DAY 4

Certified ISO/IEC 27001 Lead Implementer

Version 10.0

Document number: ISMSLID4V10.0

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

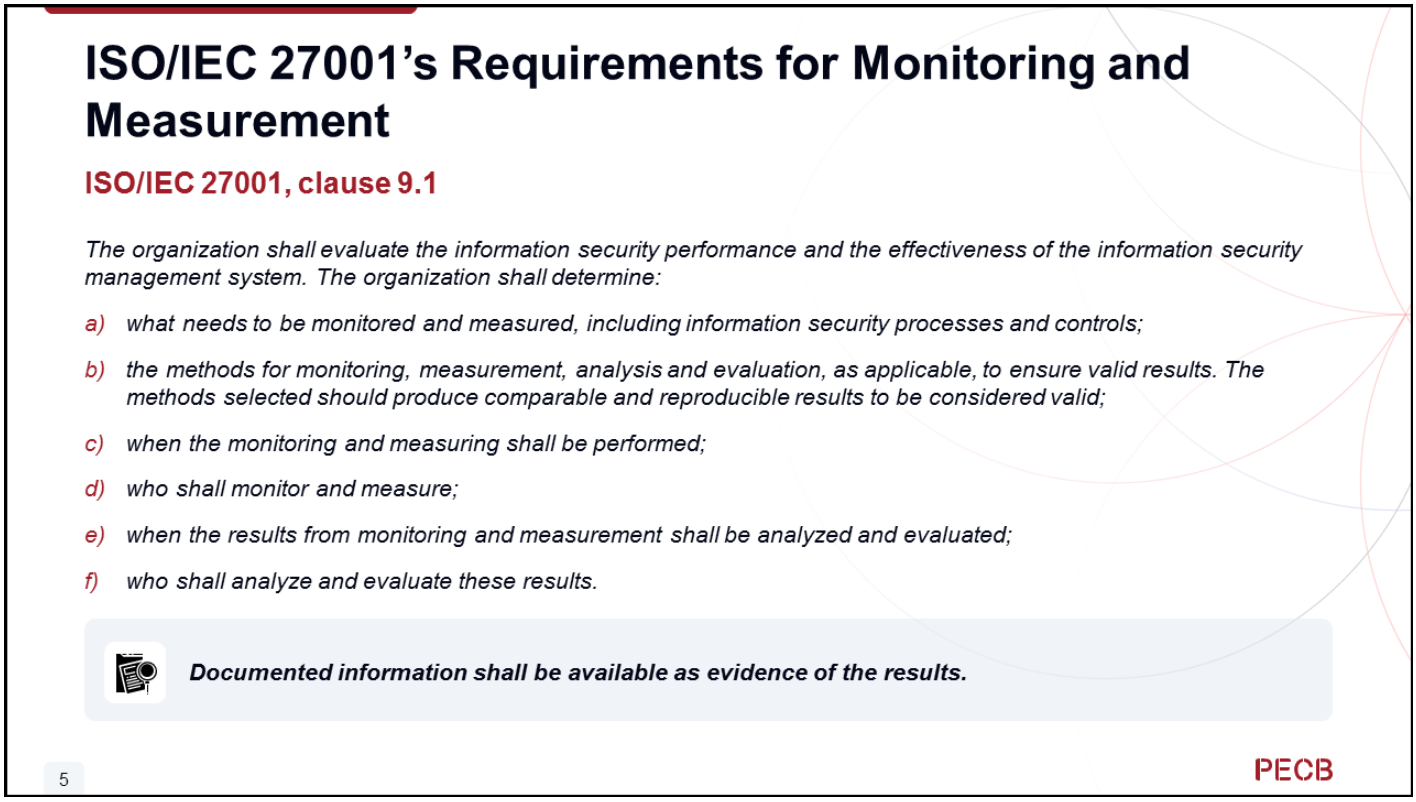
- Monitor, measure, analyze, and evaluate the effectiveness of the ISMS
- Establish ISMS performance indicators
- Establish an internal audit program, plan and perform audit activities, and follow up on nonconformities
- Prepare, conduct, and close a management review
- Treat nonconformities
- Maintain and continually improve the ISMS
- Prepare for the certification audit, stage 1 and stage 2 audit, and audit follow-up

This section aims at providing participants with information on how to determine the measurement objectives, define what aspects of an ISMS need to be monitored and measured, and establish performance indicators. Various methods of reporting the measurement results will be given, and the participant will be able to use the acquired knowledge and skills to verify the extent to which the identified ISO/IEC 27001 requirements have been met.

Monitoring, Measurement, Analysis, and Evaluation

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 9.1 Monitoring, measurement, analysis and evaluation

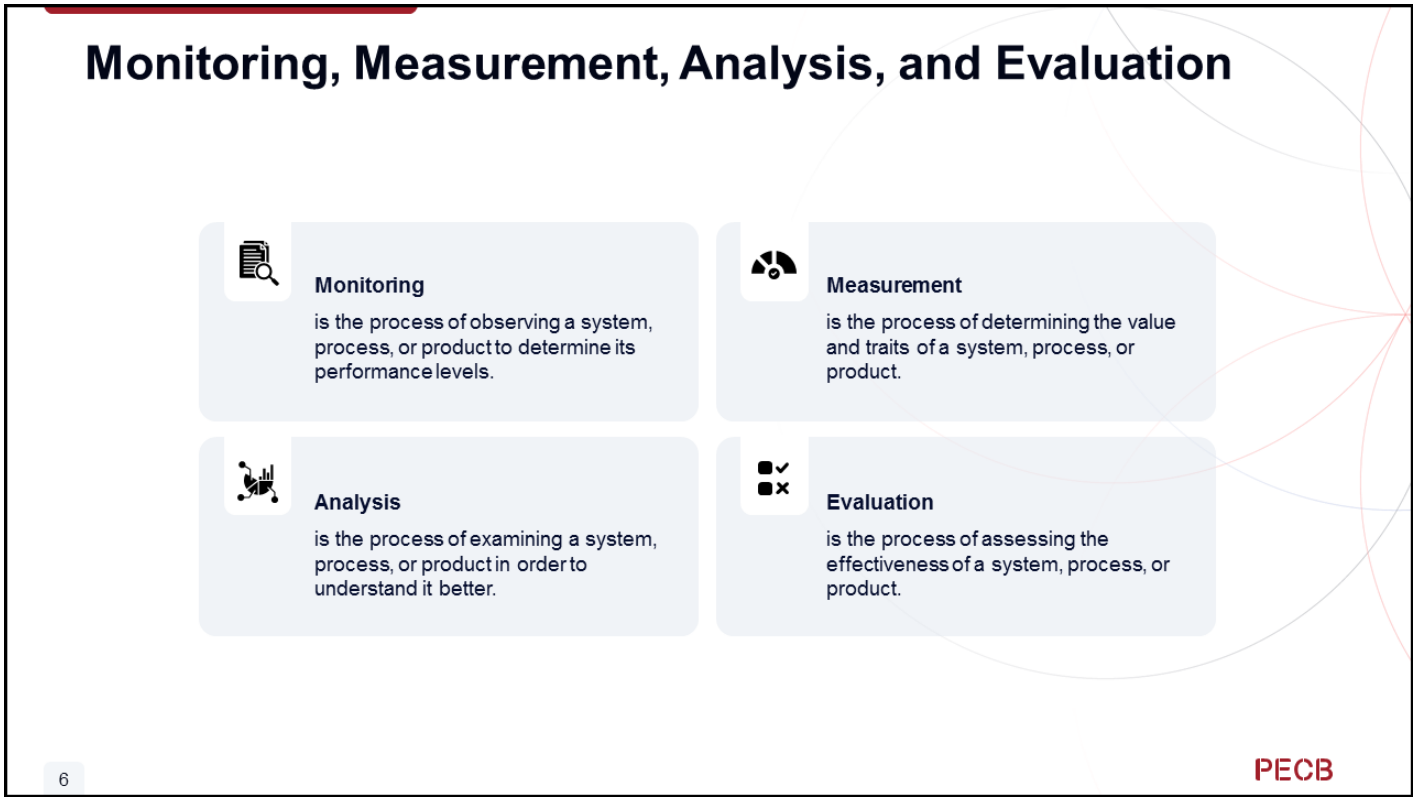
A good practice is to define the 'information need' when planning the monitoring, measurement, analysis and evaluation. An information need is usually expressed as a high level information security question or statement that helps the organization evaluate information security performance and ISMS effectiveness. In other words, monitoring and measurement should be undertaken to achieve a defined information need.

Care should be taken when determining the attributes to be measured. It is impracticable, costly and counterproductive to measure too many, or the wrong attributes. Besides the costs of measuring, analyzing and evaluating numerous attributes, there is a possibility that key issues could be obscured or missed altogether.

There are two generic types of measurements:

h.*performance measurements*, *which express the planned results in terms of the characteristics of the planned activity, such as head counts, milestone accomplishment, or the degree to which information security controls are implemented; and*

i.*effectiveness measurements*, *which express the effect that realization of the planned activities has on the organization's information security objectives.*

