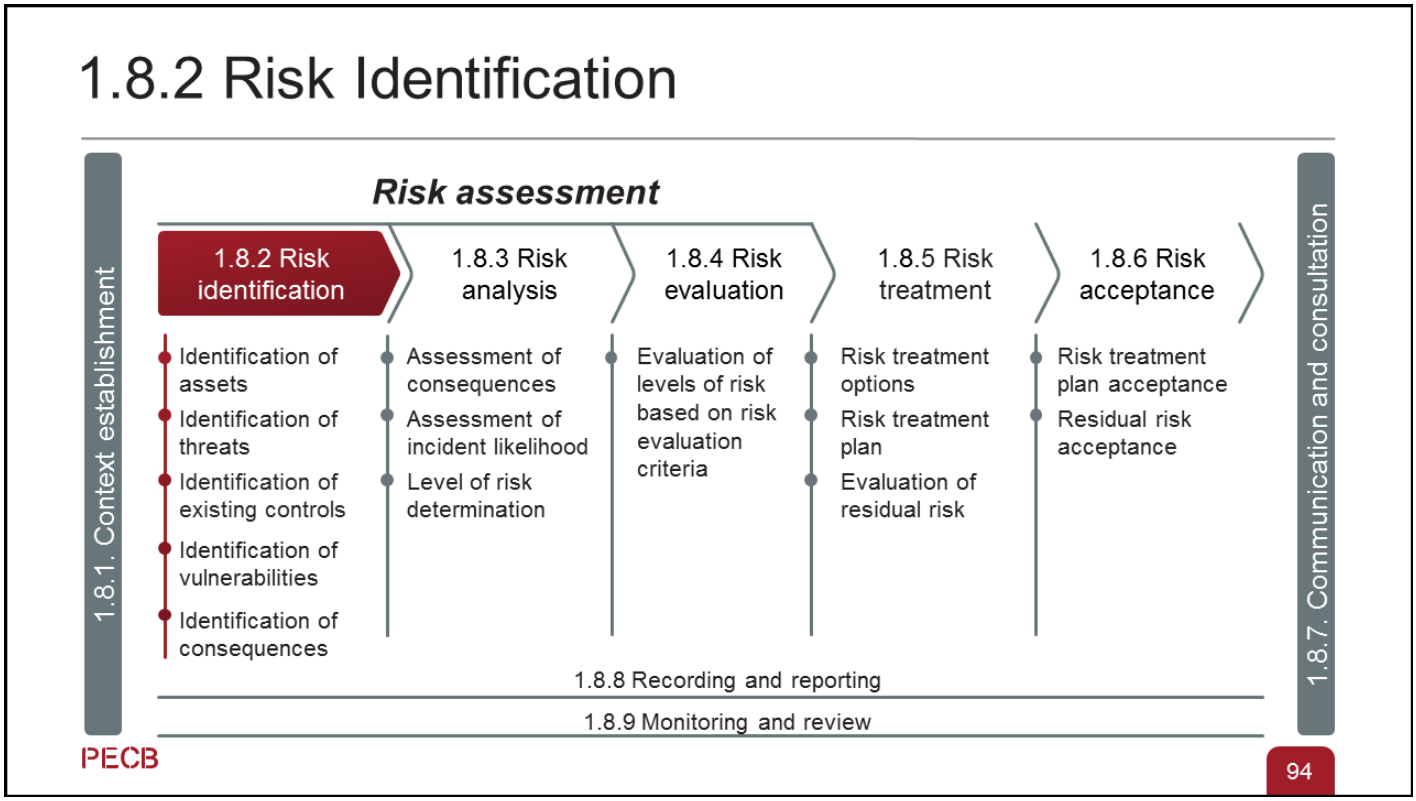


Any method of risk assessment that meets the minimum criteria of ISO/IEC 27001 is acceptable, even a method developed in-house (provided that it can produce comparable and reproducible results).

Any risk analysis at least should consider the evaluation criteria established by ISO/IEC 27001. The actions taken should produce desirable effects, prevent and reduce undesirable effects, and improve the organization's processes. In addition, the risk analysis should allow for the selection of the objective criteria for determining a level of acceptable risk.

When selecting a risk assessment methodology, you should ask:

- Have the potential impacts been identified?
- Is the probability of the occurrence of a potential impact evaluated?
- Can someone else use the same data and reach the same result?
- Can the process be repeated and give consistent results over time?
- Does the process take into account the analysis of the impact of changes?



ISO 31000, clause 6.4.2 Risk identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

The organization can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors, and the relationship between these factors, should be considered:

- *tangible and intangible sources of risk;*
- *causes and events;*
- *threats and opportunities;*
- *vulnerabilities and capabilities;*
- *changes in the external and internal context;*
- *indicators of emerging risks;*
- *the nature and value of assets and resources;*
- *consequences and their impact on objectives;*
- *limitations of knowledge and reliability of information;*
- *time-related factors;*
- *biases, assumptions and beliefs of those involved.*

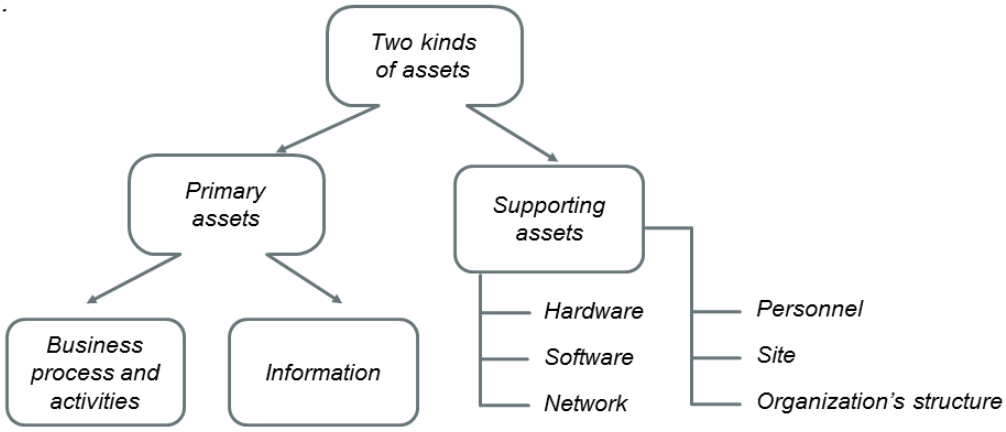
The organization should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

Identification of Assets

ISO/IEC 27005, clause 8.2.2 and Annex B.1.1

Definition of an asset

An asset is anything that has value to the organization and which, therefore, requires protection.



PECB

95

ISO/IEC 27005, clause 8.2.2 Identification of assets (cont'd)

Implementation guidance:

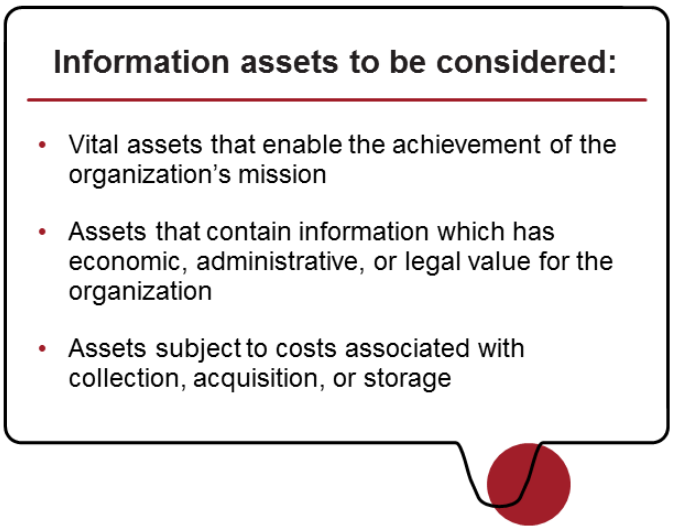
Asset identification should be performed at a suitable level of detail that provides sufficient information for the risk assessment. The level of detail used on the asset identification influences the overall amount of information collected during the risk assessment. The level can be refined in further iterations of the risk assessment.

An asset owner should be identified for each asset, to provide responsibility and accountability for the asset. The asset owner perhaps does not have property rights to the asset, but has responsibility for its production, development, maintenance, use and security as appropriate. The asset owner is often the most suitable person to determine the asset's value to the organization.

ISO/IEC 27005 divides assets into two broad categories:

1. **Primary assets:** Primary assets refer to assets that contribute to the risk analysis process. These assets include business processes and information.
2. **Supporting assets:** Supporting assets include hardware, software, computer networks, staff, sites, and organizational structures.

Identification of Information Assets



PECB

96

Organizations often own vital information assets. Nonetheless, not all assets are necessarily subject to analysis. The analysis should be focused on information assets that have economic, administrative, or legal value for the organization.

To facilitate the analysis, the information assets should be consolidated into groups having roughly the same features and the same classification level. For example, we can identify the accounting data as a single asset rather than dealing with subsets: payroll data, accounts receivable, accounts payable, bank statements, etc.

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

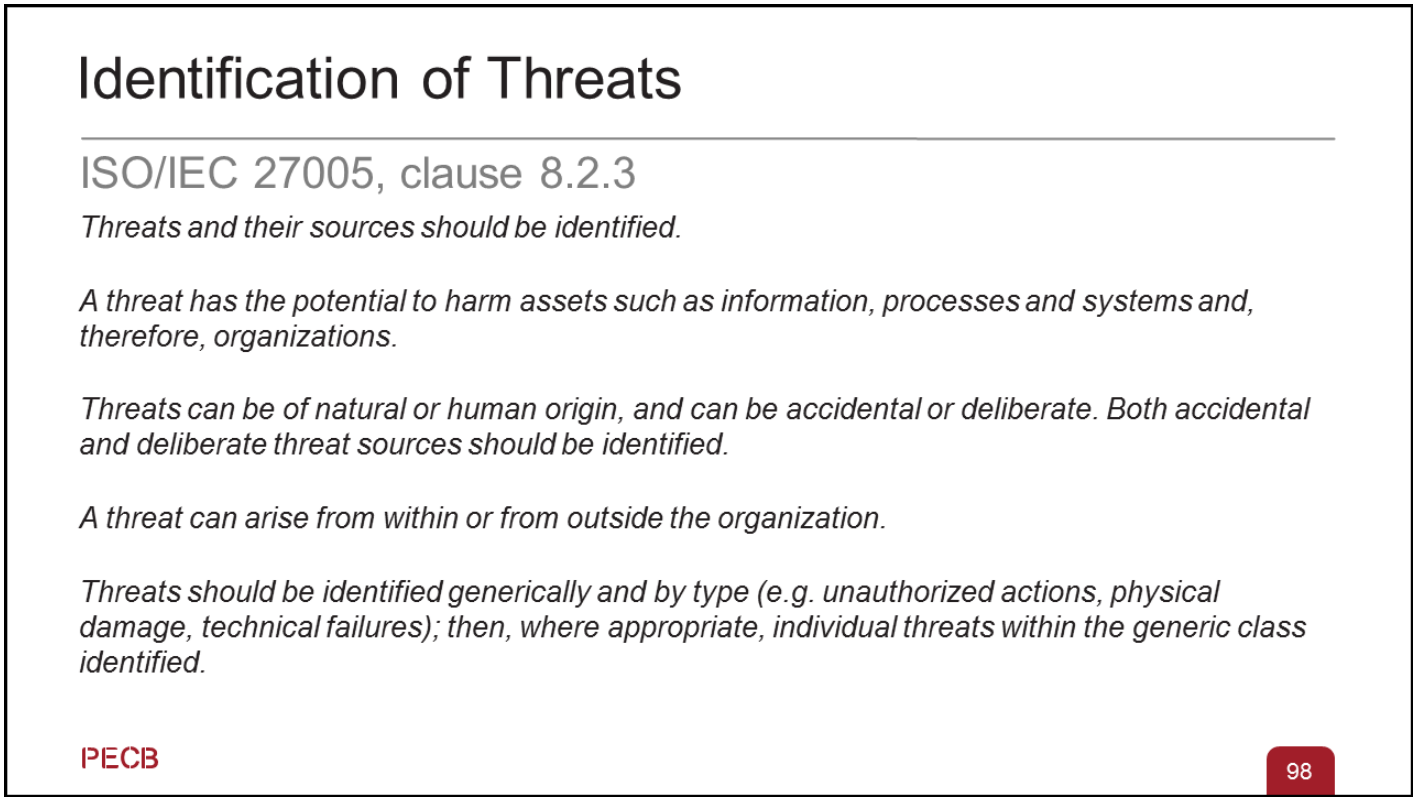
Category	Definition	Examples
Hardware	All the physical elements that support processes	Server, laptop, printer, disk drive, etc.
Software	All the programs that contribute to data processing	Operating system, word processing software , accounting software, etc.
Networks	All telecommunications devices 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.

