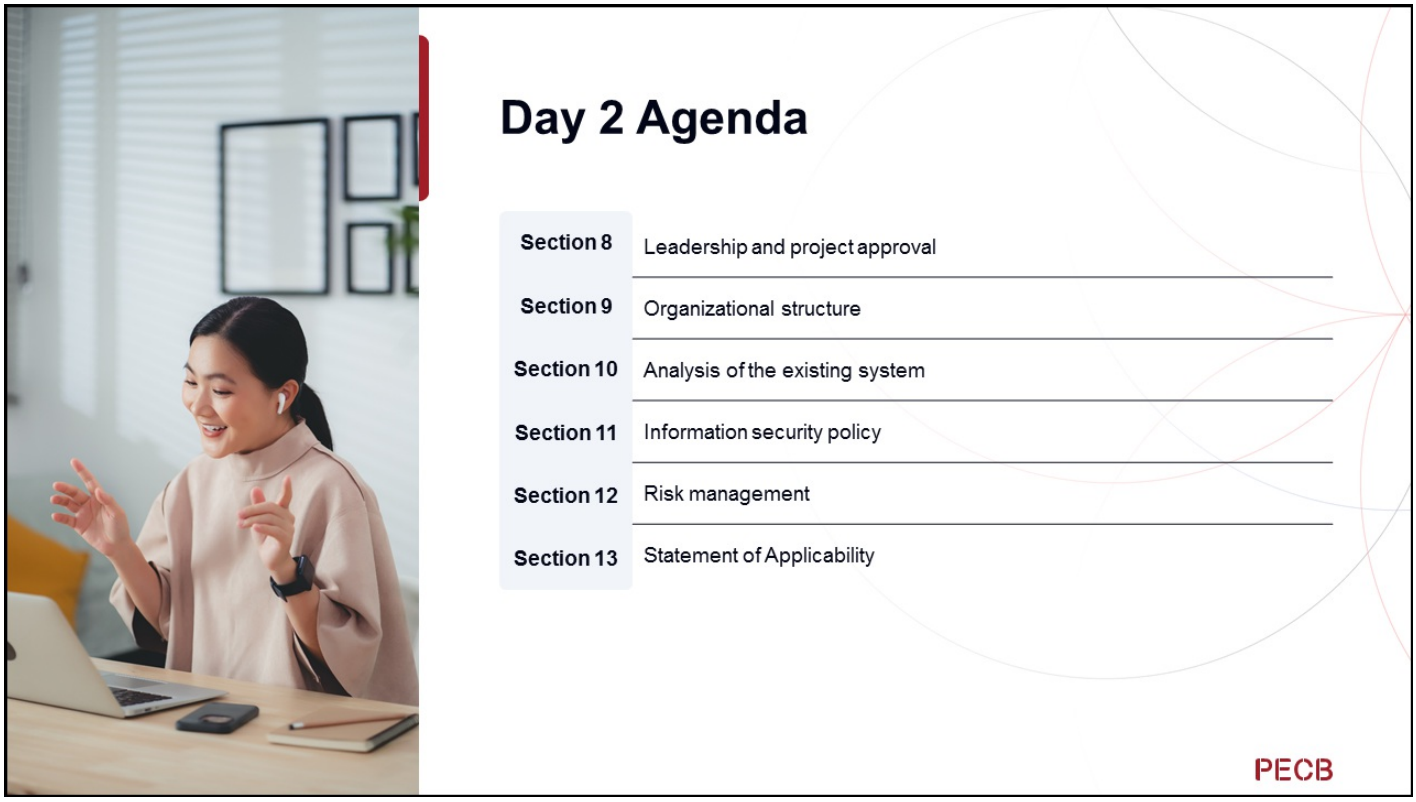
DAY 2

Certified ISO/IEC 27001 Lead Implementer

Version 10.0

Document number: ISMSLID2V10.0



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

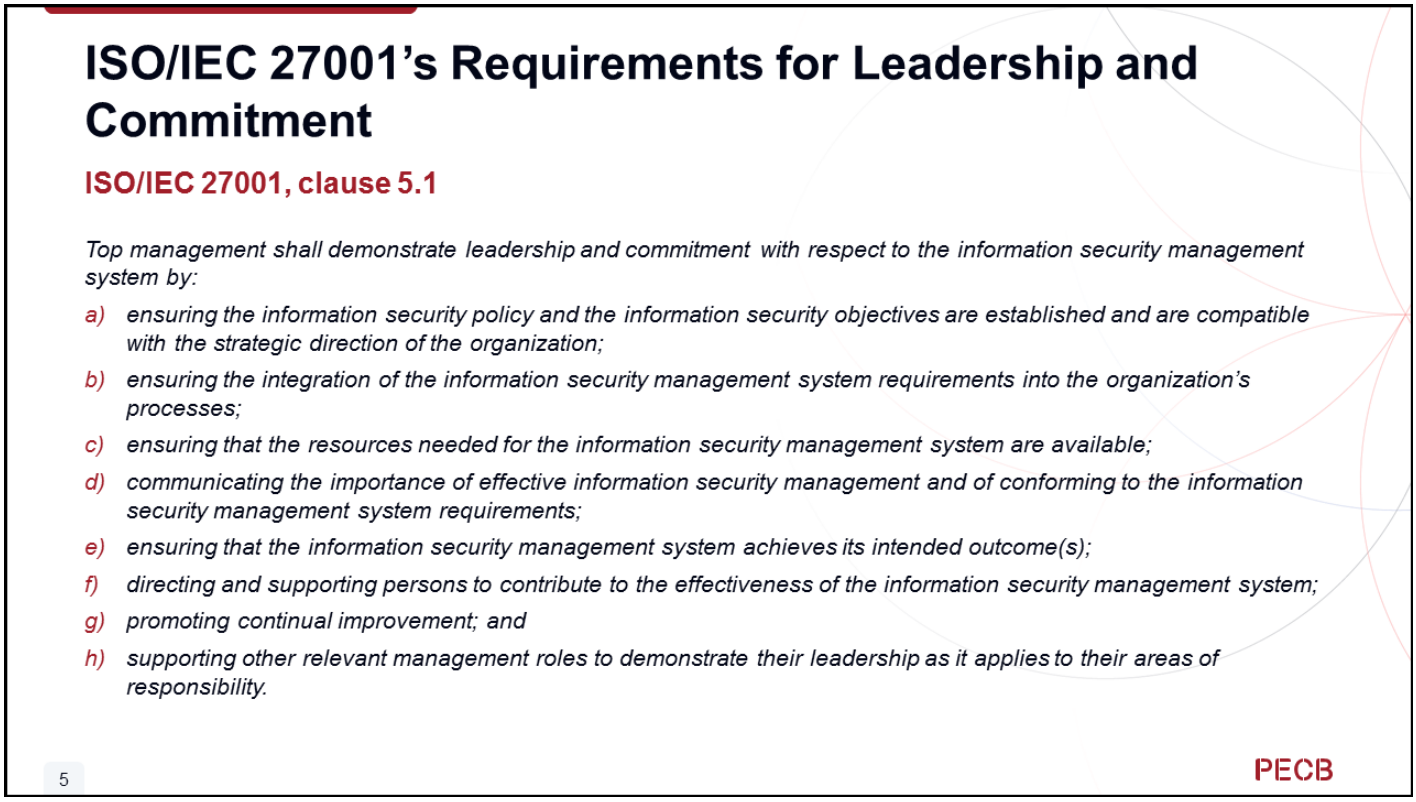
1. Establish a project team and ensure project approval for the ISMS implementation
2. Conduct a gap analysis and create a gap analysis report
3. Develop information security policies and security specific policies
4. Establish a risk management process
5. Review and select the applicable information security controls and develop a Statement of Applicability

This section provides information that will help participants in understanding the importance of the management involvement in the ISMS project and the roles and responsibilities of the individuals relevant to the project, and in developing a project plan.

Leadership and Project Approval

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

PECB

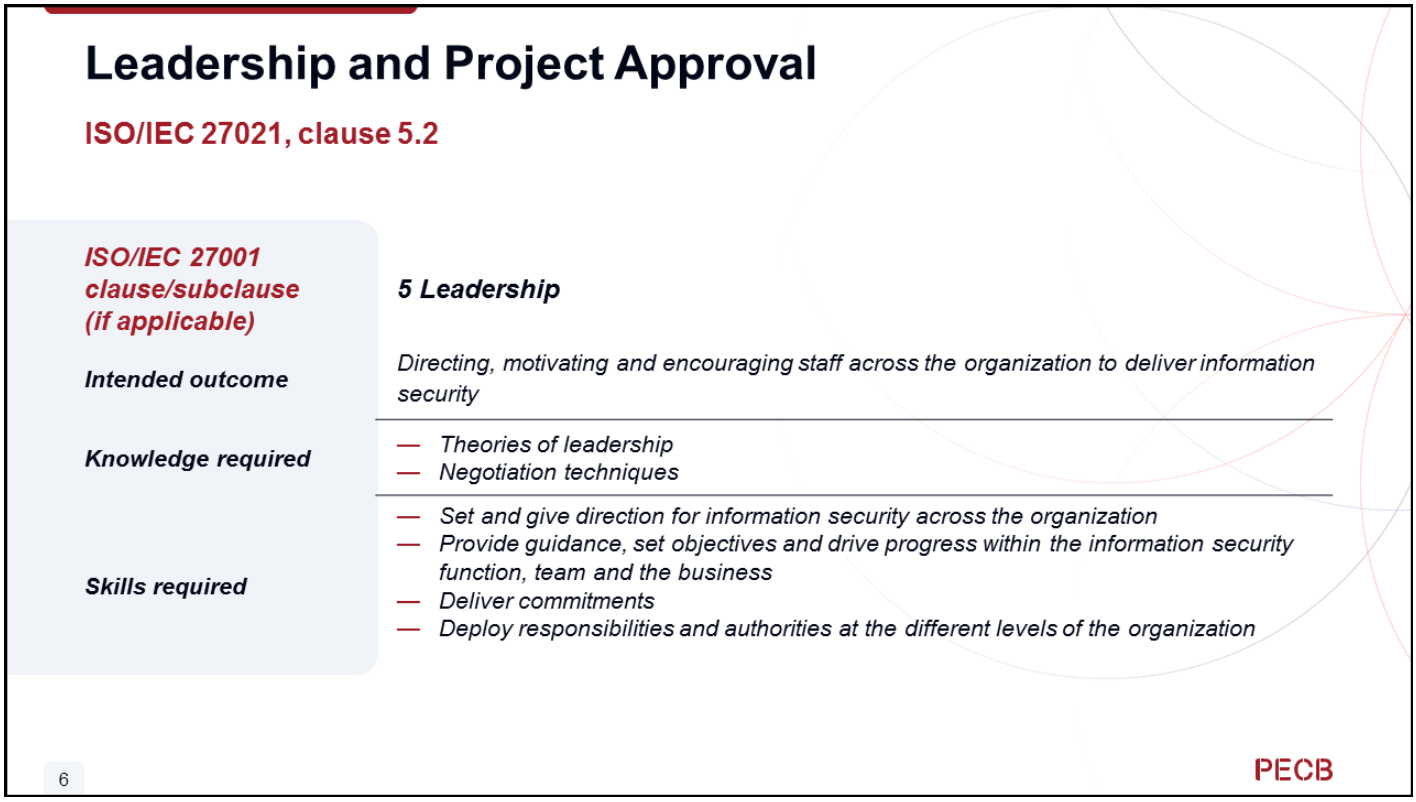


ISO/IEC 27001, clause 5.1 Leadership and commitment (cont'd)

NOTE: Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

An organization aiming to ensure compliance with ISO/IEC 27001 must:

1. Ensure its management demonstrates leadership and commitment to implement and maintain the ISMS
2. Allocate the necessary resources to implement and maintain the ISMS



Through its leadership and commitment, the management can create an environment in which all actors are fully involved and where the ISMS can operate effectively in alignment with organizational objectives. The management can use the management principles of ISO to define its role, which involves:

- Establishing the policies and setting the objectives of the organization
- Promoting policies and objectives at all organizational levels to increase awareness, motivation, and involvement
- Ensuring that the requirements of interested parties (customers, partners, shareholders, legislators, etc.) are considered at all organizational levels
- Implementing the appropriate processes and controls to meet requirements
- Establishing, implementing, and maintaining an efficient and effective ISMS
- Allocating the necessary resources
- Ensuring that internal audits are being conducted
- Conducting management reviews at least once a year
- Deciding on actions concerning the policy and objectives
- Deciding on actions to improve the management system

Note: The CISO and the CIO are two different positions 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. The 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.

1.3 Leadership and Project Approval

List of activities

Determine the ISMS resource requirements

Plan the ISMS project

Establish the ISMS project team

Ensure management approval for the ISMS project implementation

PECB

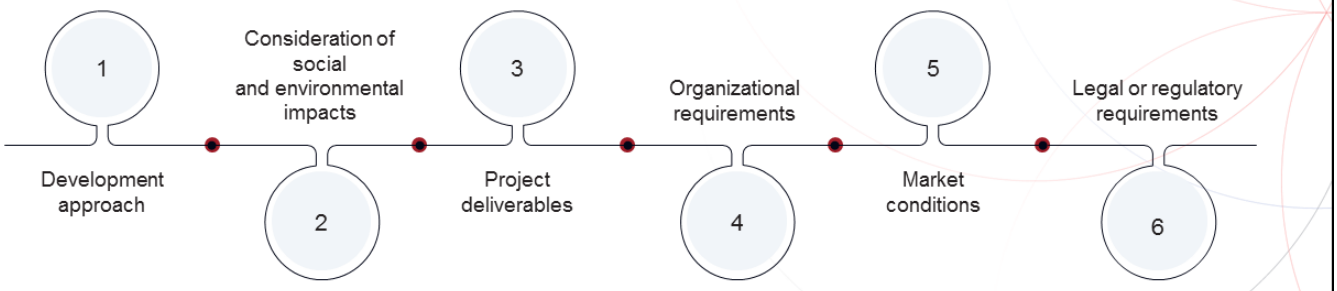
1.3.1 Determine the Necessary Resources for the ISMS

- To successfully implement the ISMS, the project manager must determine the necessary resources.
- Such resources include, but are not limited to:
  - People
  - Information and data
  - Facilities, equipment, and consumables
  - Information and communication technology (ICT) systems
  - Transportation
  - Money
  - Partners and suppliers

1.3.2 Plan the ISMS Project

PMBOK, 7th Edition

Several factors influence how project planning is conducted, including[1]:



10

PECB

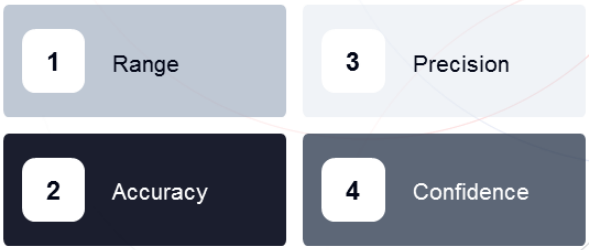
1. **Development approach: T**he chosen approach for project development can impact the timing, extent, and frequency of planning. Project planning approaches can vary, with some projects incorporating an early dedicated planning phase and progressive elaboration of plans, while others involve high-level planning followed by design and subsequent detailed planning after stakeholder agreement.
2. **Consideration of social and environmental impacts:** Initial planning now encompasses social, environmental, and financial impacts (the triple bottom line), involving product life cycle assessments that evaluate environmental effects and inform design decisions for sustainability, toxicity, and environmental concerns.
3. **Project deliverables:** The nature of project deliverables often dictates the specific planning requirements. Construction projects, for instance, necessitate extensive upfront planning to accommodate design, approvals, material procurement, logistics, and delivery. On the other hand, product development or high-technology projects may employ continuous and adaptive planning to accommodate stakeholder feedback and technological advancements.
4. **Organizational requirements:** Organizational governance, policies, procedures, processes, and culture may impose specific planning expectations on project managers, resulting in the production of particular planning artifacts.
5. **Market conditions:** Projects in highly competitive environments, such as product development, may prioritize speed to market over extensive upfront planning. In such cases, minimal planning is undertaken to minimize the cost of delay, even if it increases the risk of potential rework.
6. **Legal or regulatory requirements:** Regulatory bodies or laws might necessitate particular planning documentation as a prerequisite for granting permission to proceed or endorsing the launch of project deliverables in the market.

Estimates for the ISMS Project Plan

PMBOK, 7th Edition

- Project planning involves estimating different project aspects like work effort, duration, costs, personnel, and resources. These estimates quantify expected outcomes such as project costs and duration.
- An estimate may change during the project life cycle if changes occur to circumstances or the information in which the estimate was based.

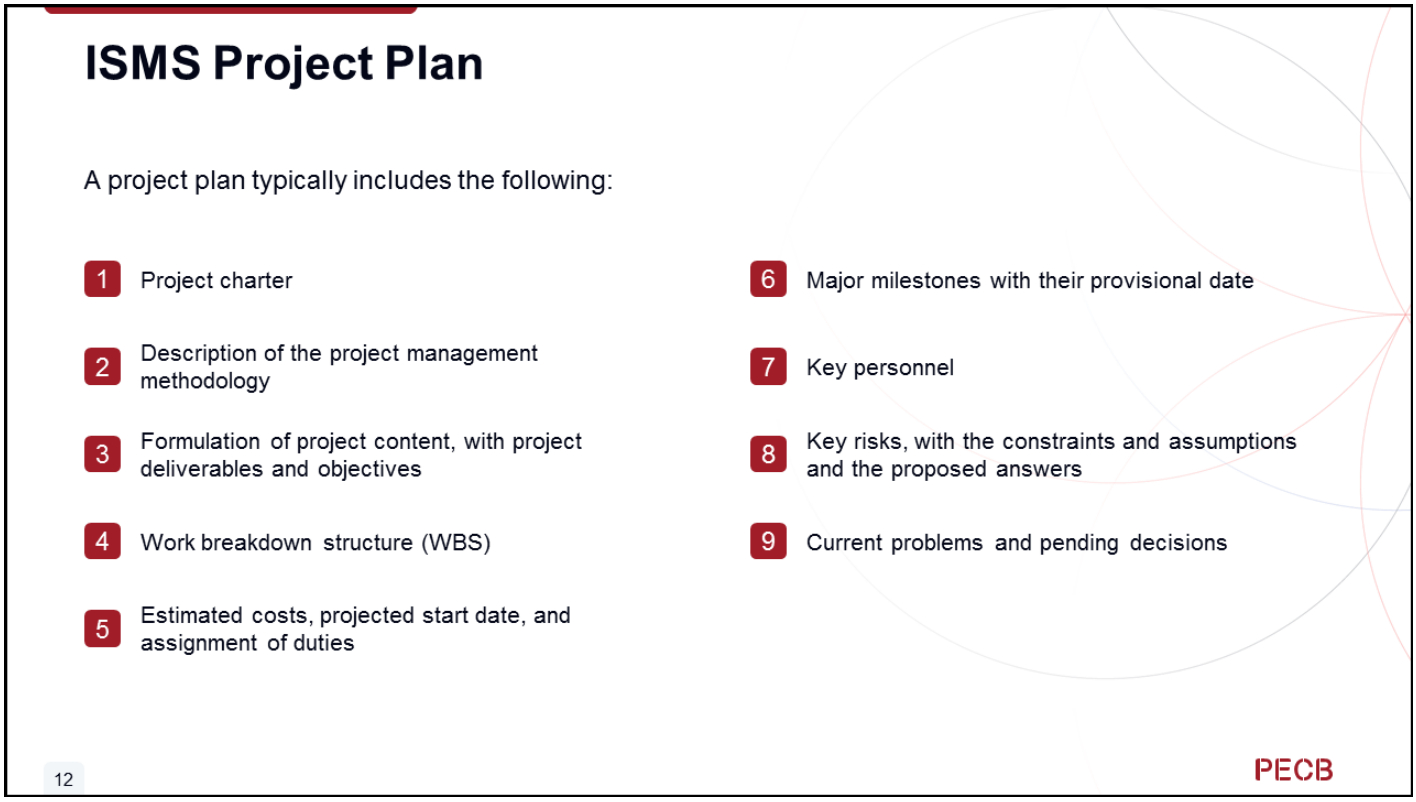
The main aspects related to estimating that may change during the project life cycle are[1]:



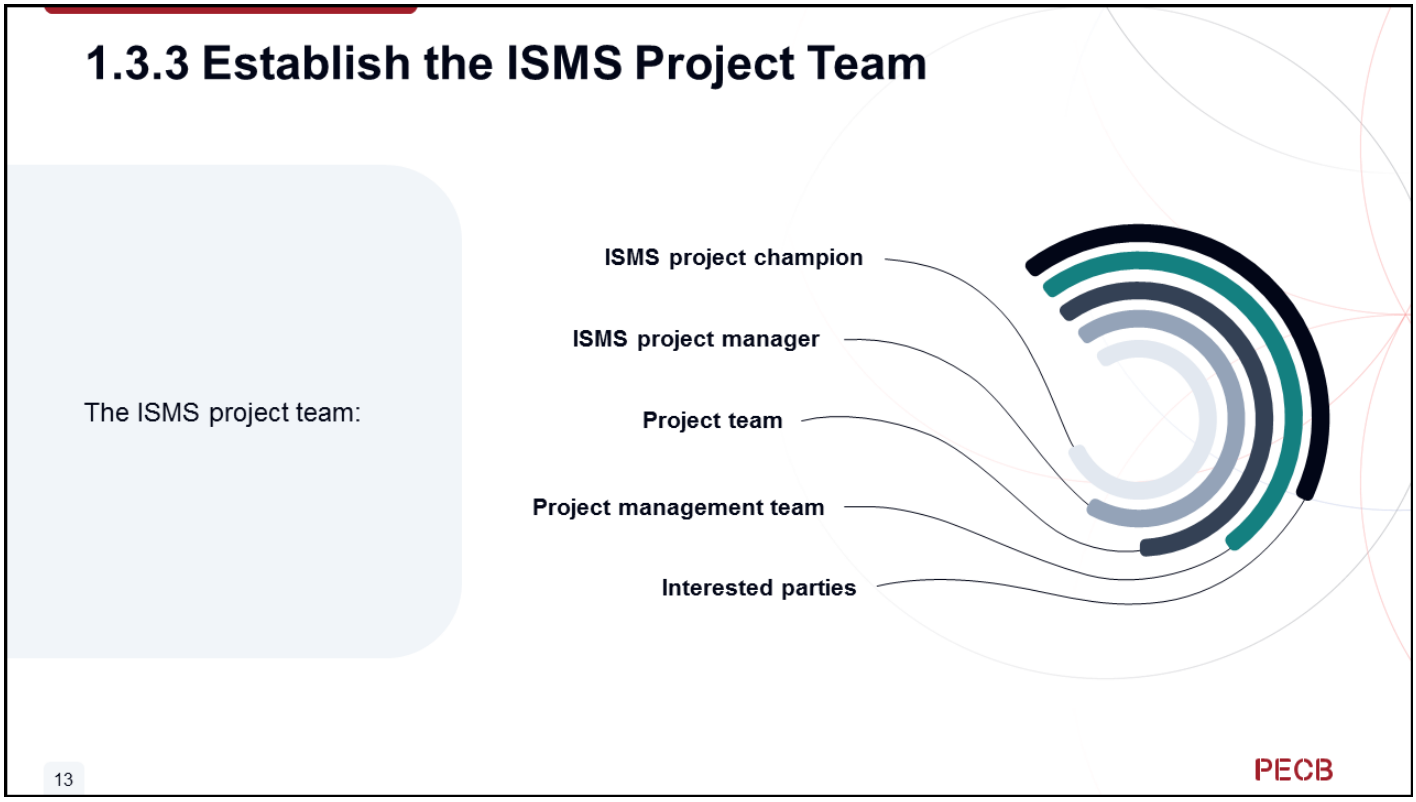
11

PECB

1. **Range** refers to the span of potential values within which an estimate may fall. At the initiation of a project, when information about the project scope, stakeholders, requirements, and risks is limited, estimates tend to have a broad range. As projects advance and more information becomes available, the range narrows. Lastly, projects well along in their life cycle have even more limited range.
2. **Accuracy** describes how correct an estimate is. The level of accuracy is linked to the range; lower accuracy corresponds to a larger potential range of values. An estimate provided at the beginning of a project is likely to have less accuracy than one developed halfway through the project as more details are known and uncertainties are reduced.
3. **Precision** denotes the level of exactitude associated with an estimate. Precision in estimates should align with the desired level of accuracy, ensuring a clear and specific understanding of the anticipated outcome.
4. **Confidence** reflects the team's assurance in the reliability and validity of the provided estimates. It depends on experiential knowledge. Previous exposure to similar projects enhances confidence levels. However, when dealing with advanced technological components where prior experience is limited, confidence in estimates is likely to be lower.



The initial project plan can be used to create project plans for subprojects for particular milestones within the big project.



Usually, the ISMS project team consists of the following:

1. **ISMS project champion:** This role is usually appointed to someone close to the decision-making level of the organization. They act as a project sponsor who ensures that the necessary resources are allocated and the project can be completed.
2. **ISMS project manager:** The project manager has a central role in the project as the success of the project depends on their work and commitment. They are responsible for all the activities in the project and for leading the project team. They are also responsible for planning the project activities in order to reach the set objectives, encouraging the project team and taking into consideration their ideas and opinions, working with the project champion to clarify and formalize the objectives, discussing the resources needed for the project, and organizing user workshops or involving users early in the project to identify their needs.
3. **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. To improve the performance of the team in charge of the ISMS project, the necessary training, tools, techniques should be provided. It is worth noting that 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. The members of this team are responsible for executing the project's tasks that are necessary to accomplish its objectives.
4. **Project management team:** This team is a subset of the project team and consists of all the persons acting under the management of the project manager that are responsible for assisting in strategic decisions and policies and helping in reaching the objectives set for the project. The members of this team are specifically engaged in project management activities.
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. The organization should strive to achieve a balance between its interests and needs and the needs and interests of its interested parties.

ISMS Project Manager

The ISMS project manager should have:

- Knowledge and skills in project management
- Knowledge of the organization and its context
- Knowledge of 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

1.3.4 Ensure Management Approval for the ISMS Project Implementation

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 organizational 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

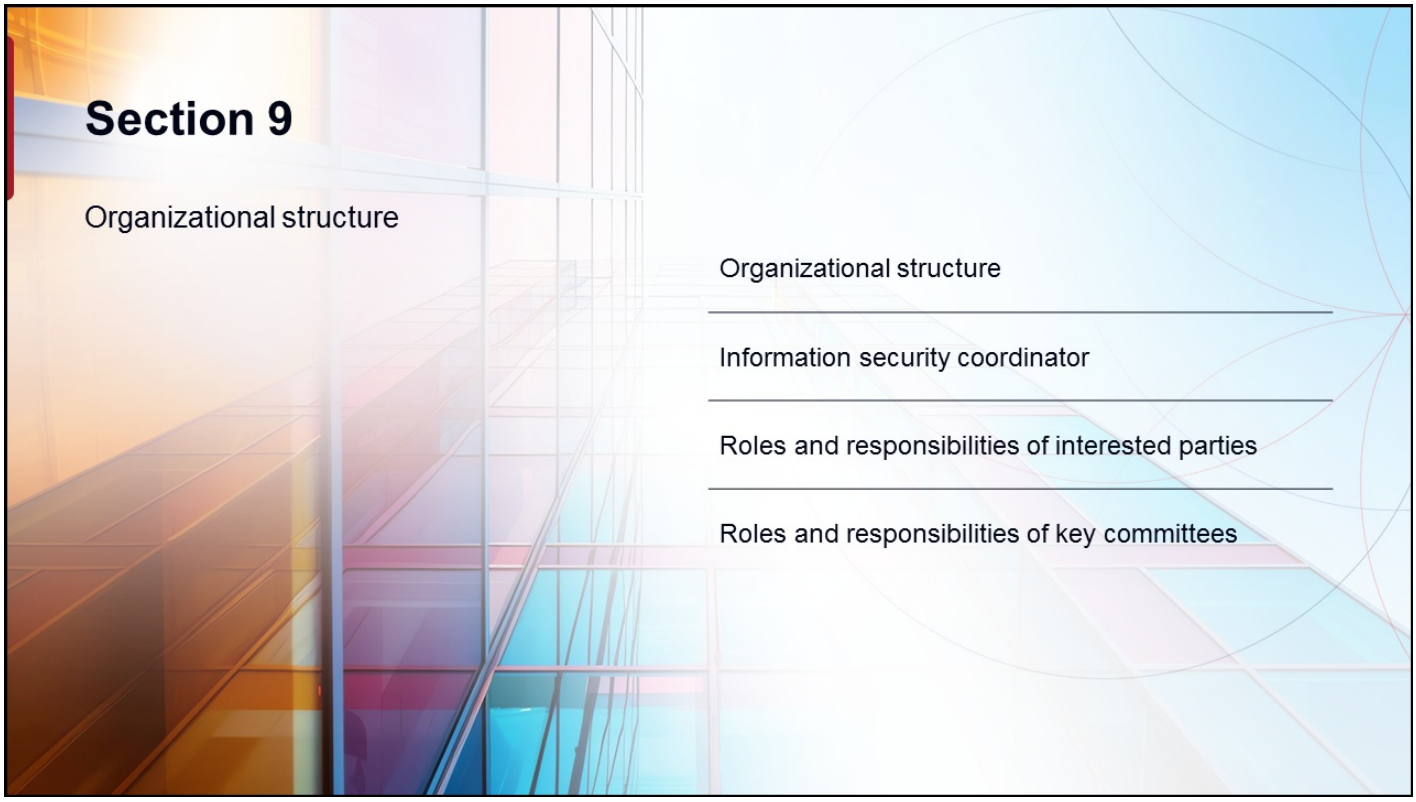
Section 8 Summary

- The management can create a collaborative environment in which the contribution of all organizational staff is encouraged and promoted.
- The ISMS project team includes the project champion, the project manager, the project management team, the project team, and the interested parties.
- The main aspects that may change and should be considered during the project life cycle are range, accuracy, precision, and confidence.
- A project plan includes, among others, a project charter, the key personnel, a description of the project management methodology.

Questions?

Quiz 7

Note: To complete Quiz 7, please go to the Quizzes Worksheet.