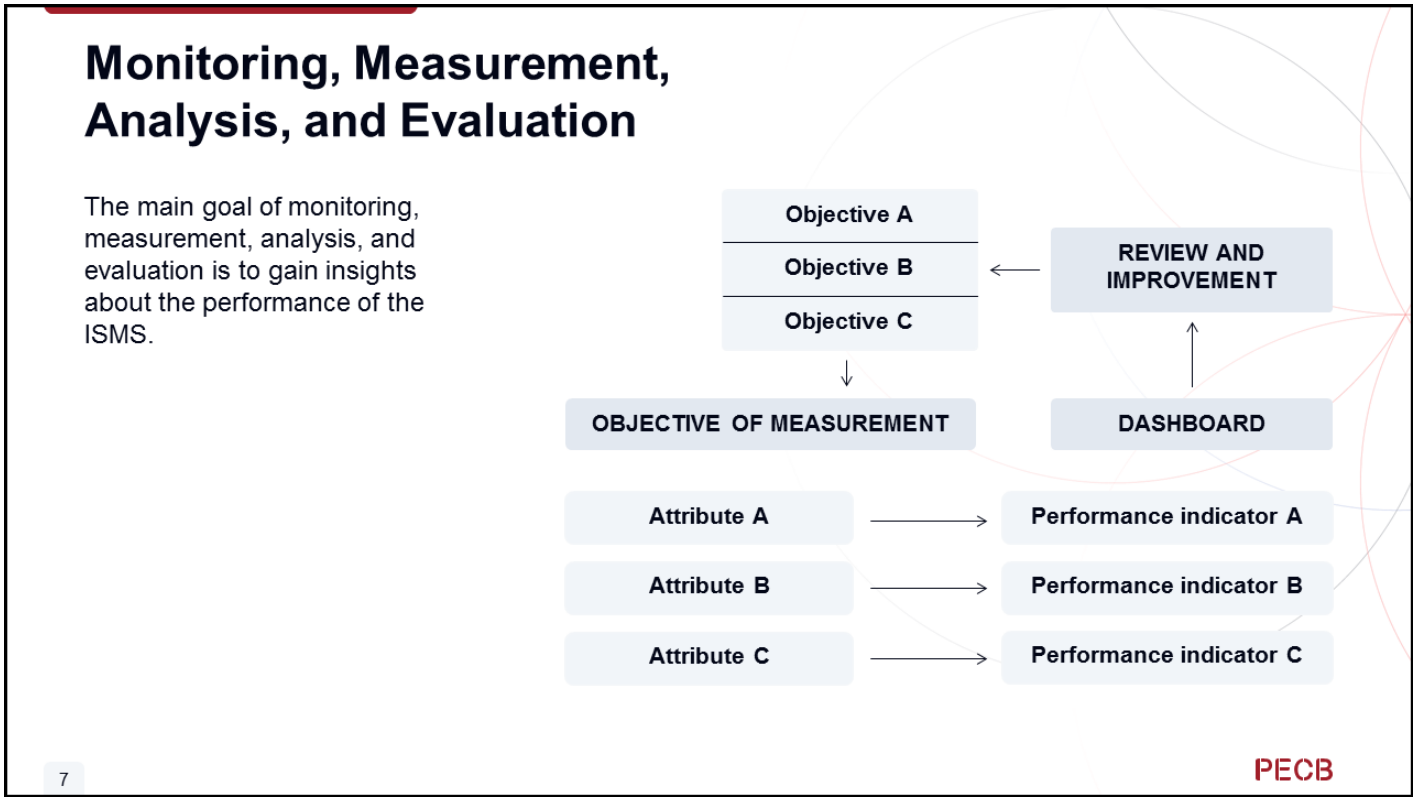


Monitoring, measurement, analysis, and evaluation are critical factors in the assessment of the performance of the ISMS. The goal is to determine the extent to which the processes meet the objectives. The outputs of these activities allow the organization to compare the actual performance levels with desired performance.

Some of the advantages of monitoring, measurement, analysis, and evaluation are:

- Determining the effectiveness and efficiency of processes
- Identifying deviations in a timely manner and treating them accordingly
- Implementing controls to ensure the realization of processes
- Identifying opportunities for continual improvement

Performance measures should be a high priority on the agenda of individuals or a team responsible for the implementation and maintenance of the information security management system.

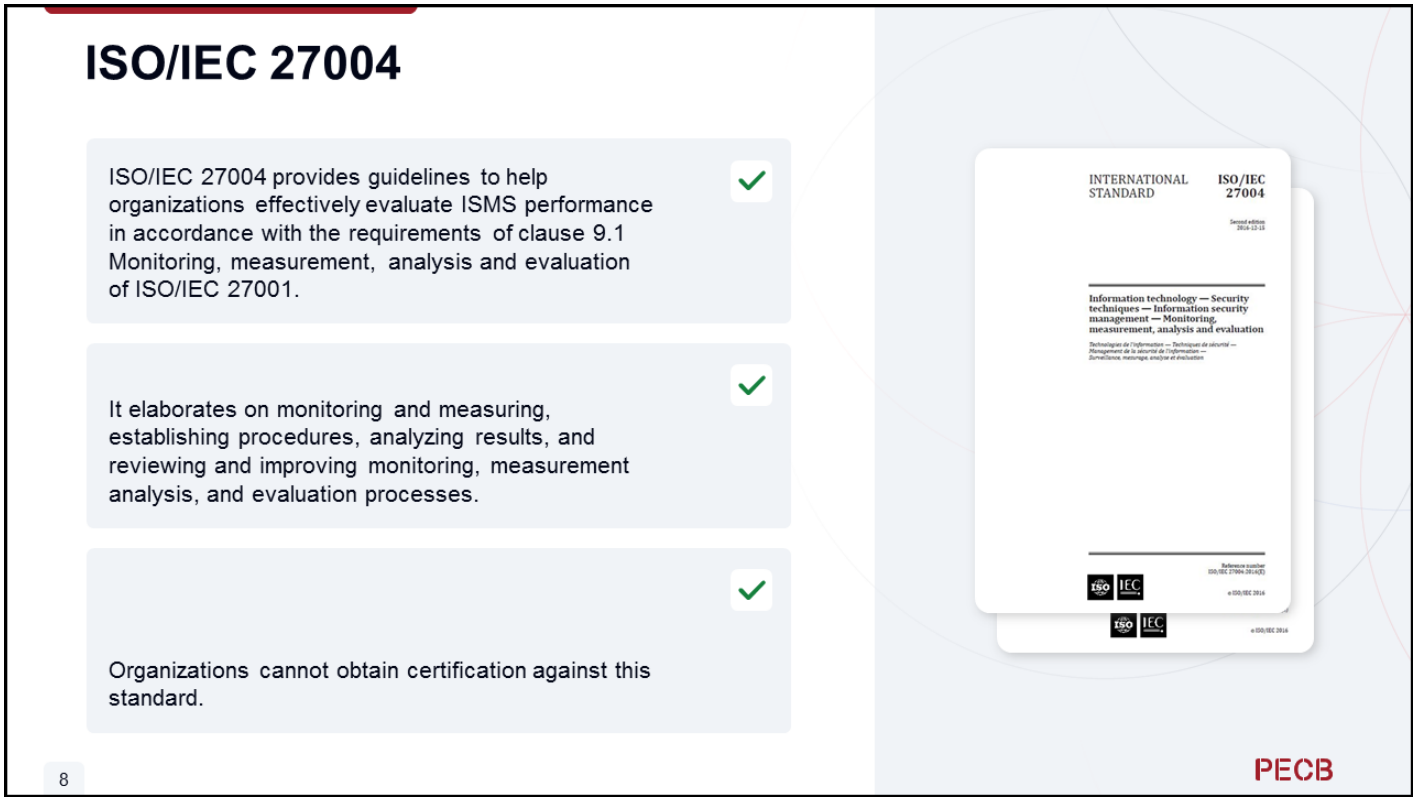


In a broader perspective, monitoring and measurement involves:

- Setting objectives for measuring and monitoring
- Selecting the attributes to be measured
- Establishing performance indicators
- Evaluating if the objectives are achieved

Example:

1. **Measurement objectives:** verify if all employees are aware of the major risks that the organization is facing
2. **Attribute:** employee that has attended the awareness session
3. **Performance indicator:** the percentage of employees that have attended the awareness session



ISO/IEC 27004, Introduction

This document is intended to assist organizations to evaluate the information security performance and the effectiveness of an information security management system in order to fulfill the requirements of ISO/IEC 27001:2013, 9.1: monitoring, measurement, analysis and evaluation.

The results of monitoring and measurement of an information security management system (ISMS) can be supportive of decisions relating to ISMS governance, management, operational effectiveness and continual improvement.

As with other ISO/IEC 27000 documents, this document should be considered, interpreted and adapted to suit each organization's specific situation. The concepts and approaches are intended to be broadly applicable but the particular measures that any particular organization requires depend on contextual factors (such as its size, sector, maturity, information security risks, compliance obligations and management style) that vary widely in practice.

This document is recommended for organizations implementing an ISMS that meets the requirements of ISO/IEC 27001. However, it does not establish any new requirements for ISMS which conform to ISO/IEC 27001 or impose any obligations upon organizations to observe the guidelines presented.

3.1 Monitoring, Measurement, Analysis, and Evaluation

List of activities

3.1.1 Set measurement objectives

3.1.2 Determine what needs to be monitored and measured

3.1.3 Determine who will monitor, measure, analyze, and evaluate

3.1.4 Establish performance indicators

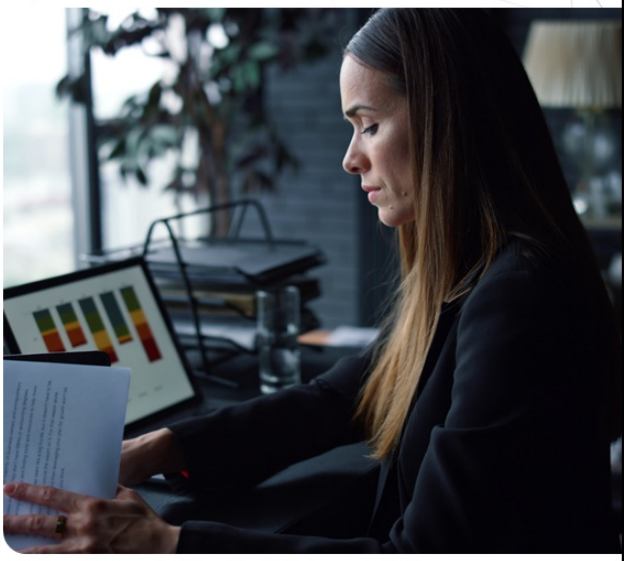
3.1.5 Select methods and determine the frequency

3.1.6 Report the results

PECB

3.1.1 Set Measurement Objectives

- The organization should evaluate its ISMS to ensure its continual suitability, adequacy, and effectiveness.
- Organizations should focus on monitoring and measuring activities linked to critical processes that facilitate the achievement of information security objectives.
- Too many measures can distort an organization's focus and blur what is truly important.



10

PECB

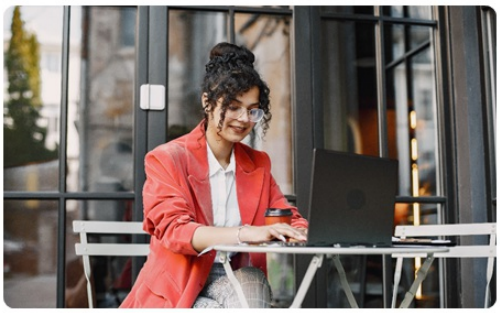
The chosen performance measures will be the means of communicating the success or failure of the ISMS. Any set of performance measures needs to be carefully selected to ensure that they are measuring the route to achieving the organization's objectives.