PECB

97

The supporting assets are generally easier to identify because they are the most tangible assets, such as facilities, furniture, and office supplies, IT equipment, and software.

ISO/IEC 27005, Annex B.1.3 provides subcategories and examples for each asset category.



ISO/IEC 27005, clause 8.2.3 Risk source (cont'd)

Some threats can affect more than one asset. In such cases, they can cause different impacts depending on which assets are affected.

Input to the threat identification and estimation of the likelihood of occurrence can be obtained from the asset owners or users, from human resources staff, from facility management and information security specialists, physical security experts, legal department and other relevant organizations including legal bodies, weather authorities, insurance companies and government authorities. Aspects of environment and culture should also be considered when addressing threats.

Internal experience from incidents and past threat assessments should be considered in the current assessment. It can be worthwhile to consult other threat catalogues (maybe specific to an organization or business) to complete the list of generic threats, where relevant. Threat catalogues and statistics are available from industry bodies, governments, legal bodies, insurance companies, etc.

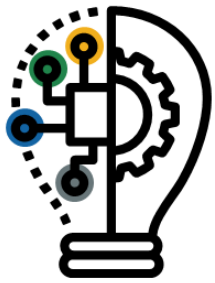
When using threat catalogues, or the results of earlier threat assessments, one should be aware that there is continual change of relevant threats, especially if the business environment or information systems change.

Identification of Existing Controls

ISO/IEC 27005, clause 8.2.4

For the identification of existing or planned controls, the following activities can be helpful:

- *reviewing documents containing information about the controls (for example, risk treatment implementation plans) if the processes of information security management are well documented all existing or planned controls and the status of their implementation should be available;*
- *checking with the people responsible for information security (e.g. information security officer and information system security officer, building manager or operations manager) and the users as to which controls are really implemented for the information process or information system under consideration;*
- *conducting an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented as to whether they are working correctly and effectively;*
- *reviewing results of audits.*



PECB

99

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, for example, 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.

In addition to considering the security controls already in place, the organization should also examine any controls that are planned to be implemented.

When the existing and planned controls are analyzed, they can be identified as ineffective or appropriate. If the control is not justified or does not address a risk, it should be rechecked to determine if it should be removed, replaced by another more appropriate control, or whether it should still remain in place, considering that its removal could trigger considerable costs.

Identification of Vulnerabilities

ISO/IEC 27005, clause 8.2.5

- *Vulnerabilities that can be exploited by threats to cause harm to assets or to the organization should be identified.*
- *The presence of a vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it.*
- *A vulnerability that has no corresponding threat may not require the implementation of a control, but should be recognized and monitored for changes.*
- *It should be noted that an incorrectly implemented or malfunctioning control or control being used incorrectly can itself be a vulnerability.*

Identification of Consequences

ISO/IEC 27005, clause 8.2.6

Organizations should identify the operational consequences of incident scenarios in terms of (but not limited to):

— *Investigation and repair time;*
— *(work)time lost;*
— *opportunity lost;*
— *health and safety;*
— *financial cost of specific skills to repair the damage; and*
— *image reputation and goodwill.*

PECB

101

The consequence of an incident scenario is determined by using the impact criteria defined during the context establishment phase. An impact may derive from one or more aspects. Consequences on assets can be calculated on the basis of financial securities or qualitative scales. These effects may be temporary or permanent, as is the case with the destruction of an asset.

The last step of risk identification is the identification of the consequences of risk event scenarios. An incident scenario is the description of a threat exploiting a vulnerability or set of vulnerabilities in terms of information security, which creates negative consequences.

The consequences of the occurrence of an incident may be evaluated differently depending on the involvement of interested parties in risk assessment. The significant impacts on the organization should be documented accordingly.

Note on terminology:

ISO/IEC 27001 uses the term “impact” and ISO/IEC 27005 the term “consequence” and describes incident scenarios as “security failures.”

Exercise 7: Identification of threats, vulnerabilities, and impacts

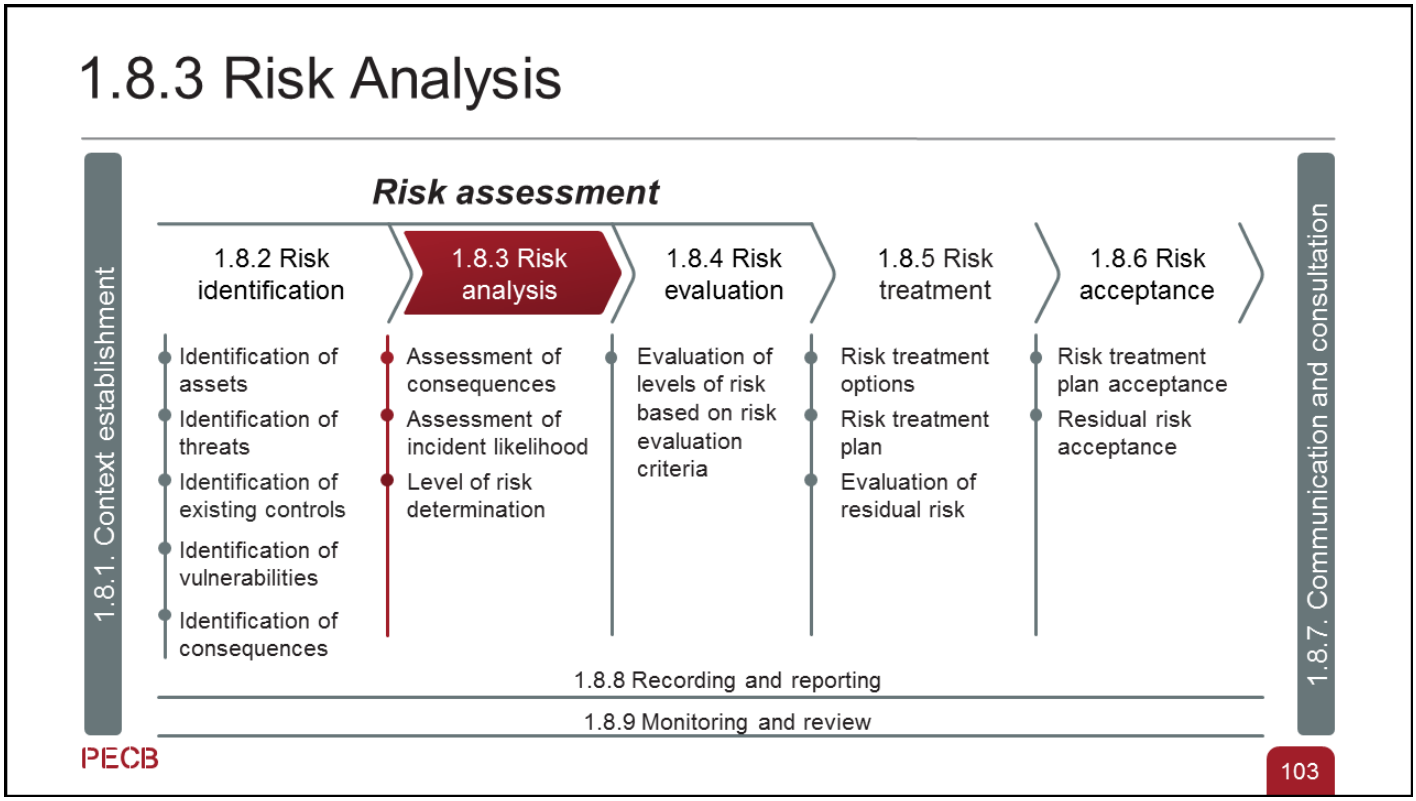
Determine the threats and vulnerabilities associated with the following scenarios and indicate the potential impacts. Then, indicate if the impacts would affect the confidentiality, integrity, or availability of the company's information.

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.

Duration of the exercise: 20 minutes

Comments: 20 minutes



Note: Risk analysis needs to be as simple as possible.

ISO 31000, clause 6.4.3 Risk analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

Risk analysis should consider factors such as:

- *the likelihood of events and consequences;*
- *the nature and magnitude of consequences;*
- *complexity and connectivity;*
- *time-related factors and volatility;*
- *the effectiveness of existing controls;*
- *sensitivity and confidence levels.*

The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

Assessment of Consequences

ISO/IEC 27005, clause 8.3.2

- *A business impact concept is used to measure consequences.*
- *The business impact value can be expressed in qualitative and quantitative forms, but any method of assigning monetary value can generally provide more information for decision making and, hence, facilitate a more efficient decision-making process.*
- *Asset valuation begins with the classification of assets according to their criticality, in terms of their importance to fulfilling the business objectives of the organization.*
- *This valuation can be determined from a business impact analysis. The value, determined by the consequence for business, is usually significantly higher than the simple replacement cost, depending on the importance of the asset to the organization in meeting its business objectives.*

PECB

104

Impact estimation is regularly conducted as part of the preparation of business continuity plans or disaster recovery plans. However, it can be used at a higher level in the context of estimating the consequences of developed incident scenarios.

Factors to be Considered

ISO/IEC 27005, Annex B.3

Immediate (operational) impact is either direct or indirect.

1) Direct:

a) *the financial replacement value of lost (part of) asset;*
b) *the cost of acquisition, configuration and installation of the new asset or back-up;*
c) *the cost of suspended operations due to the incident until the service provided by the asset(s) is restored; and*
d) *impact results in an information security breach.*

2) Indirect:

a) *opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere);*
b) *the cost of interrupted operations;*
c) *potential misuse of information obtained through a security breach;*
d) *violation of statutory or regulatory obligations; and*
e) *violation of ethical codes of conduct.*

PECB

105

The impact of the loss of an asset on the business is generally significantly higher than the simple cost of replacing that asset. To obtain an estimate which corresponds to reality, we must take into account both direct and indirect consequences.

Assessment of Incident Likelihood

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

PECB

106

After identifying the relevant incident scenarios and estimating their consequences, the probability of the occurrence of each incident scenario should be estimated. It is necessary to estimate the realistic probability of an information security incident and the impacts associated with the implemented security controls.

Slide Notes Extension

PECB

107

IEC 31010, Annex B.5.1 General

The likelihood of an event or of a particular consequence can be estimated by:

- *extrapolation from historical data (provided there is sufficient relevant historical data for the analysis to be statistically valid). This especially applies for zero occurrences, when one cannot assume that because an event or consequence has not occurred in the past it will not occur in the near future;*
- *synthesis from data relating to failure or success rates of components of the systems: using techniques such as event tree analysis, fault tree analysis or cause consequence analysis;*
- *simulation techniques, to generate, for example, the probability of equipment and structural failures due to ageing and other degradation processes.*

Experts can be asked to express their opinion on likelihoods and consequences, taking into account relevant information and historical data. There are a number of formal methods for eliciting expert judgement that make the use of judgment visible and explicit.

Consequence and likelihood can be combined to give a level of risk. This can be used to evaluate the significance of a risk by comparing the level of risk with a criterion for acceptability, or to put risks in a rank order.