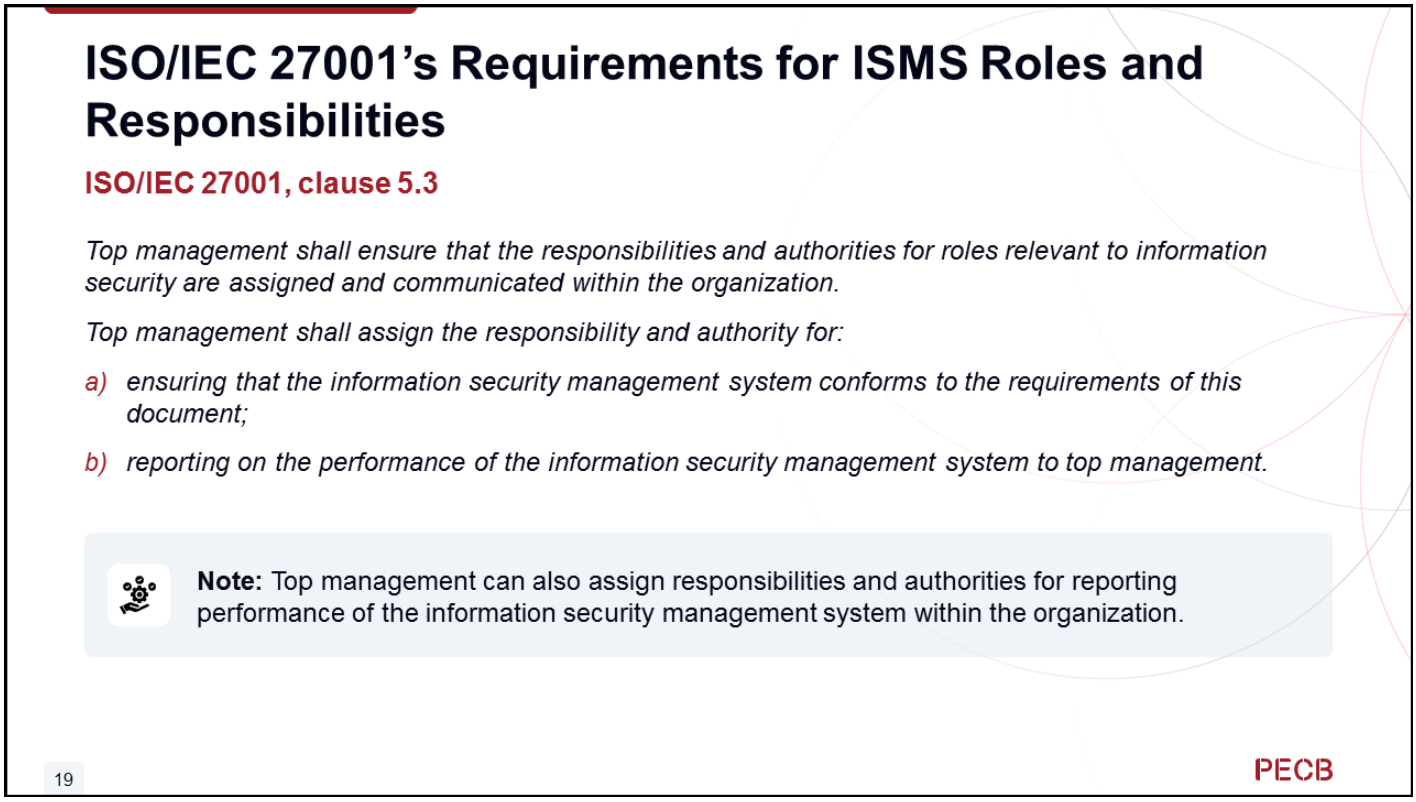


This section provides information that will help the participant gain knowledge on the organizational structure and the roles and responsibilities of interested parties and committees.

Organizational Structure

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

PECB



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.*

1.4 Organizational Structure

List of activities

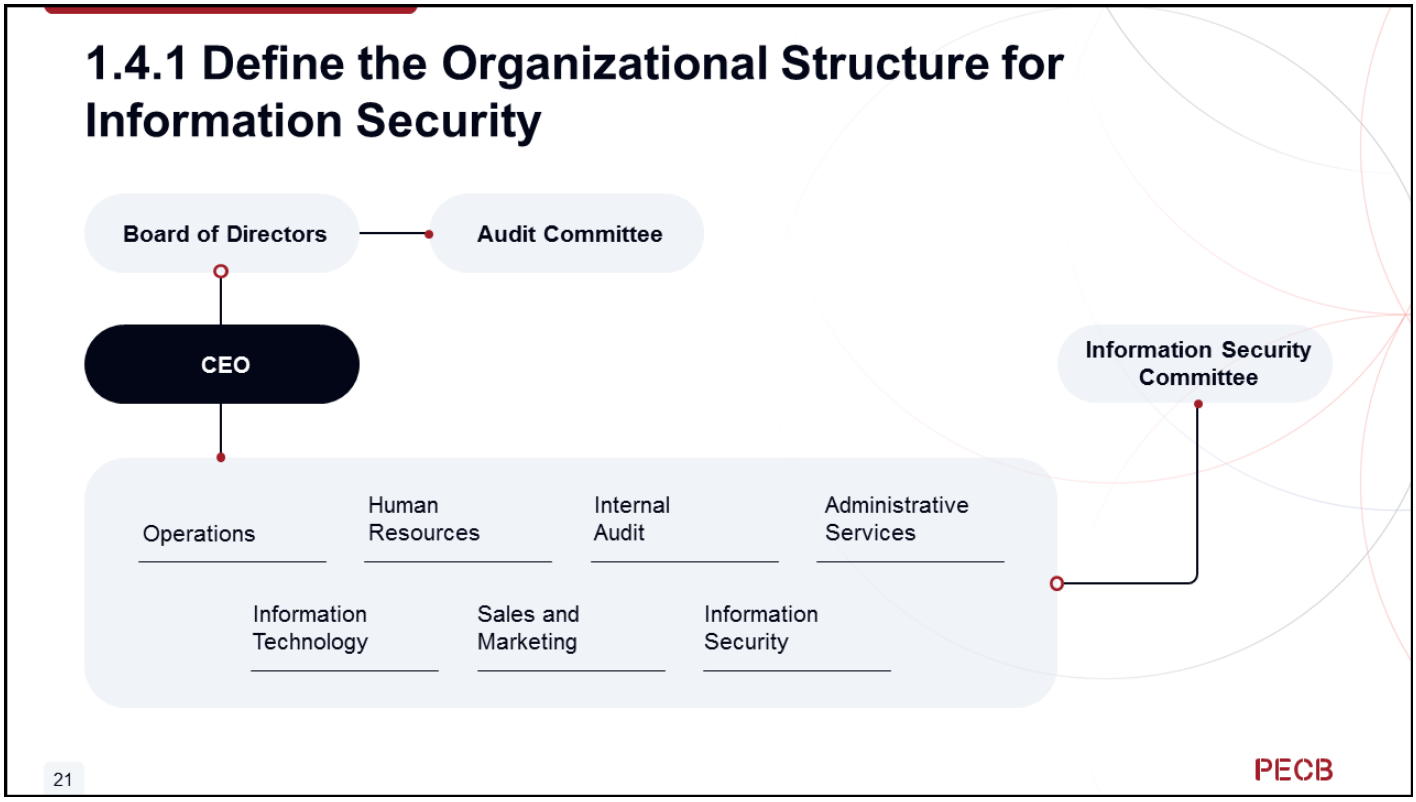
Define the organizational structure for information security

Appoint an information security coordinator

Assign the roles and responsibilities of interested parties

Define the roles and responsibilities of key committees

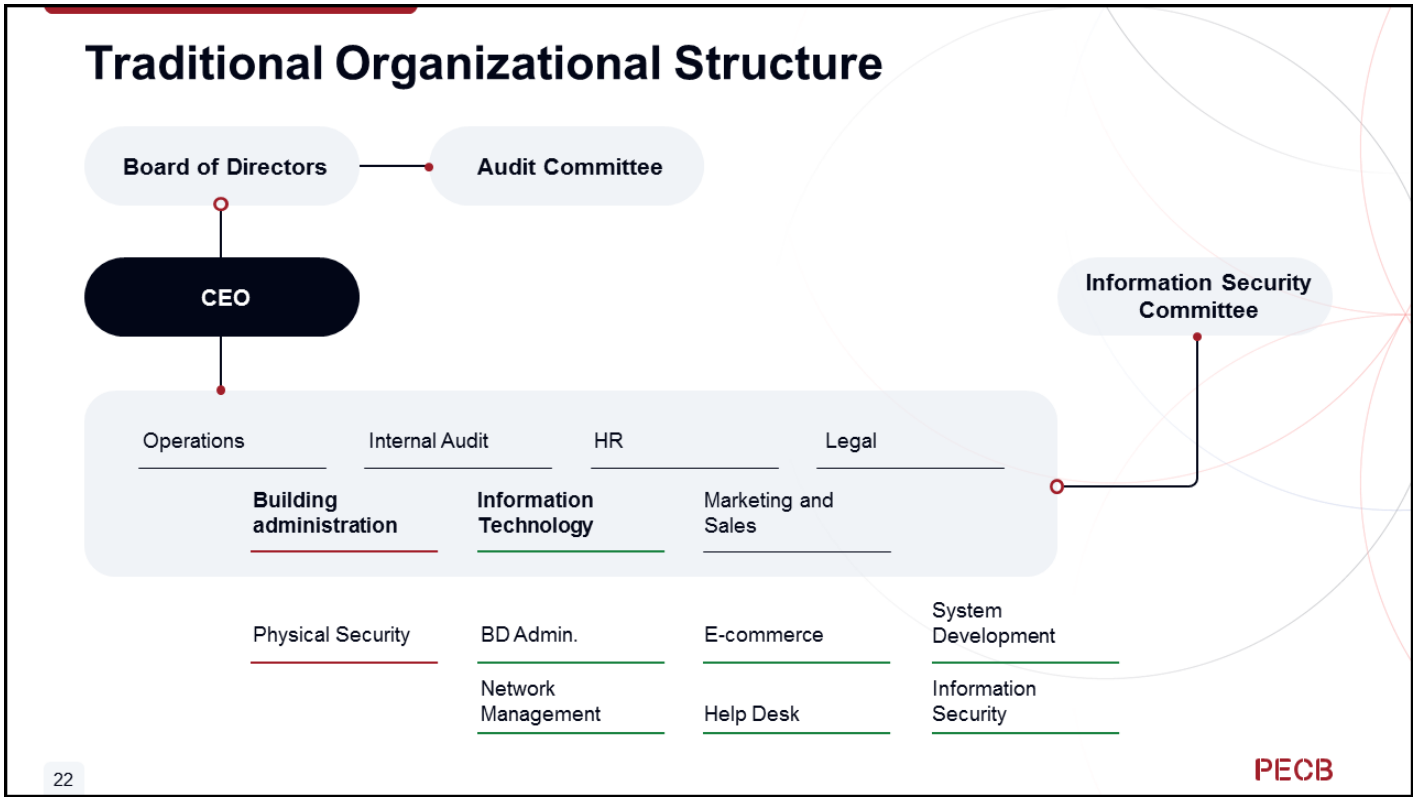
PECB



Before defining the structure of information security governance, the organization must consider several factors, including 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:

- Minimization of conflicts of interest
- Appropriate decision-making authority
- Strong support from top management
- High influence ability
- Consideration of all security concerns
- Information coverage regardless of the medium of communication



Traditionally, the information security team is attached to the IT Department of the organization. This is a commonly used model for information security governance. The main advantage of this model is that the technology and information security expertise are part of 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. Real or potential conflicts of interest
3. Poor consideration of issues related to information security
4. Issues mainly focus on operational security and technology

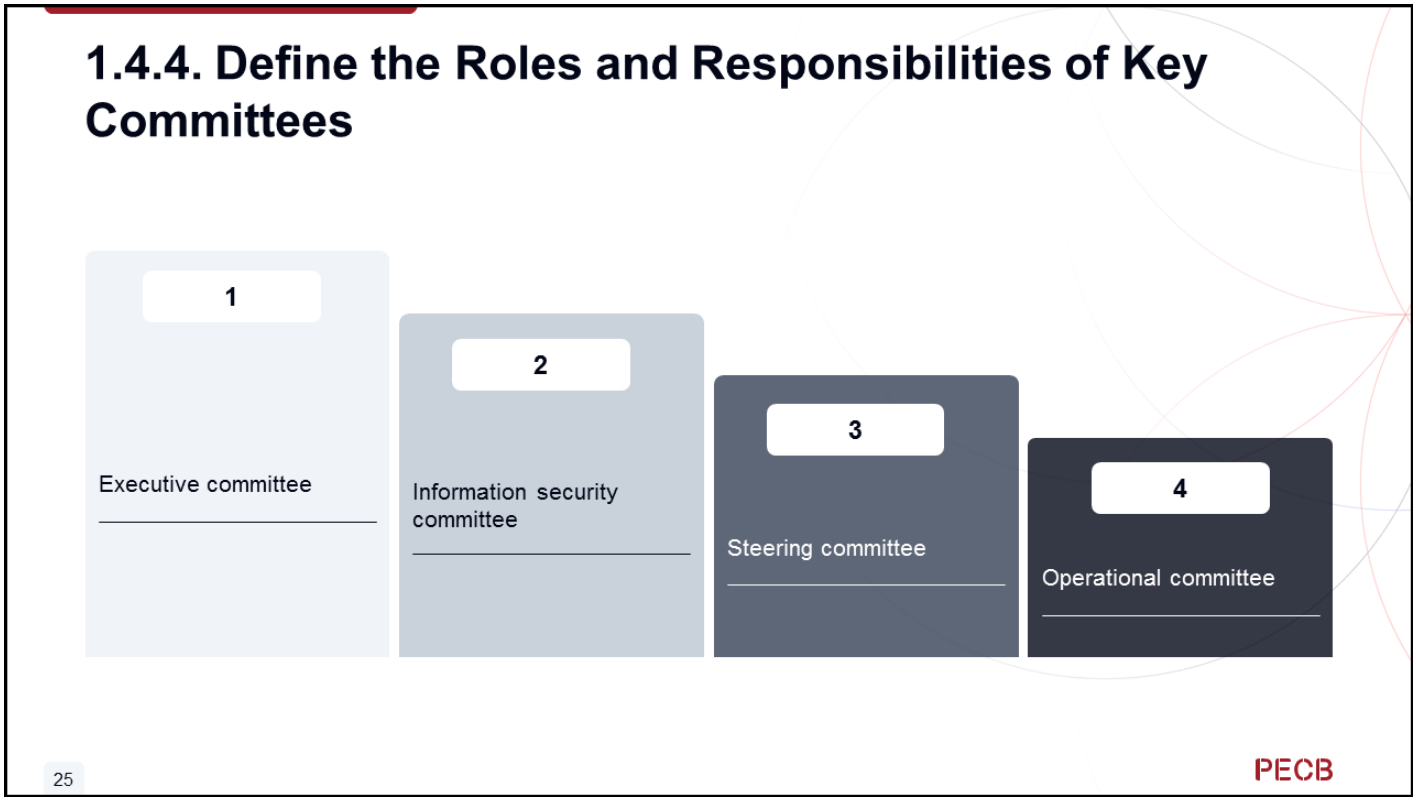
1.4.2 Appoint an Information Security Coordinator

- Information security activities should be coordinated by representatives of different parts of the organization that play relevant roles within 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

The roles and responsibilities of the interested parties who have a function or tasks directly related to the ISMS should be clearly defined. Their roles can be documented in several ways, e.g., in organizational charts, employment contracts, and policies.

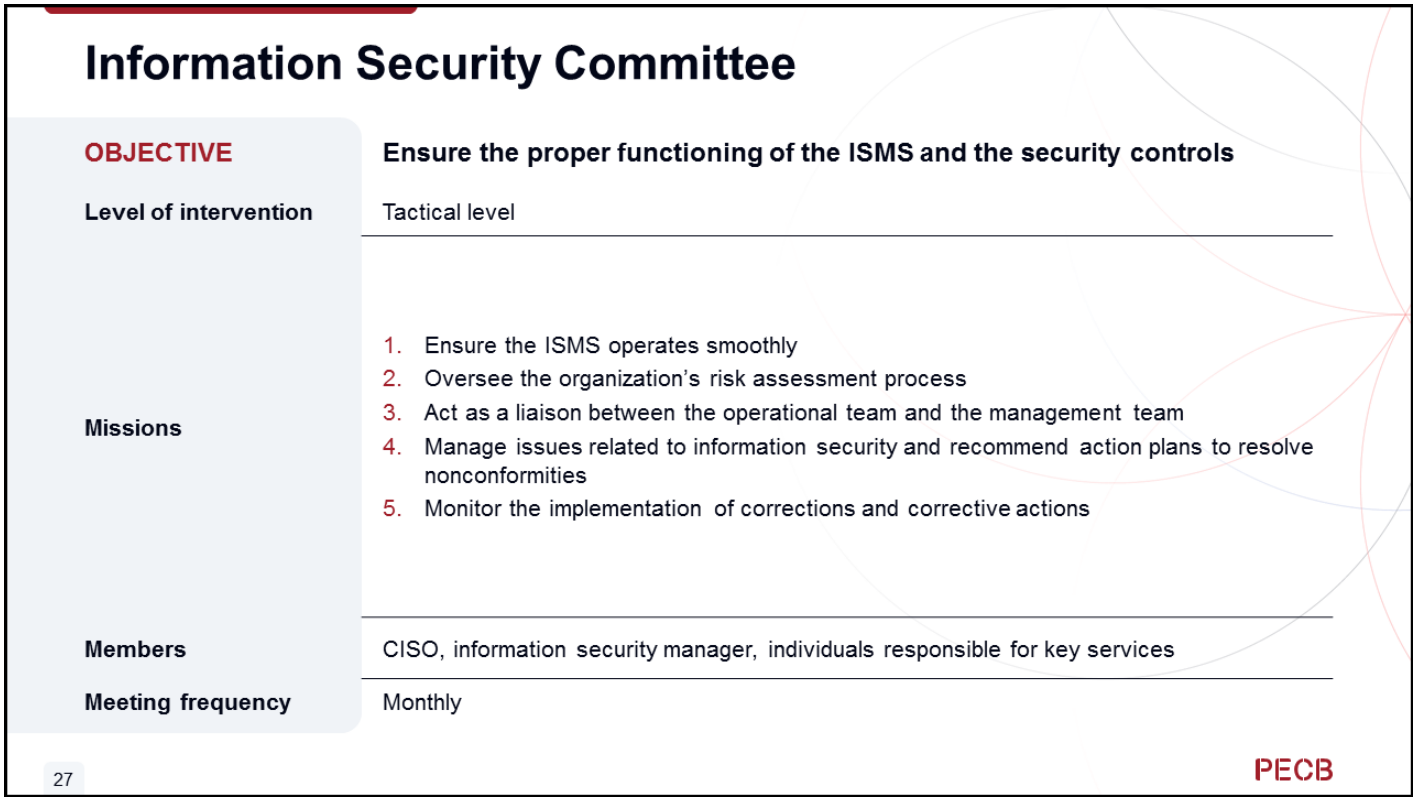


It is important to have in mind that creating these committees is not a necessity. As such, it is common to expand the scope of existing committees.

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

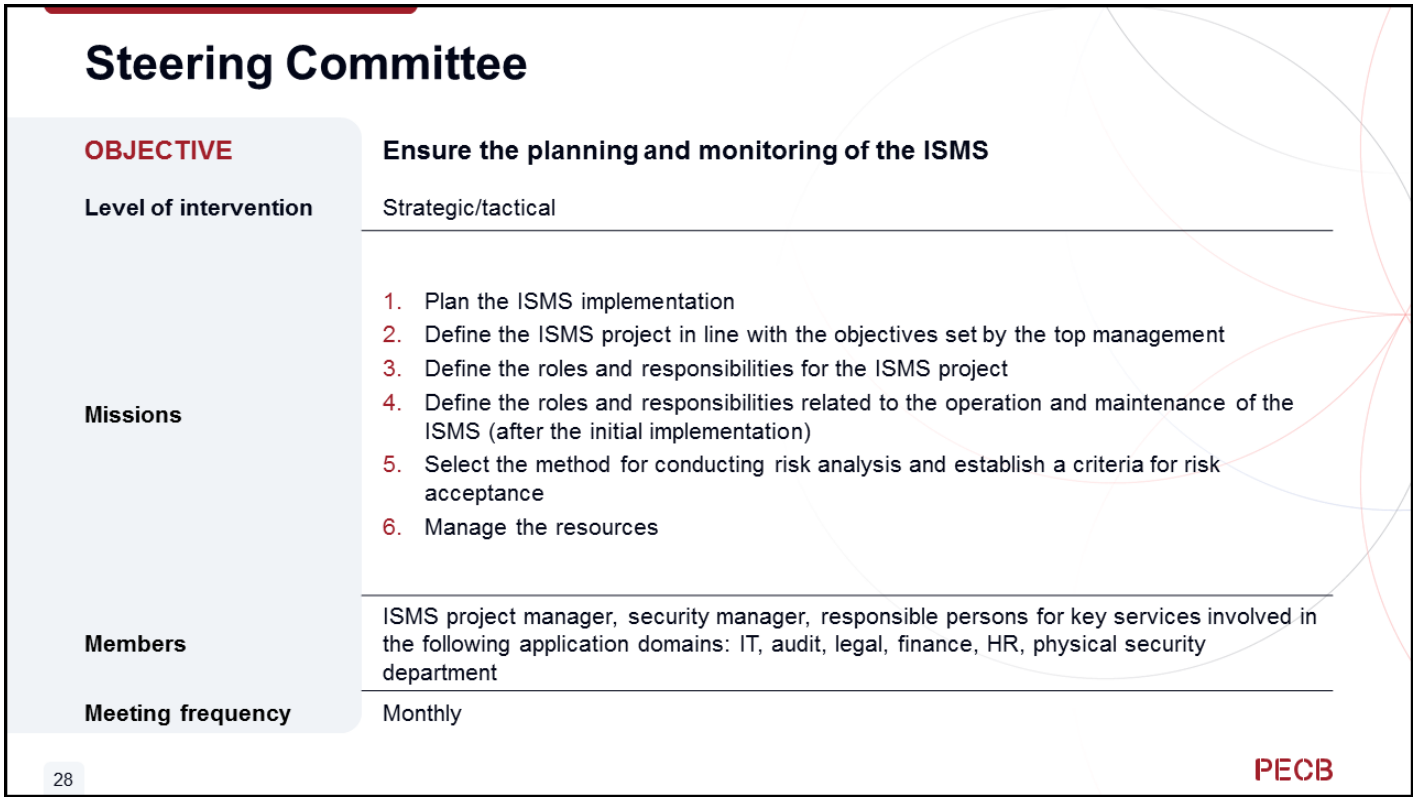
The executive committee is the body of guidance, control, validation, decision-making, and arbitration for the ISMS. It is composed of representatives of the Board of Directors of the organization. It is the only committee that is a requirement of ISO/IEC 27001 and its minimum meeting frequency should be once a year.

Organizations rarely establish specific executive committees for information security. Usually, the executive committee of the organization is responsible for the duties listed in the slide.



This committee consists of representatives from various divisions within the organization and it is usually chaired by the CISO.

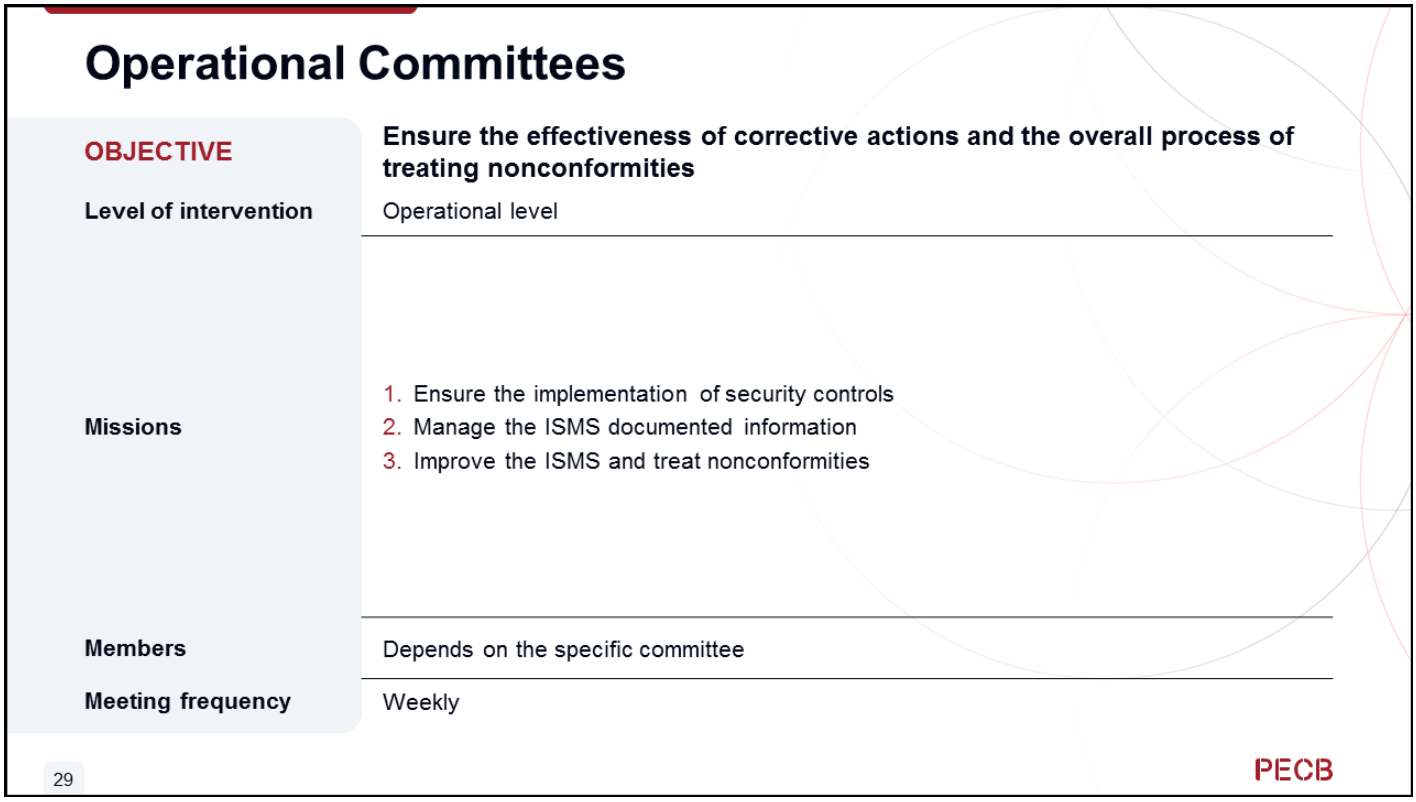
To avoid creating numerous committees within the organization, the information security committee may assume the role of the emergency committee in the event of a major incident.



The steering committee of a project involves the organization's key personnel and experts in the field to ensure the effectiveness of the project. At least the project champion and project manager should be part of the steering committee.

The level of intervention of the steering committee is both strategic and tactical because it provides direction and guidance regarding the project implementation and is involved in making decisions about project-related issues.

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



Depending on the size of the organization and its culture, certain information security responsibilities 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.

Operational committees collaborate to ensure the effective implementation of the necessary security controls. Examples of operational committees may include risk management committee, compliance and audit committee, business continuity committee, and data protection committee, among others.

The CISO can participate in various committees as a member or be represented by an information security liaison officer.

Section 9 Summary

- The roles and responsibilities of the interested parties with a function or tasks directly related to the ISMS should be clearly defined. Their roles can be documented in several ways, e.g., in organizational charts, employment contracts, and policies.
- Typically, information security coordination should involve the cooperation of managers, users, administrators, application designers, auditors, security personnel, and experts in areas such as insurance, legal issues, human resources, IT, and risk management.
- Key committees relevant to the ISMS include the executive committee, the information security committee, the steering committee, and the operational committee.

Questions?

Quiz 8

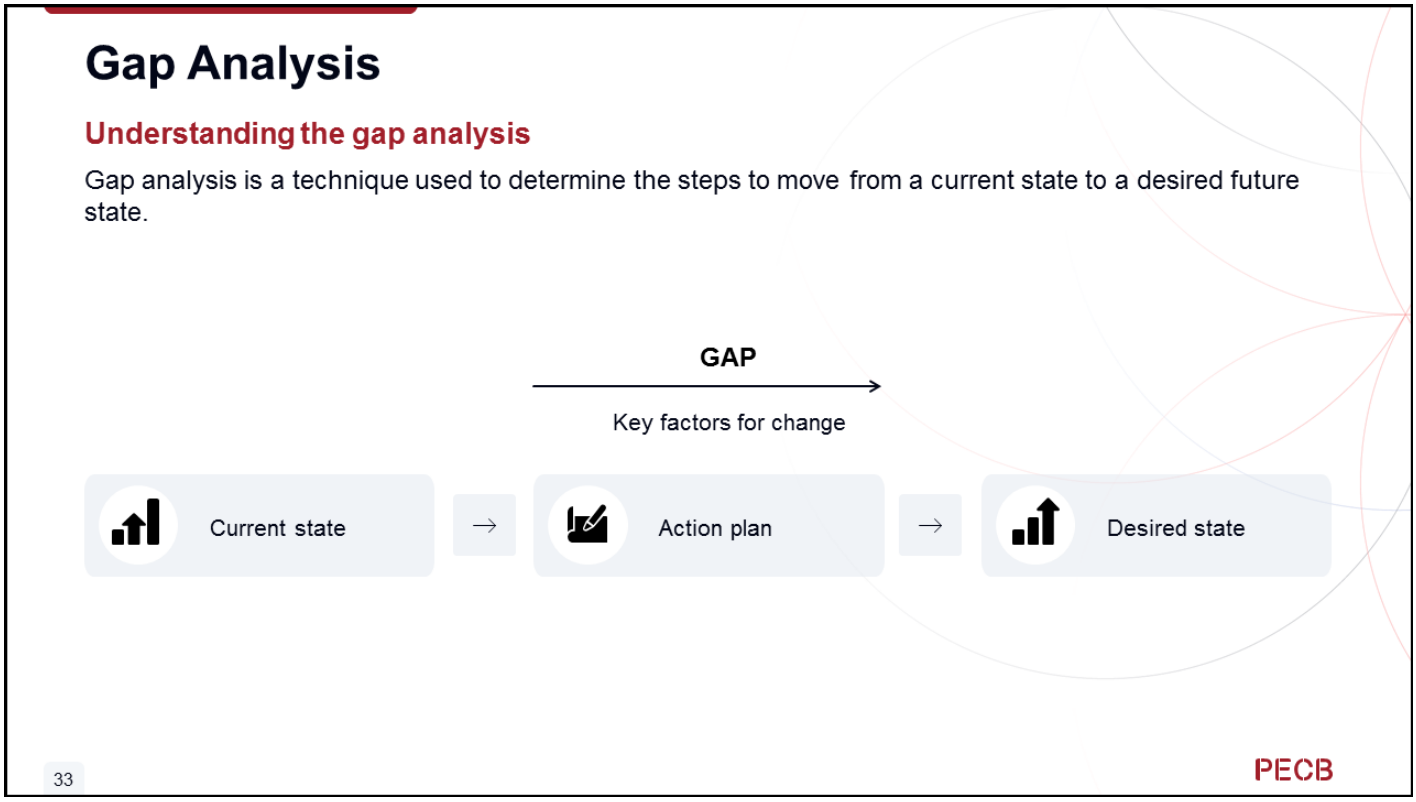
Note: To complete Quiz 8, please go to the Quizzes Worksheet.

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

Analysis of the Existing System

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

PECB

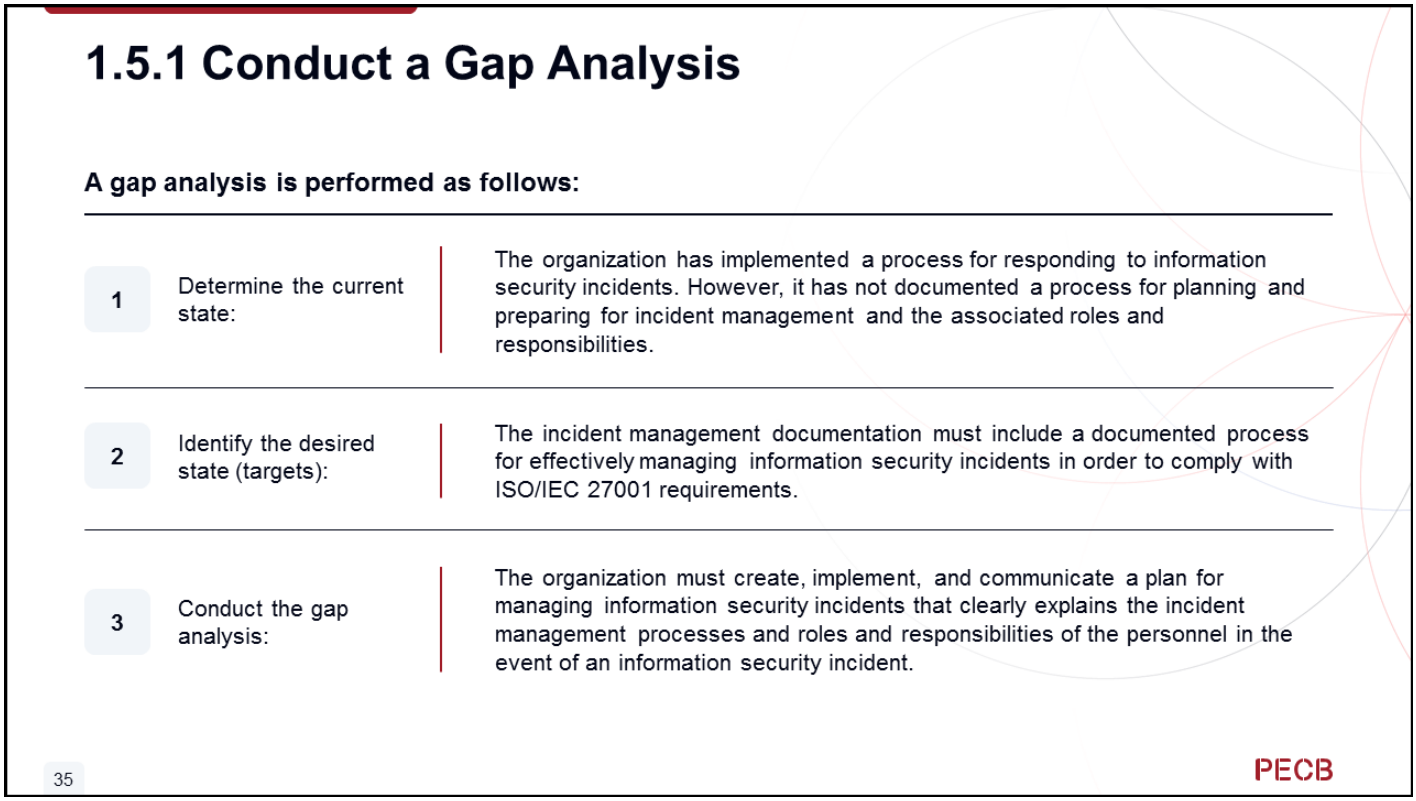


Gap analysis is conducted to determine the current state, the desired state, and the difference between the two.