The objectives of measurement in the context of an ISMS include:

- Evaluating the effectiveness of the processes, procedures, and controls in place
- Verifying the extent to which ISO/IEC 27001 requirements have been met
- Facilitating performance improvement
- Providing input for management review to facilitate decision-making and justify the needed improvements of the ISMS in place

3.1.2 Decide What Needs to Be Monitored and Measured

- The extent to which the organization's information security policy is followed and objectives are met
- The organization's critical processes, procedures, and functions
- Historical evidence of poor ISMS performance (e.g., nonconformities, near misses, false alarms, failures, incidents)
- Compliance with applicable legal and regulatory requirements, industry best practices, and organization's information security policy and objectives



Data and results of monitoring and measurement sufficient to facilitate subsequent corrective action analysis

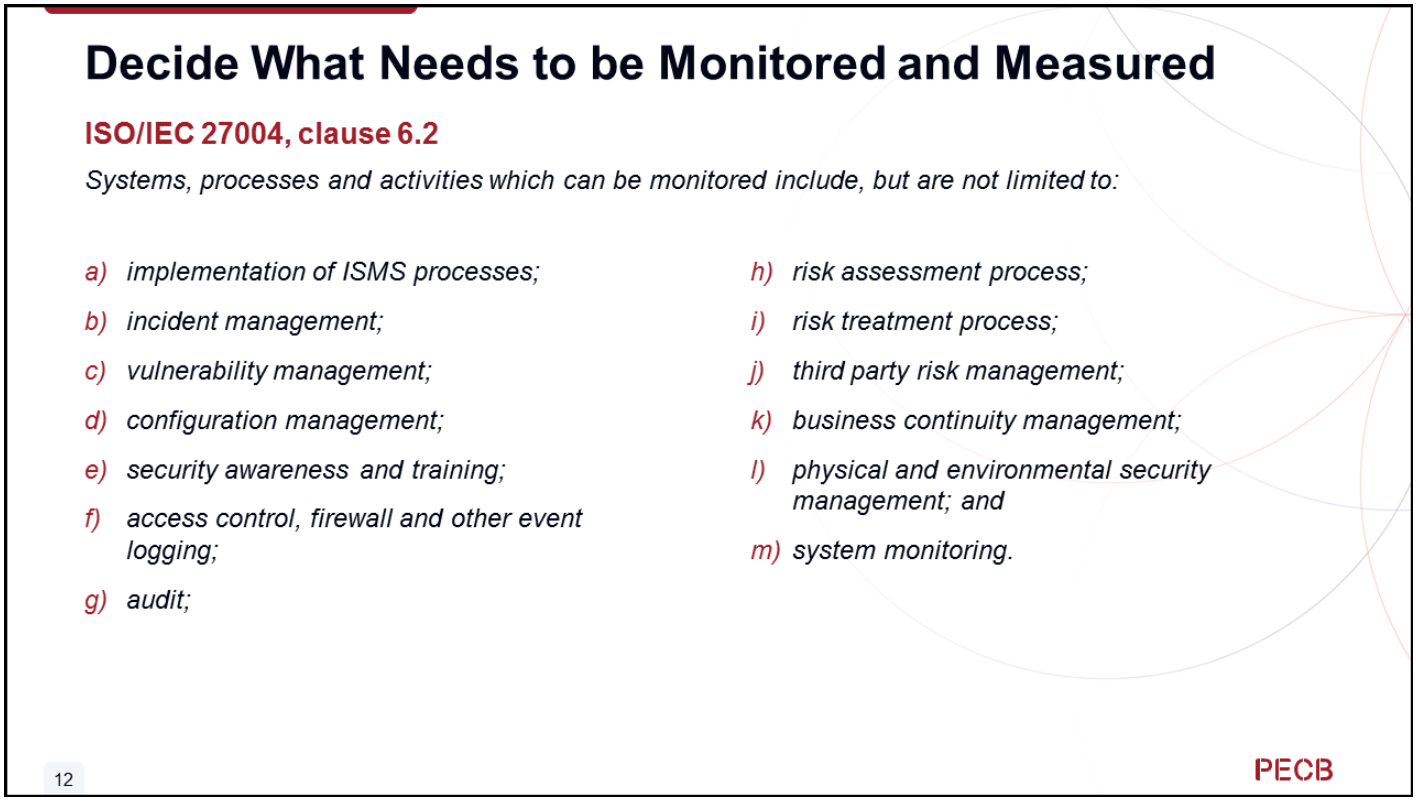
11

PECB

It is preferable to use a minimum number of effective performance measures that are related to the organization's objectives.

Each set of generic measures will only be effective for some organizations and are adequate for organizations in similar environments. The final mix of measures will be a product of operational, legislative, and cultural context.

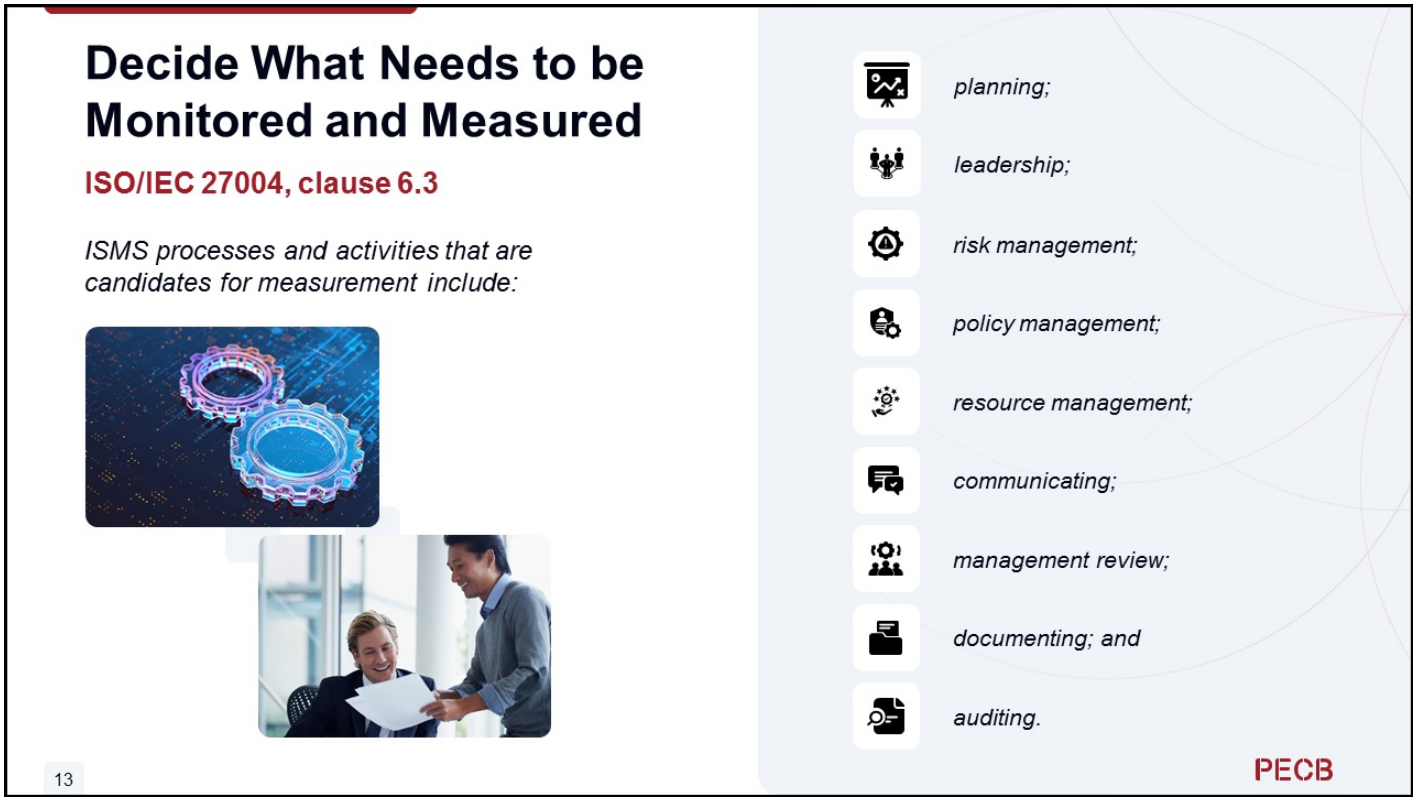
Performance measurement levels range from strategic high-level measures to more specific operational or program-level measures. The organization needs to measure only activities crucial for its operation and save time and resources on measuring activities simply because they can be measured. In terms of efficiency, the organization needs meaningful measures to indicate what is happening so that it can decide to either let an activity continue or intervene to take corrective action. In terms of effectiveness, the organization needs measures to understand if the management system is aligned with the organization's needs and objectives.



ISO/IEC 27004, clause 6.2 What to monitor (cont'd)

These monitoring activities produce data (event logs, user interviews, training statistics, incident information, etc.) that can be used to support other measures. In the process of defining attributes to be measured, additional monitoring can be required to provide supporting information.

Note that monitoring can allow an organization to determine whether a risk has materialized, and thereby indicate what action it can take to treat such a risk itself. Note also that there can be certain types of information security controls that have the explicit purpose of monitoring. When using outputs of such controls to support measurement, organizations should ensure that the measurement process takes into account whether the data used was obtained before or after any treatment action was taken.



ISO/IEC 27004, clause 6.3 What to measure (cont'd)