Assessment of Incident Likelihood

Example of a quantitative expression

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 8.3.4

- *The level of risk should be determined for all relevant incident scenarios.*
- *Risk analysis assigns values to the likelihood and the consequences of a risk. These values can be quantitative or qualitative.*
- *Risk analysis is based on assessed consequences and likelihood. Additionally, it can consider cost benefit, the concerns of stakeholders, and other variables, as appropriate for risk evaluation.*
- *The estimated risk is a combination of the likelihood of an incident scenario and its consequences.*

PECB

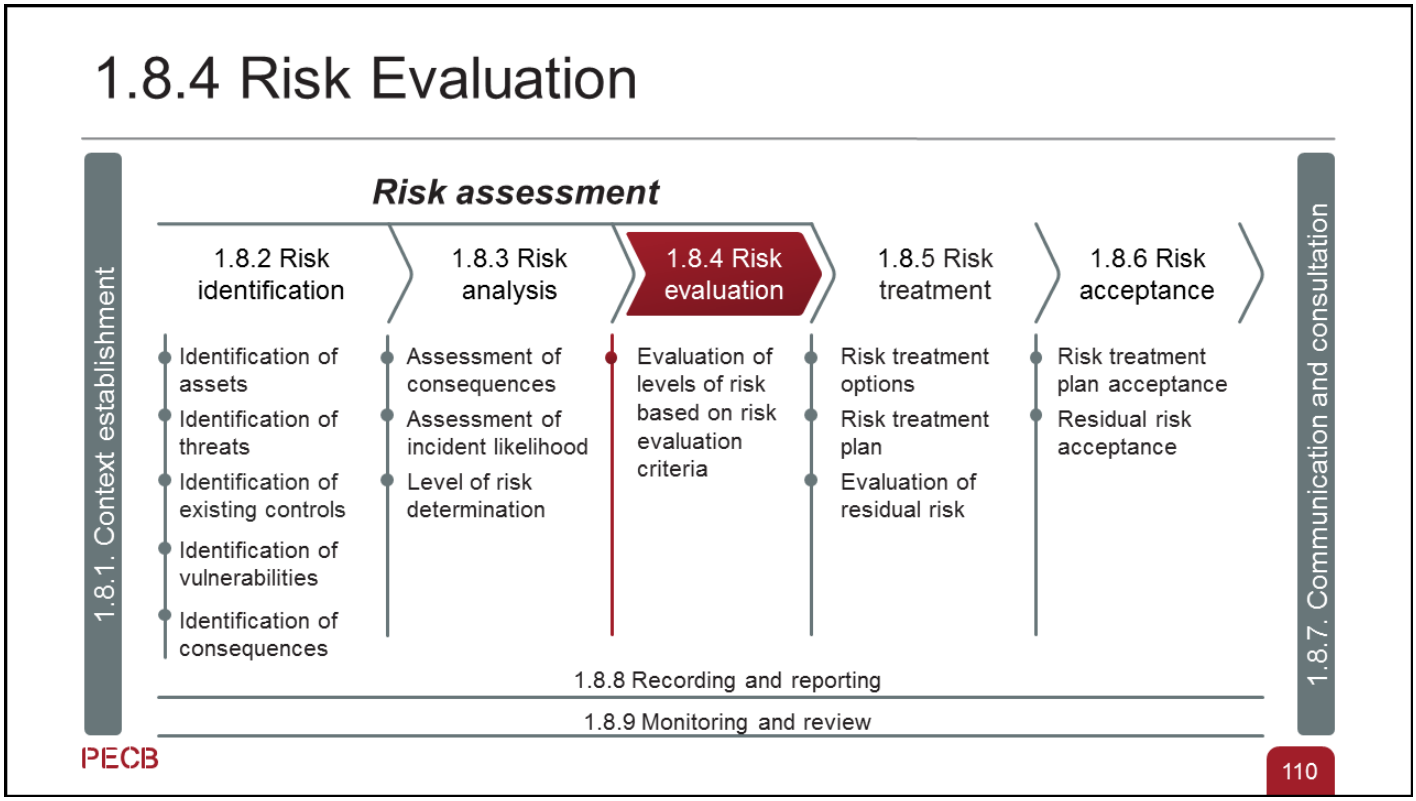
109

Numerical estimation

If the organization possesses data on past or current incidents, especially past incidents, such data can be used to estimate future risks. Nonetheless, other methods should also be used to make such estimates.

Despite the fact that data on past incidents can be useful, they are not necessarily as helpful when assessing the risks that emerge from new activities. The purpose of assessing the risks that emerge from new activities is to identify incidents with a high level of risk, which have not caused any incidents yet. In this way, potential incidents can be prevented from occurring.

It is possible to calculate the probabilities of potential incidents by using external data. For example, past data on road accidents can be used to calculate road transport risks associated with those employees who travel by car. These statistics are used to calculate the probability of more serious, but also very rare, incidents. However, such calculations are not always possible.



ISO Guide 73, clause 3.7.1 Risk evaluation

Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about risk treatment.

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.*

PECB

111

ISO/IEC 27005, clause 8.4 Risk evaluation

The nature of the decisions pertaining to risk evaluation and risk evaluation criteria used to make those decisions, is decided when establishing the context. These decisions and the context should be revisited in more detail at this stage when more is known about the particular risks identified. To evaluate risks, organizations should compare the estimated risks (using selected methods or approaches as discussed in Annex E) with the risk evaluation criteria defined during the context establishment.

Risk evaluation criteria used to make decisions should be consistent with the defined external and internal information security risk management context and take into account the objectives of the organization and stakeholder views, etc. Decisions as taken in the risk evaluation activity are mainly based on the acceptable level of risk. However, consequences, likelihood, and the degree of confidence in the risk identification and analysis should be considered as well. Aggregation of multiple low or medium risks can result in much higher overall risks and should be addressed accordingly.

Example of a Risk Evaluation

ISO/IEC 27005, Table E.3

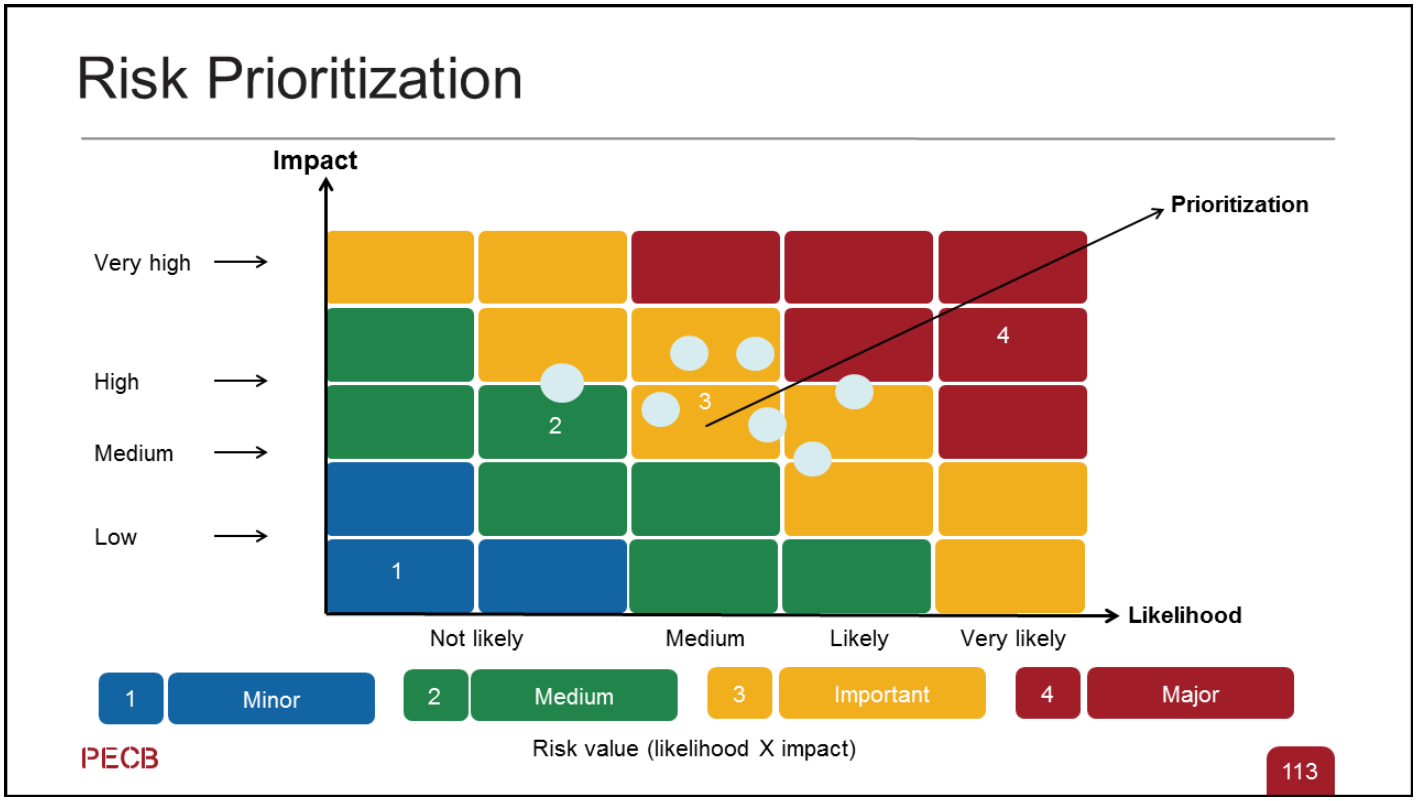
Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

PECB

112

ISO/IEC 27005, Annex E.2.3 Example 2 — Ranking of Threats by Measures of Risk

A matrix or table such as that shown in Table E.3 can be used to relate the factors of consequences (asset value) and likelihood of threat occurrence (taking account of vulnerability aspects). The first step is to evaluate the consequences (asset value) on a predefined scale, e.g. 1 through 5, of each threatened asset (column "b" in the table). The second step is to evaluate the likelihood of threat occurrence on a predefined scale, e.g. 1 through 5, of each threat (column "c" in the table). The third step is to calculate the measure of risk by multiplying (b × c). Finally, the threats can be ranked in order of their associated measure of risk. Note that, in this example, 1 is taken as the lowest consequence and the lowest likelihood of occurrence.



Risk prioritization is a commonly used process for identifying risks that matter and have an impact on the organization. Risk prioritization also supports the decision-making process by considering possible responses to various risks. Once the potential incident scenarios have been established, the criteria for the classification of risk in terms of priority should be defined.

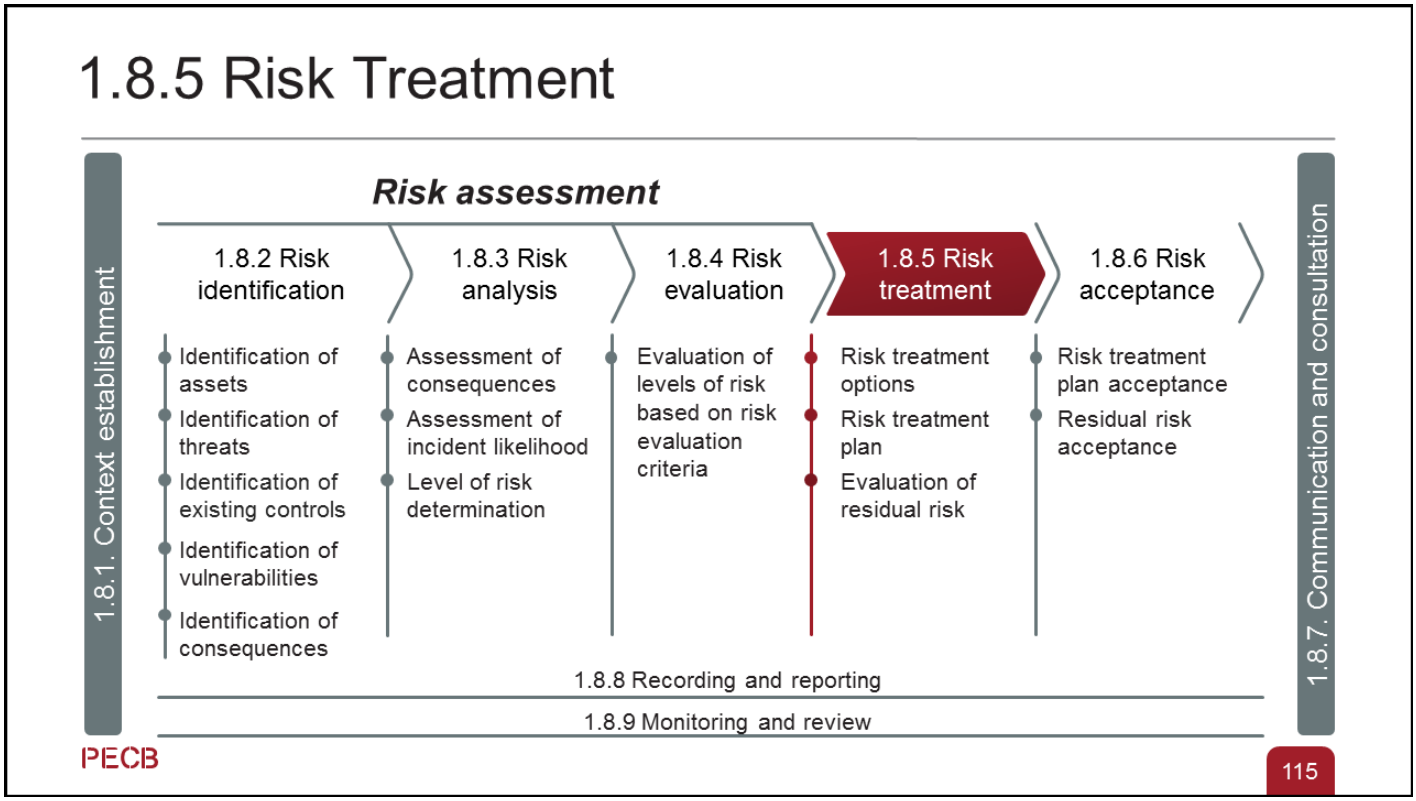
The zero value of risk does not exist. Nonetheless, it is possible to define a threshold, below which the organization accepts to not engage in any activity that reduces the level of risk.