1.5 Analysis of the Existing System

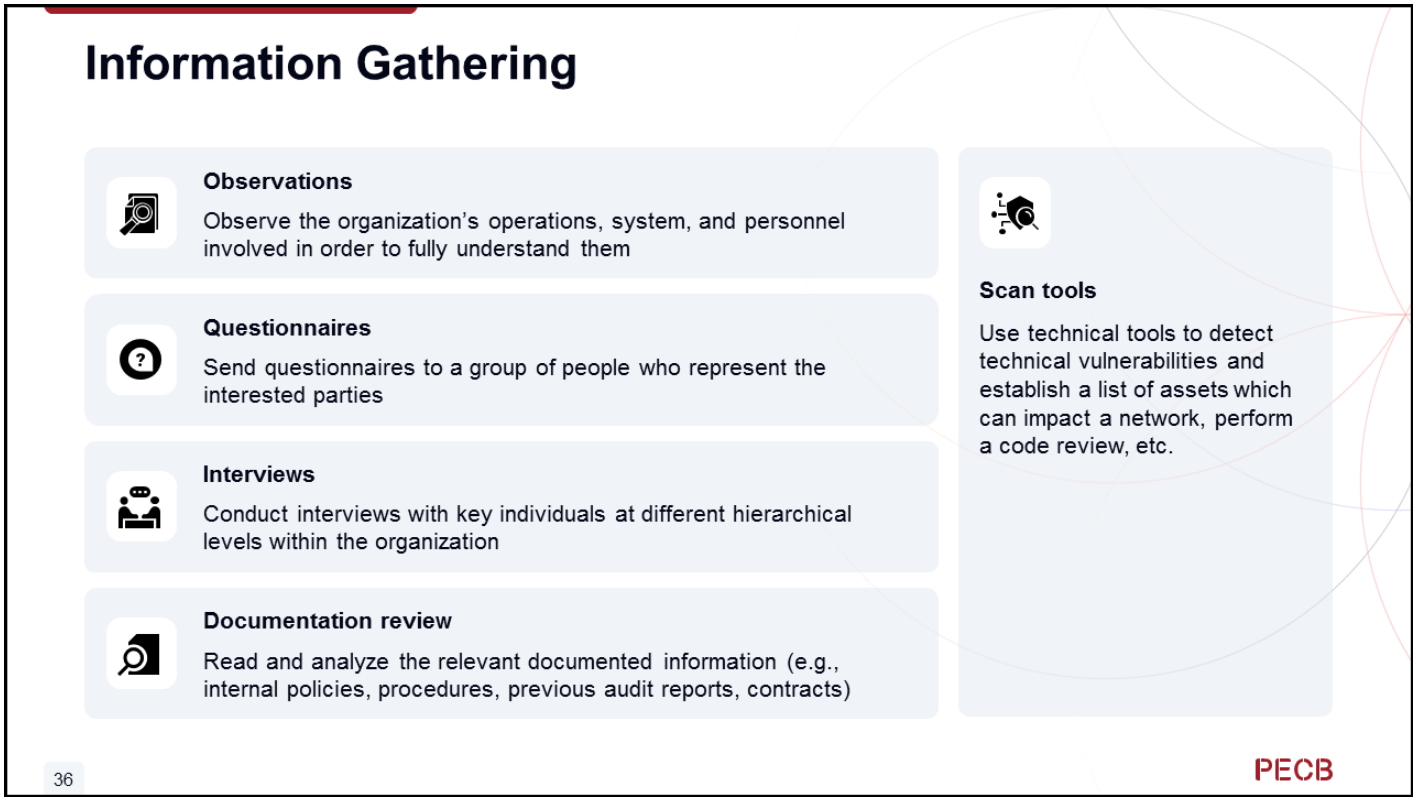
List of activities

PECB



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

Gap analysis helps identifying and measuring the investments in time, money, human, and other resources to effectively implement the ISMS.



The project manager in cooperation with the project team should collect information from multipl=e interested parties in order to have an understanding of the existing management system.

When determining the state of the existing management system, the project manager should take into account many factors, such as the method used to collect data, the individuals to be interviewed and their skills and knowledge, the availability of resources (e.g., budget, time), etc.

The following actions can be helpful in collecting information about an organization:

- Observe the organization's on-site information security processes and controls
- Conduct interviews with the individuals responsible for the management and daily operations of the ISMS
- Review the documented information containing the information security measures (processes, procedures, description of controls, reports, etc.)
- Review the internal audit reports

Conduct Interviews

Recommendations when conducting interviews:

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

37

PECB

Preparation is one of the key elements of a productive interview. An effective strategy can be to create checklists that ensure a systematic conduct of interviews and obtainment of relevant information from them. Checklists should have a section for answers, comments, and observations, as well as references to related standards, where applicable.

During the interview, it may be useful to clarify the specialized terminology related to the information security management system, such as “threats and vulnerabilities,” in a language that is more comprehensible for the interviewees.

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 interviewee is a member of the top management)
  - **Example:** Discussion with an employee from the IT Department, February 20, 2024
- **Interview objectives**
  - **Example:** Validate whether the organization has conducted trainings in accordance with its policy
- **Summary of the collected evidence** (The documented information should be collected in a clear, concise, and accurate language; only facts, not judgments, should be included; any weaknesses should be identified and reported in the gap analysis; the reference to the related standard should be listed with the clause number.)

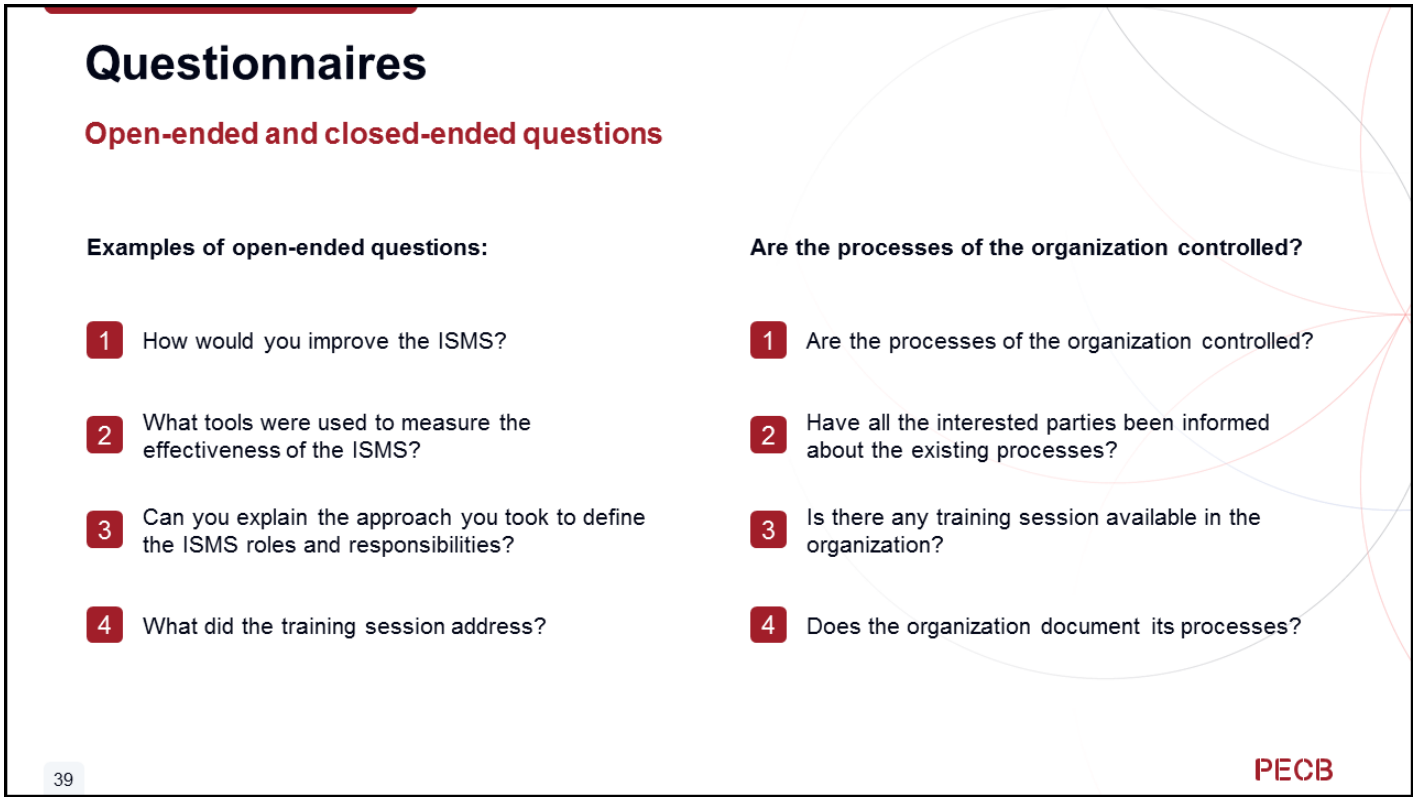
Interested parties, be them experts or not, should be interviewed regarding their activities and tasks in order to obtain information regarding information security risks in their field. Individuals responsible for business processes will provide a much more “business” oriented view on risks, e.g., the public relations officer will indicate concerns about a risk in the organization’s reputation.

Individual interviews:

The most significant advantage of individual interviews is that interviewing only one person at a time allows the interviewer to obtain more detailed information about the ISMS. In this way, the interviewer will be able to get a more comprehensive understanding of the organization and its ISMS. The interviewer is able to read the body language of the interviewee and can ask for further explanation of responses. However, the interview length can be time-consuming if there are a lot of people to be interviewed.

Group interviews:

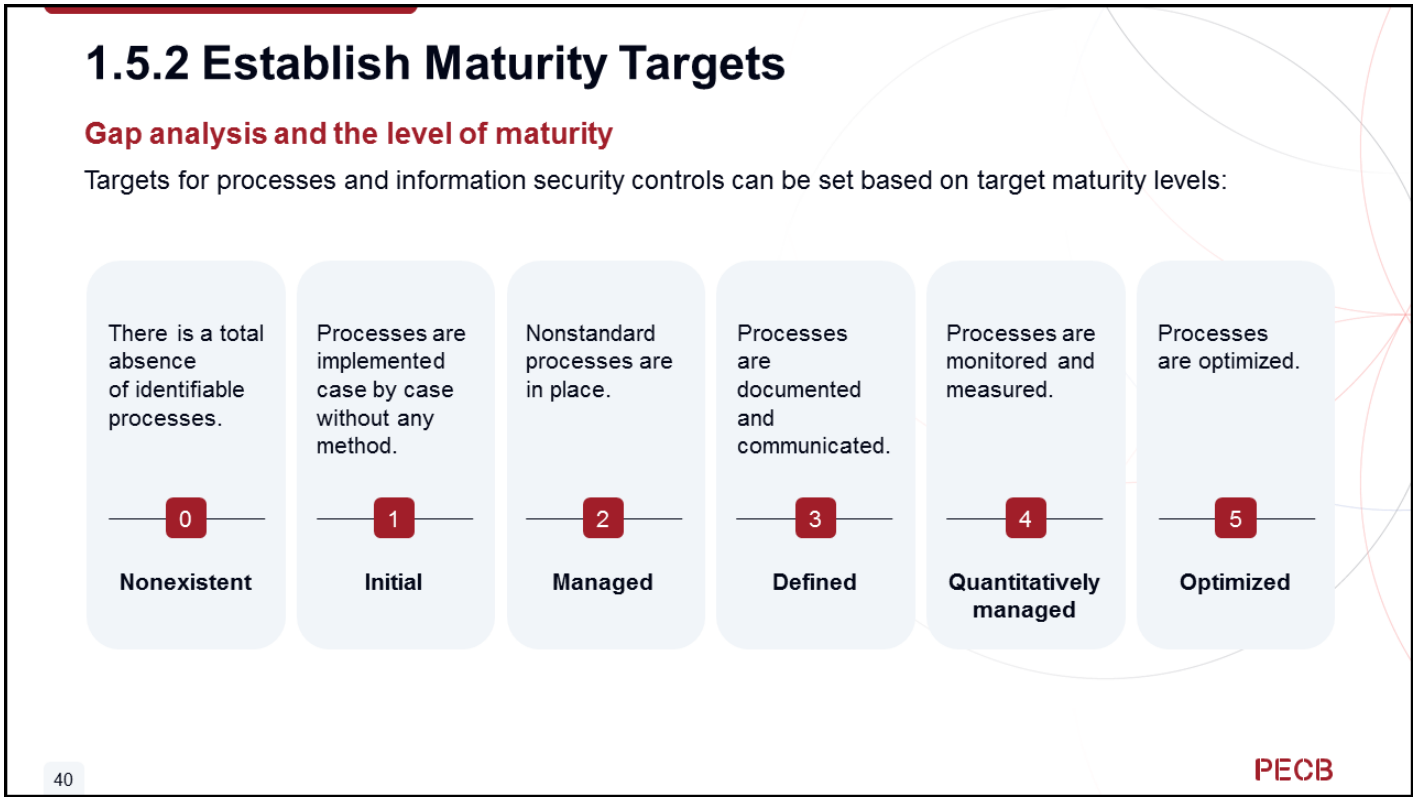
Group interviews are helpful when there is little time to conduct individual interviews or when the interviewer wants to examine the interaction between the group members. However, group interviews can produce unnatural responses, since a dominant member of the group may influence the response of others, known otherwise as the “bandwagon effect.”



The current state of the ISMS can be determined by the project team or outsourced to external consultants. External consultants may generate more neutral reports from the organization than the project team. In most cases, the current state of an ISMS is determined by the reports received from questionnaires that, depending on the choice or context, will be sent in writing or electronically.

When using questionnaires, questions can be:

- **Open-ended:** This type of questionnaire generates answers that are detailed and clarified. Interviewers obtain more valuable and complete information about the management system. However, these answers can sometimes be difficult to analyze due to the length of the content or response rate.
- **Closed-ended:** This type of questionnaire generate answers easier and faster. This type is useful for gaining general opinions about the management system. However, interviewers will lack the information or reasoning behind the answers.



0. Nonexistent: The organization is not aware that there is a total absence of the identifiable process.

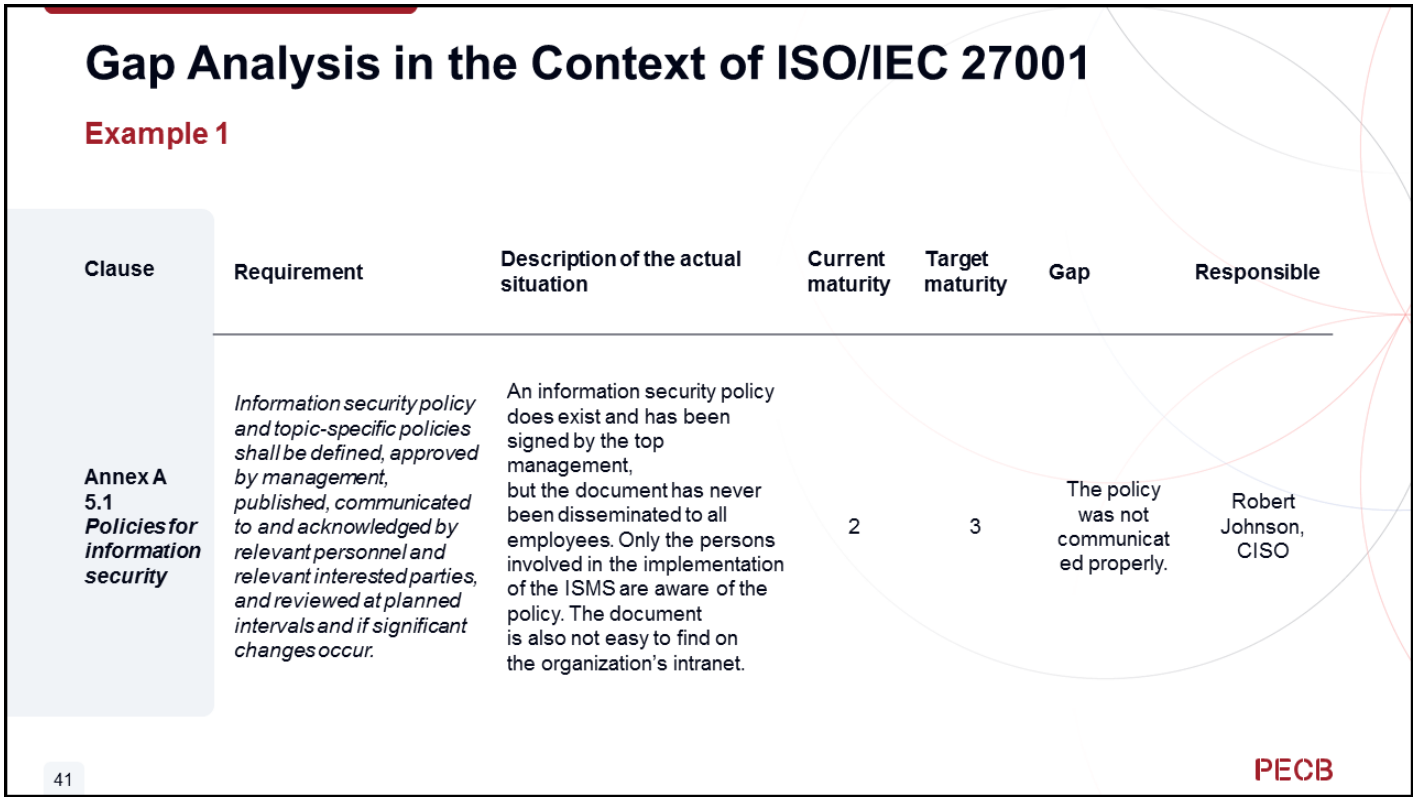
1.Initial: The organization has some processes that are implemented but there is no standardized procedure to do this.

2.Managed: The organization has some processes that are implemented using the same procedure, but there are no training and communication sessions performed with regard to these procedures. People implementing these processes rely on personal knowledge, where the probability of error is high.

3 .Defined: The organization has standardized, documented, and communicated the procedure in the training sessions. However, there is still a margin for error since these procedures are used only on individual initiatives.

4.Quantitatively managed: The organization is able to monitor and measure whether these processes are implemented as required and take action when procedures are not fully functional. The organization constantly improves these processes but there is limited or partial use of automation and tools.

5.Optimized: The organization's processes have reached a top-quality level following continual improvement and compliance with best practices. Computers are being used to automate integrated workflow in order to improve quality and efficiency and allow the organization to adapt quickly to new situations.



For the identification of existing and planned information security controls in an organization, the list of information security controls 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.

Gap Analysis in the Context of ISO/IEC 27001

Example 2

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

PECB

1.5.3 Present the Gap Analysis Report

Example of the content of a gap analysis report

- Introduction
  - Report objective
  - Methodology
- Baseline of the current information security processes and controls
  - Available tools and processes
  - Challenges with the available tools, processes, and resources
- Structured approach for making decisions related to information security
  - Identify and select a project
  - Predict the outcomes of the ISMS
  - Implement the ISMS
- Identification and analysis of gaps
- Suggested bridging options
- Summary and next steps to be taken

PECB

Gap Analysis Report

Example of a graphical representation

44

PECB

It is important to illustrate a graphical representation of any examined differences. This way, it is easier to notice any positive elements and other elements that still 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 (ISO/IEC 27001), 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 the maturity of the process) 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, in turn, 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.

Section 10 Summary

- In order to define the steps to move from a current state to a desired future state organizations should conduct gap analysis.
- The most commonly used information gathering procedures are observation, questionnaires, interviews, documented information review, and scan tools.
- There are six maturity levels that are helpful in setting targets for processes and security controls: nonexistent, initial, managed, defined, quantitatively managed, and optimized.
- A gap analysis report usually comprises the introduction, baseline of the current information security processes or controls, information security focused decision-making framework, identification and analysis of gaps, suggested bridging options, and a summary and next steps to be taken.

Questions?

Quiz 9

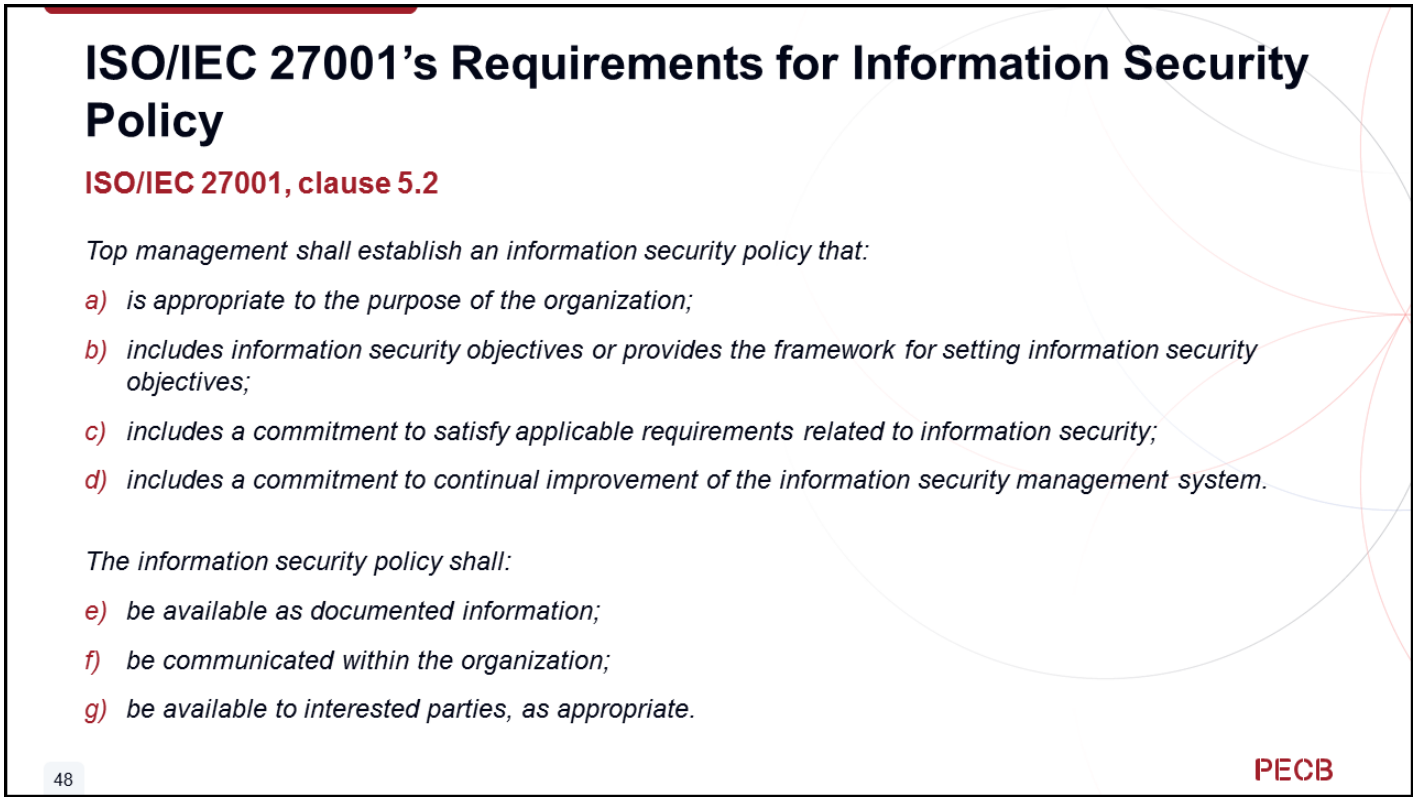
Note: To complete Quiz 9, please go to the Quizzes Worksheet.

This section provides information that will help participants gain insights into types of policies and policy models. In addition, it elaborates on how to draft, communicate, and review information security policies and specific security policies.

Information Security Policy

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

PECB



ISO/IEC 27003, clause 5.2 Policy

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.

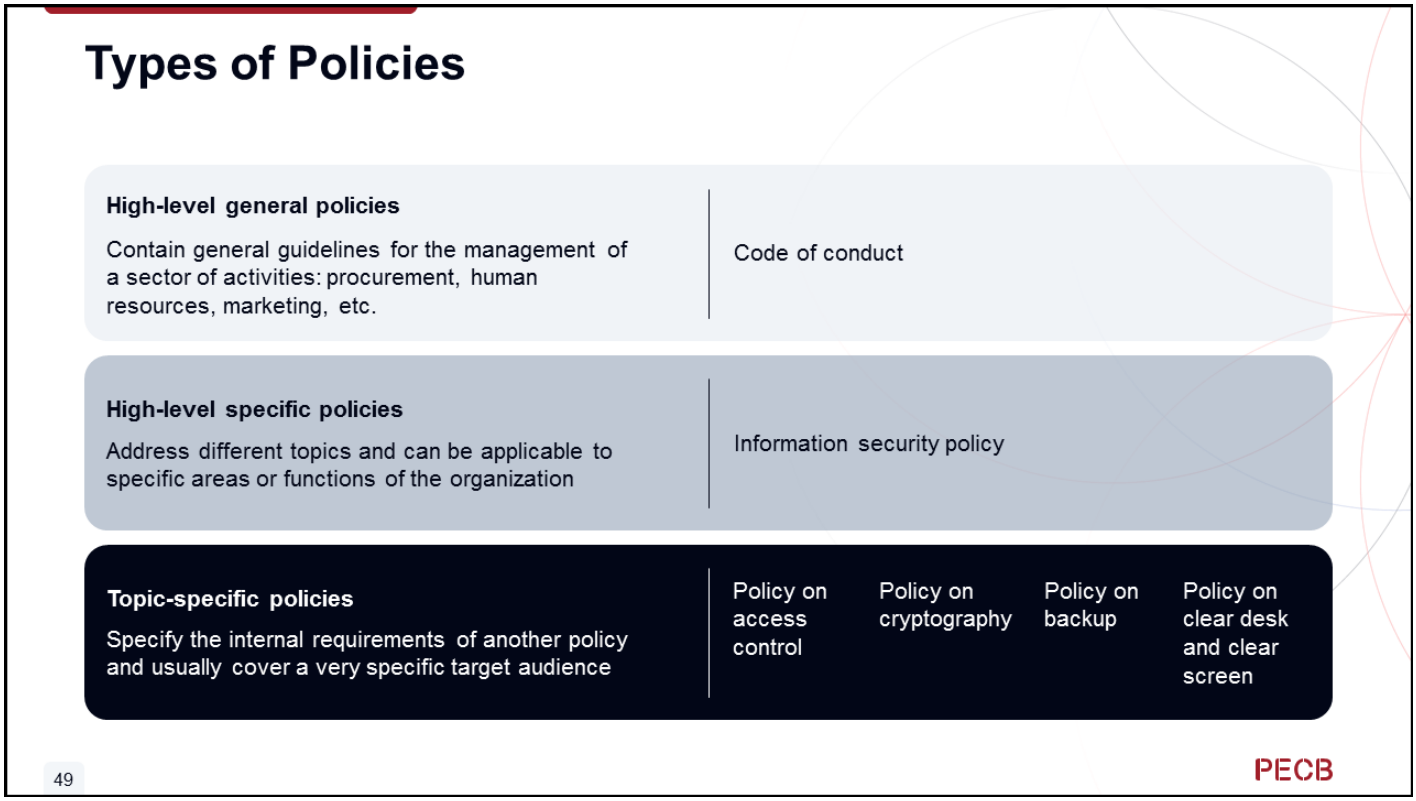
Top management should decide to which interested parties the policy should be communicated. The information security policy can be written in such a way that it is possible to communicate it to relevant external interested parties outside of the organization. Examples of such external interested parties 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.

Definitions:

- **Policy:** Clause 3.53 of ISO/IEC 27000 defines a policy as "intentions and direction of an organization, as formally expressed by its top management."
- **Guideline:** A guideline is a document stating a general rule, principle, or information on how something should be done.

  Clause 3.15 of ISO 21745 defines a guideline as "non-mandatory information leading to a compliant solution for the related requirement."



There are generally three levels of policies within an organization:

1.High-level general policies refer to broad, overarching principles and guidelines that set the tone and direction for an organization. These policies are typically strategic in nature and provide a framework for decision-making and action across various functional areas.

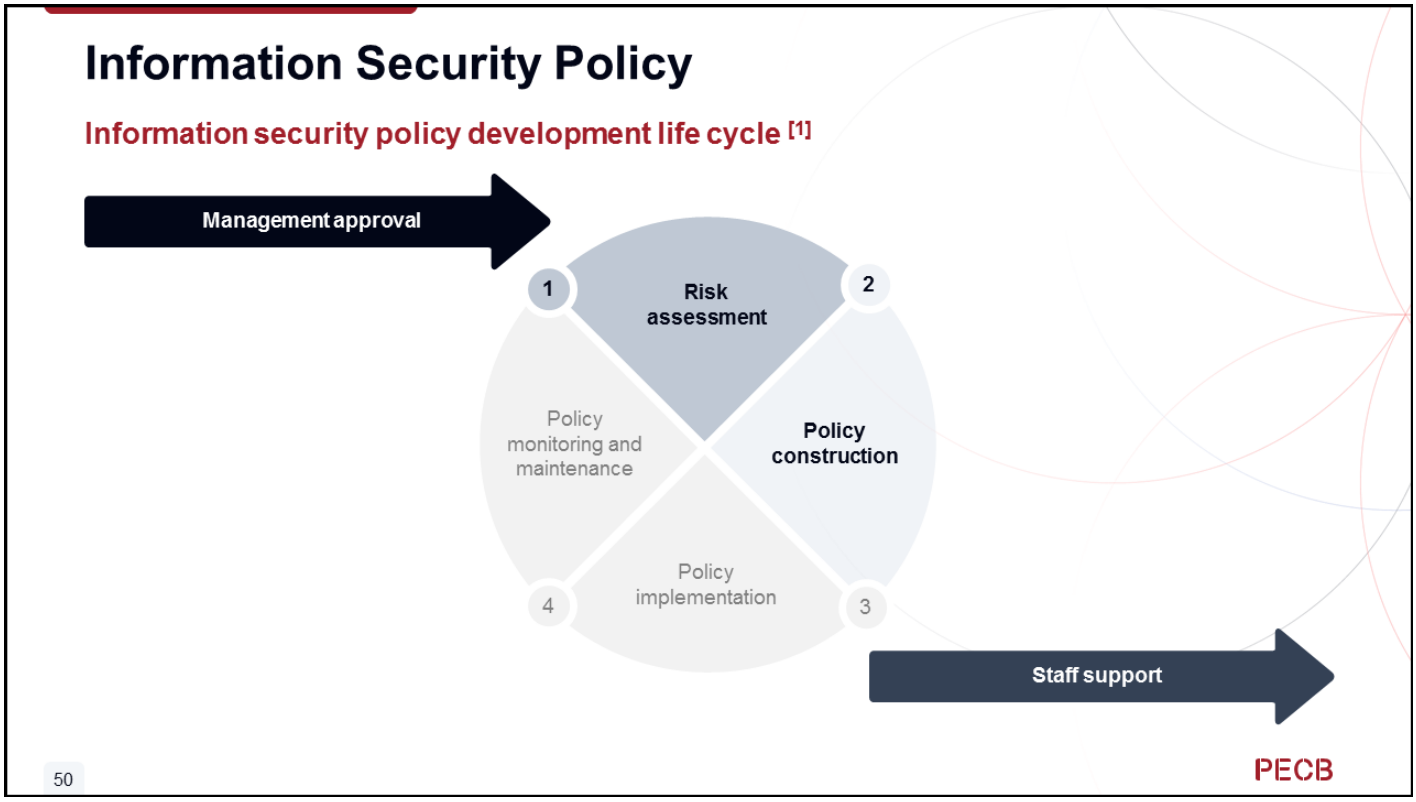
2.High-level specific policies define a subset of rules and practices still fairly general but that are related to a specific area. They are mostly subordinate to the high-level general policies.