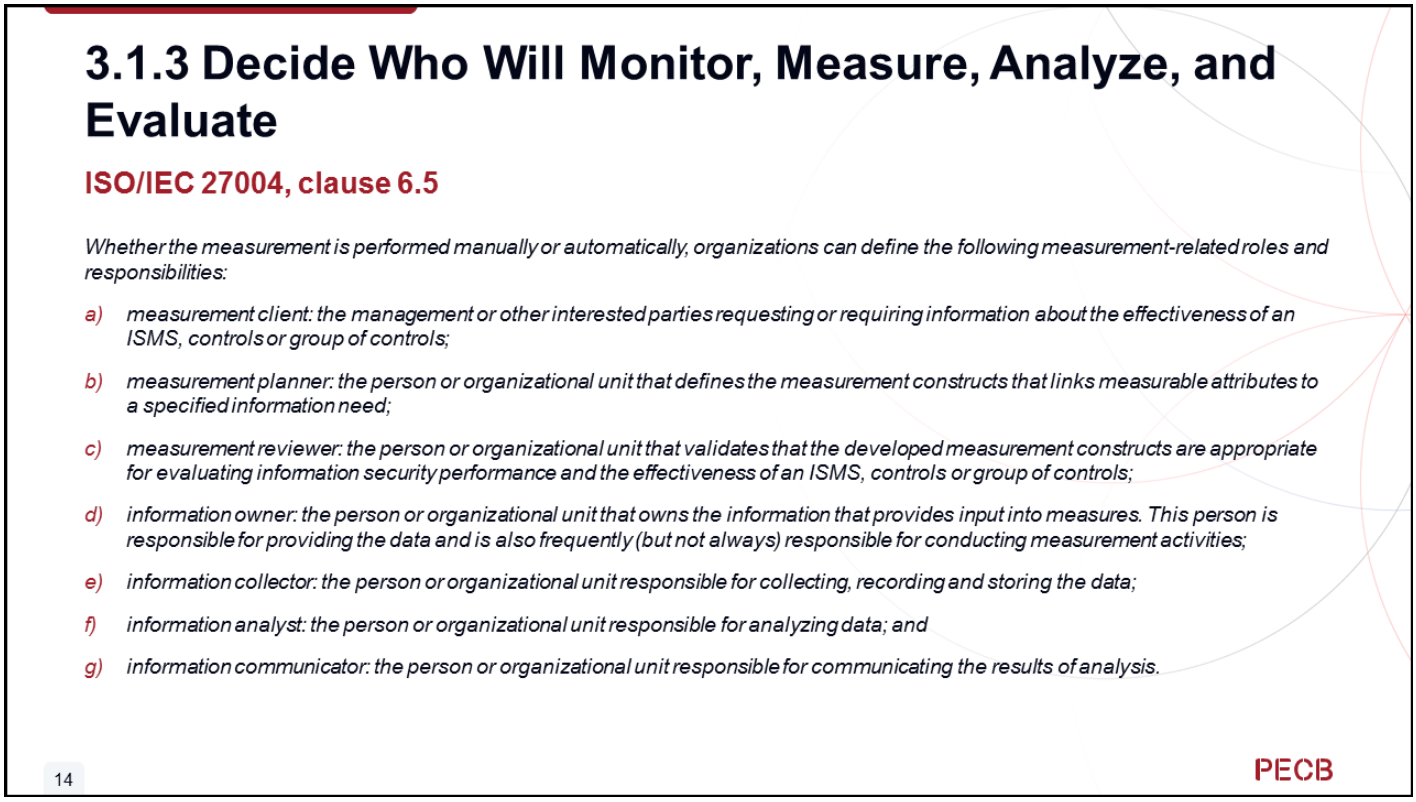
With regards to information security performance, the most obvious candidates are the organization's information security controls or groups of such controls (or even the entire risk treatment plan). These controls are determined through the process of risk treatment and are referred to in ISO/IEC 27001 as necessary controls. They can be ISO/IEC 27001:2013, Annex A controls, sector-specific controls (e.g. as defined in standards such as ISO/IEC 27010), controls specified by other standards and controls that have been designed by the organization. As the purpose of a control is to modify risk, there are a variety of attributes that can be measured, such as:

j.*the degree to which a control reduces the likelihood of the occurrence of an event;*

k.*the degree to which a control reduces the consequence of an event;*

l.*the frequency of events that a control can cope with before failure; and*

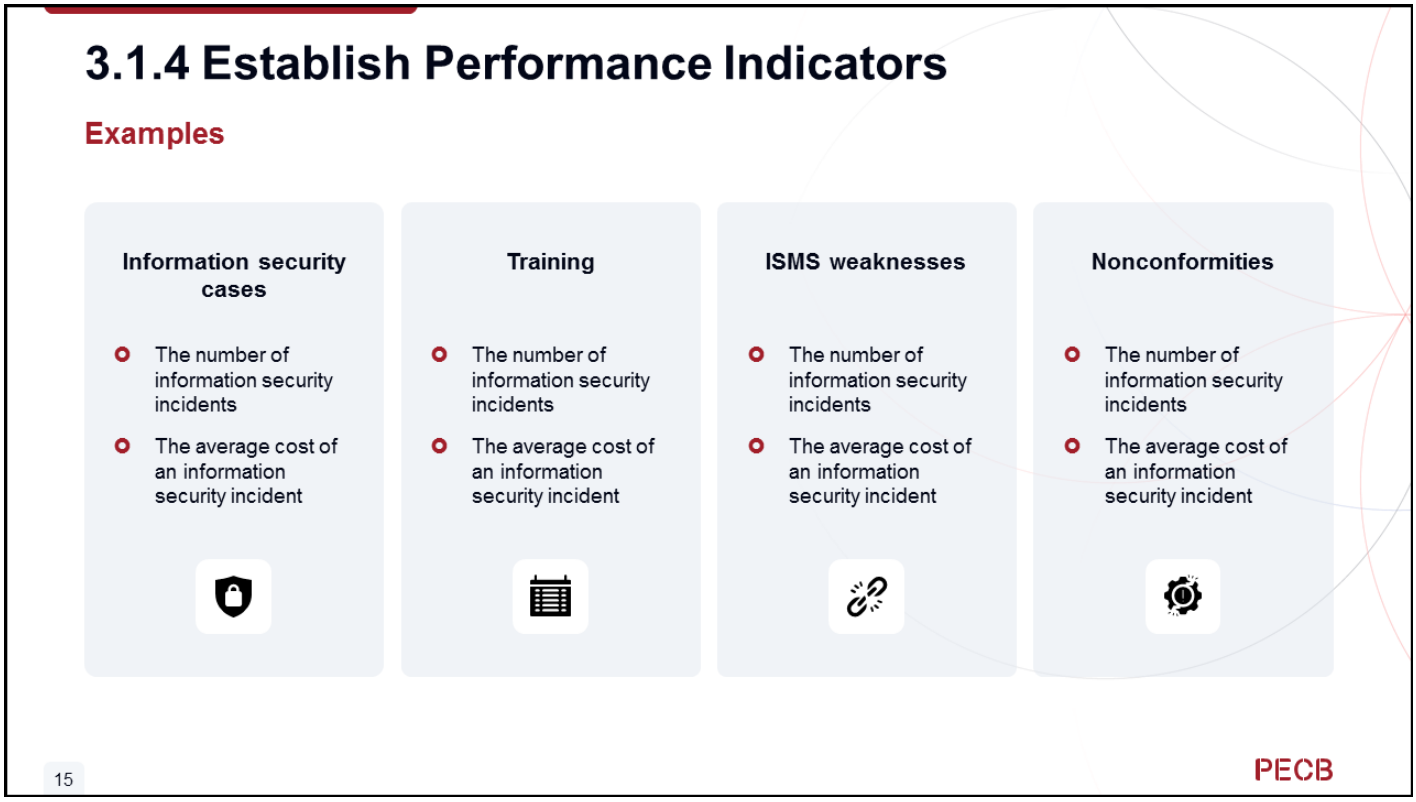
m.*how long after the occurrence of an event does it take for the control to detect that the event has occurred.*



ISO/IEC 27004, clause 6.5 Who will monitor, measure, analyze and evaluate (cont'd)

Organizations can combine some, or possibly all, of these roles.

Individuals performing different roles and responsibilities throughout the processes can require diverse skill sets and associated awareness and training.



The types and amount of performance measurements depend on the organization's requirements.

3.1.5 Select Methods and Determine the Frequency

How and when to monitor and measure?

How?

→ **Practices**

- ISO/IEC 27001 does not indicate how, nor how often, must monitoring and measurement be conducted.
- It is up to the organization to determine the methods and frequency of monitoring and measurement.
- It is best practice to use dashboards to record and report on monitoring and measurement activities with performance indicators.
- Dashboards should indicate actual performance vs. predetermined performance targets.

PECB

3.1.6 Report the Results

Examples of dashboards

Operational dashboards

Present the implemented processes and controls to the operational actors

Tactical dashboards

Measure the progress toward the achievement of tactical objectives

Strategic dashboards

Show the progress of the ISMS

17

PECB

There are many ways to report the monitoring and measurement results. The selection of the methods will depend on the target audience. The main methods include:

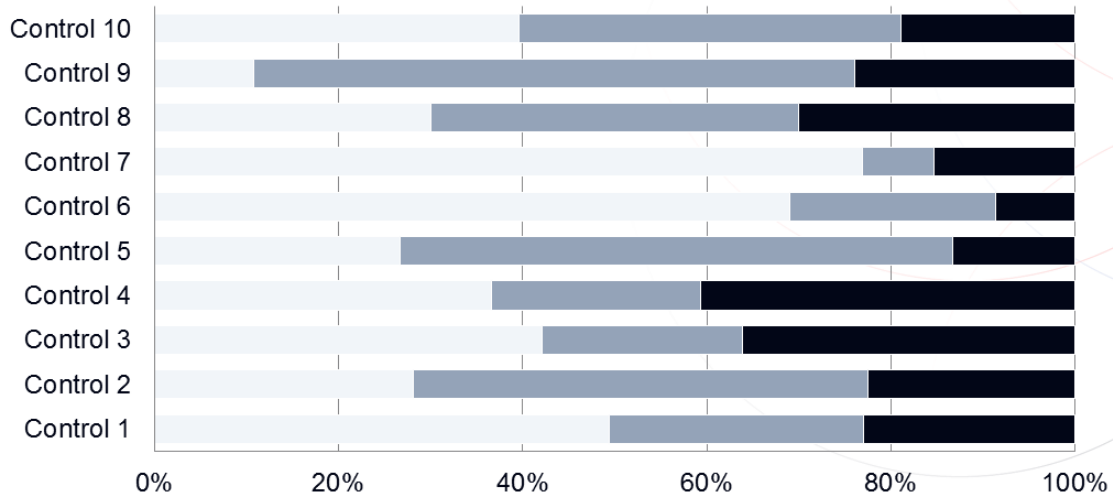
- **Tactical and operational dashboards** are less focused on strategic objectives and more tied to the effectiveness of specific controls or processes.
- **Scorecards or strategic dashboards** provide strategic information by integrating high-level indicators.
- **Reports** (from simple and static in nature, such as a list of measures for a given period, to more sophisticated cross-tab reports with nested grouping, rolling summaries, and dynamic drill-through or linking) are best used when the user needs to look at raw data in an easy-to-read format.
- **Gages** represent dynamic values including alerts, additional graphical elements, and labeling of endpoints.

Note: A dashboard is the user interface that organizes and presents information in a way that is easy to read and understand.

- The dashboard is only the presentation format.
- The indicators are the content.

I. Operational Dashboard

Example



18

PECB

Operational dashboards are used to monitor operations in real time and to notify users about deviations. Furthermore, they help in controlling operational activities and ensuring that processes stay within the targets of productivity, quality, and efficiency. They can assist in analyzing operational performance continuously so as to avoid problems and losses and, at the same time, seize opportunities, while providing data that will help improve process control and efficiency.