At the other end of the scale, there is a threshold beyond which risk is unacceptable, and as such, everything must be done to eliminate the risk source or reduce the risk.

The graph displayed on the slide, without providing any solutions, clarifies the choices that should be made. The dots in gray represent an example of the current estimated risks determined during the risk analysis process. Once the choices are made, this process allows for effective communication and improves the internal consistency of the organization's actions relative to its basic choices.

The defined areas can be mapped in any risk matrix to classify each potential generic incident, and define the type of actions required in each case.

1. **What does ISO/IEC 27005 provide?**
   A. Requirements for risk management
   B. Practical methods for information security risk management
   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 hardware categorized as?**
   A. Primary assets
   B. Secondary assets
   C. Supporting assets
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



ISO Guide 73, clause 3.8.1 Risk treatment

Process to modify risk

NOTE 1 Risk treatment can involve:

- *avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*
- *taking or increasing risk in order to pursue an opportunity;*
- *removing therisk source;*
- *changing thelikelihood;*
- *changing theconsequences;*
- *sharing the risk with another party or parties [including contracts andrisk financing]; and*
- *retaining the risk by informed decision.*

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

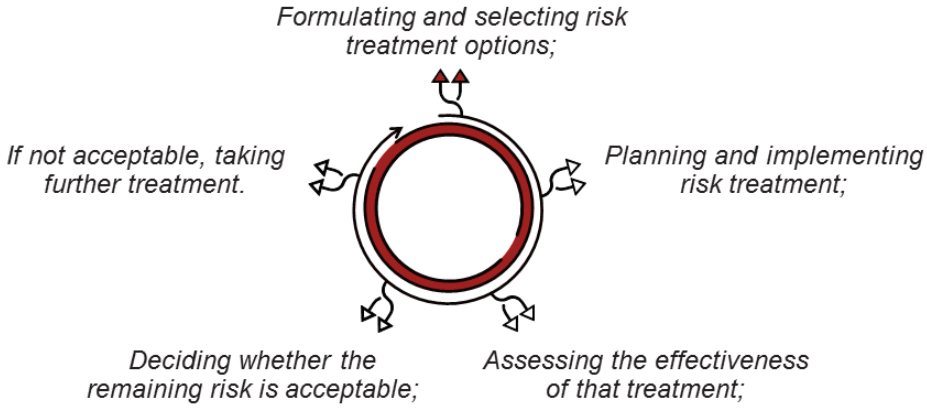
NOTE 3 Risk treatment can create new risks or modify existing risks.

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:



PECB

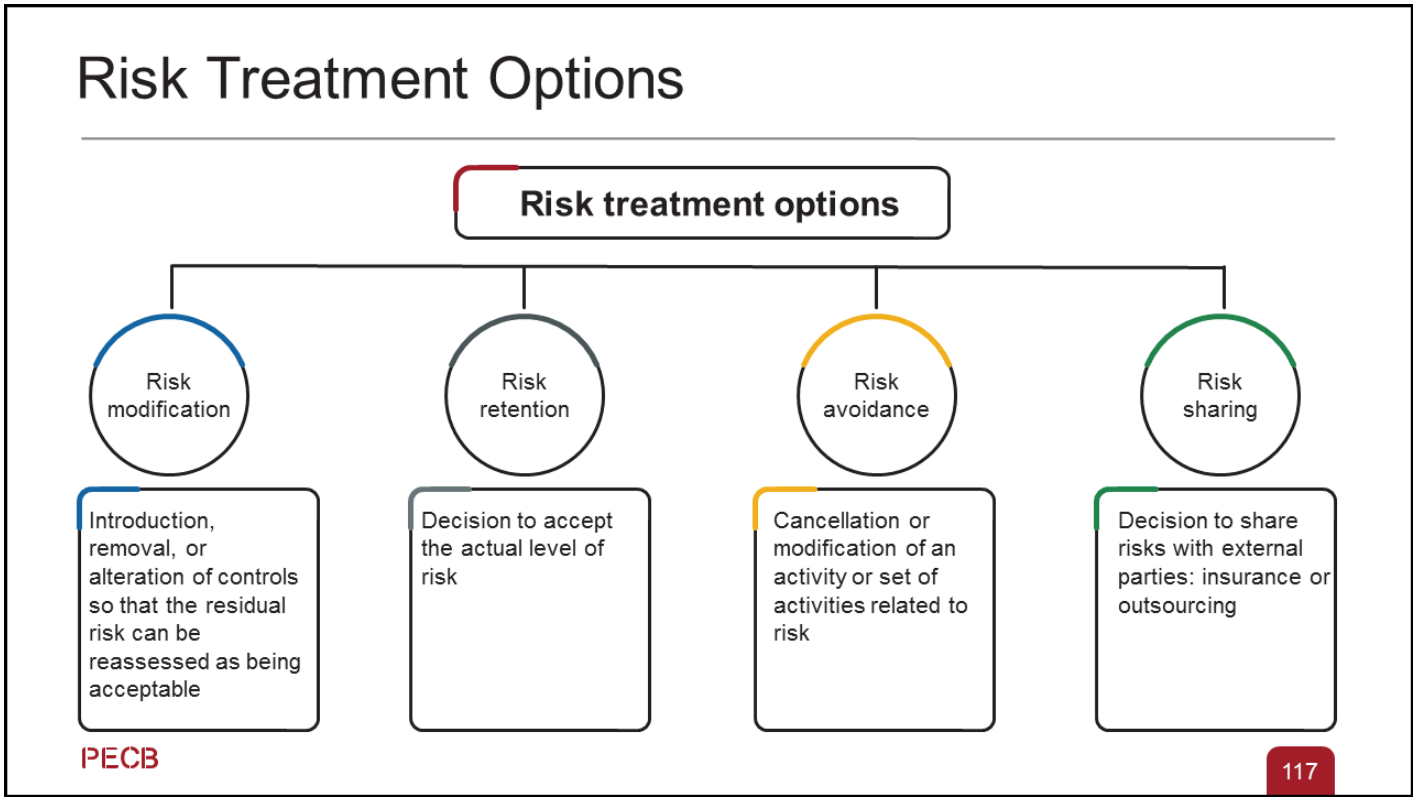
116

The risk treatment process involves the following activities:

1. Determining the options for alleviating the risk
2. Evaluating the proposed options for alleviating the risk
3. Setting up and implementing action plans to alleviate the risk

It is preferable to initially focus the effort on the treatment of high-level risks and then gradually proceed with the treatment of low-level risks.

Selecting the best risk treatment option means that the costs associated with implementing such risk treatment options do not exceed the benefits of implementing them. The costs should at least be the same as the benefits. When conducting such a cost-benefit analysis, the organization's context should be taken into account as well.



The selected risk assessment method must allow the organization to manage risks according to the following options:

ISO/IEC 27005, clause 9.2 Risk modification

Appropriate and justified controls should be selected to meet the requirements identified by the risk assessment and risk treatment. This selection should also take account of cost and timeframe for implementation of controls, or technical, environmental and cultural aspects. It is often possible to lower the total cost of ownership of a system with properly selected information security controls.

ISO/IEC 27005, clause 9.3 Risk retention

If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls and the risk can be retained.

There are certain risks for which the organization may not be able to identify the appropriate risk controls or the costs associated with such risk controls are higher than to simply let the risk materialize. In this case, the organization may decide that it is better to live with the consequences of the risk. The organization will need to document this decision so that risk owners are informed of the risks and accept the consequences of such risks.

ISO/IEC 27005, clause 9.4 Risk avoidance

When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision can be made to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated. For example, for risks caused by nature it can be most cost-effective alternative to physically move the information processing facilities to a place where the risk does not exist or is under control.

Slide Notes Extension

PECB

118

ISO/IEC 27005, clause 9.5 Risk sharing

Risk sharing involves a decision to share certain risks with external parties. Risk sharing can create new risks or modify existing, identified risks. Therefore, additional risk treatment can be necessary. Sharing can be done by an insurance that covers the consequences, or by sub-contracting a partner whose role is to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.

ISO 31000, clause 6.5.2 Selection of risk treatment options

When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Risk Treatment Plan

- 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.

PECB

119

When determining the priority of the actions to be taken to implement the chosen risk treatment option, the organization should take into account, among others, the following:

- The processes that carry the highest level of risk
- The need to communicate the results to top management

ISO 31000, clause 6.5.3 Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should be implemented.

Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.

The information provided in the treatment plan should include:

- *the rationale for selection of the treatment options, including the expected benefits to be gained;*
- *those who are accountable and responsible for approving and implementing the plan;*
- *the proposed actions;*
- *the resources required, including contingencies;*
- *the performance measures;*
- *the constraints;*
- *the required reporting and monitoring;*
- *when actions are expected to be undertaken and completed.*

Risk Treatment Plan

Example

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

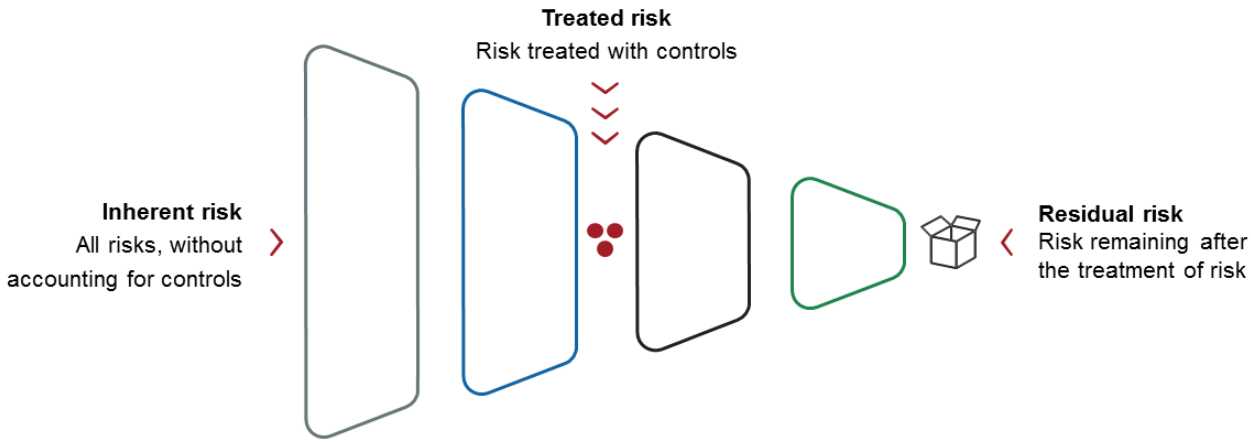
PECB

120

As presented on the slide, the risk treatment plan will likely take a more or less elaborate approach but it should at least clarify the following points:

- The actions to be taken
- The allocation of resources
- The responsibilities
- The priorities

Approval of Residual Risks



Risk owners must be aware of the residual risks and accept responsibility for them.