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 a security policy for access rights to information and technology infrastructure, a policy on internet use, a policy on the archive and destruction of documents.

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.

When other management systems are implemented in addition to the ISMS (such as a quality management system), it is advisable for the information security policies to be consistent with the relevant policies of the other management systems adopted by the organization. However, the information security policy should remain relevant to the ISMS.



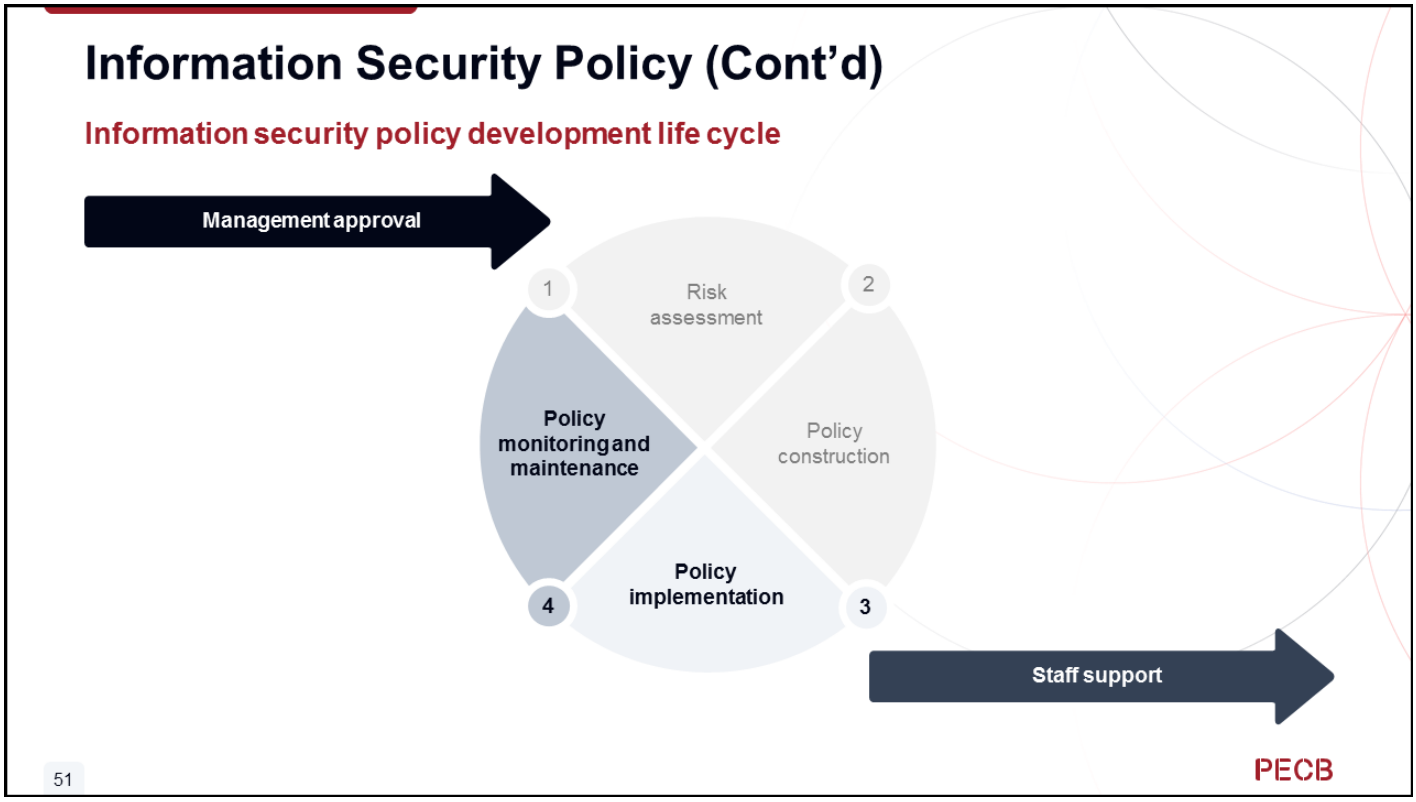
The policy development life cycle is an iterative process. The information security policy development life cycle usually comprises four phases: risk assessment, policy construction, policy implementation, and policy monitoring and maintenance. The management's approval and staff support are needed throughout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

It is the responsibility of the top management to approve the policies and ensure that they are communicated 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 established 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.

1.6 Information Security Policy

List of activities

1.6.1 Create policy models

1.6.2 Draft the information security policy

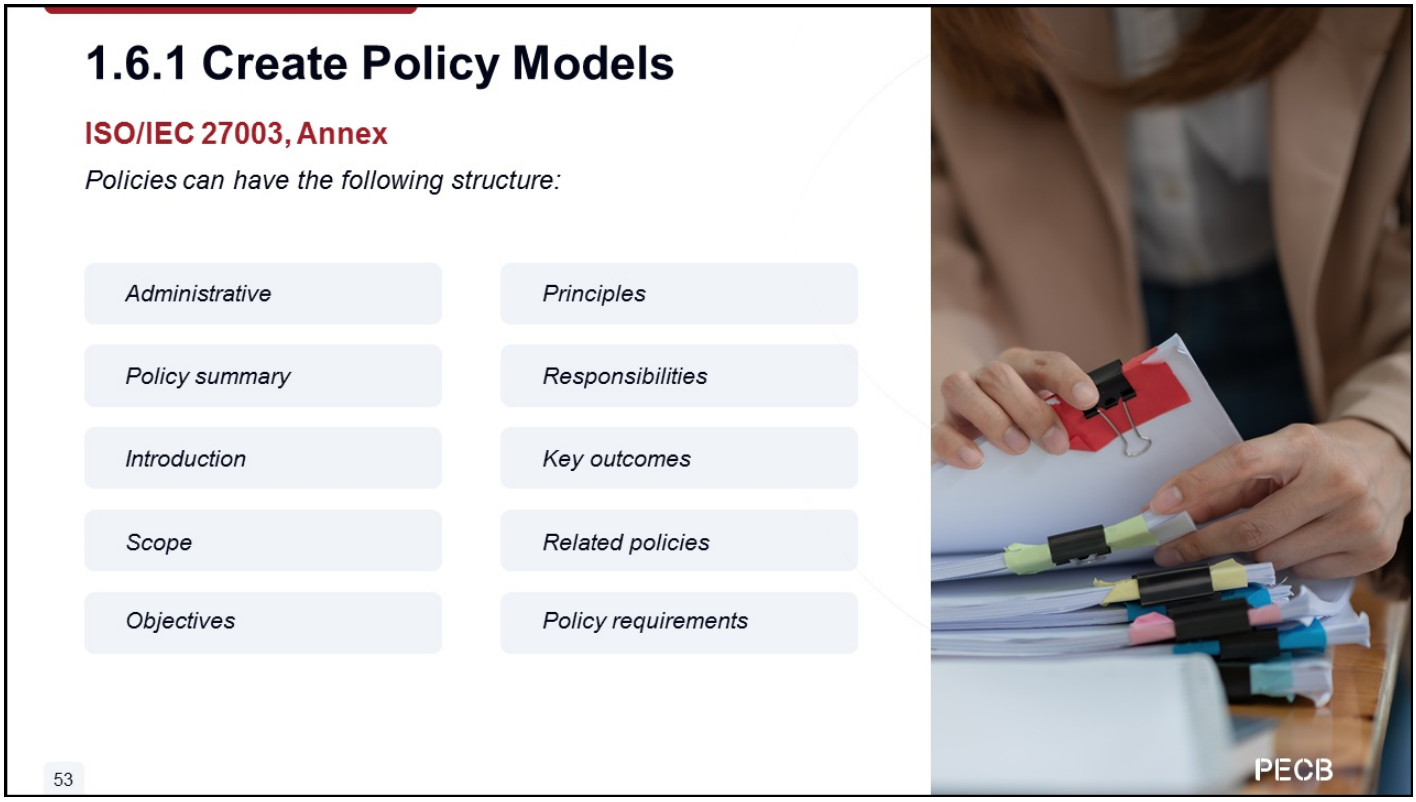
1.6.3 Draft specific security policies

1.6.4 Obtain management approval for the policies

1.6.5 Communicate the policies

1.6.6 Control, evaluate, and review the policies

PECB



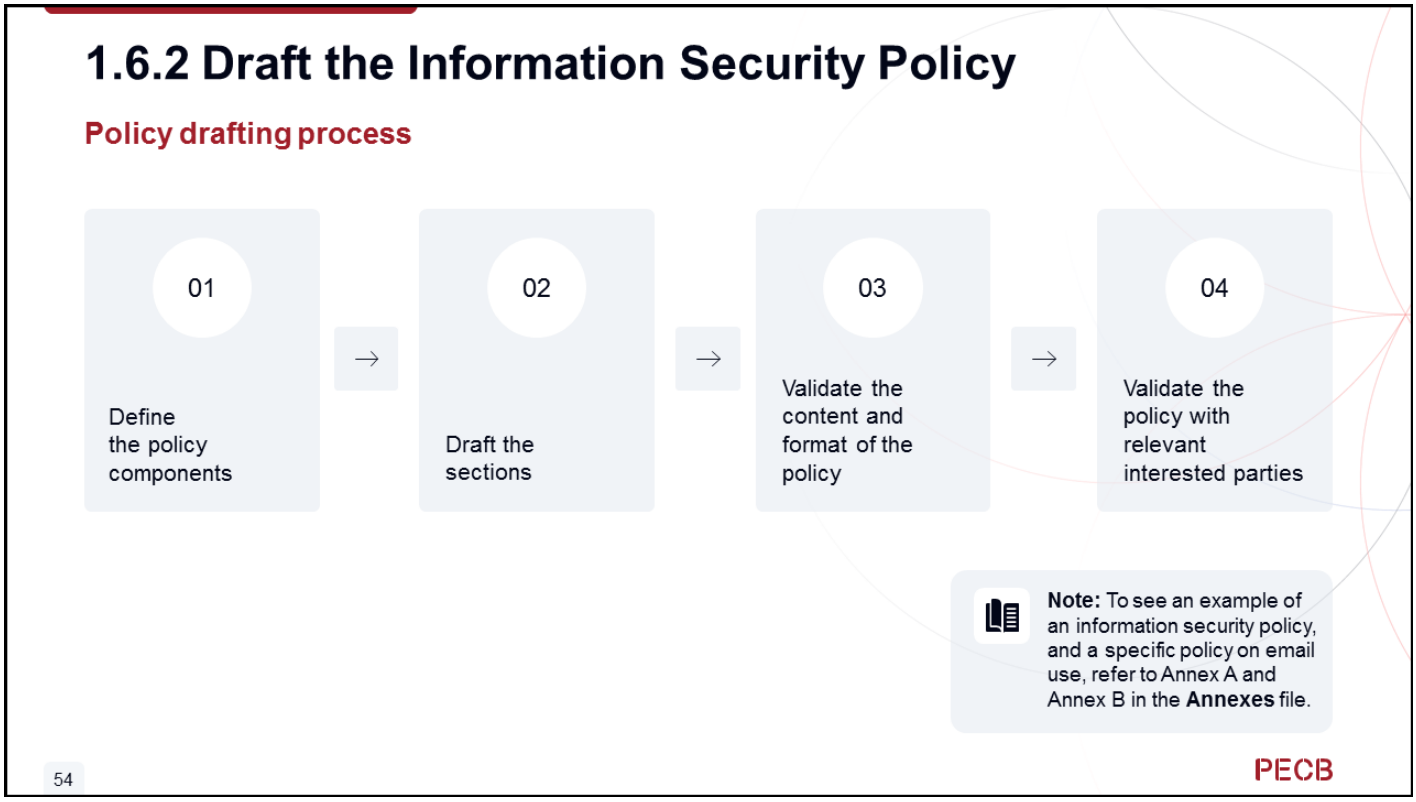
ISO/IEC 27003, Annex A Policy framework (cont'd)

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).



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

1. **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.
2. **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.
3. **Validate the content and format of the policy:** The person responsible for drafting the policy has to validate the content 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 of all employee communication if an organizational policy focused on employee privacy 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.
4. **Validate the policy with interested parties:** To ensure that the policy is understood by all relevant parties, the organization should obtain feedback from them. This stage may last longer, depending on the number of the interested parties.

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.

1.6.3 Draft Specific Security Policies

The organization may need to establish other specific policies to ensure information security. When established, these policies should align with the information security and other policies.

Examples of specific policies that would need to be established and aligned with information security policy include, but are not limited to:

- Data privacy and protection policy
- Cybersecurity policy
- Physical security policy
- Third-party and vendor management policy
- Human resources and employee security policy
- Incident response and crisis management policy
- Email use policy
- Internet and acceptable use policy
- Password management policy
- Remote work policy
- Social media and external communications policy

PECB

1.6.4 Obtain Management Approval for the Policies

While subject-matter experts can be involved in developing the information security policy, the top management is ultimately accountable for establishing the policy. As such, prior to the publication, the top management must review and approve the information security policy.

The approval is usually made in the form of a signature by the individual at the top of the hierarchy. However, the approval process may belong to a committee.

56

PECB

ISO/IEC 27002, clause 5.1 Policies for information security

Guidance

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

1.6.5 Communicate the Policies

Main modes of communication

Intranet

Meeting

Distribution of hard copies

New employee orientation session

57

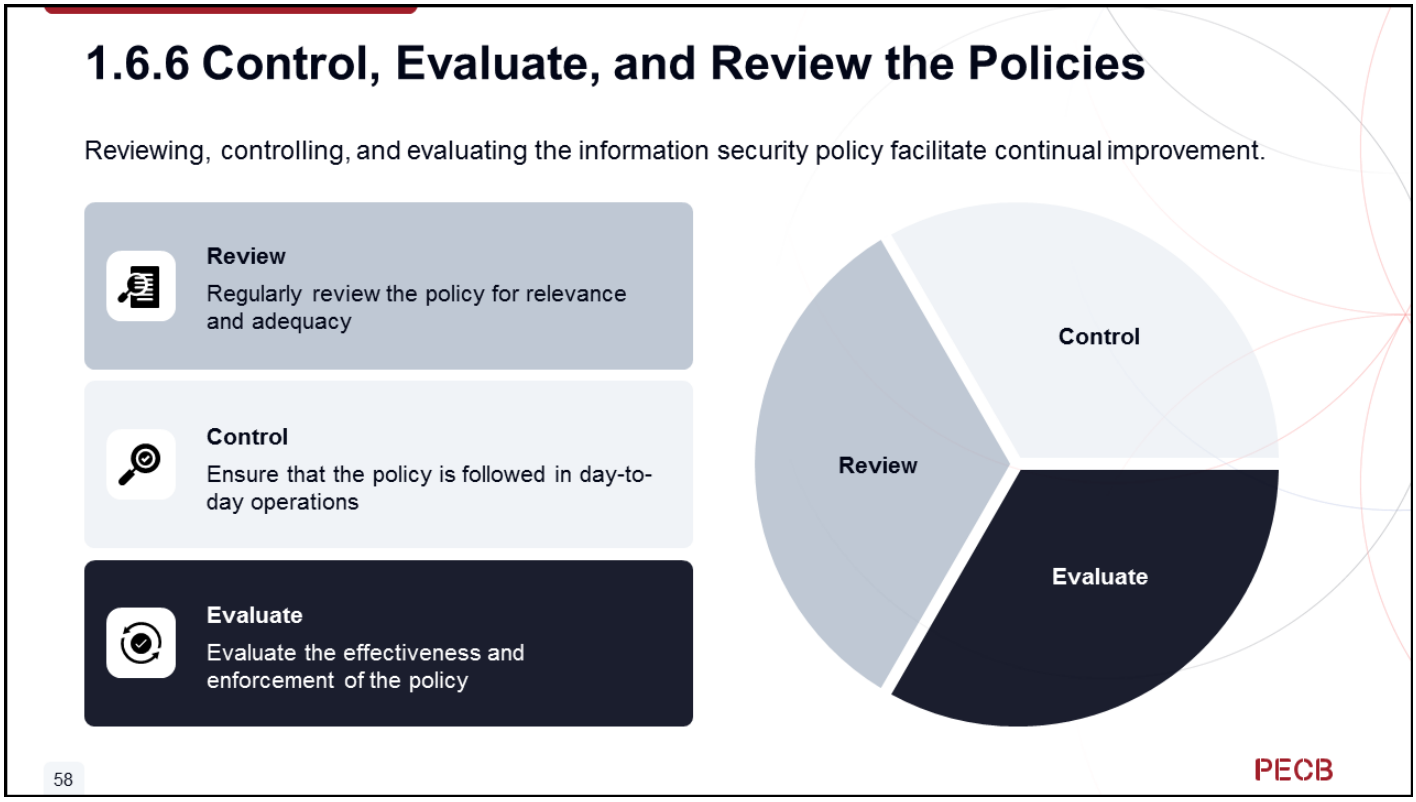
PECB

Presenting evidence which shows that relevant interested parties have been informed can be helpful during a certification audit. The organization should be able to demonstrate that its members understand and adhere to the policy.

ISO/IEC 27002, clause 5.1 Policies for information security

Guidance

The information security policy and topic-specific policies should be communicated to relevant personnel and interested parties in a form that is relevant, accessible and understandable to the intended reader. Recipients of the policies should be required to acknowledge they understand and agree to comply with the policies where applicable. The organization can determine the formats and names of these policy documents that meet the organization's needs. In some organizations, the information security policy and topic-specific policies can be in a single document. The organization can name these topic-specific policies as standards, directives, policies or others.



Review: The organization must review its security policy at planned intervals and after major changes to ensure that it is aligned with its business objectives and the applicable legal requirements.

Control: The management must ensure that everyone in the organization adheres to the information security policy when carrying out their day-to-day responsibilities. They must also provide a formal disciplinary process for employees who violate the policy. During this process, factors such as the nature and severity of the breach and its impact on the business should be considered (ISO/IEC 27002, clause 6.4 Disciplinary process).

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

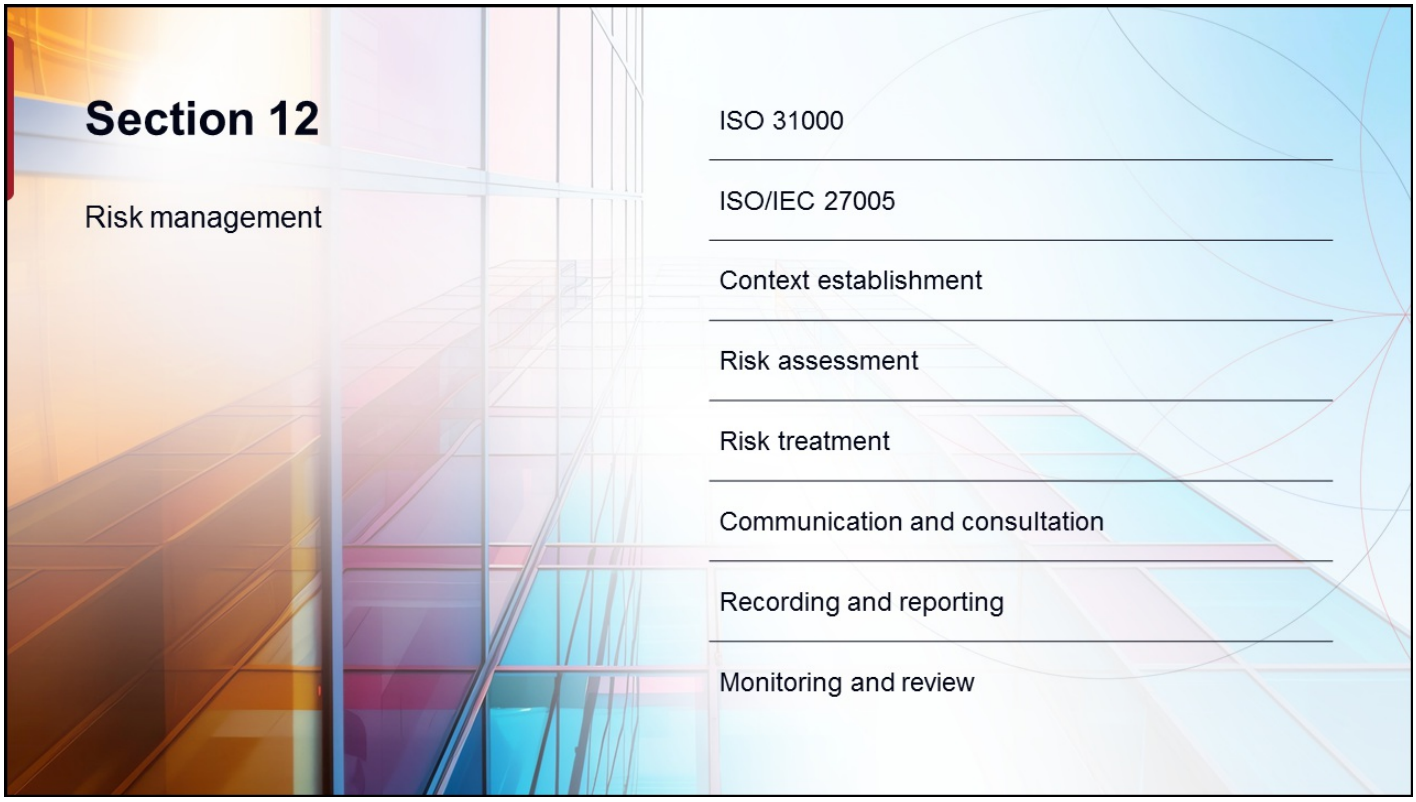
Section 11 Summary

- 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: deciding on the policy components, drafting the policy sections, and validating the contents and the format of the policy.
- The information security policy and topic-specific policies should be communicated to relevant personnel and interested parties in a form that is relevant, accessible, and understandable to the intended reader.
- The review, control, and evaluation of the information security policy facilitate the initiation of a continual improvement process.

Questions?

Quiz 10

Note: To complete Quiz 10, please go to the Quizzes Worksheet.

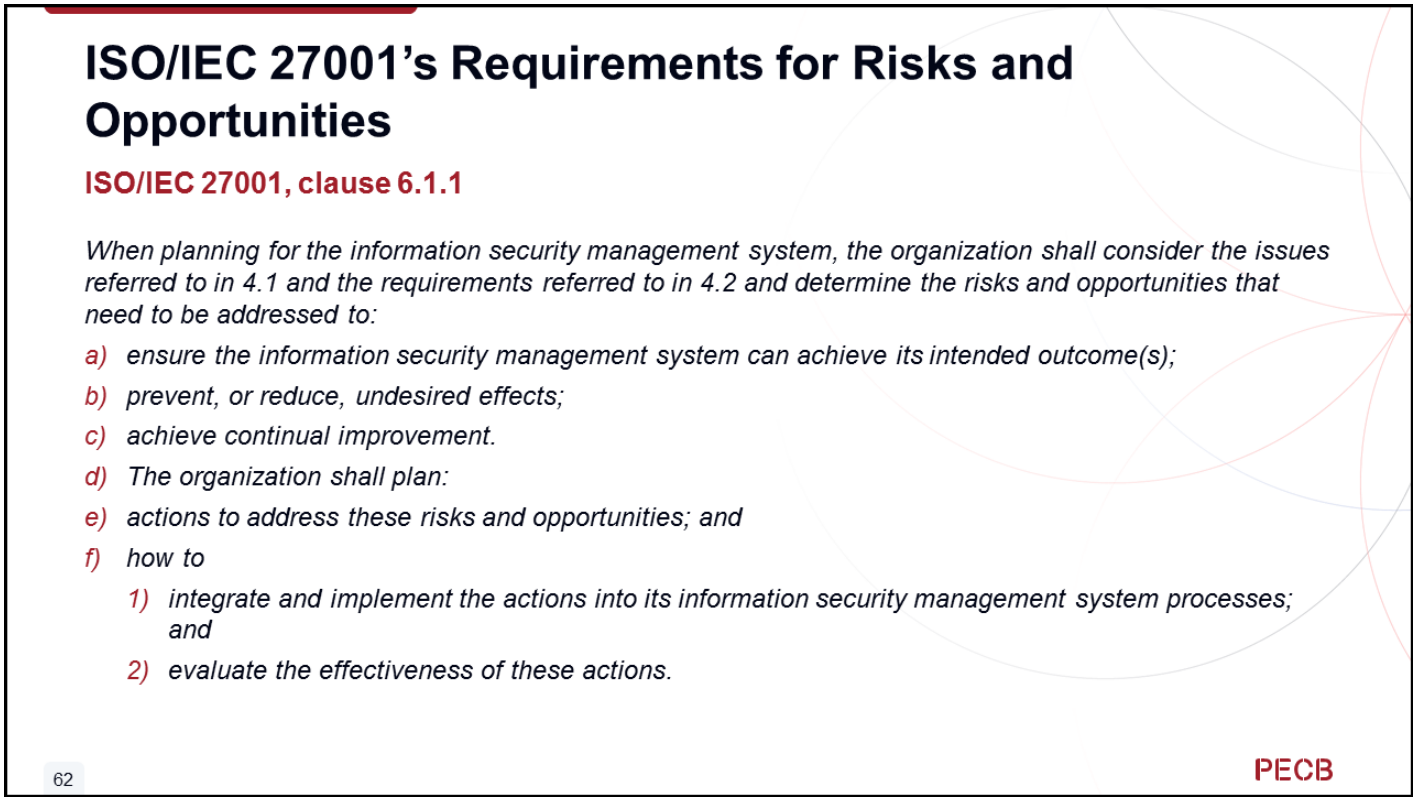


This section provides information that will help participants understand the risk management process, including the phases of context establishment, risk assessment, risk treatment, risk acceptance, communication and consultation, recording and reporting, and monitoring and review.

Risk Management

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

PECB

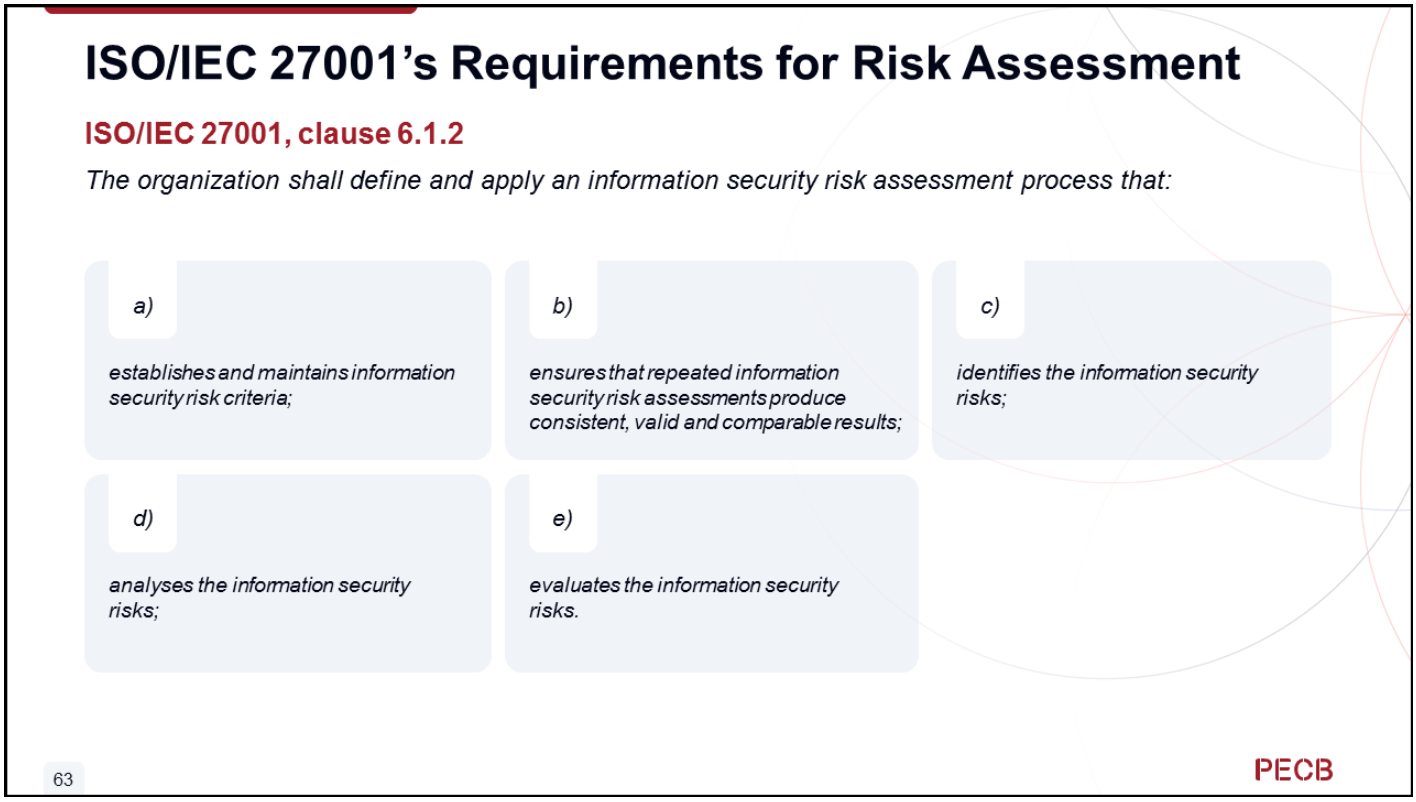


ISO/IEC 27003, clause 6.1.1 General

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".