II. Tactical Dashboard

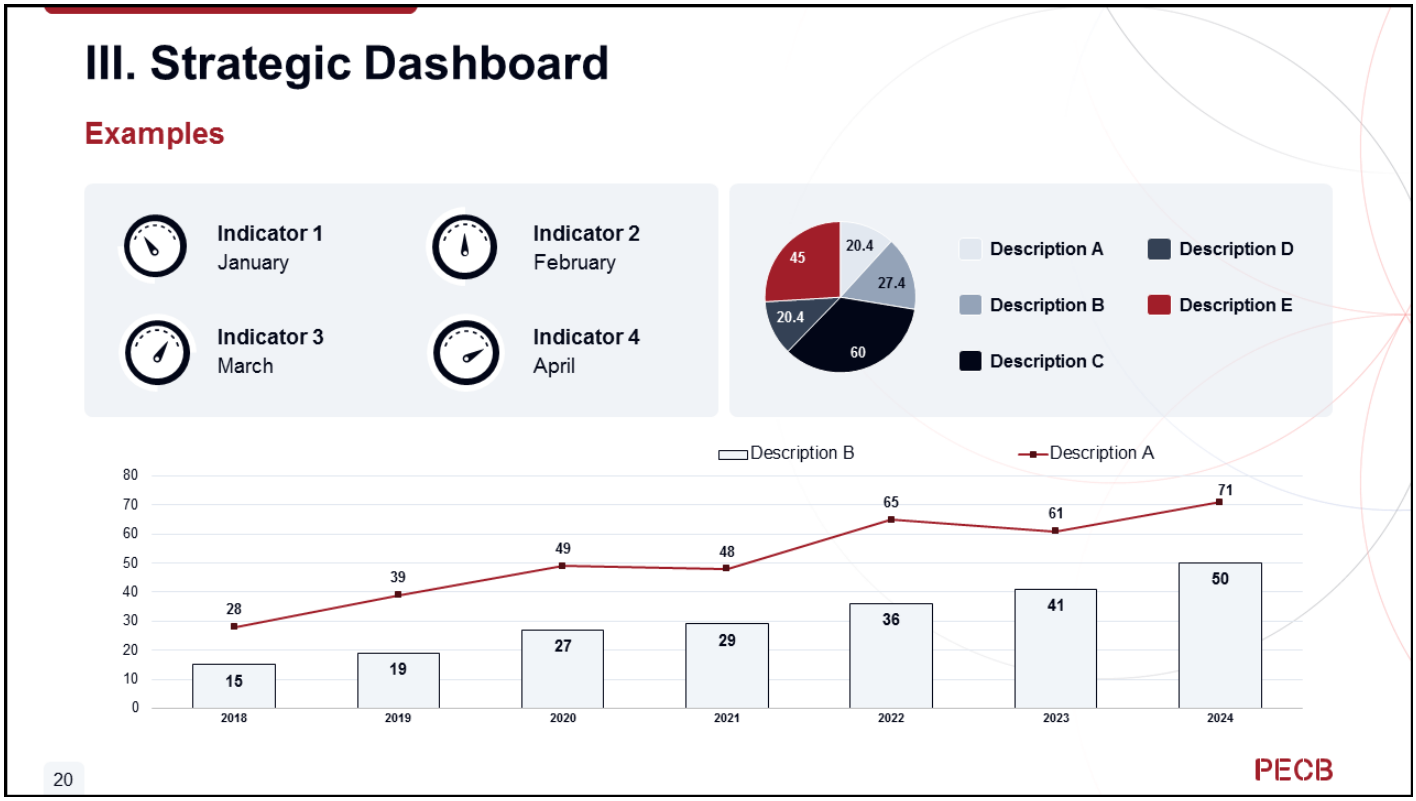
Example

Evaluation of procedures										
No.	Procedure evaluated	Notes to weaknesses and strengths	Level of compliance							
			1	2	3	4	5	6	7	8	9
1	Policy communication									X	
2	Planning of changes								X		
3	Resource allocation								X		
4	Competence, awareness, and training				X						
5	Control of documented information										X
6	Monitoring and measurement								X		
7	Corrective action					X					
8	Management review						X				
9	Internal audits								X		
10	Continual improvement									X	
	Overall assessment								X		

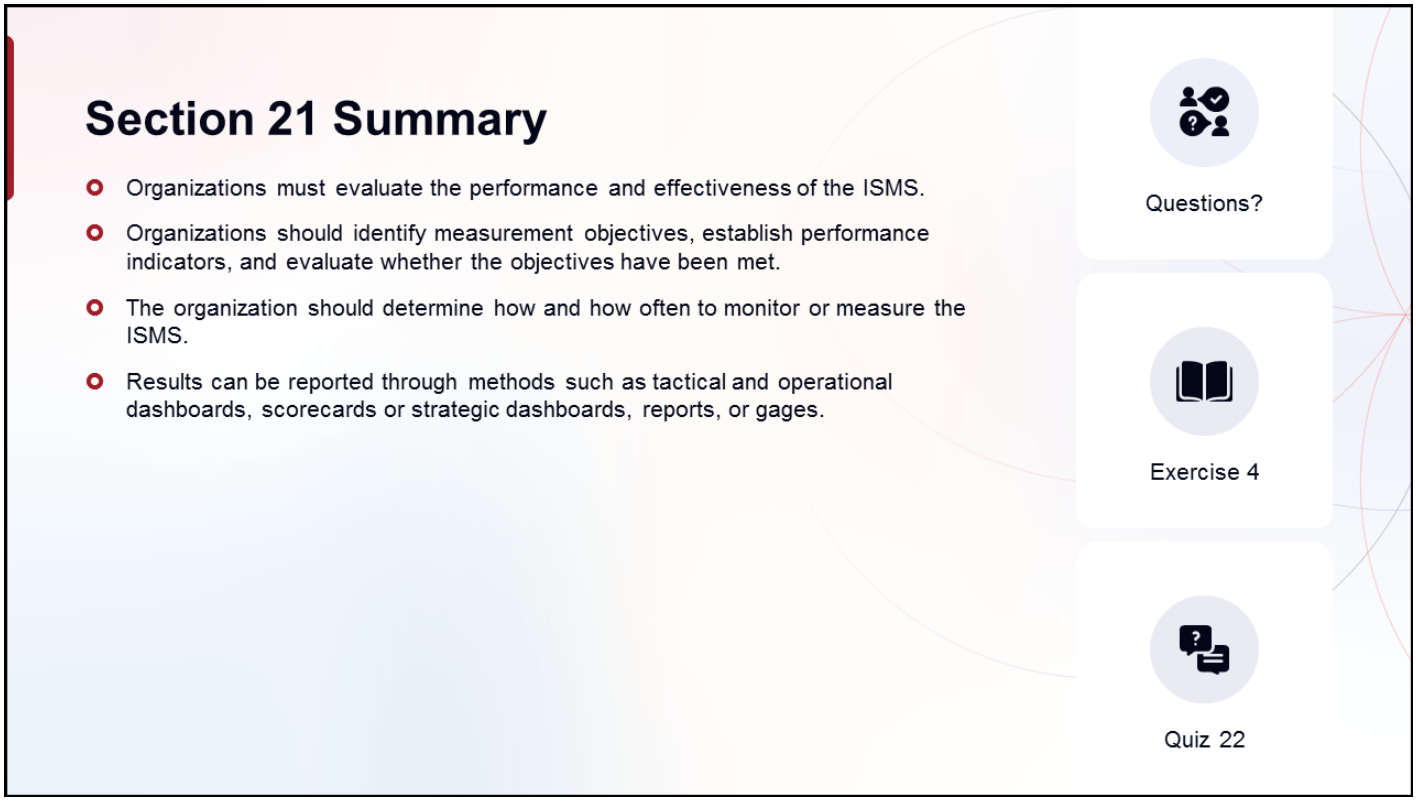
19

PECB

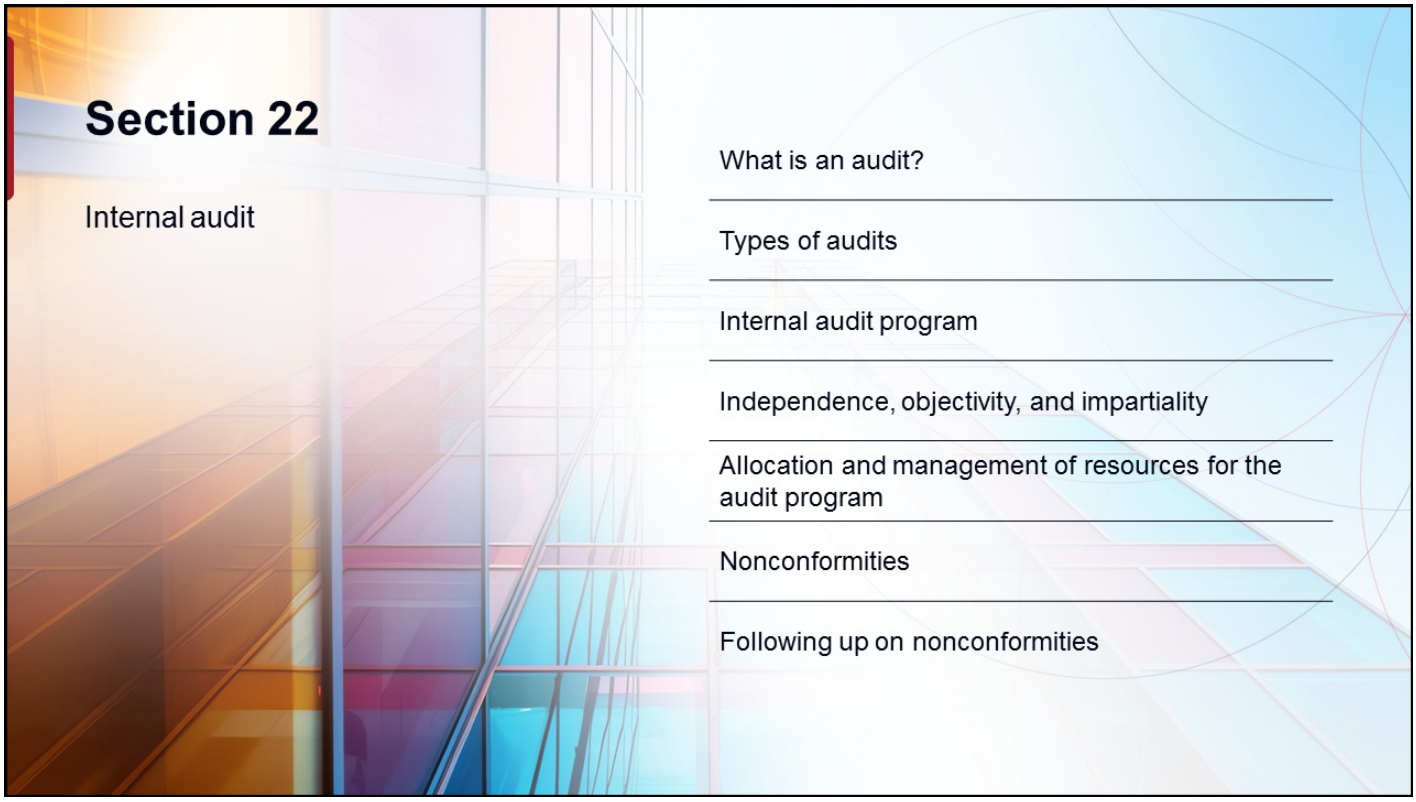
The example on the slide presents the evaluation of the conformity of the procedures related to the management system in a tactical dashboard.