PECB

121

Residual risk can be defined as the risk that remains after the implementation of controls aiming to reduce the inherent risk, and can be summarized as follows:

Residual risk = Inherent risk - Treated risk

After the implementation of a risk treatment plan, there are always residual risks. **The value of risk reduction following risk treatment should be evaluated, calculated, and documented.** Residual risks can be difficult to evaluate, but an estimation should at least be made to ensure that the value of residual risks is within the organization's risk acceptance criteria. The organization also must put in place residual risk surveillance mechanisms.

If the residual risk is considered as unacceptable after the controls have been implemented, a decision must be made to treat the risk completely. One alternative could be to identify other risk treatment options such as sharing the risk (insurance or outsourcing), which would reduce the risk to an acceptable level. Another option could be to accept the risk (on purpose). Even though it is best practice to completely eliminate risks that exceed the organization's risk acceptance criteria, it is not always possible to reduce all risks to an acceptable level.

In all circumstances, residual risks must be understood, accepted, and approved by management.

Exercise 8: Risk treatment options

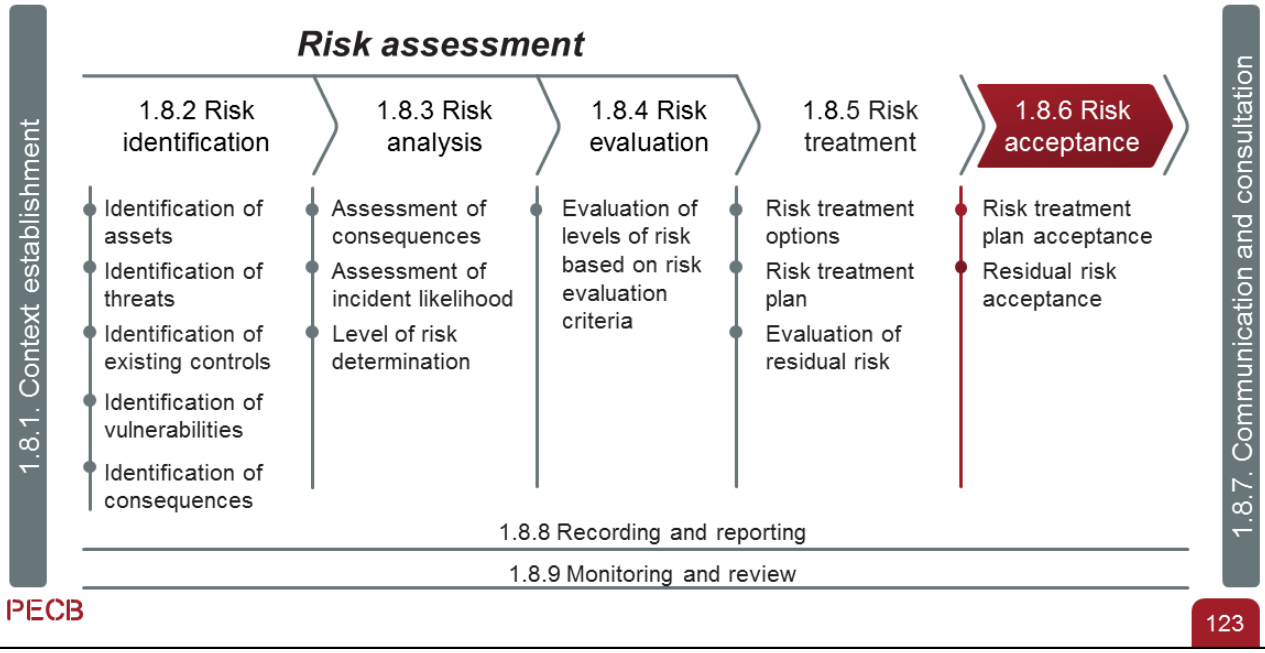
Upon conducting a thorough risk assessment, you have found that 0.5% of electronic transactions (turnover of $10 million) made by credit card on the company's application are fraudulent in nature. The management of *e-Scooter* must take an important decision on how to address this risk.

Propose four risk treatment options to address the risk and list the activities that should be taken based on these options.

Duration of the exercise: 20 minutes

Comments: 15 minutes

1.8.6 Risk Acceptance

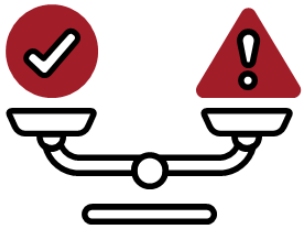


ISO/IEC 27005, clause 10 Information security risk acceptance

Risk treatment plans should describe how assessed risks are to be treated to meet risk acceptance criteria. It is important for responsible managers to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval.

Risk Acceptance

- Risk acceptance is acknowledging the potential costs and benefits that an organization incurs if it accepts the risk.
- Risk acceptance differs across industries, organizations, and departments within an organization.



PECB

124

ISO Guide 73, clause 3.7.1.6 Risk acceptance

Informed decision to take a particular risk

NOTE 1 Risk acceptance can occur withoutrisk treatmentor during the process of risk treatment.

NOTE 2 Accepted risks are subject tomonitoringandreview.

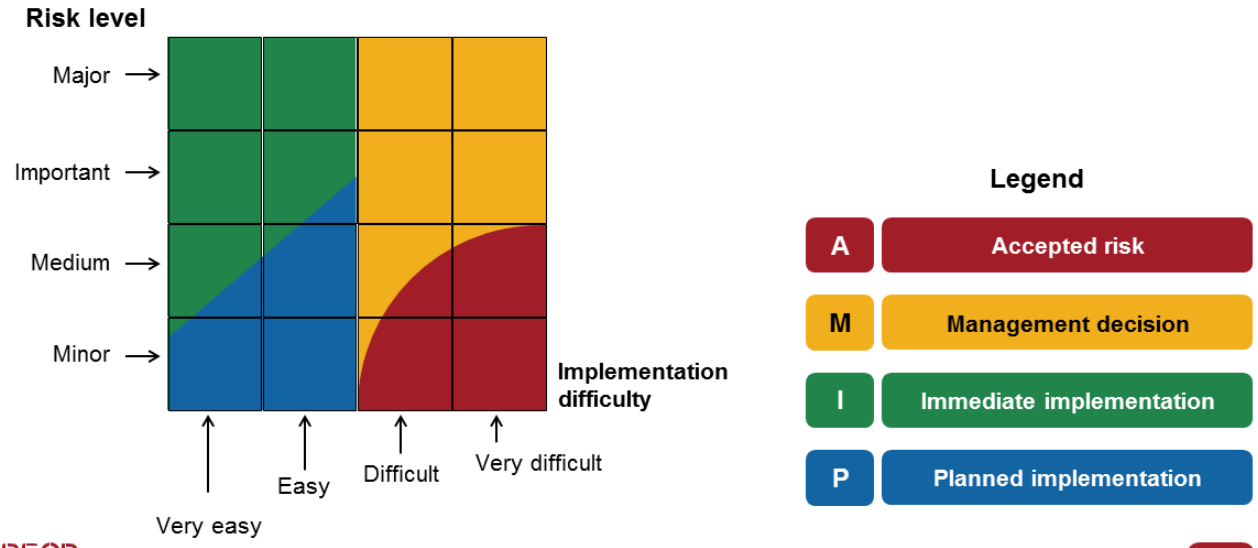
Examples of risk acceptance:

1. **Investing** — Most investments contain a certain level of risk.
2. **Insurance —** The insurance industry is based on risk assumptions for a defined fee.
3. **Derivatives —** Contracts that derive their value from exchange rates; risk is transferred from one organization to the other.
4. **Projects —** Projects contain the risk of cost overruns.
5. **Business equity** — Each equity owned by an organization is at risk. This risk is accepted under the assumption that the potential returns increase as the risk increases.

Source: Popov, Georgi, Bruce K. Lyon, and Bruce Hollcroft. *Risk Assessment: A Practical Guide to Assessing Operational Risks.* New Jersey: Wiley, 2016.

Risk Treatment Plan Acceptance

Presentation to top management (example)



PECB

125

It is the management's decision to define the expectations regarding the risk treatment plan for each risk level.

As shown on the slide, for "major level" risks that have an implementation difficulty ranked between very easy and easy, the risk treatment plan must be implemented immediately. In contrast, if the implementation difficulty is ranked between difficult and very difficult, then the top management should decide on how to proceed with the risk treatment plan.

However, for "minor or medium" level risks, the risk treatment plan could be implemented immediately, or the risk could simply be accepted based on the implementation difficulty of the risk treatment plan.

Residual Risk Acceptance

ISO/IEC 27005, clause 10

Residual risk acceptance by risk owners

- *It is important for responsible managers to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval.*
- *Risk acceptance criteria can be more complex than just determining whether or not a residual risk falls above or below a single threshold.*

Acceptance of Risks that do not Meet the Risk Acceptance Criteria

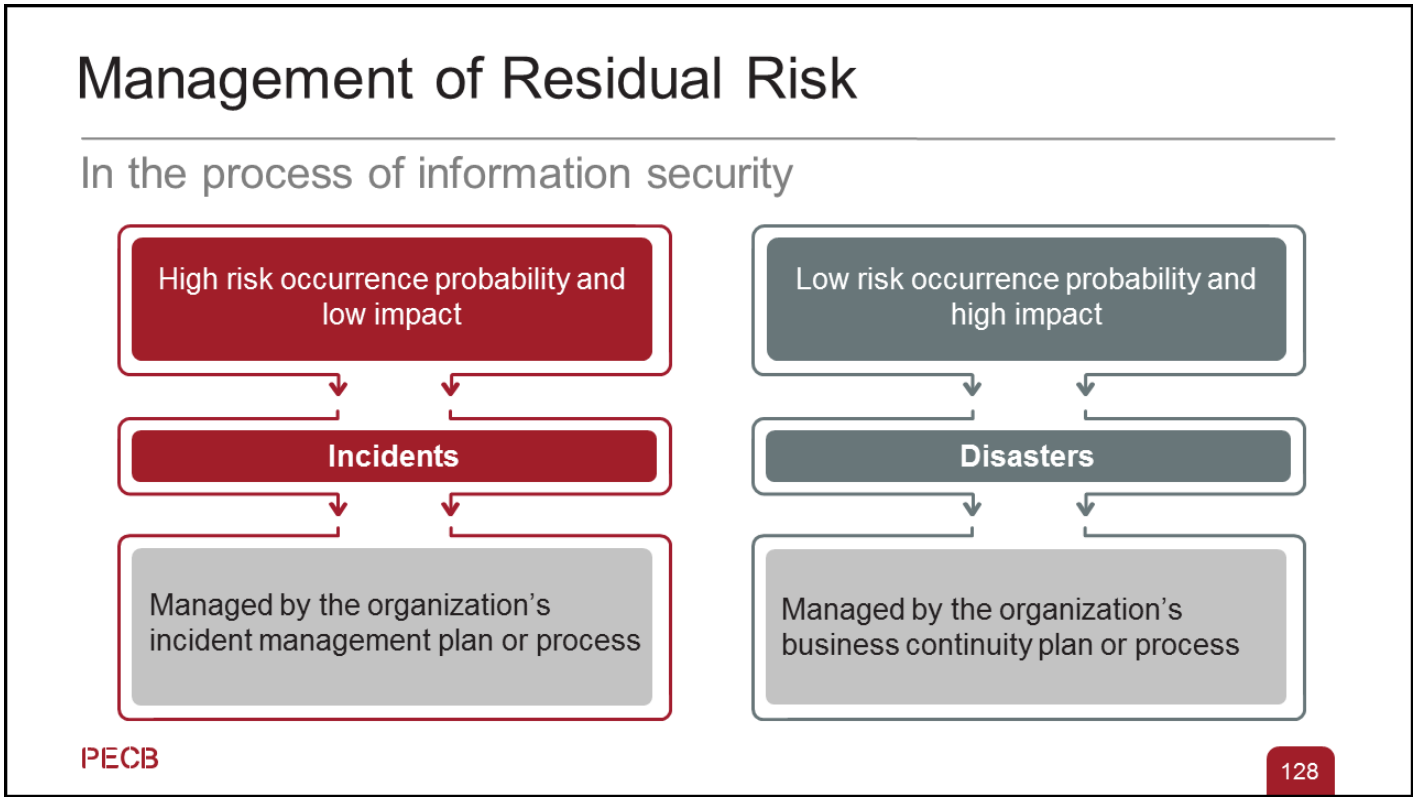
ISO/IEC 27005, clause 10

- *In some cases, the level of residual risk does not meet risk acceptance criteria because the criteria being applied do not take into account prevailing circumstances.*
- *For example, it can be argued that it is necessary to accept risks because the benefits accompanying the risks are very attractive, or because the cost of risk modification is too high.*
- *Such circumstances indicate that risk acceptance criteria are inadequate and should be revised if possible.*

PECB

127

ISO/IEC 27005, clause 10 Information security risk acceptance (cont'd)
However, it is not always possible to revise the risk acceptance criteria in a timely manner. In such cases, decision-makers can accept risks that do not meet normal acceptance criteria. If this is necessary, the decision maker should explicitly comment on the risks and include a justification for the decision to override normal risk acceptance criteria.