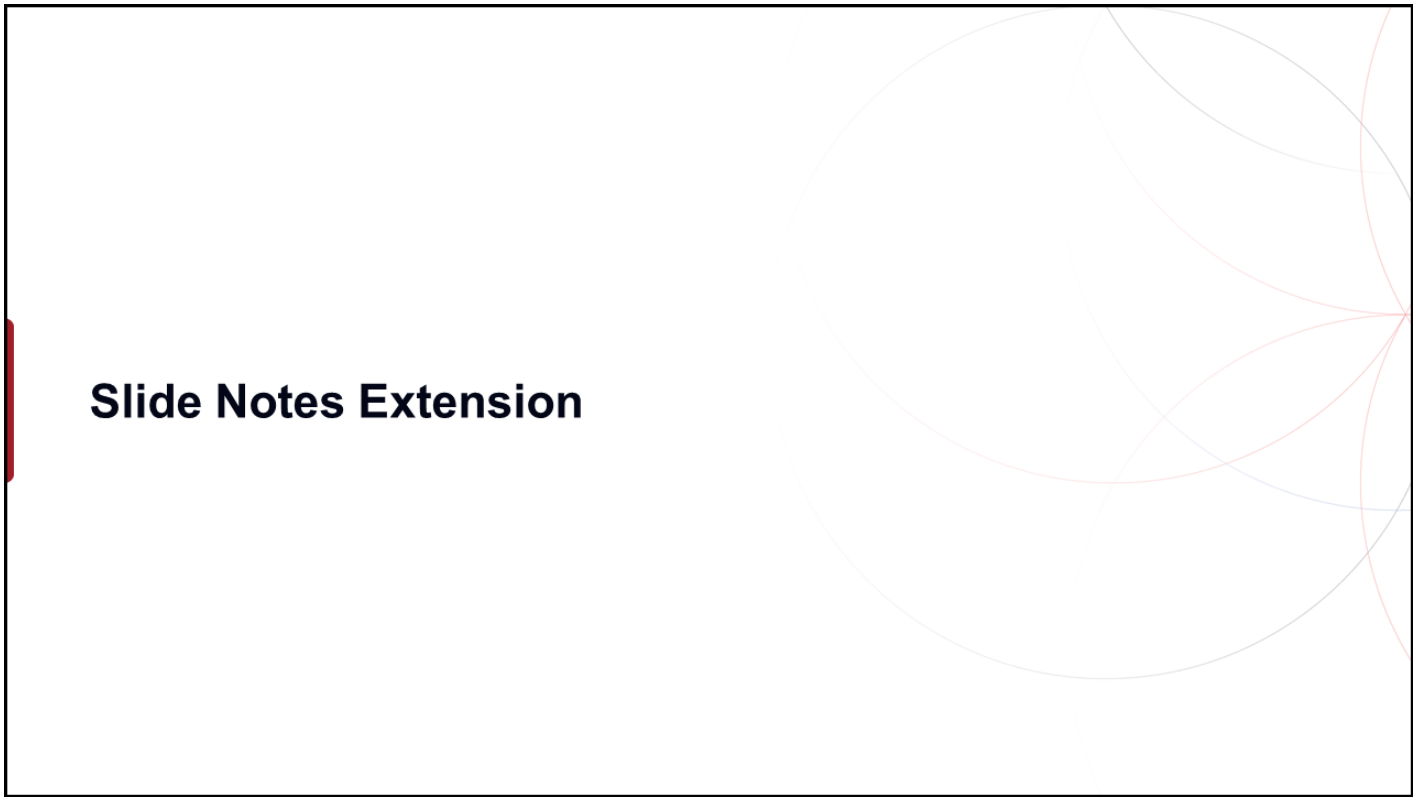


ISO/IEC 27001, clause 6.1.2 Information security risk assessment (cont'd)

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 analyzed 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.

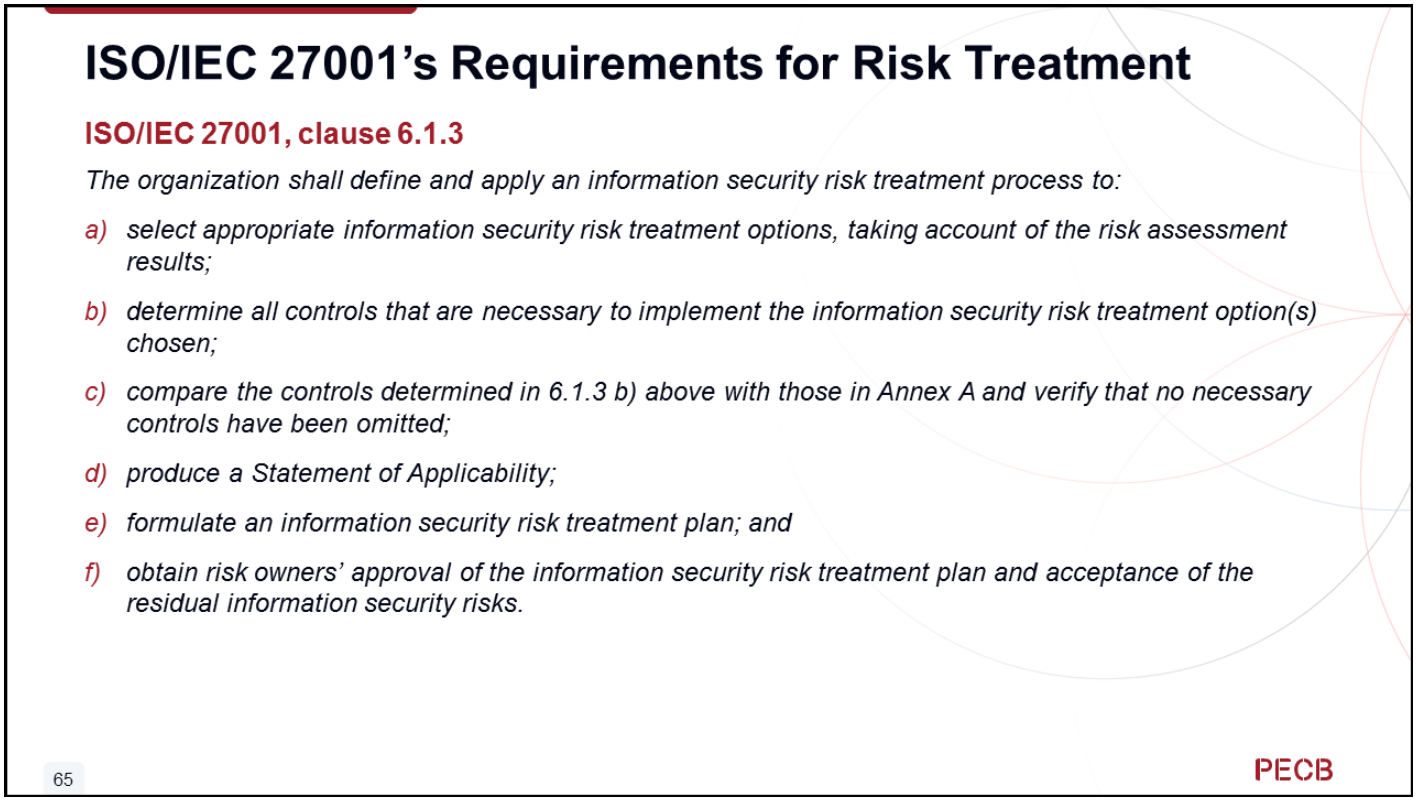
ISO 31000 is referenced in ISO/IEC 27001 as a general model. ISO/IEC 27001 requires that for each identified risk the risk analysis is based on assessing the consequences resulting from the risk and assessing the likelihood of those consequences occurring to determine a level of risk.

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 analyzed 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.

Slide Notes Extension

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, 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.*

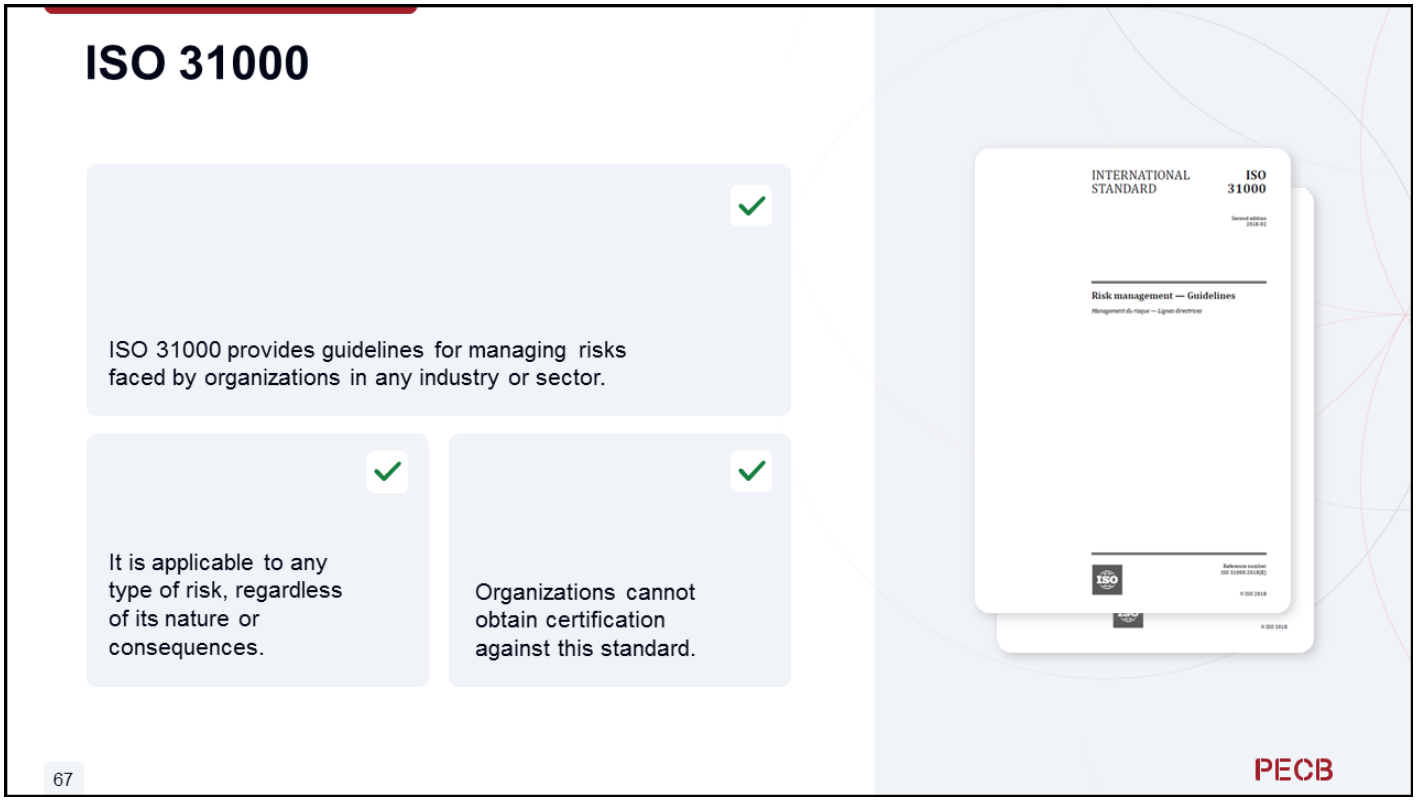
Other useful content can include:

- *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, 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.

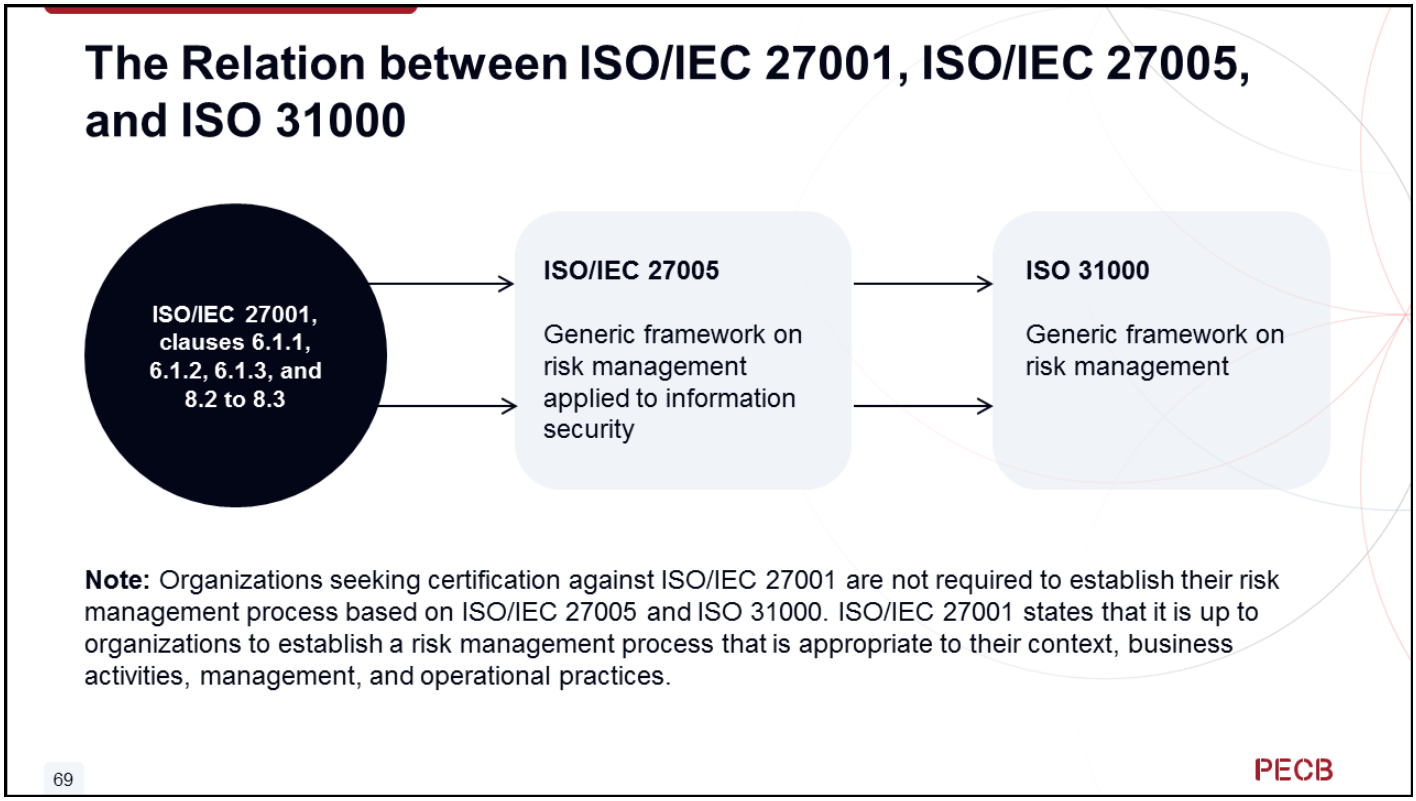
ISO/IEC 27005 supplements the guidance of ISO/IEC 27003 and supports the guidelines of ISO 31000.

ISO/IEC 27005, clause 1 Scope

This document provides guidance to assist organizations to:

- *fulfill the requirements of ISO/IEC 27001 concerning actions to address information security risks;*
- *perform information security risk management activities, specifically information security risk assessment and treatment.*

This document is applicable to all organizations, regardless of type, size or sector.



Based on the ISO 31000 framework, ISO/IEC 27005 explains in detail how to conduct a risk assessment and a risk treatment within the context of information security, taking into account the Plan-Do-Check-Act (PDCA) cycle for risk management. As such, organizations who establish their risk management program based on ISO/IEC 27005 and ISO 31000 can easily address the requirements of ISO/IEC 27001 on risk management (clauses 6.1.2 and 6.1.3).

ISO/IEC 27005, Introduction

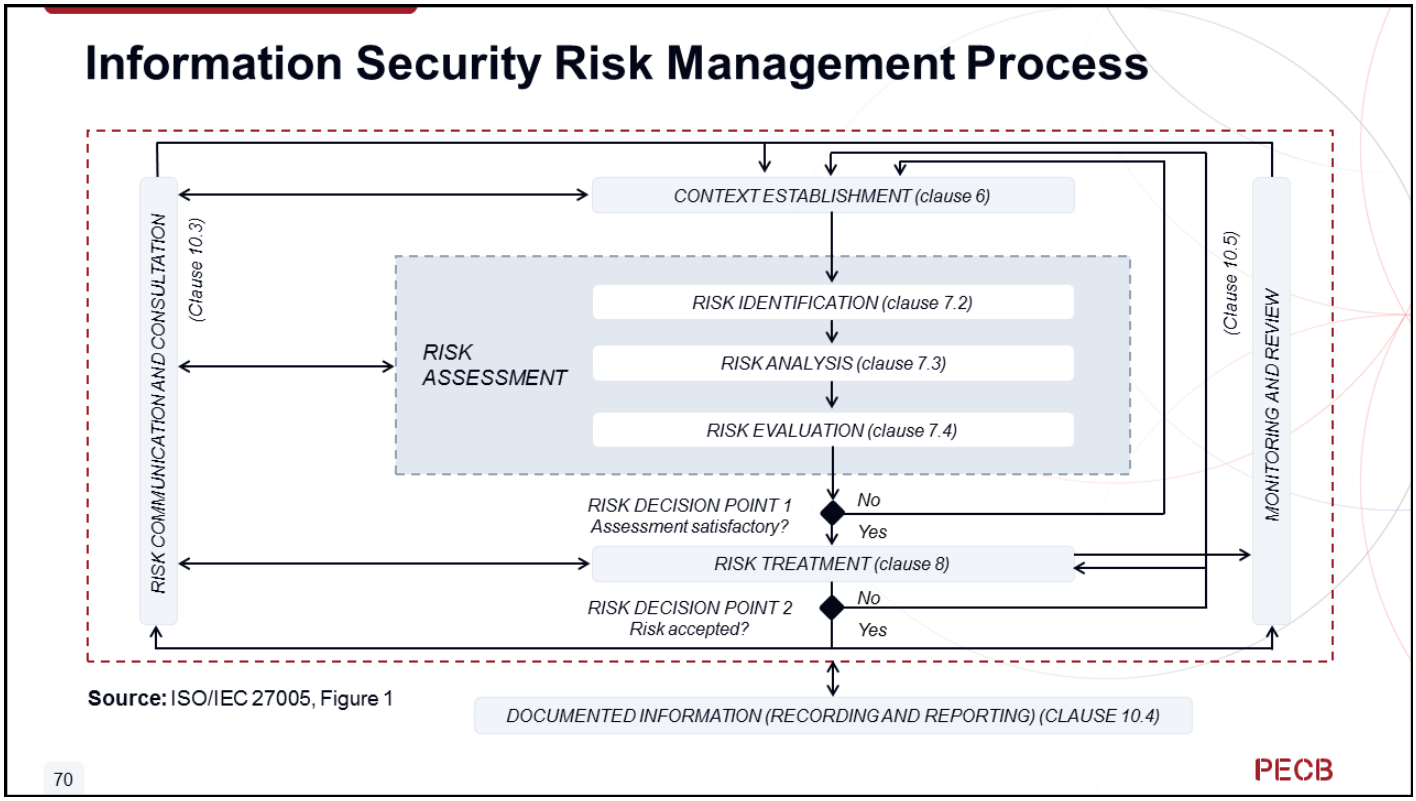
This document provides guidance on:

- *implementation of the information security risk requirements specified in ISO/IEC 27001;*
- *essential references within the standards developed by ISO/IEC JTC 1/SC 27 to support information security risk management activities;*
- *actions that address risks related to information security;*
- *implementation of risk management guidance in ISO 31000 in the context of information security.*

This document contains detailed guidance on risk management and supplements the guidance in ISO/IEC 27003.

This document is intended to be used by:

- *organizations that intend to establish and implement an information security management system (ISMS) in accordance with ISO/IEC 27001;*
- *persons that perform or are involved in information security risk management (e.g. ISMS professionals, risk owners and other interested parties);*
- *organizations that intend to improve their information security risk management process.*



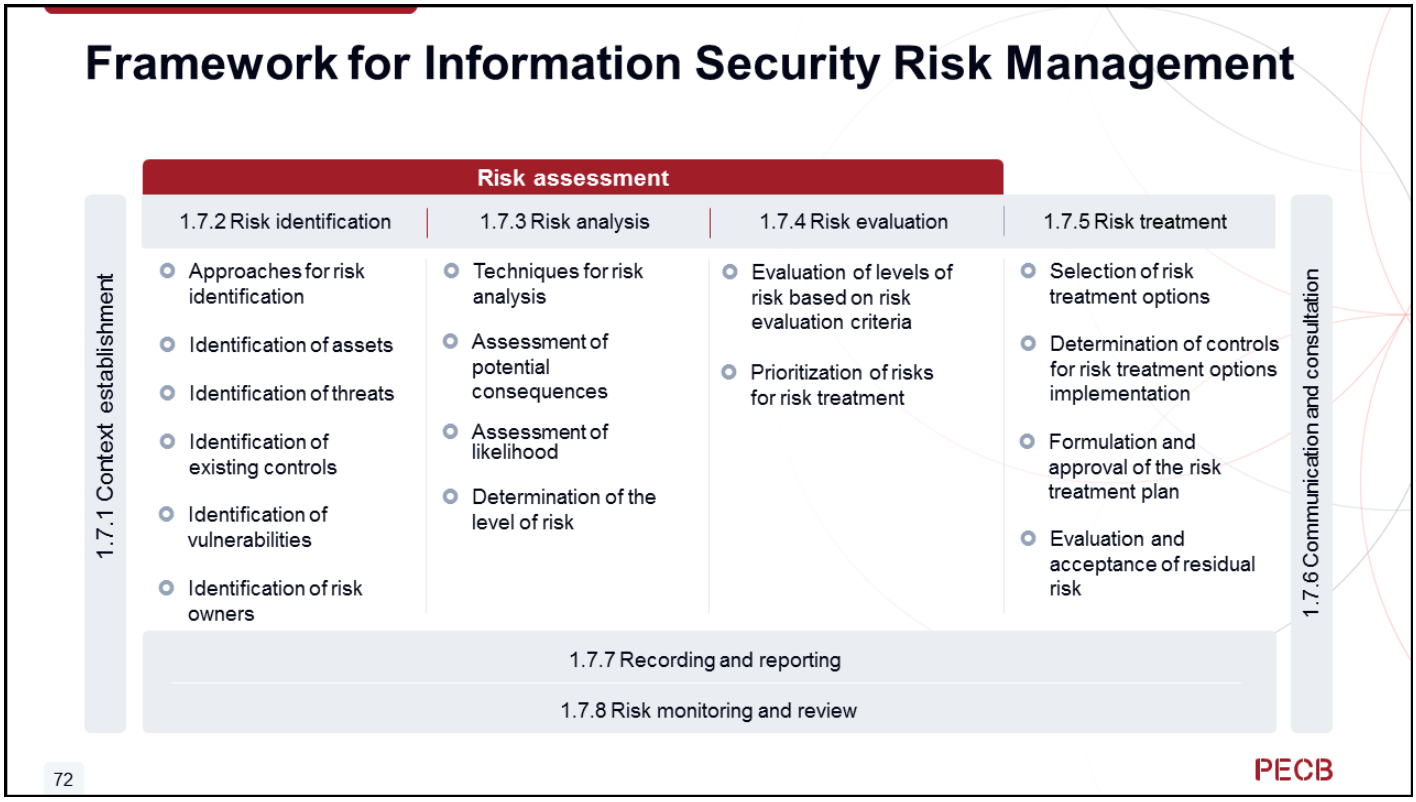
As illustrated in the figure, the risk management process should be iterative for risk assessment and risk treatment activities. If the risk assessment activities have provided sufficient evidence that the planned actions will reduce the risk to an acceptable level, the next step is to implement risk 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.

1.7 Risk Management

List of activities

PECB



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

1.7.1 Context Establishment

ISO/IEC 27005, clause 5.1 and ISO/IEC 27000, clauses 3.22 and 3.38

Context establishment means assembling the internal and external context for information security risk management or an information security risk assessment.

External context

External environment in which the organization seeks to achieve its objectives
Note 1 to entry: External context can include the following:

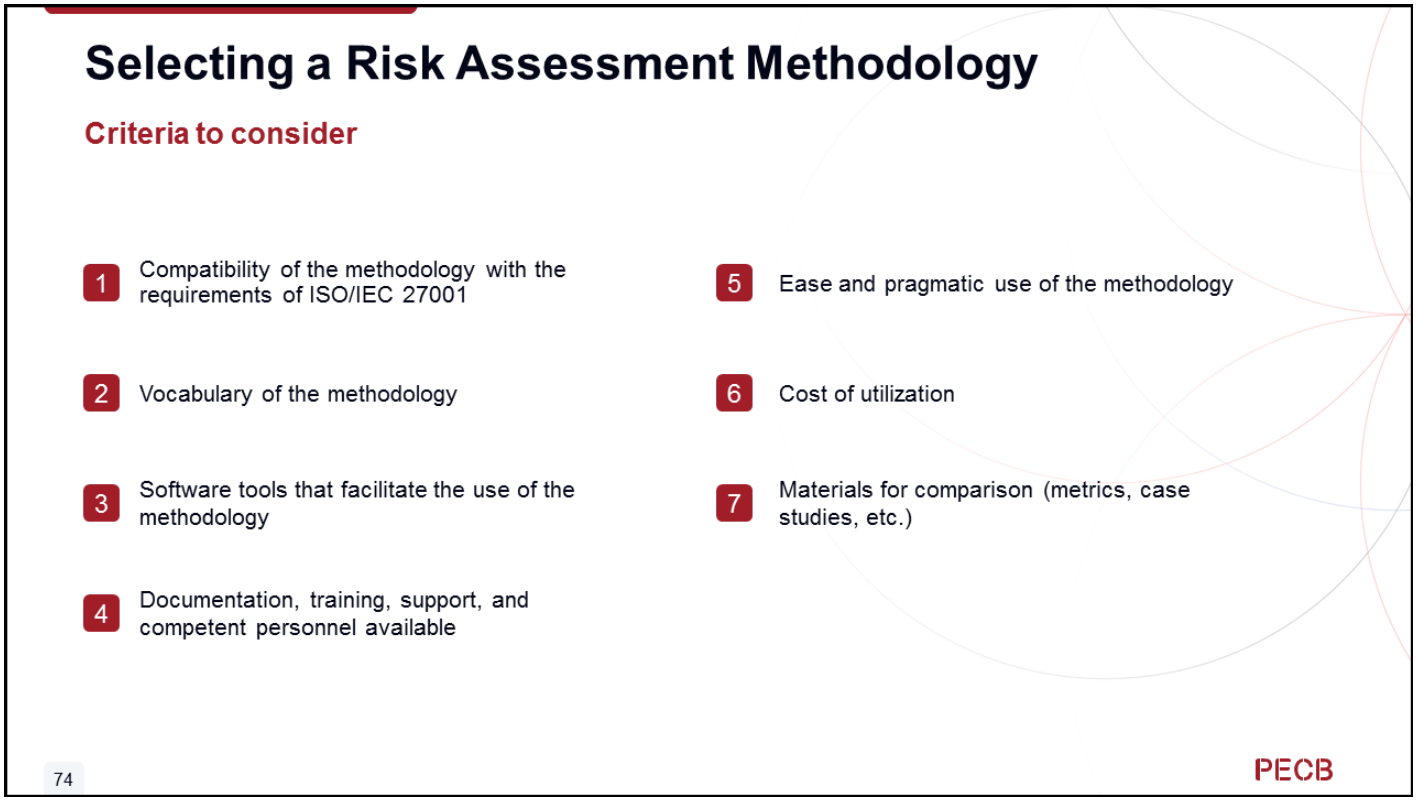
- *the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;*
- *key drivers and trends having impact on the objectives of the organization;*
- *relationships with, and perceptions and values of, external stakeholders.*

Internal context

Internal environment in which the organization seeks to achieve its objectives
Note 1 to entry: Internal context can include:

- *governance, organizational structure, roles and accountabilities;*
- *policies, objectives, and the strategies that are in place to achieve them;*
- *the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);*
- *information systems, information flows and decision-making processes (both formal and informal);*
- *relationships with, and perceptions and values of, internal stakeholders;*
- *the organization's culture;*
- *standards, guidelines and models adopted by the organization;*
- *form and extent of contractual relationships.*

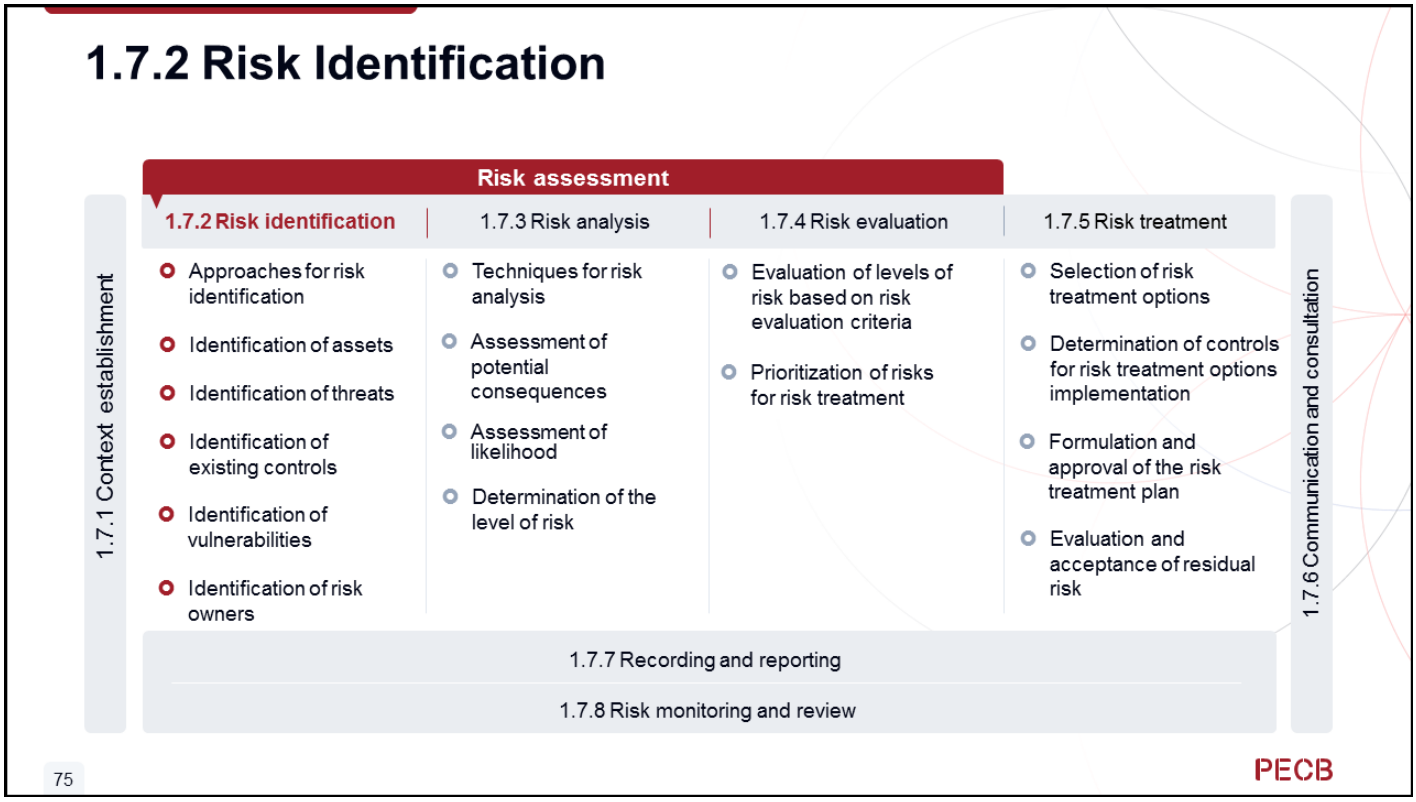
PECB



Any risk assessment method 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).

When selecting a risk assessment methodology, the following questions should be addressed:

- 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 produce consistent results over time?
- Does the process take into account the analysis of the impact of changes?