Strategic dashboards are tools that support managers at any level in an organization and provide a quick overview that decision-makers need to monitor the financial health of the business. Dashboards of this type focus on high-level measures of performance and forecasts.



Note: To complete Quiz 22 and Exercise 4, please go to the Quizzes Worksheet and Exercises Worksheet respectively.



Although the information in this section is applied to internal auditing, the elements of an audit program are essentially the same for first, second, or third party audits. The tools, procedures, and techniques are essentially the same.

The activities performed in internal audits can vary depending on the program objectives, the degree of independence of auditors, the roles of auditors, and business planning. When such differences are significant, additional explanations have been provided in the notes of this section.

This section aims to provide insights into the importance of audit for organizations and the differences between internal and external audits. The section further elaborates on the planning and carrying out of audit activities, and the allocation and management of resources for the audit program. An important factor in this regard is detecting nonconformities as part of the audit and following up on them.

Internal Audit

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's Requirements for Internal Audit

ISO/IEC 27001, clauses 9.2.1

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its information security management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

✓ Regular internal audit activities allow the continual assessment of the effectiveness of the ISMS and the identification of opportunities for improvement.

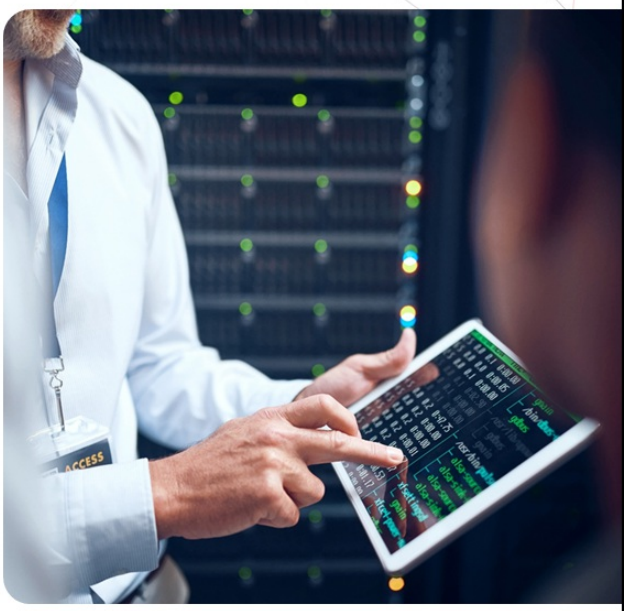
PECB

What Is an Audit?

ISO 19011, clause 3.1

Definition: *Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled*

Simply put, auditing is asking the auditee what they do and how they do it, in order to check whether their practices are in compliance with organizational policies, procedures, and processes as well as national and international standard requirements.



25

PECB

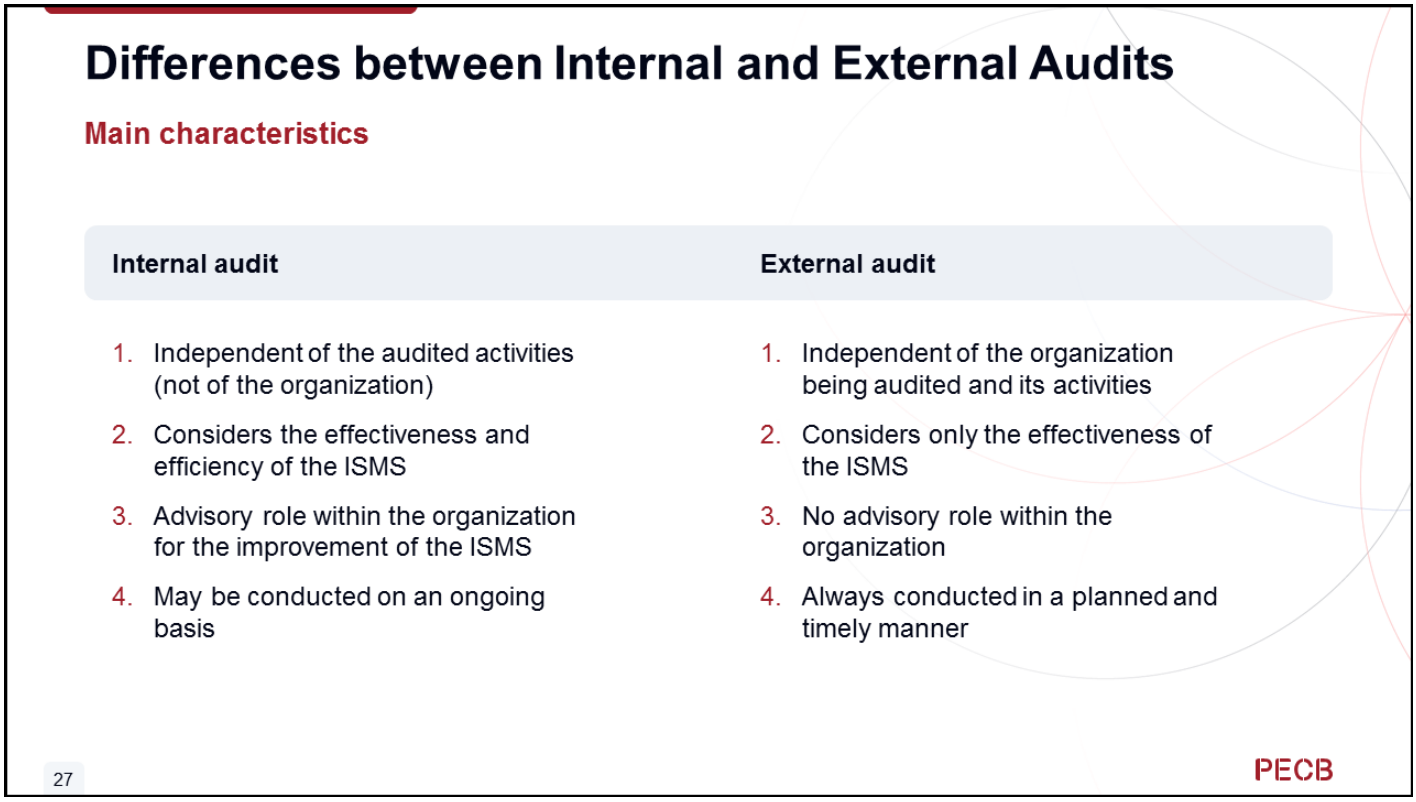
An audit is an assessment based on evidence and facts. This assessment points out the strengths and weaknesses of the management system. Audit results are communicated to the organization's top management, who then undertake the required and appropriate measures.

- A financial audit determines whether an organization's accounting practices comply with legal requirements and recognized principles.
- An administrative audit determines the effectiveness of the overall administrative practices of an organization.
- An ISMS audit determines the effectiveness of information security processes and controls in an organization.

First party audits are best known as internal audits. Internal audit is an independent and objective activity that gives an organization assurance on the level of control over operations, gives recommendations to improve operations, and contributes to creating added value. Internal audits are conducted by the organization itself for the purpose of management reviews and other internal needs.

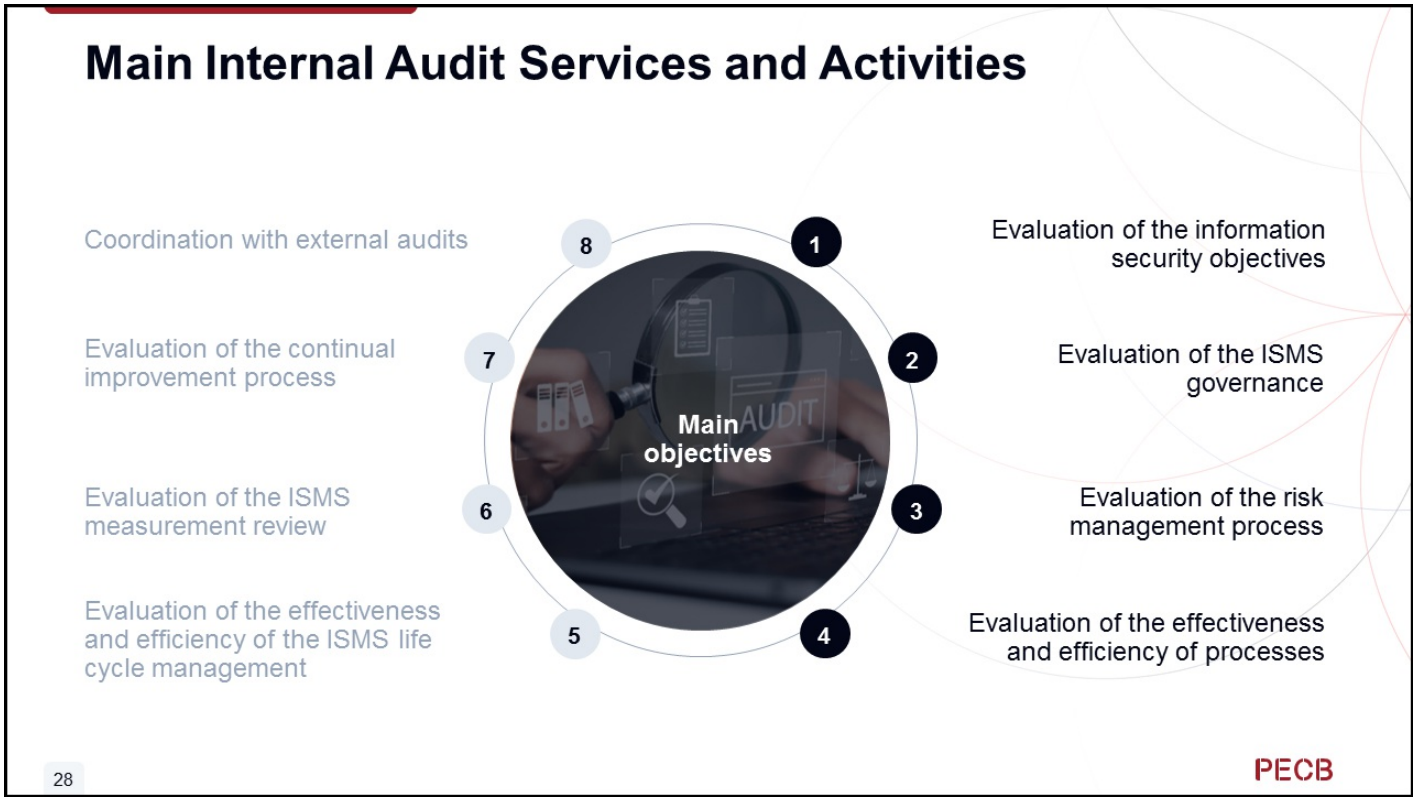
Second and third party audits are both known as external audits. The main difference between the two is in certification. On the one hand, second party audits are conducted by parties that have an interest in the organizations that is being audited (e.g., customers) and is not intended for certification purposes. On the other hand, third party audits are conducted by external and independent audit organizations (e.g., certification bodies, governmental agencies) and the aim is to obtain certification.