After risk acceptance, not all residual risks disappear. The risks with high occurrence and low impact are managed by the organization's incident management plan or process. The risks with low occurrence and high impact (disaster) are managed by the organization's business continuity plan or process.

1.8.7 Communicating and Consultation

ISO 31000, clause 6.2

- *The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required.*
- *Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making.*
- *Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.*
- *Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.*

PECB

129

Good communication and consultation requires honest talks and meetings with all the relevant interested parties so that all their needs are identified and fulfilled.

To achieve desirable results, it is important to firstly develop a communication strategy and then implement it.

The second important part is consultation. The risk manager is considered as an internal consultant or coach that helps less experienced employees in acquiring the necessary expertise in risk management so as to achieve risk optimization objectives.

1.8.8 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.*

PECB

1.8.9 Monitoring and Review

ISO 31000, clause 6.6

- *The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes.*
- *Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.*

PECB

131

ISO 31000, clause 6.6 Monitoring and review (cont'd)

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback.

The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.

Exercise 9: Monitoring and reviewing the risk management process

Based on the case study, explain why it is important for e-Scooter to monitor and review its risk management process. List three risks that the company would be facing in case it fails to take such actions.

Duration of the exercise: 20 minutes

Comments: 15 minutes

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 objective of risk communication?**
   A. To promote awareness and understanding of risk
   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?

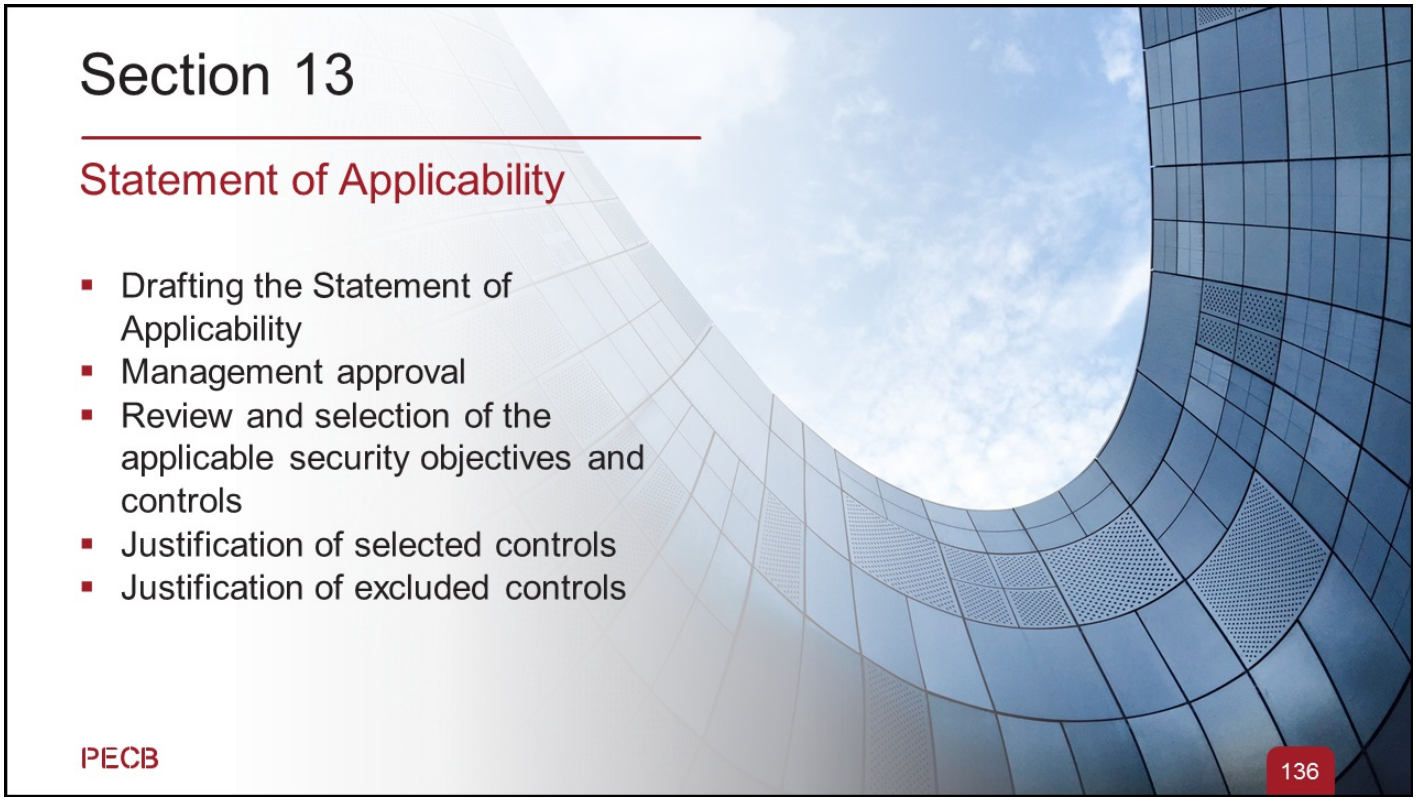
A. Share the risk
B. Modify the risk
C. Trade the risk

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

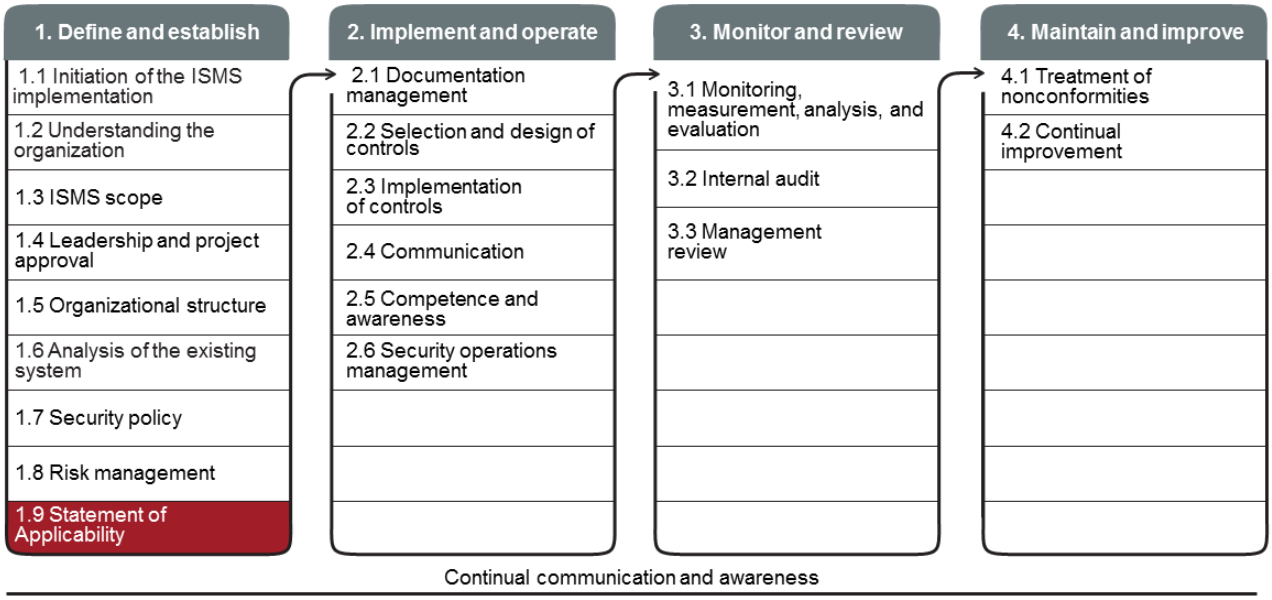
Section summary

- ISO 31000 underlines the importance of integrating the risk management in the organization's processes, activities, or systems.
- ISO/IEC 27005 divides assets into two broad categories: primary assets and supporting assets.
- Risk analysis needs to be as simple as possible.
- Risk prioritization is used to identify risks that have an impact on the organization.
- Some of the examples of risk acceptance include investing, insurance, derivatives, projects, and business equity.



This section provides information that will help the participant identify security controls to be included in the ISMS, justify the choice of the selected and excluded security controls, and obtain formal approval from the management for the implementation of the information security management system.

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 and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A.

NOTE

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

PECB

138

An organization wishing to comply with ISO/IEC 27001 shall at least:

- Be able to demonstrate that its ISMS is aligned with the mission of the organization and its objectives and business strategies
- Take into account issues related to information security within their areas of activities such as risk, legal, and regulatory constraints and customer requirements

Note: The organization is free to select controls from any source or to create them itself. What is required is that a “sanity check” is performed by reviewing the controls in Annex A and ensuring that each of them is considered.

Statement of Applicability

Definition

- A Statement of Applicability (SoA) is a documented statement listing the control objectives and 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.

PECB

139

The Statement of Applicability is more than just a checklist of security controls of ISO/IEC 27001 Annex A to be implemented in the organization's information security management system. It is a key document of the ISMS that serves as a reference for the external auditor during the certification audit; as such, this is one of the first documented information that will be subject to analysis. It is also one of the documented piece of information that the organization's management must validate and approve before initiating the ISMS operations.

Notes on terminology:

- The Statement of Applicability is ISO/IEC 27001-specific. There is no equivalent in other management system standards such as ISO 9001 or ISO 14001.
- Even in other languages, many organizations use the English term "Statement of Applicability" or its acronym SoA or SOA.

1.9 Statement of Applicability

List of activities

1.9.1 Review and select the applicable control objectives and controls

1.9.2 Initiate the Statement of Applicability

1.9.3 Ensure management approval

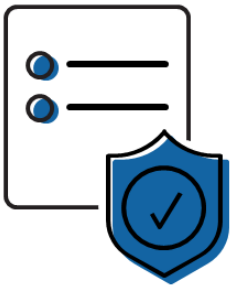
1.9.4 Justify the selected controls

1.9.5 Justify the excluded controls

1.9.6 Finalize the Statement of Applicability

1.9.1 Review and Select the Applicable Security Objectives and Controls

- The organization must review the 114 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.