ISO/IEC 27005, clause 3.2.4 Risk identification

Process of finding, recognizing and describing risks

- *Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences.*
- *Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and interested parties' needs.*

ISO 31000, clause 6.4.2 Risk identification

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*

Approaches for Risk Identification

ISO/IEC 27005, clause 7.2.1

There are two approaches commonly used to perform risk identification.

a)	*b)*
Event-based approach: identify strategic scenarios through a consideration of risk sources, and how they use or impact interested parties to reach those risk's desired objective.	*Asset-based approach: identify operational scenarios, which are detailed in terms of assets, threats and vulnerabilities.*

76

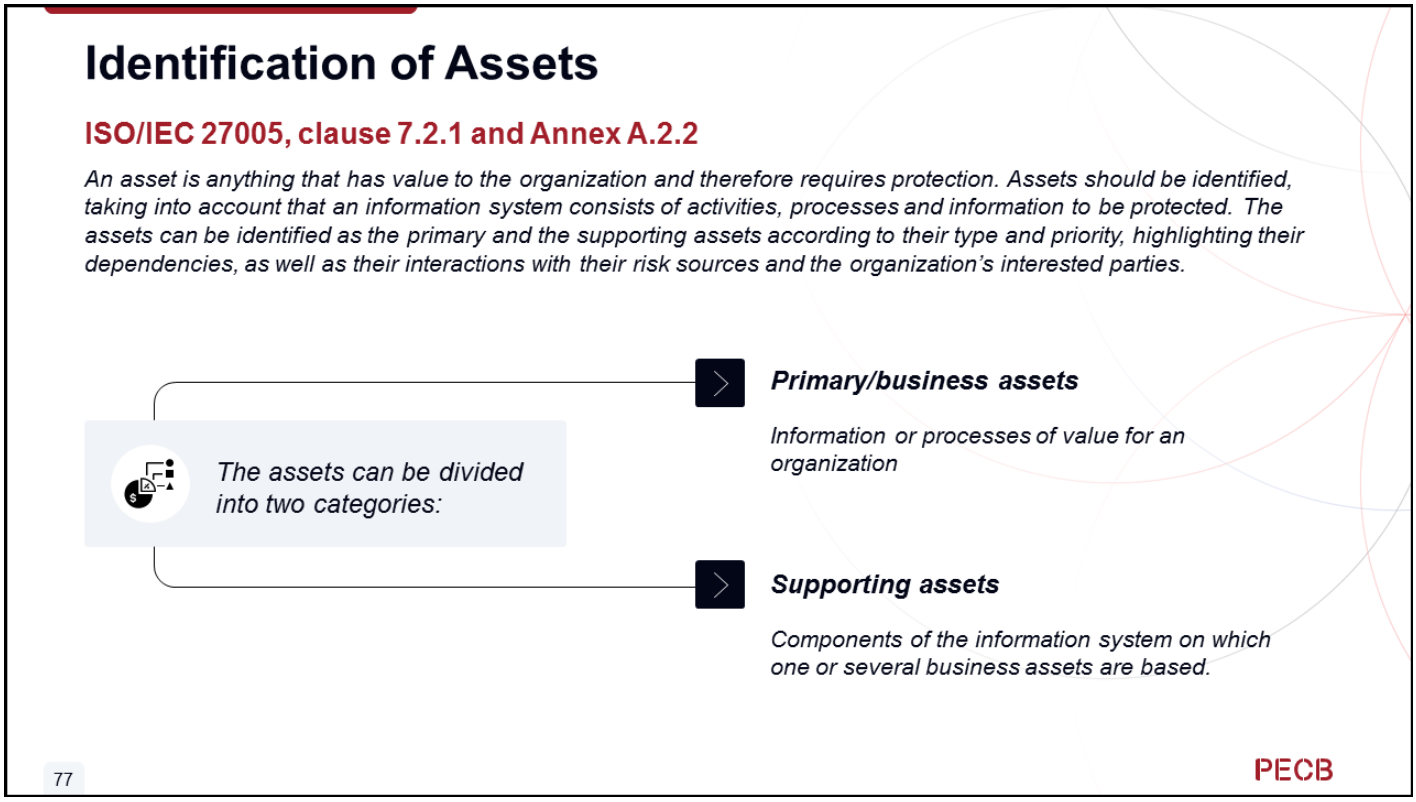
PECB

ISO/IEC 27005, clause 7.2.1 Identifying and describing information security risks (cont'd)

In an event-based approach, the underlying concept is that risks can be identified and assessed through an evaluation of events and consequences. Events and consequences can often be determined by a discovery of the concerns of top management, risk owners and the requirements identified in determining the context of the organization. Interviews with top management and those people in the organization who have a responsibility for a business process can assist in identifying not only the relevant events and consequences, but also the risk owners.

An event-based approach can establish high level or strategic scenarios without spending a considerable amount of time in identification of assets on a detailed level. This allows the organization to focus its risk treatment efforts on the critical risks. Evaluation of events using this approach can make use of historical data where risks remain unchanging for long periods, and allows the interested parties involved to reach their objectives. However, in the case of risks for which historical data are not available or reliable, the advice based on knowledge and experience of experts or investigation of risk sources can assist evaluation.

With an asset-based approach, the underlying concept is that risks can be identified and assessed through an inspection of assets, threats and vulnerabilities. If all valid combinations of assets, threats and vulnerabilities can be enumerated within the scope of the ISMS, then, in theory, all the risks would be identified. For further steps of risk assessment, a list of assets associated with information and information-processing facilities should be drawn up.



ISO/IEC 27005, Annex A.2.2 Assets (cont'd)

The primary/business assets are often used in the event-based approach (identification of events and their consequences on business assets).

The supporting assets are often used in the asset-based approach (identification and analysis of vulnerabilities and threats on these assets) and in the risk treatment process (specification of the asset(s) to which each control should be applied).

Business and supporting assets are related, therefore risk sources identified for supporting assets can impact business assets.

For this reason, it is important to identify the relationships between the assets, and to understand their value to the organization. Misjudging the asset value can lead to a misjudgment of the consequences related to the risk but can also affect the understanding of the likelihood of threats under consideration.

Identification of Primary Assets

Information assets to be considered:

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

Business processes to be considered:

- Processes whose loss or degradation makes it impossible to accomplish the mission of the organization
- Processes that contain sub-processes or that involve proprietary technology
- Processes that, if modified, can greatly affect the accomplishment of the organization's mission
- Processes that are necessary for the organization to comply with contractual, legal, or regulatory requirements

78

PECB

During risk identification, classification can help in analyzing the information that is considered valuable for the organization. For example, a member of the team that conducts risk assessment can analyze the financial information of the organization and others can analyze information related to customers. The information should be classified based on its characteristics and the security level it requires.

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	The physical elements of a computer system that support processes	Processor, random access memory, printer, disk drive, etc.
Software	The programs that contribute to data processing	Operating system, word processing software, accounting software, etc.
Networks	Telecommunication devices interconnecting several physically remote computers or elements of an information system	Router, firewall, network cable, switch, bridge, etc.
Personnel	The people involved in the information system	Owner, user, developer, trustee, client, decision-maker, etc.
Sites	Physical places where operations take place	Server room, staff residence, secure area, etc.
Organizational structure	Organizational framework that includes personnel structures to perform the activities	Headquarters, division, department, project teams, subcontractors, suppliers, etc.

79

PECB

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.

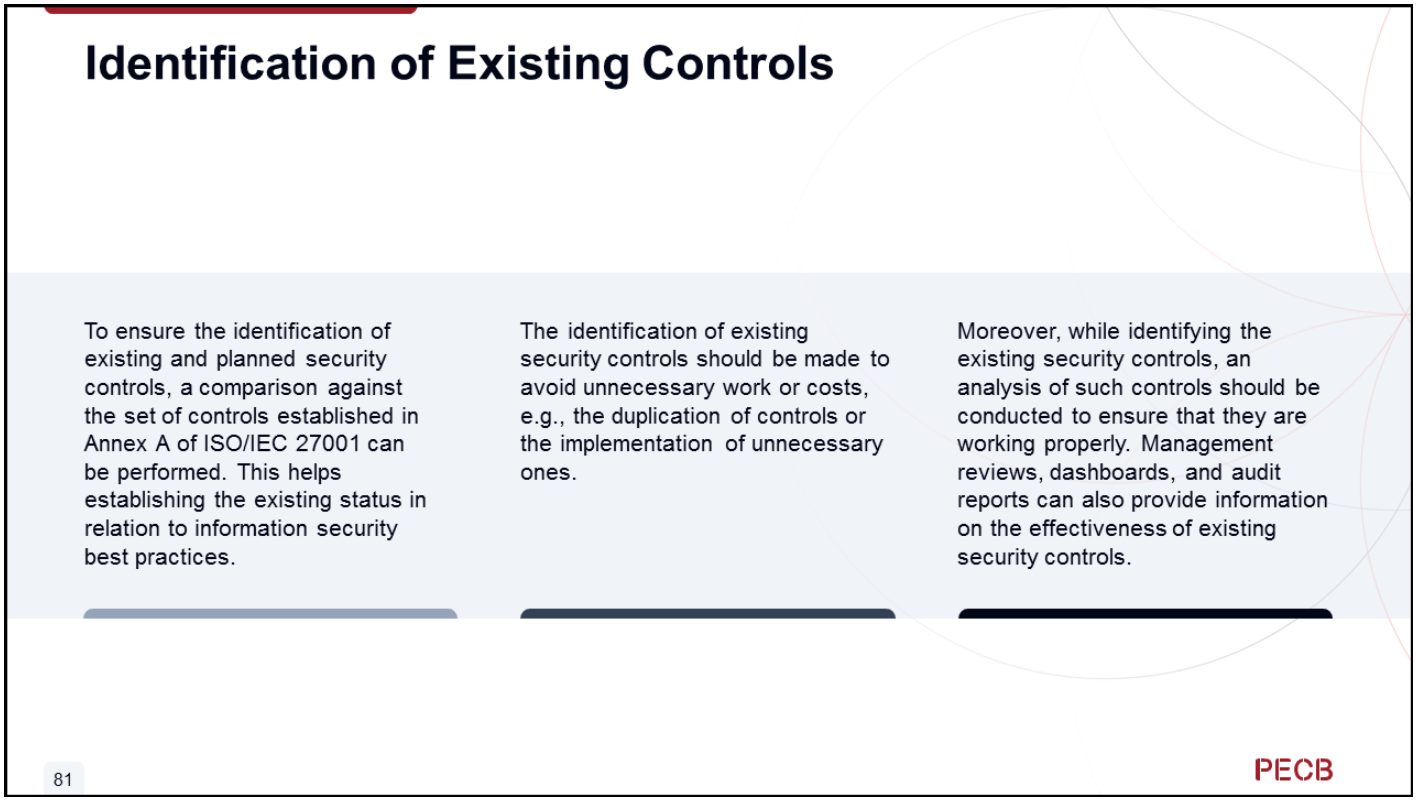
Identification of Threats

ISO/IEC 27005, clause 7.2.1

- *The identification of threats enables organizations to make better decisions related to risk treatment options and activities.*
- *The list of threats is not exhaustive. New threats may appear instantaneously due to trends in technology and the evolving capabilities of threat agents.*

The asset-based approach can identify asset-specific threats and vulnerabilities and allows the organization to determine specific risk treatment on a detailed level.

PECB



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.

ISO/IEC 27005, clause 7.2.1 Identifying and describing information security risks

Management of information security risks should not be constrained by arbitrary or restrictive views of how risks should be structured, grouped, aggregated, split or described. Risks can appear to overlap or be subsets or specific instances of other risks. However, controls for individual risks should be considered and identified separately from wider risks or aggregated risks for the purposes of risk treatment.

Identification of Vulnerabilities

ISO/IEC 27005, Annex A.2.5.3

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

Test methods include:

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

82

ISO/IEC 27005, Annex A.2.5.3 Methods for assessment of technical vulnerabilities (cont'd)

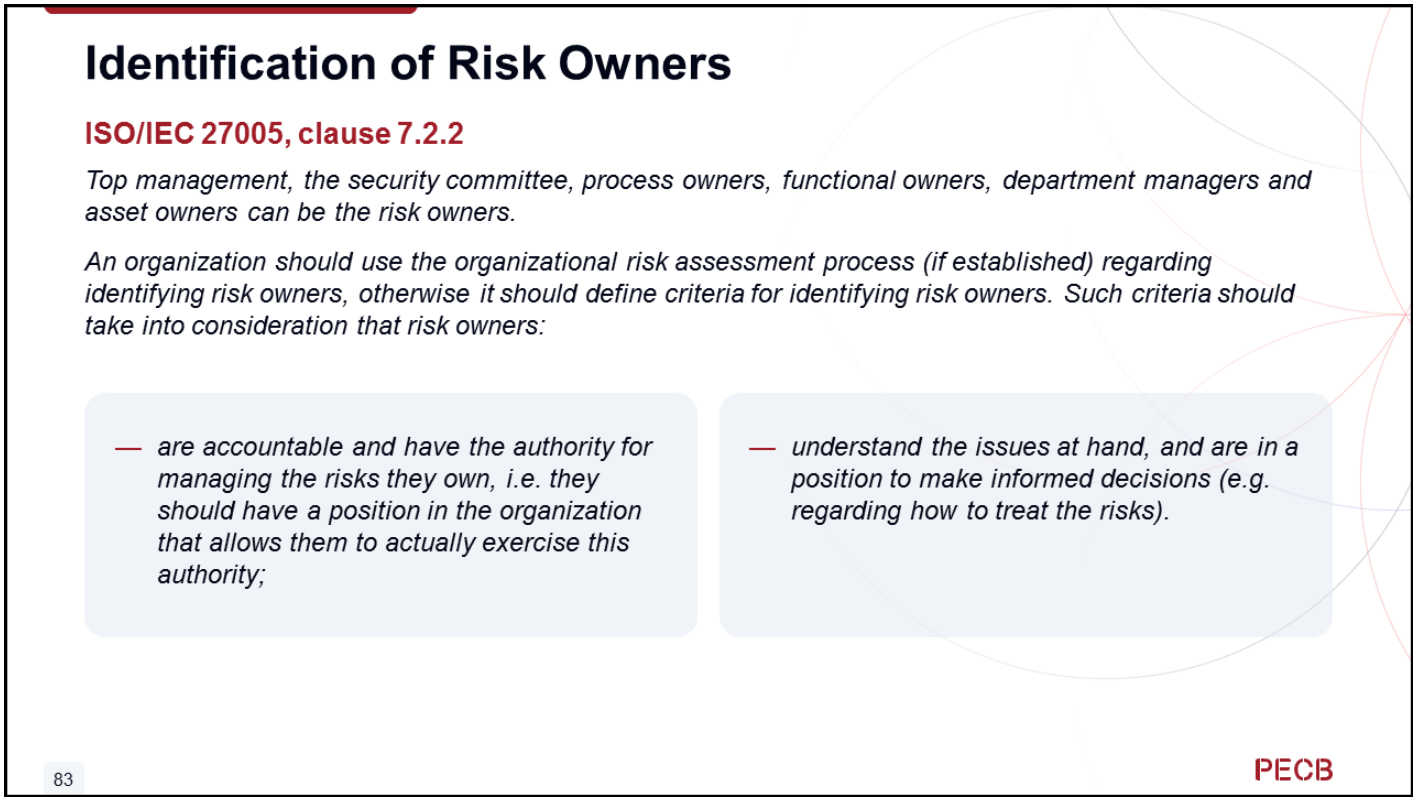
An automated vulnerability-scanning tool is used to scan a group of hosts or a network for known vulnerable services [e.g. system allows anonymous File Transfer Protocol (FTP), Sendmail relaying]. However, some of the potential vulnerabilities identified by the automated scanning tool do not necessarily represent real vulnerabilities in the context of the system environment (e.g. some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements). Some of the vulnerabilities flagged by the automated scanning software can actually not be vulnerable for a particular site but can be configured that way because their environment requires it. This test method can therefore produce false positives.

Security testing and evaluation (STE) is another technique that can be used in identifying ICT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g. test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an ICT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the ICT system are secured. Penetration testing, when used in the risk assessment process, can be used to assess an ICT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the ICT system from the viewpoint of a threat source and to identify potential failures in the ICT system protection schemes.

Code review is the most thorough (but also most expensive) way of vulnerability assessment.

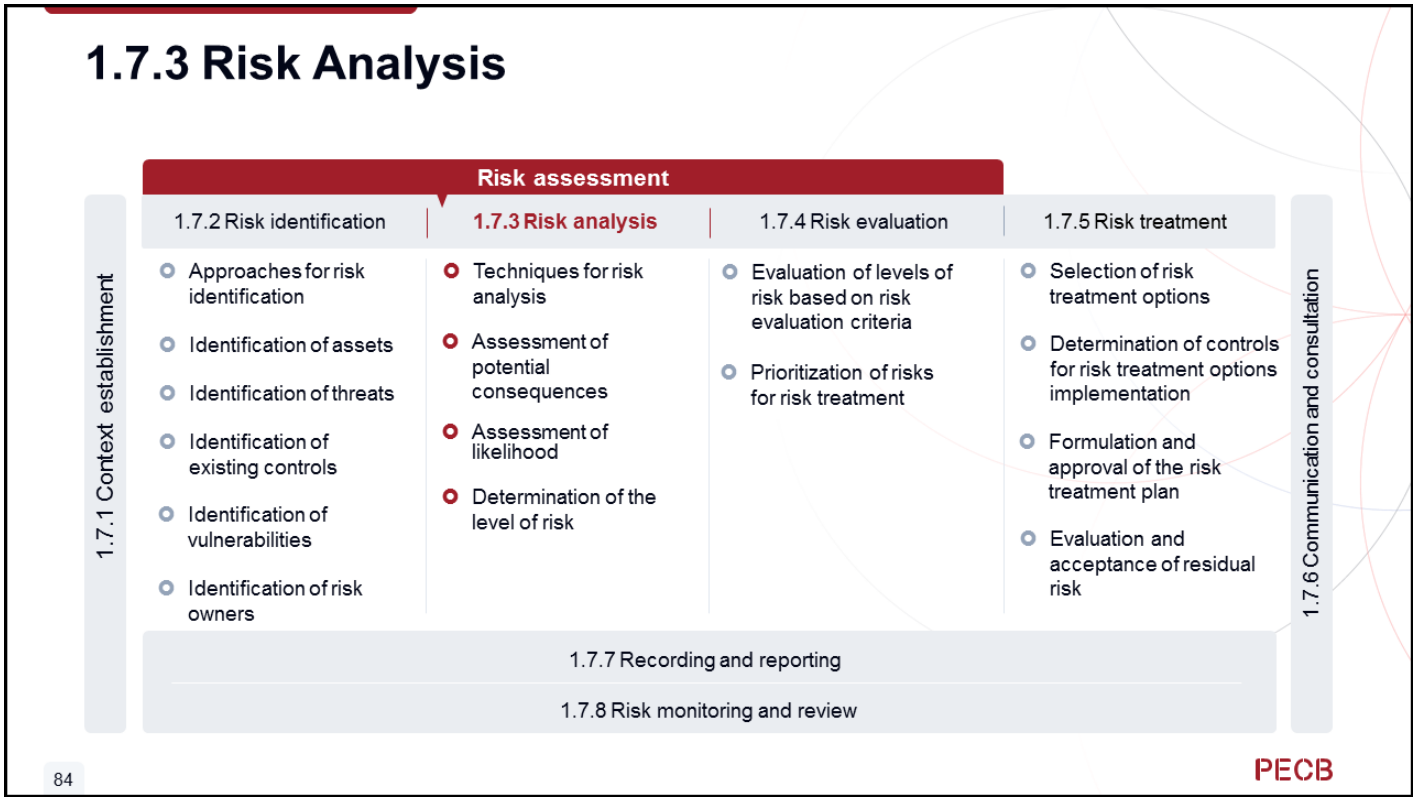
The results of these types of security testing help identify a system's vulnerabilities.



ISO/IEC 27005, clause 7.2.2 Identifying risk owners (cont'd)

The level of risk and to what asset the risk should apply can serve as the basis for identifying risk owners.

The allocation should take place as part of the risk assessment process.



ISO/IEC 27005, clause 3.2.5 Risk analysis

Process to comprehend the nature of risk and to determine the level of risk

Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

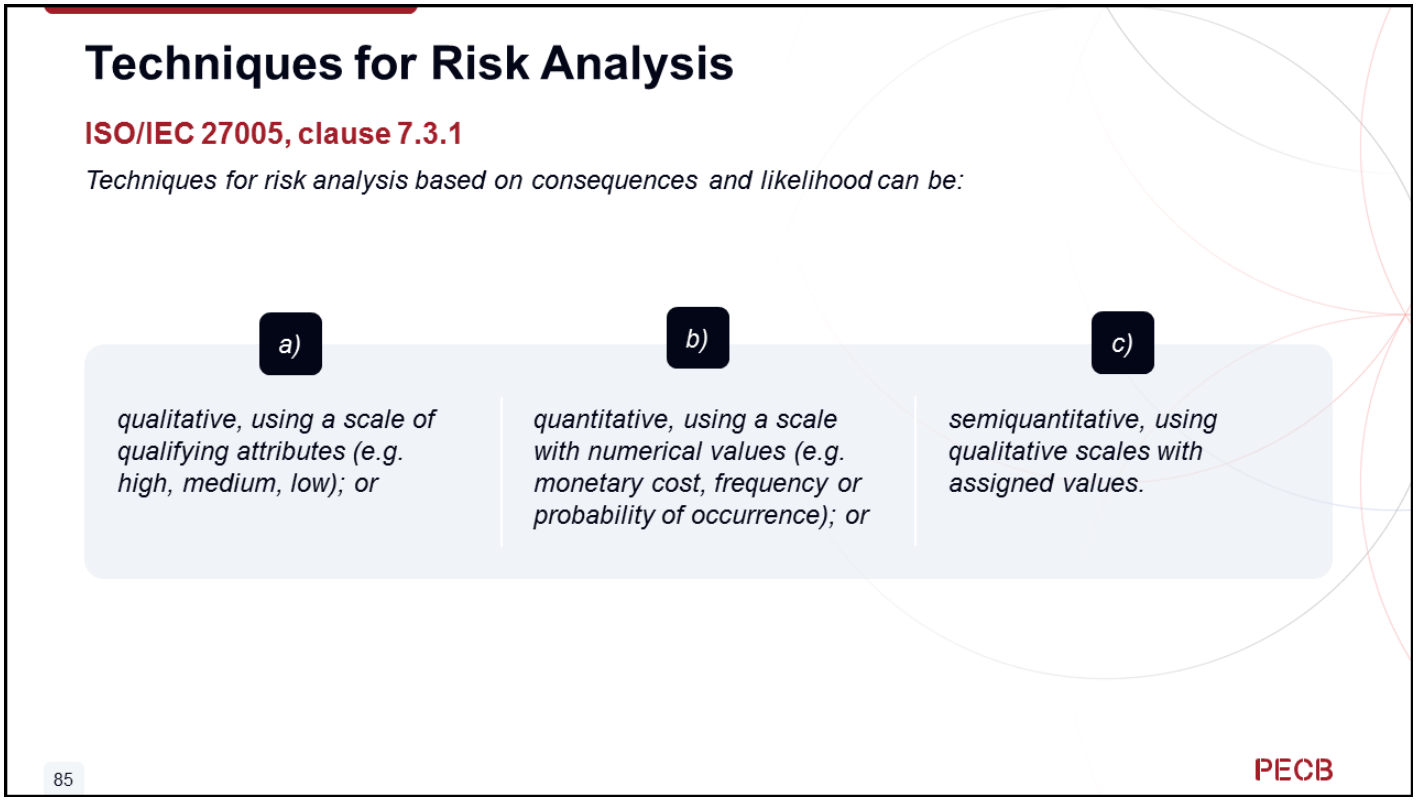
Note 2 to entry: Risk analysis includes risk estimation.

ISO 31000, clause 6.4.3 Risk analysis

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.



Qualitative analysis

This type of analysis supports the communication of risk results to decision makers. When using a qualitative approach to risk analysis, a clear explanation of all the terms employed and the basis for all criteria should be recorded because, unless each value is clearly defined or characterized by meaningful examples, different experts relying on their individual experiences could produce significantly different results. To counter this and to increase the chances for repeatability and reproducibility, explanatory notes for the assessed values can be written (e.g., explaining that X value is high because of Y or Z reasons) by using properly defined functions to combine qualitative values.

Quantitative analysis

A purely quantitative risk analysis may not always be possible or advisable. Some of the reasons for this include insufficient information about the system or the activity being analyzed, lack of data, biases, assumptions, or beliefs of those involved. Another reason can be the fact that the costs can outweigh the benefits of such an analysis. Furthermore, the outcome of the quantitative results may not always be clear and may require interpretation and explanation, particularly to explain the assumptions and constraints on using the results. Under such circumstances, a comparative semi-quantitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

Where full quantification has been carried out, it needs to be acknowledged that the calculated levels of risk are estimated. One should be careful to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

Semi-quantitative analysis

Scales may be linear or logarithmic, or have some other relationship; the formulas used can also vary. This type of analysis can provide the benefits of both quantitative and qualitative risk analyses.

Assessment of Potential Consequences

ISO/IEC 27005, clause 7.3.2

Failure to adequately preserve the security of information can lead to loss of its confidentiality, integrity or availability. Loss of confidentiality, integrity or availability can have further consequences for the organization and its objectives. Consequence analysis can be performed bottom up from the information security consequences by considering what can happen if there is a loss of confidentiality, integrity or availability of the information in question. Typically, the risk owner can estimate the consequence if the event occurs. The following elements should be taken into consideration:

- *estimation (or measure based on experience) of the losses (time or data) due to the event as result of interrupting or disturbing operations;*
- *estimation/perception of severity of the consequence (e.g. expressed in money);*
- *recovery costs depending on whether recovery can be done internally (by the risk owner team), or there is a need to call an external entity.*

86

PECB

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 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.

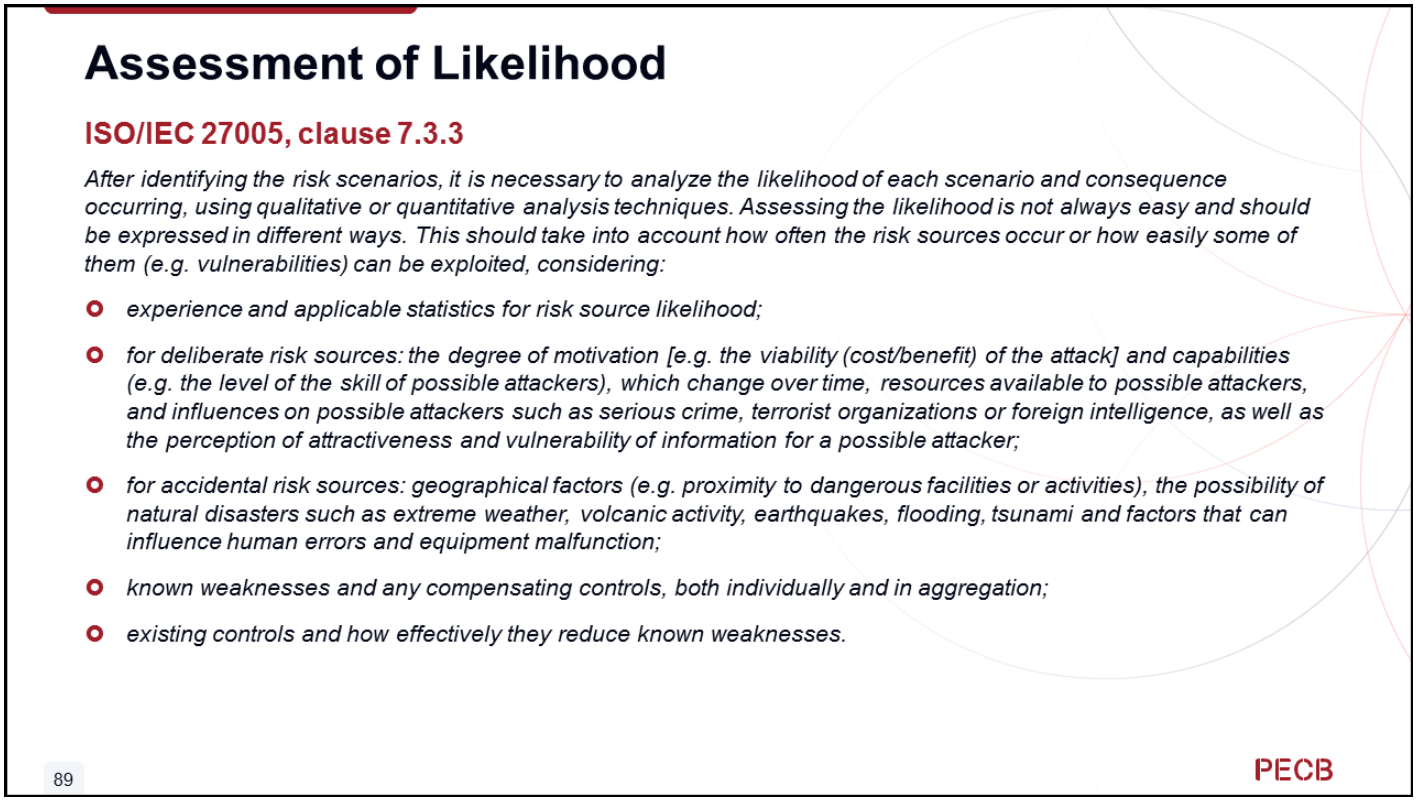
Example of a Consequence Scale

ISO/IEC 27005, Table A.1

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

PECB

Note: To complete Exercise 2, please go to the Exercises Worksheet.



ISO/IEC 27005, clause 7.3.3 Assessing likelihood (cont'd)

Estimation of likelihood is intrinsically uncertain, not only because it considers things that have not yet happened and are therefore not fully known, but also because likelihood is a statistical measure and is not directly representative of individual events. The three basic sources of assessment uncertainty are:

- *personal uncertainty originating in the judgment of the assessor, which derives from variability in the mental heuristics of decision making;*
- *methodological uncertainty, which derives from the use of tools that inevitably model events simplistically;*
- *systemic uncertainty about the anticipated event itself, which derives from insufficient knowledge (in particular, if evidence is limited or a risk source changes with time).*

To increase the reliability of estimating likelihood, organizations should consider using:

a. *team assessments rather than individual assessments;*
b. *external sources, such as information security breach reports;*
c. *scales with range and resolution appropriate to the organization's approach;*
d. *unambiguous categories, such as "once a year", rather than "infrequent".*

When assessing the likelihood of events, it is important to recognize the difference between independent and dependent events. The likelihood of events that depend on each other is conditioned by the relationship between them (e.g. a second event can be inevitable if a first event occurs) so that separate assessment of both their likelihoods is not necessary. The likelihood of relevant independent events are all essential contributors to the likelihood of a consequence to which they contribute.

Example of a Qualitative Likelihood Scale

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

PECB

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.

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 judgment 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.

Example of a Quantitative Likelihood Scale

Possible example event	Frequency	Likelihood
Last year, the organization reported 36 incidents related to password reset.	36 incidents/1 year	Three incidents per month
The organization's system has been compromised six times last year from a third-party intruder who gained access to employees' credentials.	6 system attacks/1 year	Once every two months

PECB

Determination of the Level of Risk

ISO/IEC 27005, clause 7.3.4

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

92

Numerical estimation

If organizations have relevant information on past incidents, such data can be used to estimate future risks. However, organizations should also explore other methods 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.

It is possible to calculate the probabilities of potential incidents by using external data. For example, 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.