Note: Third party audits are performed by auditors who are external to and independent of the organization being audited.



Internal audits are independent, objective, and advisory activities performed with the aim of improving an organization's functions. In addition, internal audits contribute to the objectives of the organization by providing a systematic and structured methodology to evaluate and improve the effectiveness of the risk management process, its control, and decision-making.

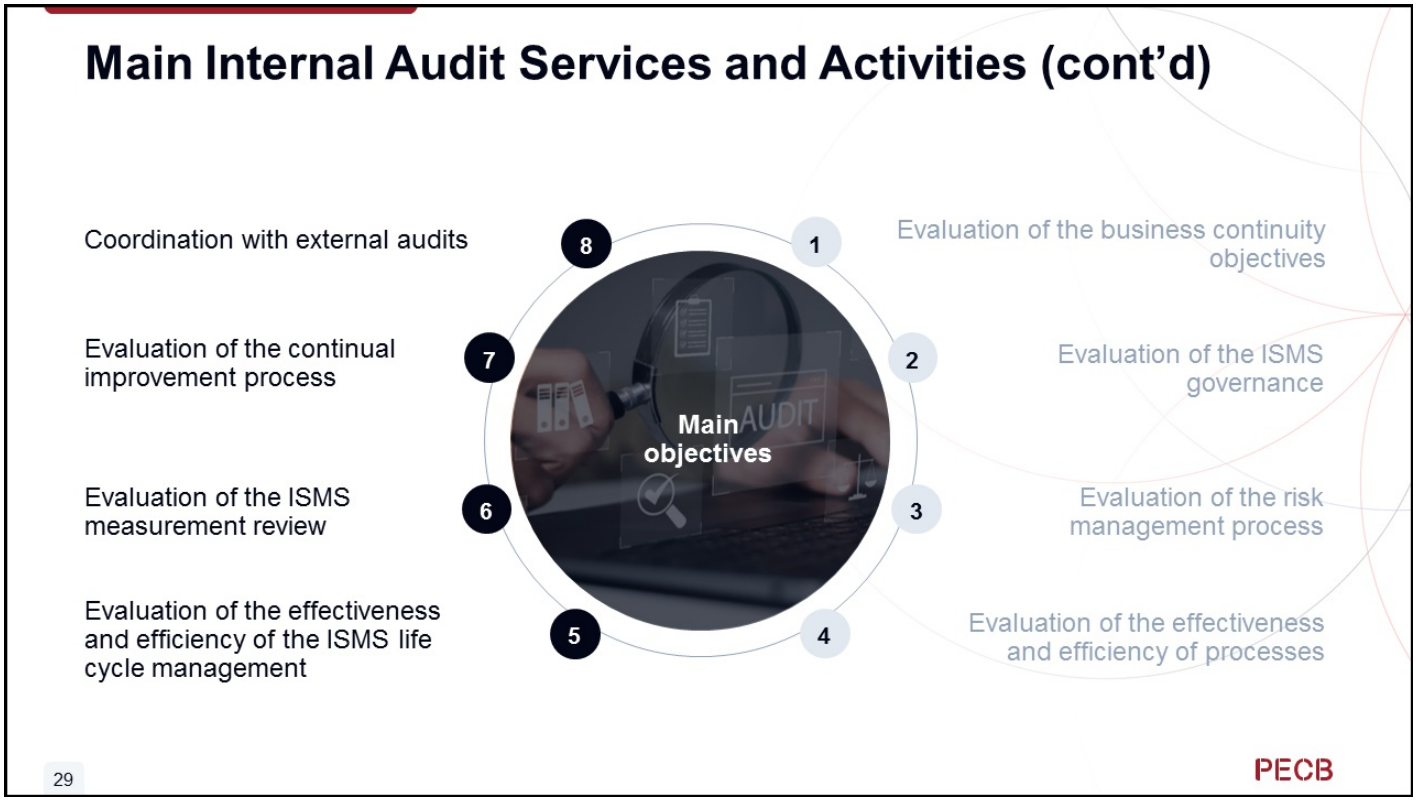
Internal audits aim to safeguard the organization's assets, promote operational efficiency, check the accuracy and reliability of information, and encourage adherence to policies and procedures.



The objectives of the internal audit should be reviewed and approved by the organization's top management. In the context of a management system certification, the objectives of the internal audit should at least cover the evaluation of activities related to the management system. However, the internal audit may cover several other audit activities such as financial, administrative, quality assurance, etc. The objectives of the internal audit are defined based on the size of the organization, its sector of activity, and its mission.

The main activities of the internal audit are:

1. **Evaluation of the information security objectives:** The internal auditor should evaluate whether the organization's information security objectives are well aligned with its business plan and strategic direction.
2. **Evaluation of the ISMS governance:** The internal auditor should validate if the organization's management supports activities related to the management system and whether the roles and responsibilities of interested parties are clearly defined.
3. **Evaluation of the risk management process:** The internal auditor should evaluate whether the organization has implemented and maintains an ongoing risk management with regard to the ISMS. Unlike an external auditor, an internal auditor may participate as an interested party in identifying and assessing the risks faced by the organization.
4. **Evaluation of the effectiveness and efficiency of processes and controls:** The internal auditor should evaluate the adequacy, effectiveness, and efficiency of information security processes and controls in operation to determine whether they are in line with the normative, legal, regulatory, and contractual requirements, as well as with the internal policies of the organization.

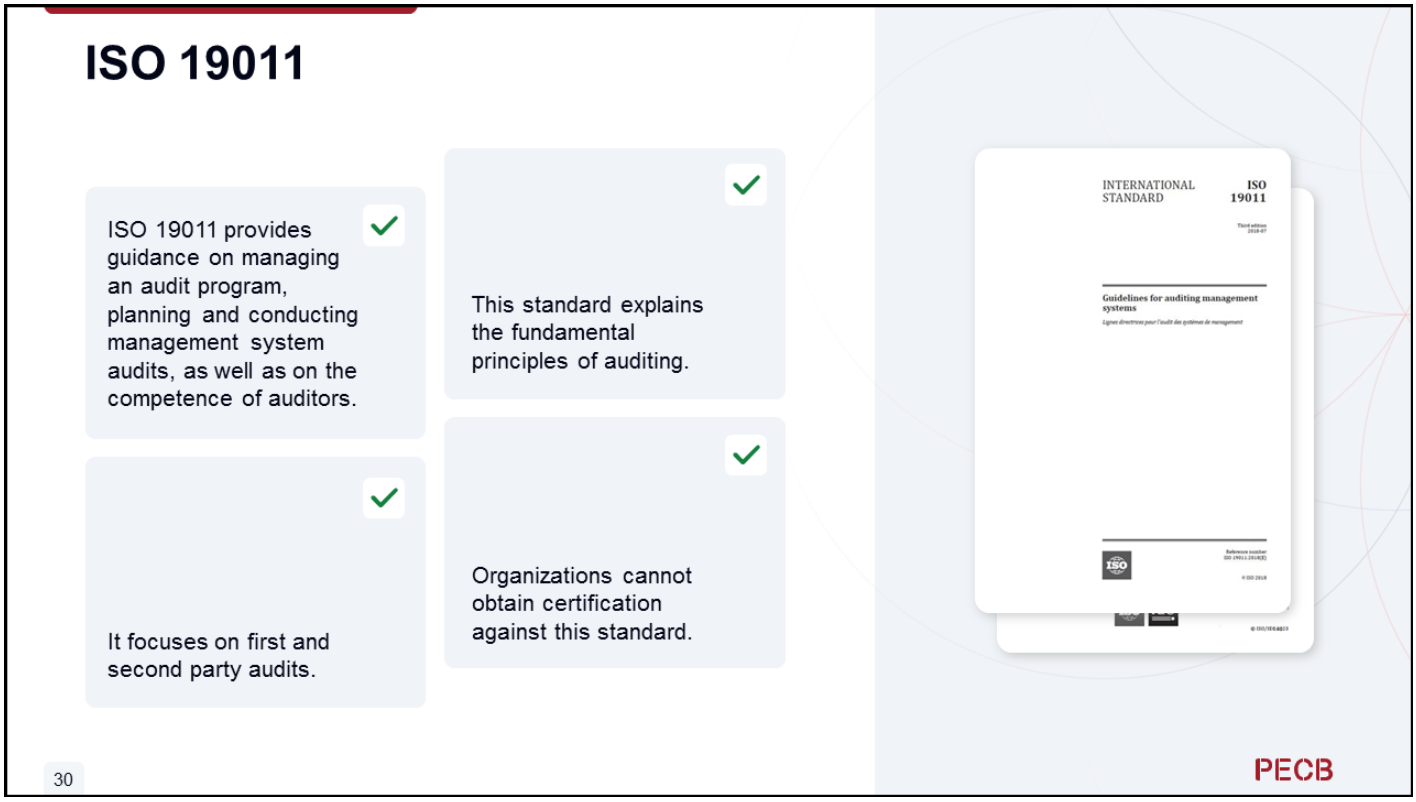


5.Evaluation of the effectiveness and efficiency of the ISMS life cycle management: The internal auditor should evaluate the effectiveness and efficiency of the life cycle management processes and safety measures related to information security matters including the planning, preparation, implementation, operation, monitoring, review, update, and improvement of the management system.

6.Evaluation of the ISMS measurement review: The internal auditor should make sure that the organization periodically conducts a measurement review of the management system to validate whether the objectives of the organization are met.

7.Evaluation of the continual improvement process: The internal auditor should make sure that the organization is implementing corrective and preventive actions to address its nonconformities and to improve the effectiveness and efficiency of the ISMS.