PECB

141

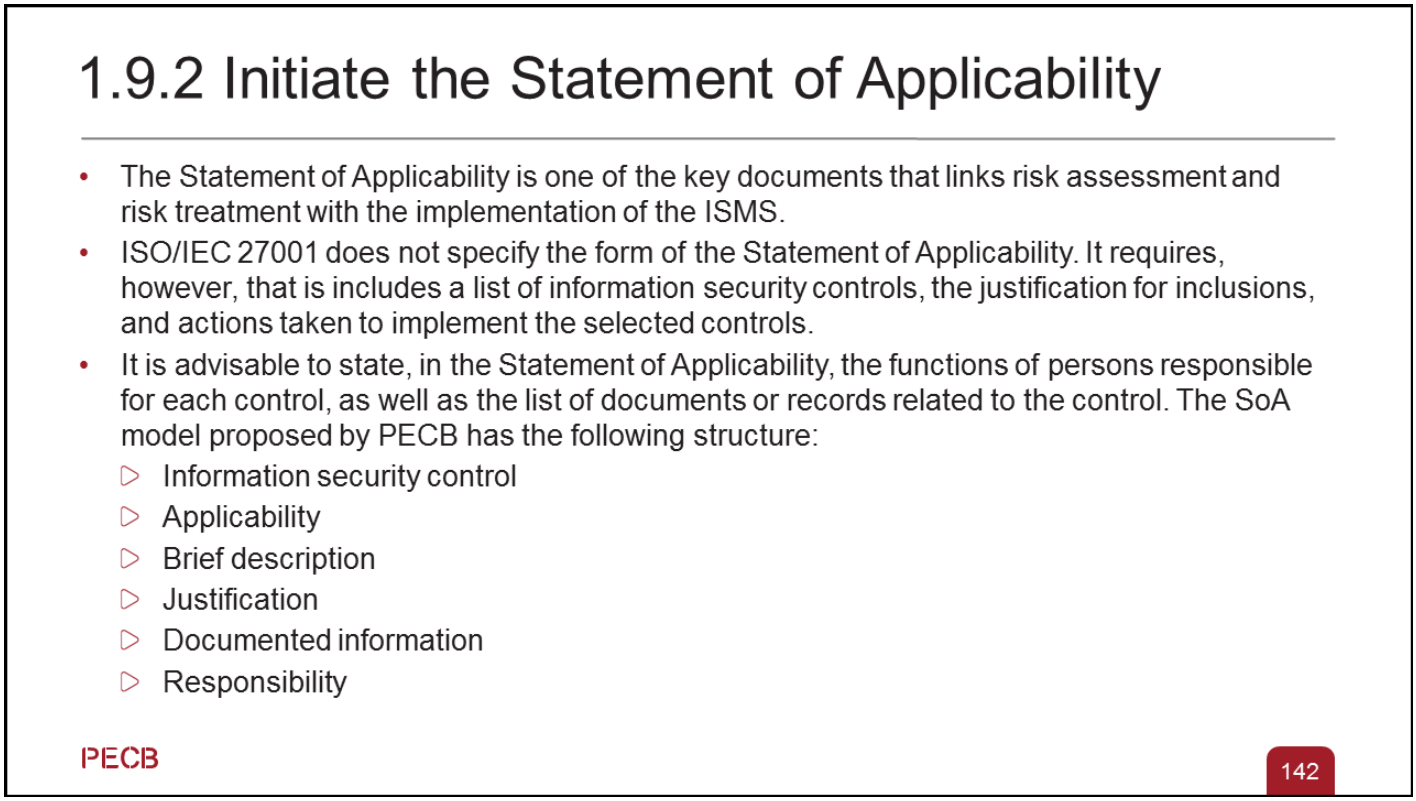
Initially, the organization must review the 114 security controls in Annex A to identify those that are applicable and those that will not be considered in the context of the ISMS. The choice of applying a security control should be primarily justified by the risk assessment. That is why the Statement of Applicability should not be drafted before the filing of the risk analysis and risk treatment report.

The security controls proposed in Annex A may be sufficient to address all risk scenarios that the organization has identified. Other repositories to implement additional security controls (e.g. COBIT, PCI, etc.) can be used and integrated in the ISMS. It should be noted that additional security controls must also be described in the Statement of Applicability.

Most organizations report more than 80 security controls. One, however, should avoid exaggeration. An ISMS that contains only the mandatory security controls may not be effectively protected. Conversely, the decision to declare all relevant controls without taking the time to assess the needs of the organization may be equally ineffective. Security controls may then be implemented without addressing a real need, thereby considerably increasing the burden of system maintenance.

Moreover, the selection of security controls should take a cost/benefit analysis into account. Given that the ISMS supports the organization in achieving its business objectives, it is subject to economic imperatives. Implemented security controls need to be “profitable” for the organization.

To conclude, in the logic of the standard, the security controls declared in the ISMS should be aligned with the organization’s activities and not vice versa.



The SoA must include all the implemented controls and all planned-but-not-yet-implemented controls, irrespective of their sources. In addition, the SoA must list any controls from ISO/IEC 27001 Annex A which the organization deemed as inapplicable. There must be a justification for the inclusion or exclusion of each control.

The PECB SoA model contains:

1. **Information security control:** In this section, the control of Annex A of ISO/IEC 27001 is listed.
2. **Applicability:** In this section, it is stated whether the control is applicable to the organization or not. A control is considered to be applicable if its implementation will help treat the identified risks, if it is required by law, if it is a contractual requirement, and so on. The applicability of controls depends on the organization, the nature and severity of risks, and the ISMS scope.
3. **Brief description:** This section provides a description of the control and indicates how it was (or planned to be) implemented in the organization. A simple way to do this is to use the "6Ws" method (who, what, when, where, why, how), except the "why" that is to be addressed in the "justification" section.
    - **For example:** An information security policy (what), approved by the top management (who) is effective from December 21, 2017 (when). A copy was sent (how) to all employees and other relevant interested parties (who). The official version is available on the intranet (where).
4. **Justification:** In this section, the reasons for selecting or excluding a security control are given.
5. **Documented information:** In this section, the documents (policies and procedures) or records related to the security control are mentioned.
6. **Responsibility:** The owner of the control is the person who is responsible for organization's actions related to this control. The name and position of this person must be included in the SoA. If the control is not applicable, the person that is able to prove its inapplicability should be identified and contacted as to facilitate the work of auditors (internal and external).

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

PECB

143

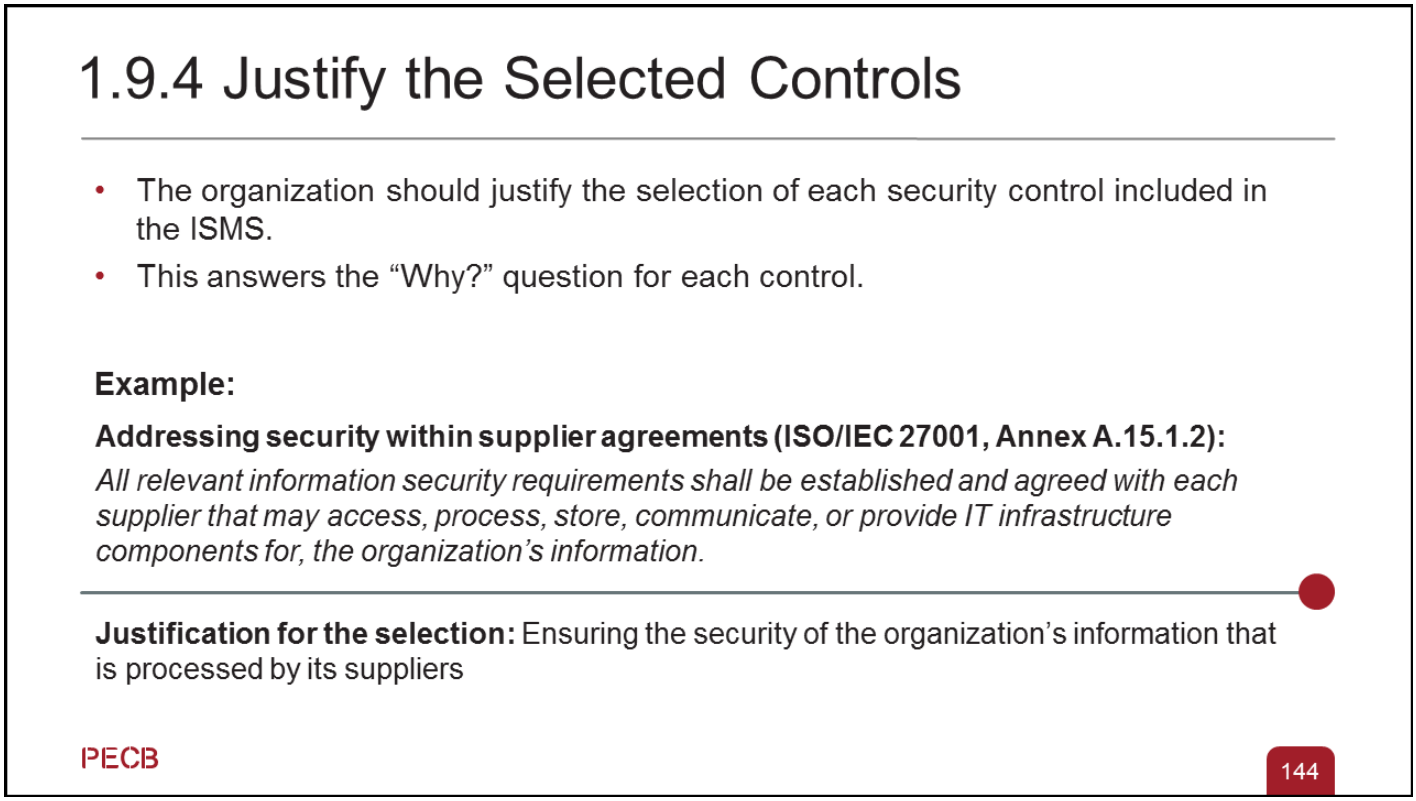
To obtain the approval of the management for the ISMS implementation, the following documented information should be prepared in advance:

- Risk analysis report
- Risk treatment plan (including the identification of residual risks)
- Statement of Applicability

Usually, the abovementioned documented information is presented in a management review meeting alongside with a progress report of the draft of the ISMS. Following this management review, the organization's management is expected to provide:

- Approval of the Statement of Applicability
- Authorization to implement the ISMS
- Written permission of the management regarding the ISMS implementation

Following the formal authorization to implement the ISMS, it is a good practice to make an official announcement.



Other examples of justifications related to the selected controls:

ISO/IEC 27001, Annex A.12.1.2 Change management

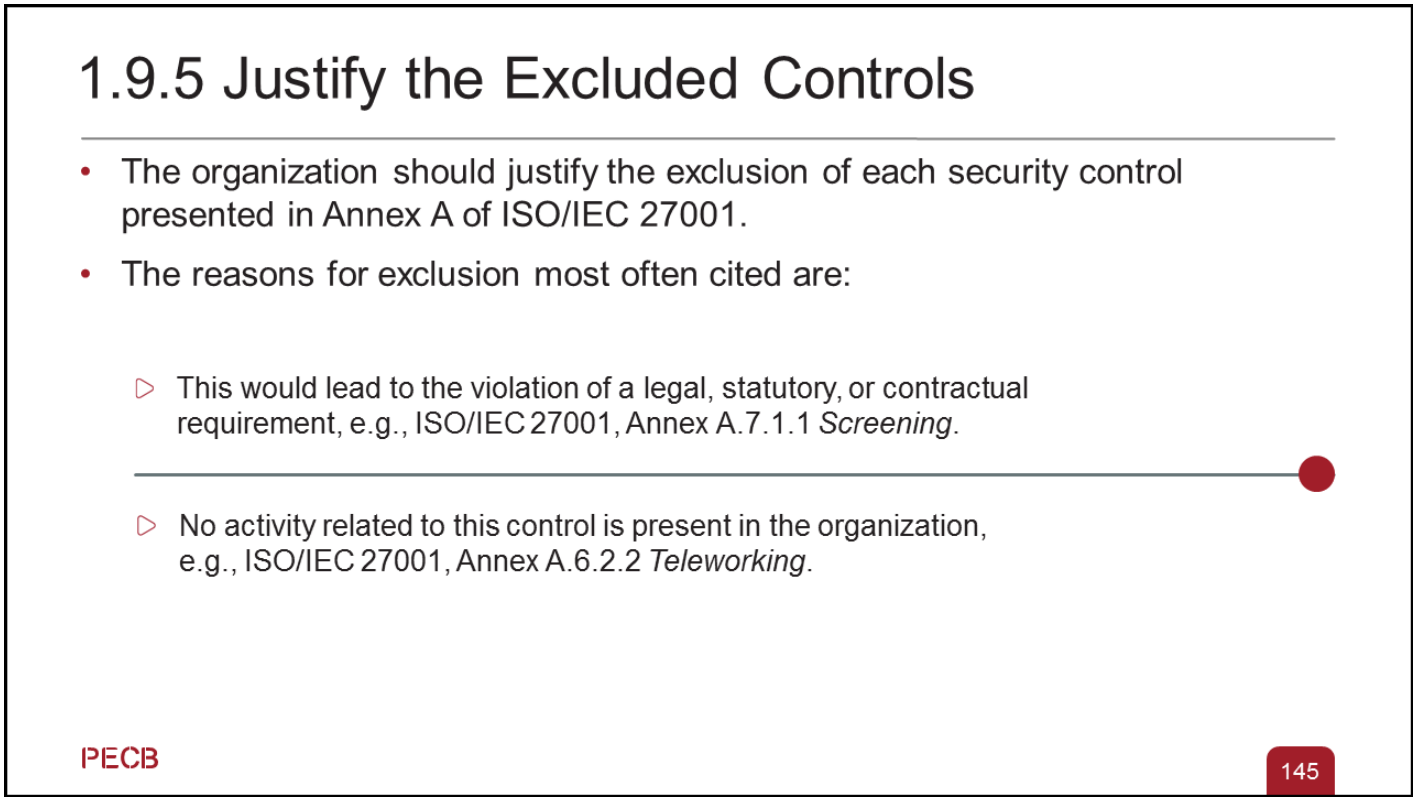
Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

Justification of the selection: Ensuring the confidentiality, integrity, and availability of information and means of processing information belonging to the organization when there are changes to systems and information processing methods

ISO/IEC 27001, Annex A.17.1.2 Implementing information security continuity

The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Justification of the selection: Ensuring the availability of information in a timely manner when an interruption or power outage affects critical business processes



Here are some examples of reasons that may lead to the exclusion of security controls:

ISO/IEC 27001, Annex A.7.1.1 Screening

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Justification of the exclusion: In compliance with the collective agreement with the employees, no security checks will be made.

ISO/IEC 27001, Annex A.6.2.2 Teleworking

A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Justification of the exclusion: Teleworking is prohibited in the organization.

There are cases when organizations declare a control as applicable and explain what it covers and its limitations. For instance, the control on screening (A.7.1.1) does not require using all the necessary means to conduct a thorough investigation of every person, such as credit investigation, criminal record investigation, verification of qualifications, etc. An organization could simply claim that they will conduct the inspect the original certificates and verify two references for each candidate.

1.9.6 Finalize the Statement of Applicability

Example

Control	Applicable	Description	Justification	Documentation	Responsible
ISO/IEC 27001, Annex A.5.1.1 *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

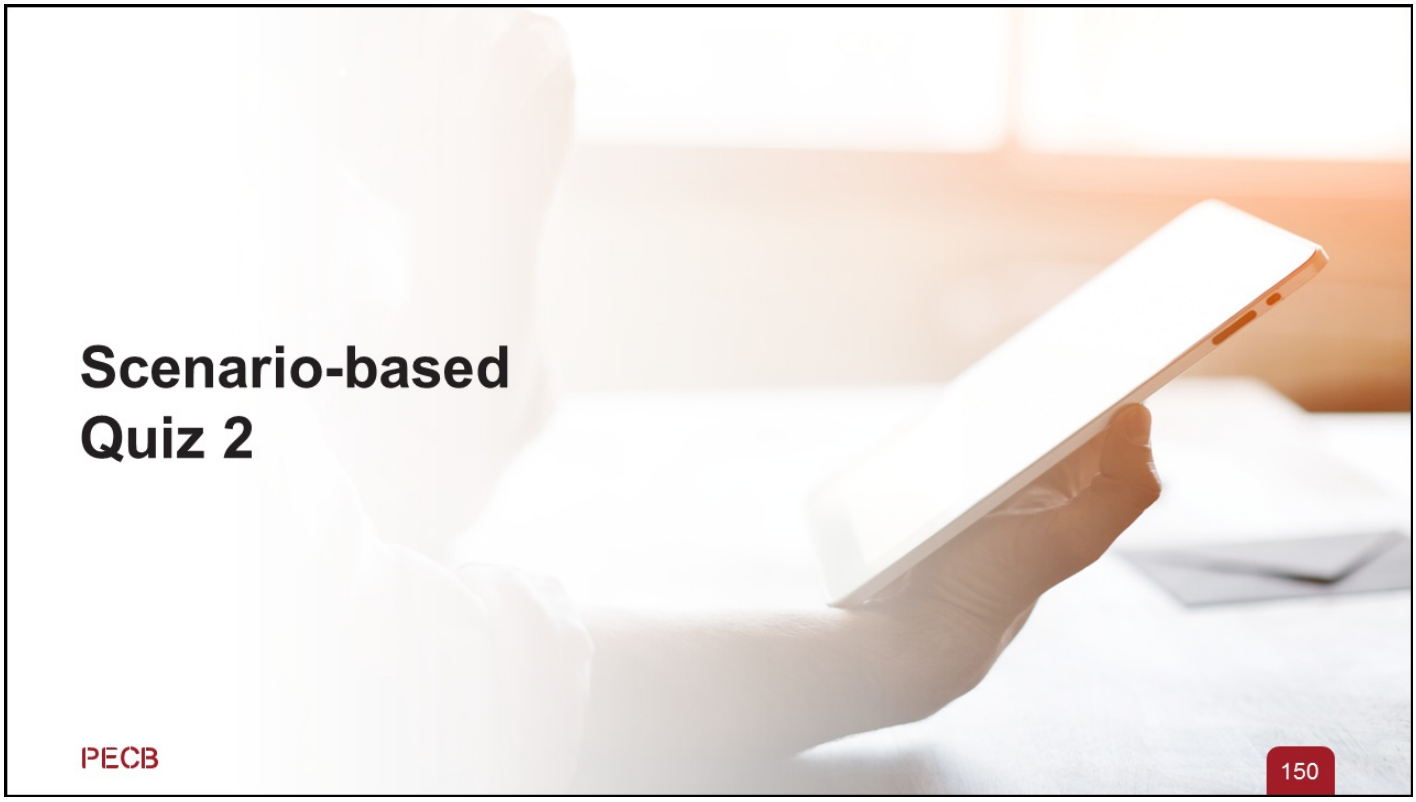
Control	Applicable	Description	Justification	Documentation	Responsible
ISO/IEC 27001 Annex A.5.1.2 *Review of the policies information security*	Yes	The information security policy is reviewed annually in the management review meeting and the formal resolution is extended for another year. In case of 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.6.2.2 *Teleworking*	No	----------	Our organization has no activities related to teleworking.	N/A	IT manager

PECB

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

Section summary

- A Statement of Applicability (SoA) is a documented statement listing the control objectives and controls that are relevant and applicable to the organization's information security management system.
- The Statement of Applicability is one of the key documents that links risk assessment and risk treatment with the implementation of the ISMS.
- To obtain the approval of the management for the ISMS implementation, the following documented information should be prepared in advance: risk analysis report, risk treatment plan (including the identification of residual risks), and Statement of Applicability.



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.

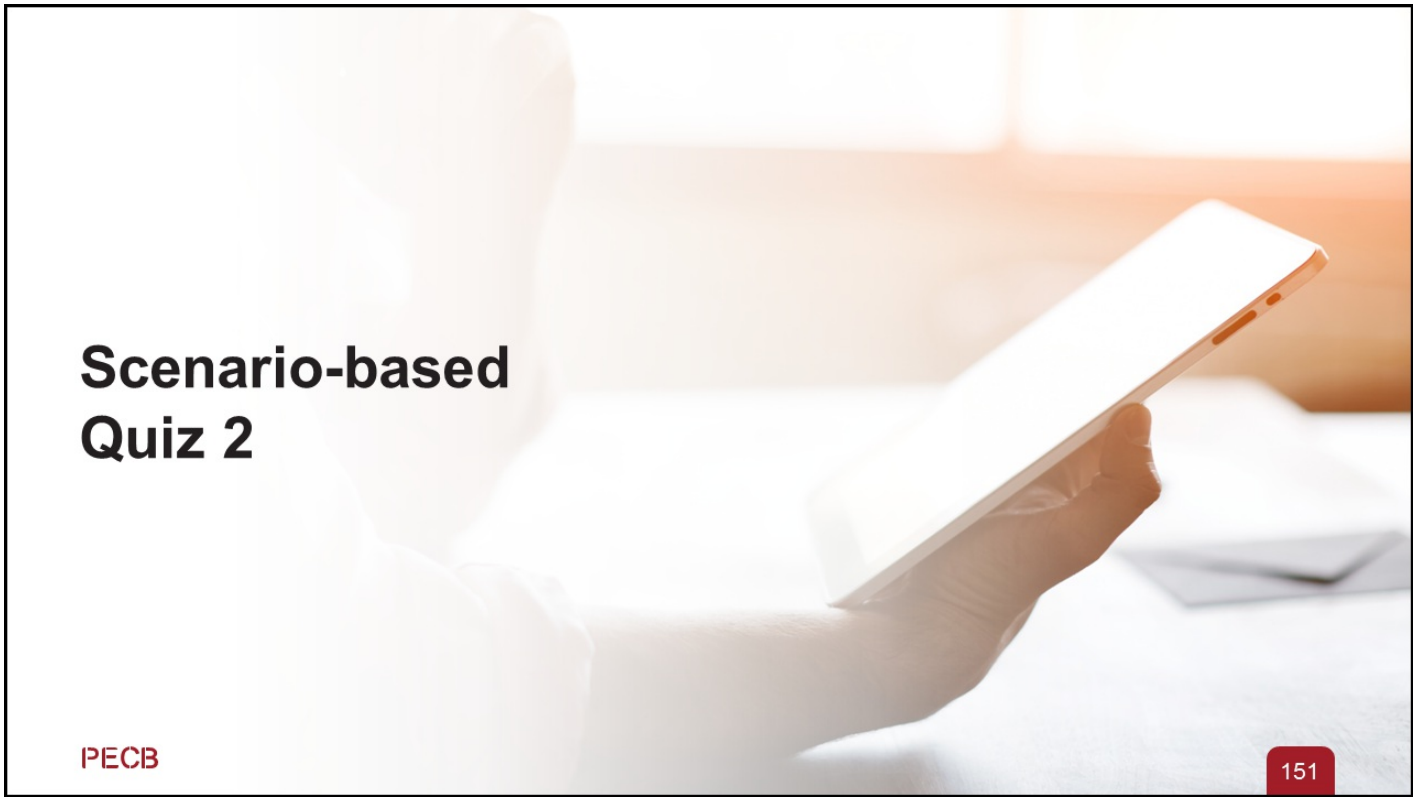
Answer the following questions by referring to the above-mentioned scenario:

1.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

2.Which ISMS scope boundary has *Research Metric* defined?

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



3.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

4.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

5.*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

Slide Notes Extension

PECB

152

Summary of Day 2

The following topics were covered in the second day of this training course:

- Creation and content of the business case
- ISMS project team and project plan
- Management approval
- Information security organizational structure
- Roles and responsibilities of interested parties and committees
- Analysis of the existing system
- Gap analysis
- The establishment of maturity targets
- Information security policy
- Types of policies and policy models
- Training and awareness sessions
- Control, evaluation, and review
- Risk management process
- Risk assessment approach and methodology
- Risk identification, estimation, evaluation, and treatment
- Statement of Applicability and management decision to implement the ISMS
- Justification of selected controls and justification of excluded controls

Blank Page for Note Taking

Blank Page for Note Taking