Example of a Qualitative Approach for Level of Risk Determination

ISO/IEC 27005, Table A.3

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

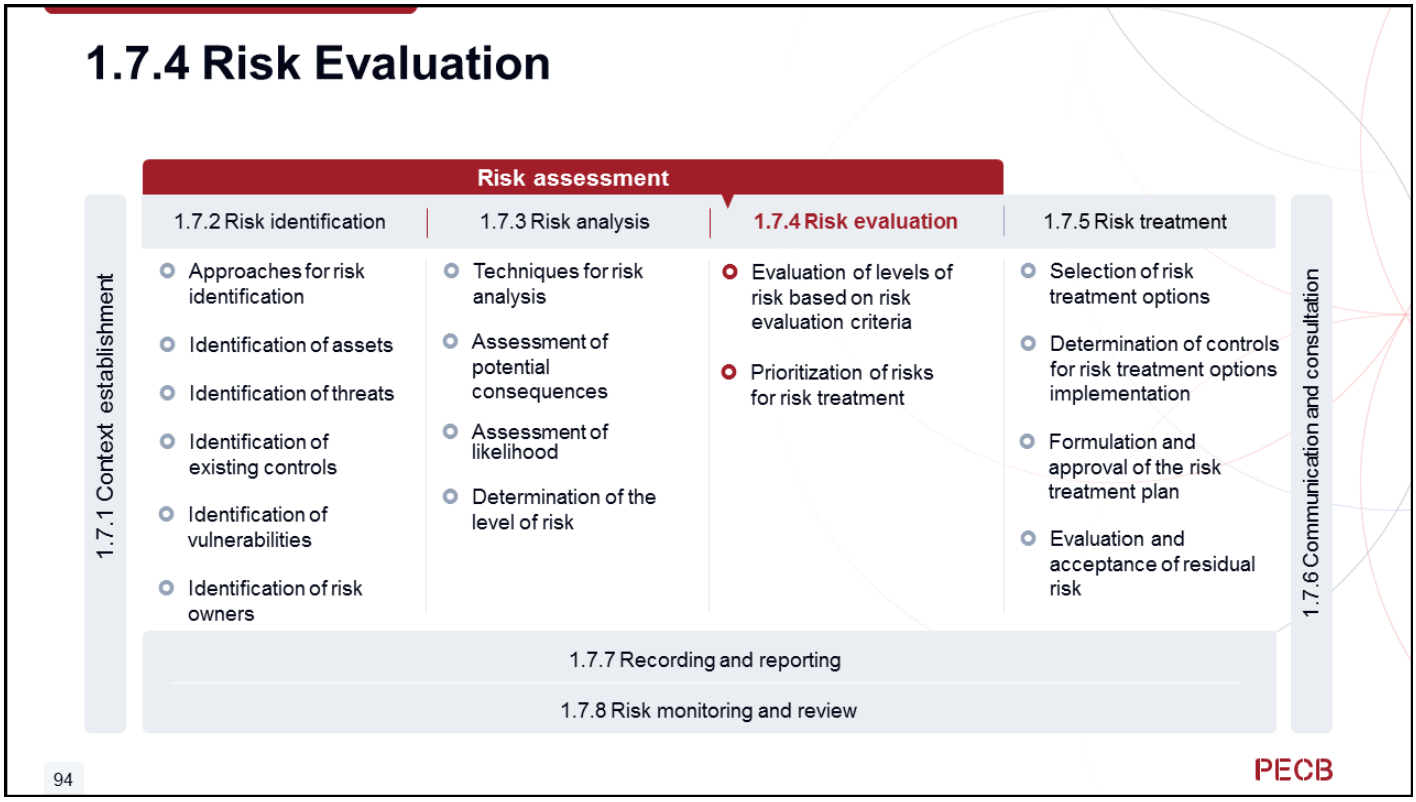
93

PECB

ISO/IEC 27005, Annex A.1.1.2.3 Level of risk

The utility of qualitative scales and the consistency of risk assessments that derive from them depend entirely on the consistency with which the category labels are interpreted by all interested parties.

The levels of any qualitative scale should be unambiguous, its increments should be clearly defined, the qualitative descriptions for each level should be expressed in objective language and the categories should not overlap with each other.



ISO/IEC 27005, clause 3.2.6 Risk evaluation

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

Note 1 to entry: 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.

95

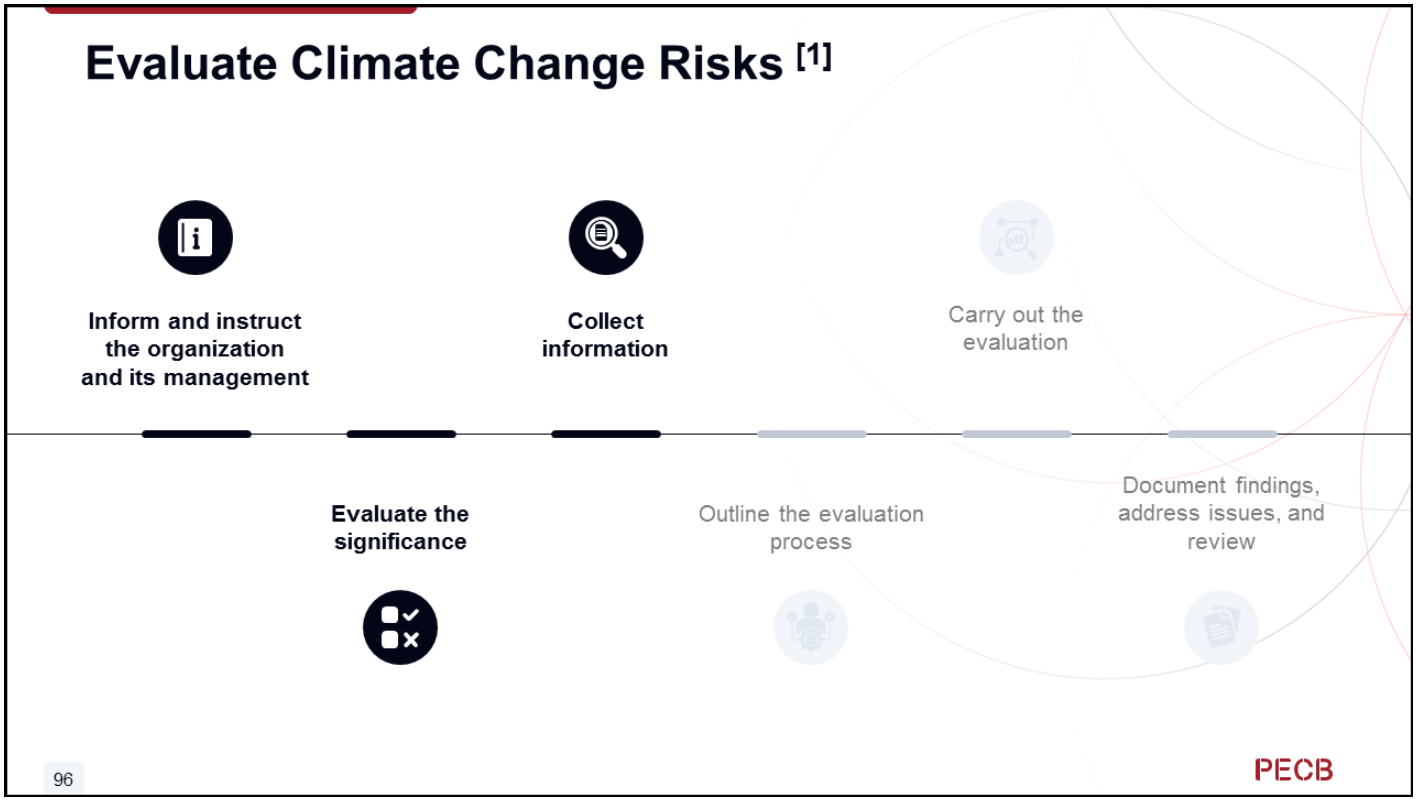
PECB

ISO/IEC 27005, clause 7.4.1 Comparing the results of risk analysis with the risk criteria

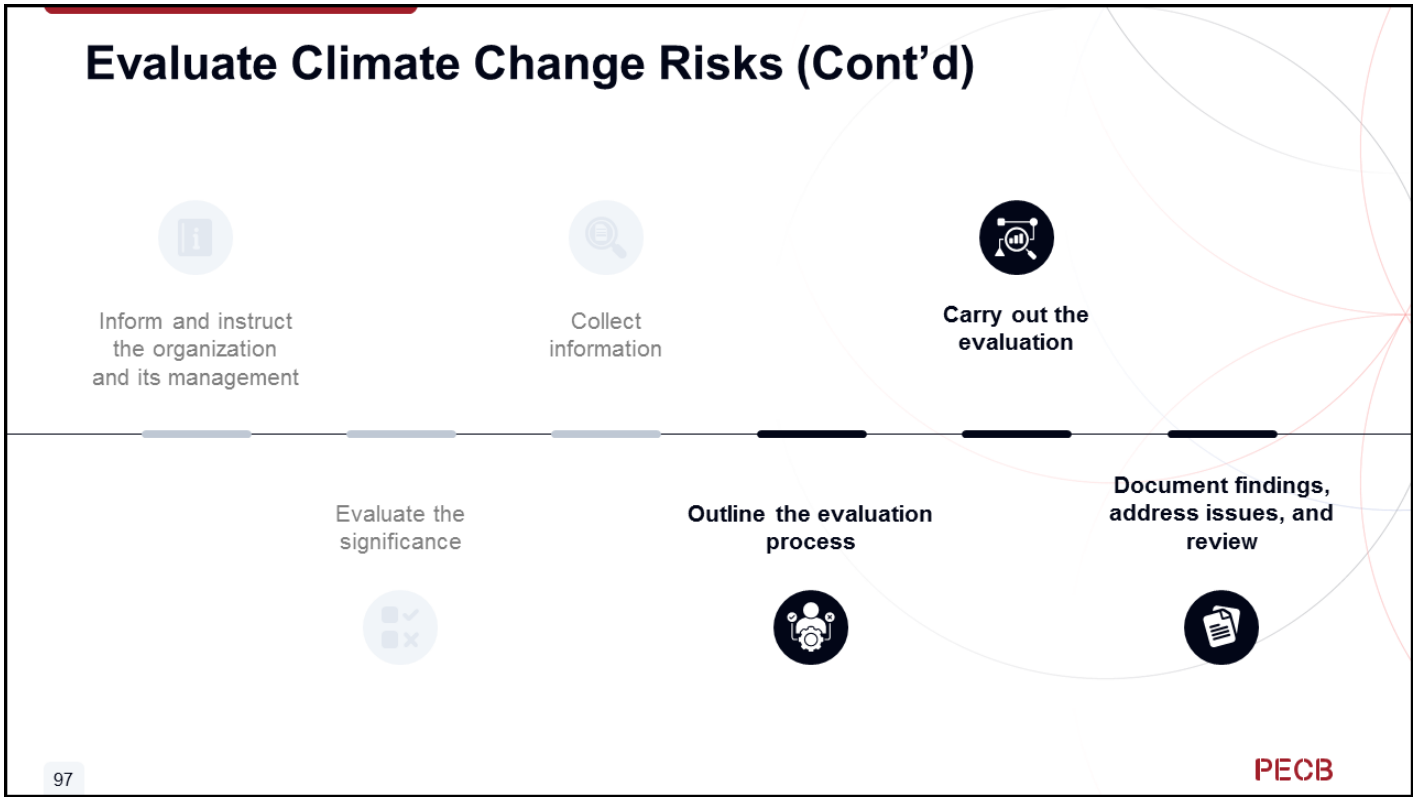
Risk evaluation decisions should be based on the comparison of assessed risk with defined acceptance criteria, ideally taking into account the degree of confidence in the assessment. In some cases, such as the frequent occurrence of relatively low consequence events, it can be helpful to consider their cumulative effect over some timescale of interest, rather than the risk of each event considered individually, as this can provide a more realistic representation of overall risks.

There can be uncertainties in defining the boundary between those risks that require treatment and those that do not. Under certain circumstances, using a single level as the acceptable level of risk that divides risks that require treatment from those which do not is not always appropriate. In some cases, it can be more effective to include an element of flexibility into the criteria by incorporating additional parameters such as cost and effectiveness of possible controls.

The levels of risk can be validated based on consensus among risk owners and business and technical specialists. It is important that risk owners have a good understanding of the risks they are accountable for that accords with the results of objective assessment. Consequently, any disparity between assessed levels of risk and those perceived by risk owners should be investigated to determine which better approximates to reality.



1. **Inform and instruct the organization and its management:**
   - Provide comprehensive education to the organization and management about the implications of climate change
   - Ensure understanding of scientific findings, trends, and technical terminology related to climate change
   - Enable informed decision-making by equipping the organization with knowledge about climate risk management
   - Gain support from senior management through climate risk education by highlighting the importance and potential impacts of addressing climate risks
   - Foster awareness and commitment within the organization to effectively manage climate change risks
2. **Evaluate the significance:**
   - Initiate a materiality assessment to understand climate change impacts on interested parties
   - Evaluate climate risks specific to the organization
   - Engage in a thorough materiality assessment to identify potential risks affecting long-term business sustainability
   - Engage board of directors, employees, customers, and regulators through surveys and feedback sessions to determine material risks and concerns
   - Utilize existing resources such as internal documentation and industry research to gain insights into the organization's exposure to climate risks
3. **Collect information:**
   - Collect historical data regarding climate and weather impact on the organization's operations
   - Analyze current local and global data along with predictive models to understand potential future climate change implications
   - Focus on gathering data related to physical risks such as the vulnerability of facilities, supply chain disruptions, and community resilience, as well as transition risks including regulatory changes, market shifts, and technological advancements



4.Outline the evaluation process:

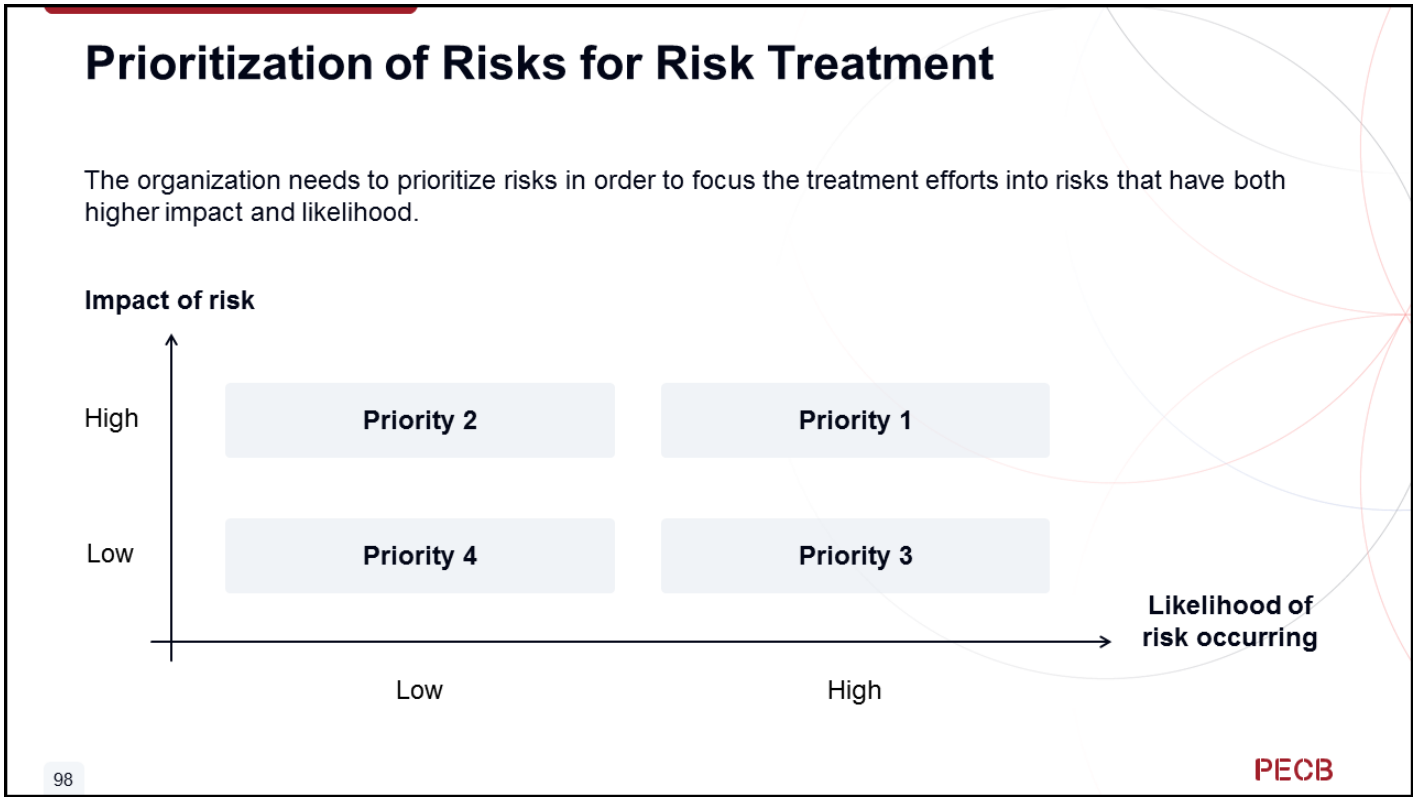
- Develop a structured roadmap for conducting a climate risk assessment, outlining key elements such as responsible parties, scope, timeline, and methodology
- Find individuals who are experts in the relevant field within the organization and establish clear guidelines for the assessment process
- Determine the assessment's scope, considering factors like regulatory requirements, stakeholder expectations, and available resources

5.Carry out the evaluation:

- Address physical and transition risks separately during the assessment process
- Evaluate the potential impact of weather-related disasters on physical assets and operations
- Assess the effects of regulatory policies, market dynamics, and technological advancements on the organization's business model and financial performance

6.Document findings, address issues, and review:

- Communicate assessment findings to internal and external stakeholders, including mitigation and adaptation strategies
- Develop plans to mitigate identified risks and adapt to changing conditions, incorporating both physical and transition risks
- Periodically reassess climate risks and adjust mitigation strategies accordingly to ensure ongoing resilience and responsiveness to evolving threats and opportunities



Organizations need to prioritize risks in order to focus the treatment efforts into risks that have both higher impact and likelihood. In order to prioritize risks, they should first be identified. In this way, risk is managed more effectively.

The concept of zero risk does not exist, but it is possible to define a threshold below the risk that the organization accepts to not engage in any activity for reducing the risk. On the other hand, there is a threshold beyond which risk is unacceptable and its source should be eliminated or reduced.

Risk prioritization allows organizations to determine the actions that should be taken for treating the risks based on their levels.

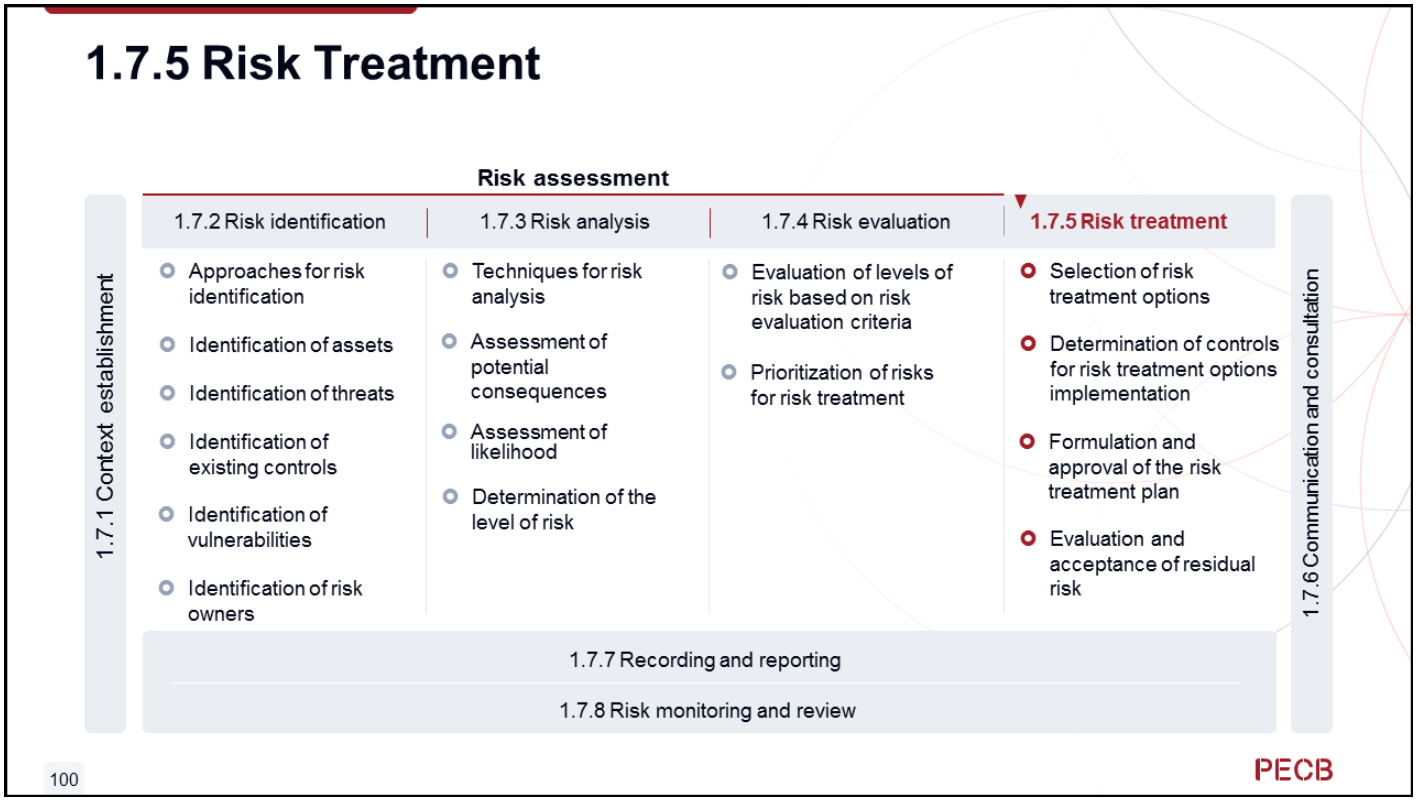
ISO/IEC 27005, clause 7.4.2 Prioritizing the analyzed risks for risk treatment

Risk evaluation uses the understanding of risk obtained by risk analysis to make proposals for deciding about the next step to take. Those should refer to:

- *whether a risk treatment is required;*
- *priorities for risk treatment considering assessed levels of risks.*

Risk criteria used to prioritize risks should consider the objectives of the organization, contractual, legal and regulatory requirements and the views of relevant interested parties. Prioritization as taken in the risk evaluation activity are mainly based on the acceptance criteria.

Note: To complete Quiz 11, please go to the Quizzes Worksheet.



ISO/IEC 27005, clause 3.2.7 Risk treatment

Process to modify risk

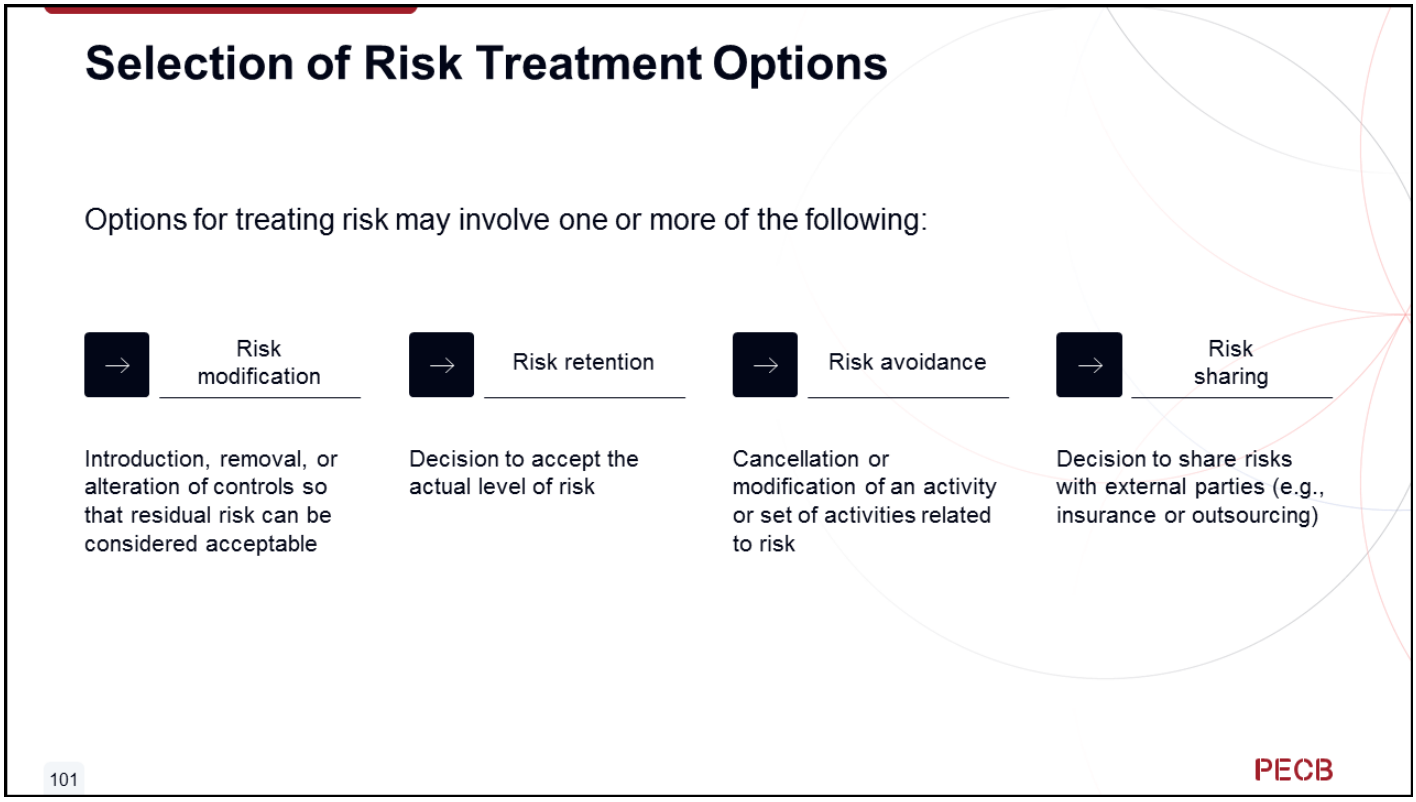
Note 1 to entry: Risk treatment can involve:

- *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 the risk source;*
- *changing the likelihood;*
- *changing the consequences;*
- *sharing the risk with another party or parties (including contracts and risk financing); and*
- *retaining the risk by informed decision.*

Note 2 to entry: Information security risk treatment does not include "taking or increasing risk in order to pursue an opportunity" but the organization can have this option for general risk management.

Note 3 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 4 to entry: Risk treatment can create new risks or modify existing risks.



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.

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.

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 such cases, the organization may decide that it is better to live with the consequences of the risk. The organization has to document this decision so that risk owners are informed of the risks and accept the consequences.

Risk denial is defined as the failure to accept the responsibility of managing the identified risks, which, in most cases, results in negative consequences for the organization. Therefore, organizations should acknowledge the existence of risks and select an appropriate risk treatment option.

Determination of Controls for Risk Treatment Options Implementation

ISO/IEC 27005, clause 8.3

The determination of controls can include new controls not yet implemented, or can include using controls that exist in the organization. However, a control that is already in operation should not automatically be included in the risk assessment because:

- *the control is not necessary to manage one or more information security risks;*
- *it can be a control that does in some way help manage one or more information security risks but is not sufficiently effective to be included in the risk assessment or managed by the ISMS, or;*
- *it can be currently operating for reasons not related to information security (e.g. quality, efficiency, effectiveness or compliance), or;*
- *it is currently operating but from an information security perspective can be removed as it does not have enough effect to justify its continuing status as an essential control.*

102

PECB

ISO/IEC 27005, clause 8.3 Determining all controls that are necessary to implement the information security risk treatment options (cont'd)

If a custom control is defined, the control wording should accurately and fairly describe what the control is and how it operates. As applicable and appropriate, this wording can usefully include such aspects as:

- *is it a documented control;*
- *who owns the control;*
- *how it is monitored;*
- *how it can be evidenced;*
- *any exceptions;*
- *frequency of operation of the control;*
- *the tolerance for the control;*
- *if it is not obvious then the reason why the control exists.*

Formulation and Approval of the Risk Treatment Plan

ISO/IEC 27005, clause 8.6.1

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

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

103

PECB

ISO/IEC 27005, clause 8.6.1 Formulation of the risk treatment plan (cont'd)

The purpose of this activity is to create plan(s) for treating specific sets of the risks that are on the list of prioritized risks. There are two possible interpretations of the term "plan" in the context of risk treatment. The first is a project plan, i.e. a plan to implement the organization's necessary controls. The second is a design plan, i.e. the plan that not only identifies necessary controls but also describes how the controls interact with their environment and each other to modify risks. In practice, both can be used.

Every risk that needs treatment should be treated in one of the risk treatment plans. An organization can choose to have several risk treatment plans, which together implement all required aspects of risk treatment.

While creating the risk treatment plan, organizations should consider the following:

- *priorities in relation with the level of risk and urgency of treatment;*
- *whether different types of controls (preventive, detective, corrective) or their composition are applicable;*
- *whether it is necessary to wait for a control to be settled before starting to implement a new one on the same asset;*
- *whether there is a delay between the time the control is implemented and the moment where it is fully effective and operational.*

For each treated risk the treatment plan should include the following information:

- *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 indicators;*
- *the constraints;*
- *the required reporting and monitoring;*
- *when actions are expected to be undertaken and completed;*
- *implementation status.*

Slide Notes Extension

ISO/IEC 27005, clause 8.6.1 Formulation of the risk treatment plan (cont'd)

The risk treatment plan actions should be ranked by priority in relation with the level of risk and urgency of treatment. The higher the level of risk, and in some cases the frequency of risk occurrence, the sooner the control is to be implemented.

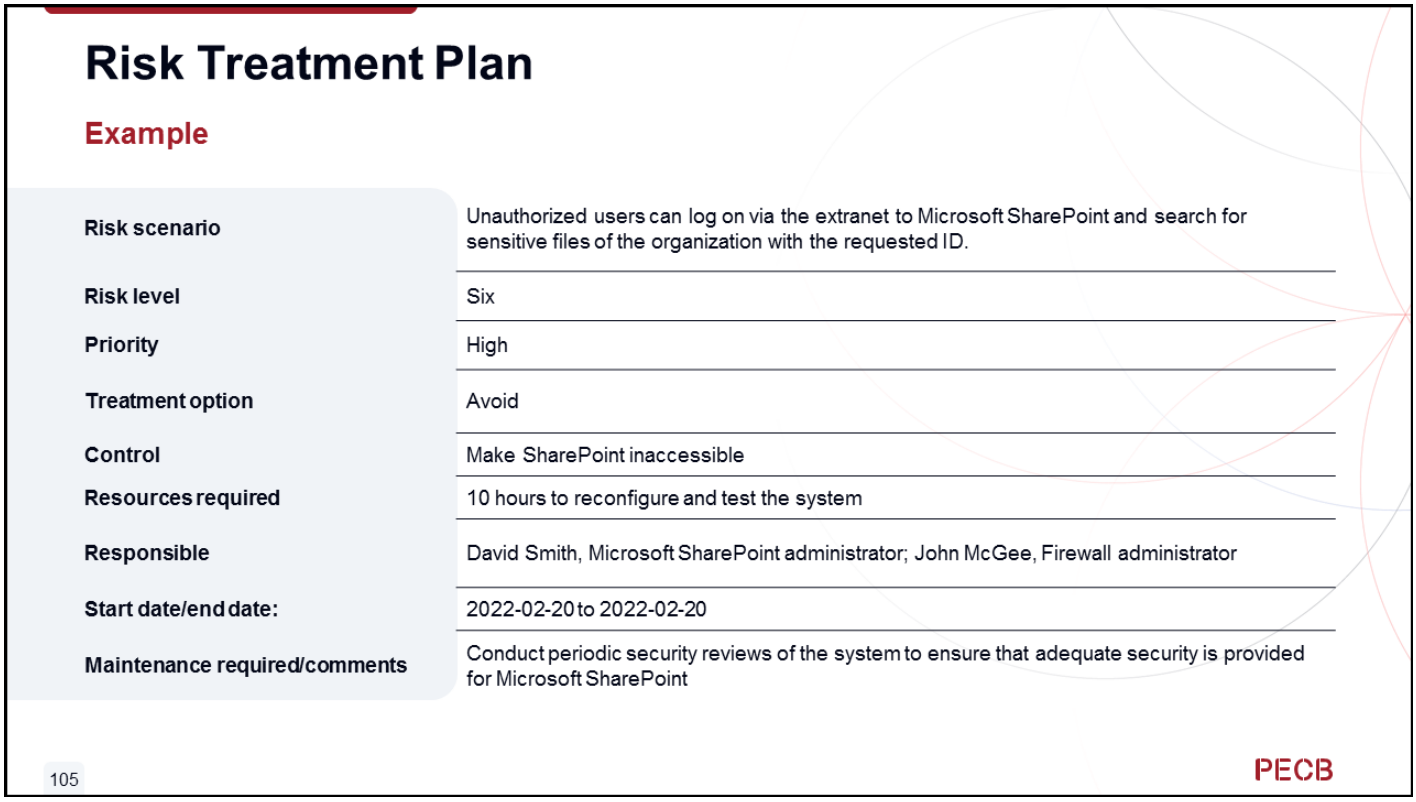
For each listed risk within the risk treatment plan, detailed implementation information should be tracked and can include but is not limited to:

- *names of risk owners and persons responsible for the implementation;*
- *implementation dates or timelines;*
- *control activities planned to test the implementation result;*
- *implementation status;*
- *cost level (investment, operation).*

ISO/IEC 27005, clause 8.6.2 Approval by risk owners

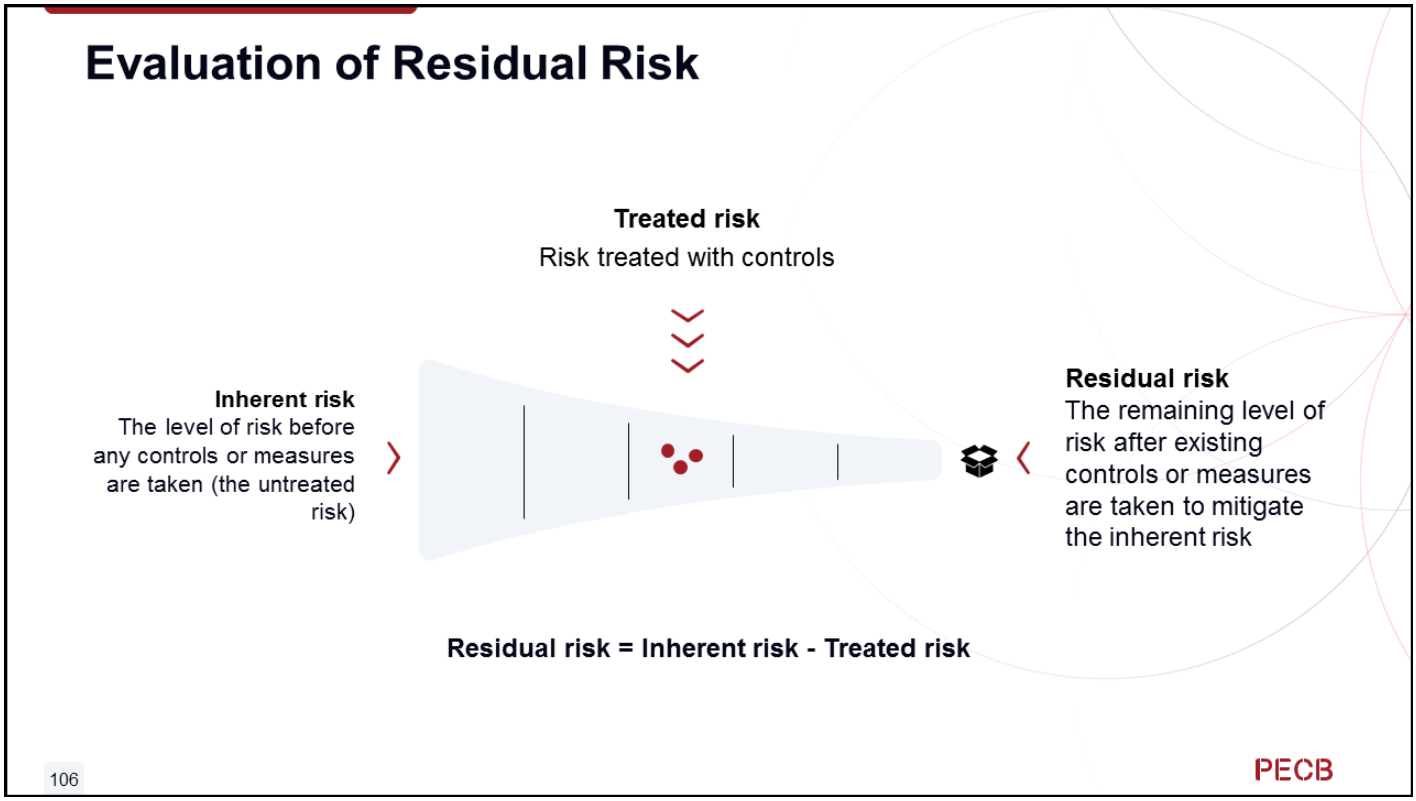
The information security risk treatment plan should be approved by the risk owners once it is formulated. Risk owners should also decide on the acceptance of residual information security risks. This decision should be based on defined risk acceptance criteria.

The results of the risk assessment, the risk treatment plan and the remaining risks should be understandable to the risk owners so that they can discharge their accountabilities properly.



The table presented on the slide illustrates a risk treatment plan. 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 resources to be allocated
- The responsibilities to be undertaken
- The priorities to be sequenced



After the implementation of a risk treatment plan, there are always residual risks. Risk owners must be aware of the residual risks and be responsible for them. 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 also implement mechanisms to monitor residual risk surveillance.

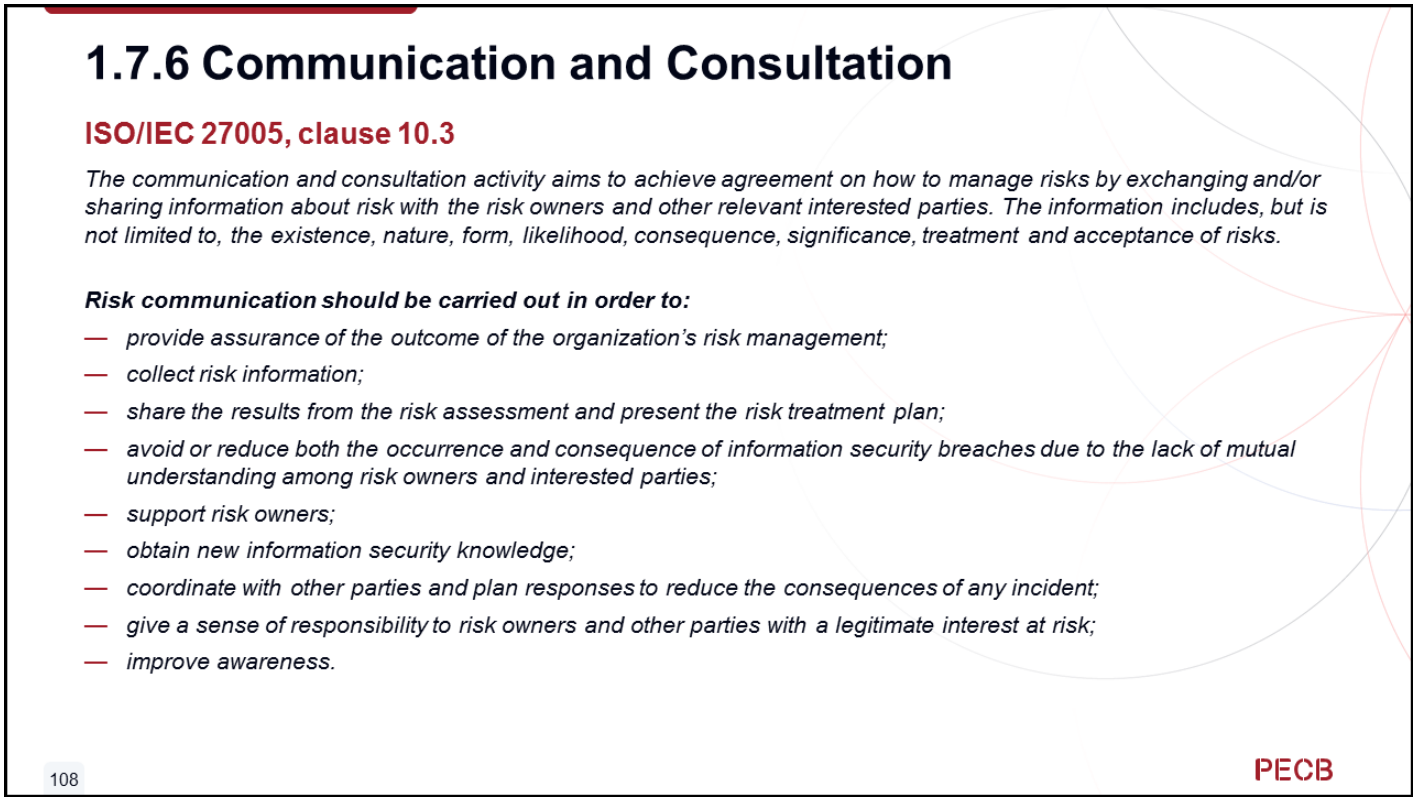
If the residual risk is considered as unacceptable after the controls have been implemented, a decision must be made to treat the risk completely. One alternative could be to identify other risk treatment options such as sharing the risk (insurance or outsourcing), which would reduce the risk to an acceptable level. Another option could be to accept the risk. 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.

Acceptance of Residual Risks

ISO/IEC 27005, clause 8.6.3

- *Risk acceptance can involve a process to achieve endorsements of treatments prior to a final risk acceptance decision. It is important for risk owners to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval. Depending on the risk assessment process and risk acceptance criteria, this can require a manager with a higher level of authority than the risk owner to agree to the risk acceptance.*
- *It can take some time to implement a plan to treat assessed risks. Risk criteria can allow levels of risk to exceed a desired threshold to a defined extent if there is a plan in place to reduce that risk in an acceptable time. Risk acceptance decisions can take into account timeframes in risk treatment plans and whether or not risk treatment implementation progress is in line with what is planned.*
- *Some risks can vary over time (regardless of whether this change is due to implementation of a risk treatment plan). Risk acceptance criteria can consider this and have risk acceptance thresholds that depend on the length of time that an organization can be exposed to an assessed risk.*

PECB



Good communication and consultation requires honesty between all the relevant interested parties.

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

ISO/IEC 27005, clause 10.3 Communication and consultation (cont'd)

ISO/IEC 27001:2022, 6.1.2 c) 2), requires that owners of the information security risks be identified. Risk ownership can be deliberately confused or concealed. Even when risk owners can be identified, they can be reluctant to acknowledge that they are responsible for the risks that they own, and obtaining their participation in the risk management process can be difficult. There should be a defined communication procedure for informing those concerned about risk ownership.

ISO/IEC 27001:2022, 6.1.3 f), requires the risk owners to approve the risk treatment plan(s) and to decide on the acceptance of residual risks. Communication between risk owners and staff responsible for the implementation of the ISMS is an important activity. There should be an agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners, and perhaps other interested parties and decision-makers. The information includes, but is not limited to, the existence, nature, form, likelihood, significance, treatment and acceptance of risks. Communication should be bi-directional.

An organization should develop risk communication plans for normal operations as well as for emergencies. The risk communication and consultation activity should be performed continually.

1.7.7 Recording and Reporting

ISO 31000, clause 6.7

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

109

PECB

ISO/IEC 27005, clause 10.4.1 General

ISO/IEC 27001 specifies requirements for organizations to retain documented information concerning the risk assessment process and results; the risk treatment process and results.

ISO/IEC 27005, clause 10.4.2 Documented information about processes

Documented information about the information security risk assessment process should contain:

a. *a definition of the risk criteria (including the risk acceptance criteria and the criteria for performing information security risk assessments);*
b. *reasoning for the consistency, validity and comparability of results;*
c. *a description of the risk identification method (including the identification of risk owners);*
d. *a description of the method for analyzing the information security risks (including the assessment of potential consequences, realistic likelihood and resultant level of risk);*
e. *a description of the method for comparing the results with the risk criteria and the prioritization of risks for risk treatment.*

Documented information about the information security risk treatment process should contain descriptions of:

- *the method for selecting appropriate information security risk treatment options;*
- *the method for determining necessary controls;*
- *how ISO/IEC 27001:2022, Annex A, is used to determine that necessary controls have not been inadvertently overlooked;*
- *how risk treatment plans are produced;*
- *how risk owners' approval is obtained.*

Slide Notes Extension

ISO/IEC 27005, clause 10.4.3 Documented information about results

As organizations are required to perform risk assessments at planned intervals or when significant changes are proposed or occur, there should at least be evidence of a schedule, and risk assessments being performed in accordance with that schedule. If a change is proposed, or has occurred, then there should be evidence of the performance of an associated risk assessment. Otherwise, the organization should explain why the change is significant or not.

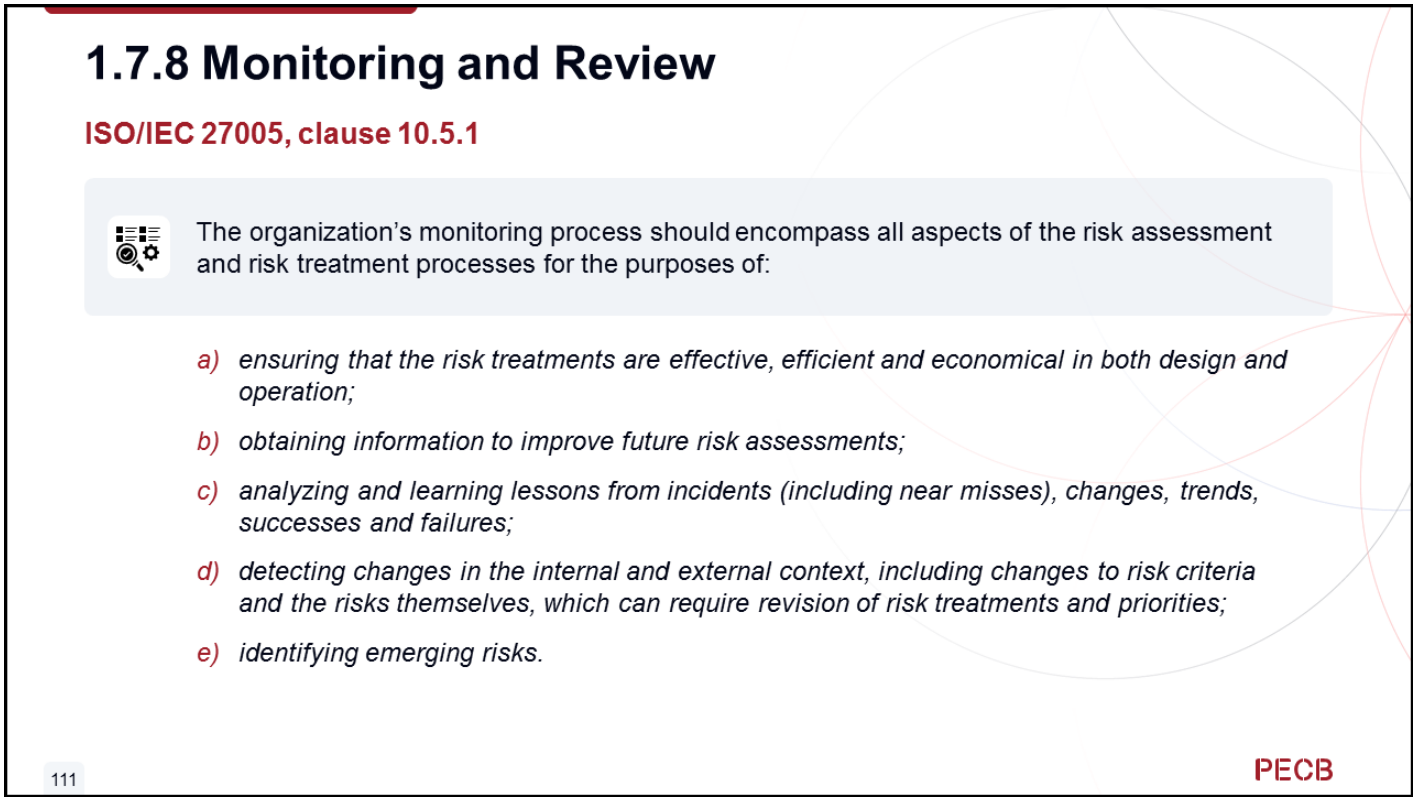
Documented information about the information security risk assessment results should contain:

a. *the identified risks, their consequence and likelihood;*
b. *the identity of the risk owner(s);*
c. *the results of applying the risk acceptance criteria;*
d. *the priority for risk treatment.*

Recording of the rationale for risk decisions is also recommended, in order to both learn from error in individual cases and facilitate continual improvement.

Documented information about the information security risk treatment results should contain:

- *identification of the necessary controls;*
- *where appropriate and available, evidence that these necessary controls act to modify risks, so as to meet the organization's risk acceptance criteria.*



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

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.

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analyzing 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.

ISO/IEC 27005, clause 10.5.2 Monitoring and reviewing factors influencing risks

Risks are not static. Event scenarios, asset values, threats, vulnerabilities, likelihoods and consequences can change abruptly without any indication. Constant monitoring should be carried out to detect these changes. This can be supported by external services that provide information regarding new threats or vulnerabilities. Organizations should ensure the continual monitoring of relevant factors, such as:

a. *new sources of risk, including freshly reported vulnerabilities in IT;*
b. *new assets that have been included in the risk management scope;*
c. *necessary modification of asset values (e.g. due to changed business requirements);*
d. *identified vulnerabilities to determine those becoming exposed to new or re-emerging threats;*
e. *changes in patterns of use of existing or new technologies that can open up new possible opportunities for attack;*
f. *changes in laws and regulations;*
g. *changes in risk appetite and perceptions of what is now acceptable and what is no longer acceptable;*
h. *information security incidents, both inside and outside of the organization.*

Section 12 Summary

- ISO 31000 provides guidelines for managing risks faced by organizations in any industry or sector, whereas ISO/IEC 27005 provides guidelines for information security risk management.
- ISO/IEC 27005 divides assets into two broad categories: primary/business assets and supporting assets.
- Risk identification aims to find, recognize, and describe risks that might help or prevent an organization achieving its objectives.
- Risk analysis aims to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk.
- Risk evaluation aims to compare the results of risk analysis with risk criteria to determine whether the risk or its magnitude is acceptable or tolerable.
- Risk treatment aims to select and implement options for addressing risks.
- Risk acceptance aims to review and approve the proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval.

Questions?

Quiz 12

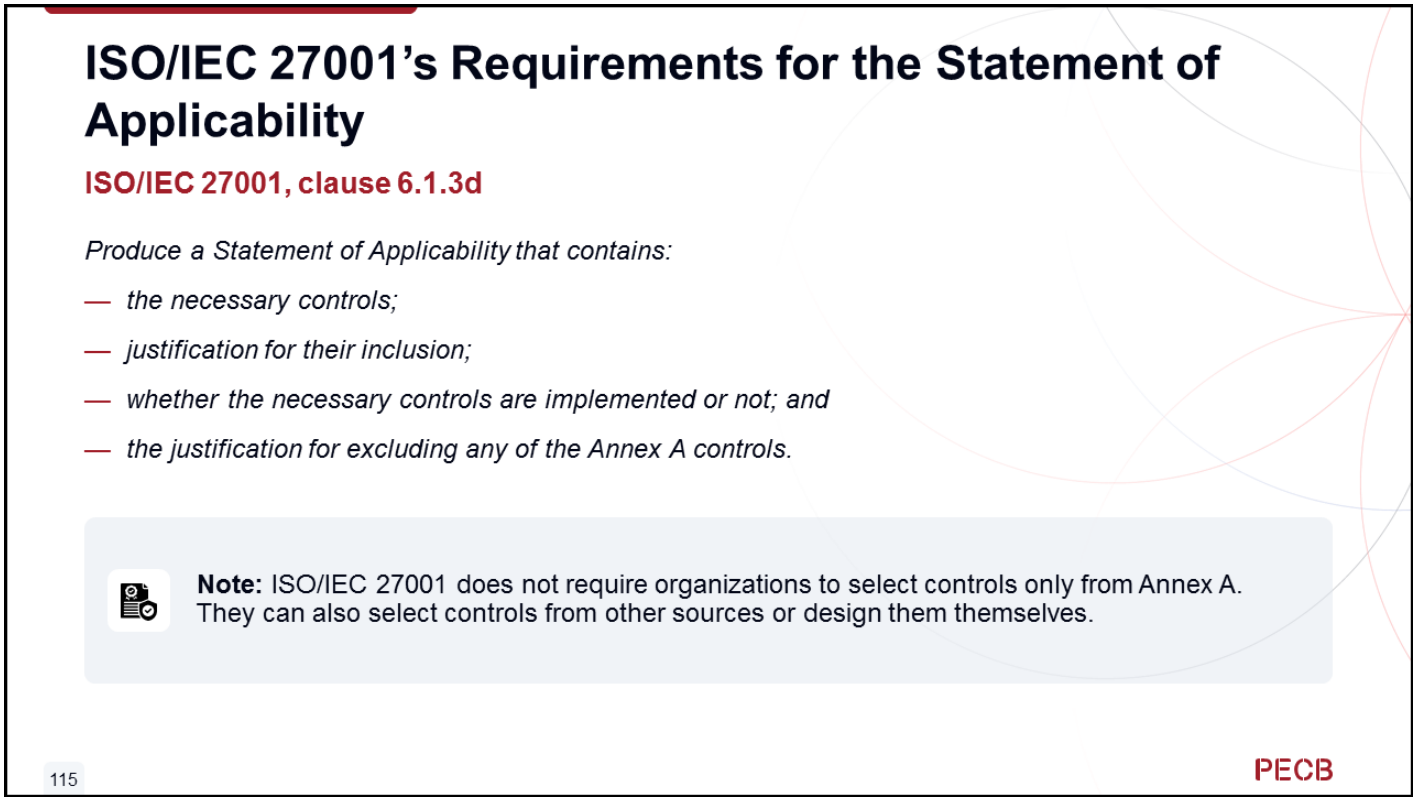
Note: To complete Quiz 12, please go to the Quizzes Worksheet.

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.

Statement of Applicability

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

PECB



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.

Note: According to ISO/IEC 27001 and ISO/IEC 27005, the selection of controls and development of the Statement of Applicability are part of the risk treatment process. As outlined in ISO/IEC 27005, after it has prioritized the risks for risk treatment, the organization should:

1. Select appropriate information security risk treatment options
2. Determine all controls that are necessary to implement the risk treatment options
3. Compare the determined controls with the controls of ISO/IEC 27001
4. Produce a Statement of Applicability
5. Formulate the risk treatment plan

For the purposes of this training course, the Statement of Applicability has been explained in a separate section to emphasize its importance to the ISMS.

Statement of Applicability

A Statement of Applicability (SoA) is a documented statement listing the controls that are relevant and applicable to the organization's ISMS.

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 in the Annex.

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.

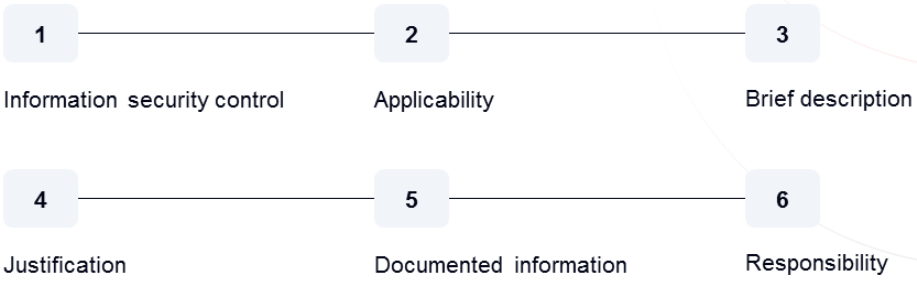
116

Notes on terminology:

- The Statement of Applicability is specific to ISO/IEC 27001. 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.

Statement of Applicability

- ISO/IEC 27001 does not provide detailed explanations on how the Statement of Applicability should be developed. It only briefly mentions that it must contain a list of information security controls, the justification for their inclusion, and justification for the exclusion of controls, if any, from Annex A.
- Organizations can include in the SoA the following:



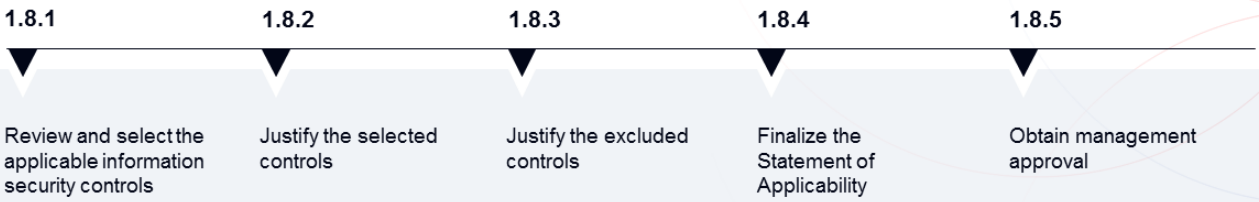
117

PECB

1. **Information security control:** In this section, the control of Annex A of ISO/IEC 27001 or any other source identified by the organization 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 is 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.
4. **Justification:** In this section, the reasons for selecting or excluding a security control are given.
5. **Documented information:** In this section, the documents (e.g., policies and procedures) related to the security control are mentioned.
6. **Responsibility:** In this section, the name and function of the individual responsible for the control is written.

1.8 Statement of Applicability

List of activities



Review and select the applicable information security controls

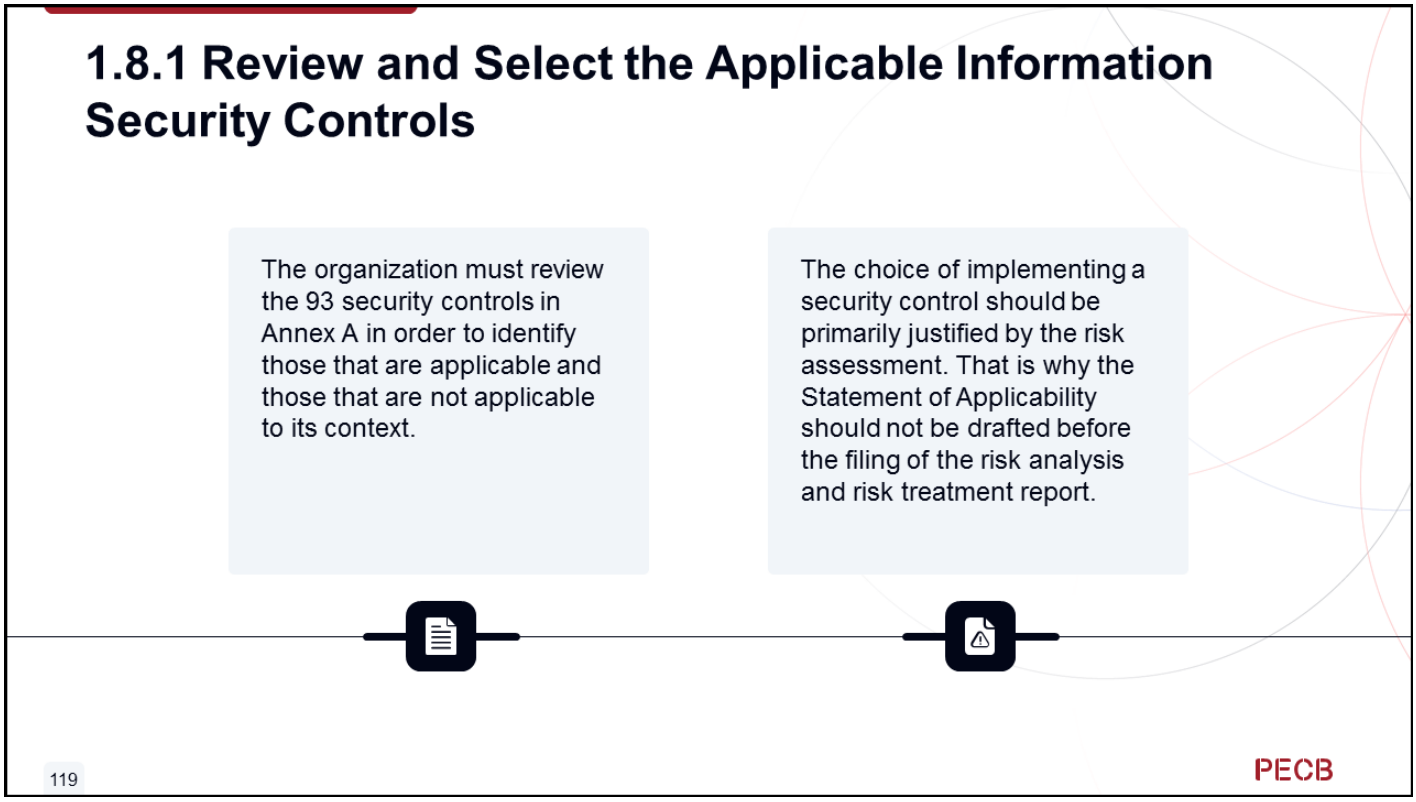
Justify the selected controls

Justify the excluded controls

Finalize the Statement of Applicability

Obtain management approval

PECB



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. Organizations should avoid implementing more controls than necessary as their implementation may cause financial losses for them and no benefits. They also should avoid implementing fewer controls than needed as risks may not be addressed adequately due to the lack of controls.

1.8.2 Justify the Selected Controls

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

120

Addressing information security within supplier agreements (ISO/IEC 27001, Annex A.5.20):
Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.

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

PECB

Other examples of justifications related to the selected controls:

ISO/IEC 27001, Annex A.5.29 Information security during disruption

The organization shall plan how to maintain information security at an appropriate level during disruption.

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

ISO/IEC 27001, Annex A.8.32 Change management

Changes to information processing facilities and information systems shall be subject to change management procedures.

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*

1.8.3 Justify the Excluded Controls

- The organization should justify the exclusion of each security control presented in Annex A of ISO/IEC 27001.

The reasons for exclusion most often cited are:

This would lead to the violation of a legal, statutory, or contractual requirement, e.g., ISO/IEC 27001, Annex A.6.1 Screening.

→

No activity related to this control is present in the organization, e.g., ISO/IEC 27001, Annex A.6.7 Remote working.

121

PECB

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

ISO/IEC 27001, Annex A.6.1 Screening

Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and 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.6.7 Remote working

Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

***Justification of the exclusion**: Remote working 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.6.1) 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.

1.8.4 Finalize the Statement of Applicability

Example

Control	Applicable	Description	Justification	Documentation	Responsible
ISO/IEC 27001, Annex A.5.1 *Policies for information security*	Yes	The information security policy, approved by the management, is effective as of December 21, 2022. A copy of this policy was sent to all employees and other relevant interested parties. The official version is available on the intranet.	The policy will be implemented to provide guidance on information security and to ensure that the information security practices comply with business requirements, laws, and regulations.	Security-policy-3213PO	Information security manager
ISO/IEC 27001, Annex A.6.7 *Remote working*	No	----------	Our organization has no activities related to remote working.	N/A	IT manager

PECB

1.8.5 Obtain Management Approval

- Extensive collaboration, time, effort, and strong commitment from upper management are essential for enterprise-level SoA planning.
- The resulting SoA should be a concise control chart, subject to examination and approval by top management or relevant authority.

PECB

Audits often cause anxiety for companies, leading top management to push information security roles to address nonconformities prior to audits. When properly formulated, the SoA ensures compliance with information security requirements, minimizing any major issues.[1]

Section 13 Summary

- A Statement of Applicability (SoA) is a documented statement listing the controls that are relevant and applicable to the organization's ISMS. 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.
- The organization must review the 93 security controls in Annex A in order to identify those that are applicable and those that are not applicable to its context.
- The choice of implementing a security control should be primarily justified by the risk assessment. That is why SoA should not be drafted before the filing of the risk analysis and risk treatment report.

Questions?

Quiz 13

Note: To complete Quiz 13, please go to the Quizzes Worksheet.

Note: To complete the Scenario-based Quiz 2, please go to the Quizzes Worksheet.

Day 2 Summary

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

- Leadership and commitment
- Organizational structure
- Analysis of the existing system
- Information security policy
- Specific security policies
- Risk assessment
- Risk treatment
- Communication and consultation
- Statement of Applicability
- Justifications for selected and excluded controls

Note: To complete Homework 4-7, please go to the Exercises Worksheet.