8.Coordination with external audits: The internal auditor should check whether the internal audit and the external audit activities are well coordinated. The aim of the internal audit is to ensure that the organization performs adequate monitoring of external audit reports and action plans that they have established and approved.



The guidelines of this standard are intended to be flexible, so they can be easily adapted to the size, nature, and complexity of the organization to be audited. The responsibility of properly applying the guidelines falls on each auditor.

ISO 19011:2018 has the following structure:

1. *Scope*
2. *Normative references*
3. *Terms and definitions*
4. *Principles of auditing*
5. *Managing an audit program*
6. *Conducting an audit*
7. *Competence and evaluation of auditors*

Annex A (informative) Additional guidance for auditors planning and conducting audits

3.2 Internal Audit

List of activities

3.2.1 Plan an internal audit program

3.2.2 Appoint a competent person

3.2.3 Ensure independence, objectivity, and impartiality

3.2.4 Plan audit activities

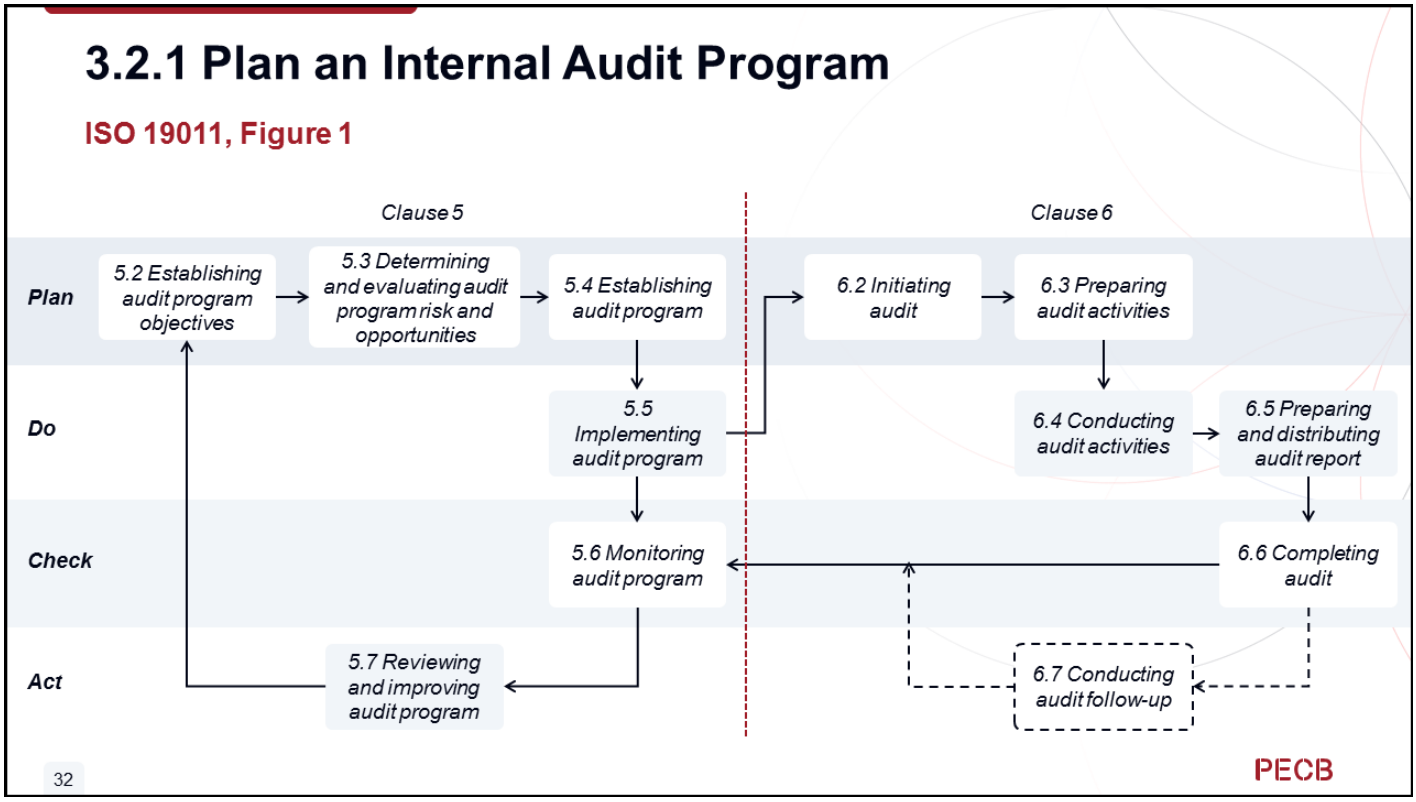
3.2.5 Allocate and manage resources

3.2.6 Perform audit activities

3.2.7 Document nonconformities

3.2.8 Follow up on nonconformities

PECB



ISO 19011, clause 3.4 Audit program

Arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose

The audit program should follow the steps of the PDCA (Plan-Do-Check-Act) model. The audit program can include more than one audit depending on the size and complexity of the organization. Joint or combined audits can be conducted as well.

Establishing an Internal Audit Program

ISO/IEC 27001, clause 9.2.2

The organization shall plan, establish, implement and maintain an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit program(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit program(s) and the audit results.

33

PECB

ISO/IEC 27003, clause 9.2 Internal audit

Auditors also evaluate whether the ISMS is effectively implemented and maintained. An audit program describes the overall framework for a set of audits, planned for specific time frames and directed towards specific purposes. This is different from an audit plan, which describes the activities and arrangements for a specific audit. Audit criteria are a set of policies, procedures or requirements used as a reference against which audit evidence is compared, i.e. the audit criteria describe what the auditor expects to be in place.

If the outcome of the audit includes nonconformities, the auditee should prepare an action plan for each nonconformity to be agreed with the audit team leader. A follow-up action plan typically includes:

i.*description of the detected nonconformity;*

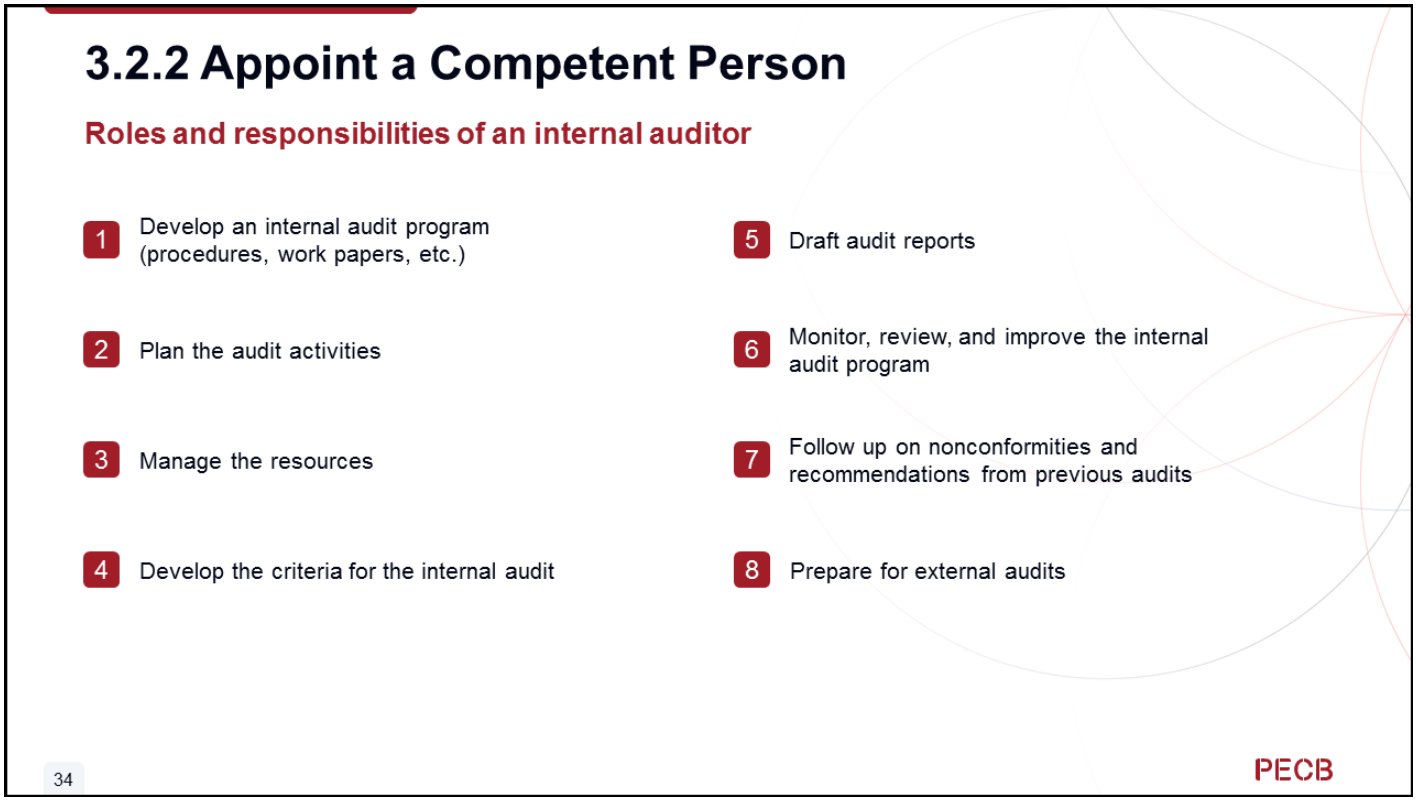
j.*description of the cause(s) of nonconformity;*

k.*description of short term correction and longer term corrective action to eliminate a detected nonconformity within a defined timeframe; and*

l.*the persons responsible for implementing the plan.*

Audit reports, with audit results, should be distributed to top management.

Results of the previous audits should be reviewed and the audit program adjusted to better manage areas experiencing higher risks due to nonconformity.



ISO 19011, clause 5.4.1 Roles and responsibilities of the individual(s) managing the audit program

The individual(s) managing the audit program should:

a. *establish the extent of the audit program according to the relevant objectives and any known constraints;*
b. *determine the external and internal issues, and risks and opportunities that can affect the audit program, and implement actions to address them, integrating these actions in all relevant auditing activities, as appropriate;*
c. *ensuring the selection of audit teams and the overall competence for the auditing activities by assigning roles, responsibilities and authorities, and supporting leadership, as appropriate;*
d. *establish all relevant processes including processes for:*
    - *the coordination and scheduling of all audits within the audit program;*
    - *the establishment of audit objectives, scope(s) and criteria of the audits, determining audit methods and selecting the audit team;*
    - *evaluating auditors;*
    - *the establishment of external and internal communication processes, as appropriate;*
    - *the resolutions of disputes and handling of complaints;*
    - *audit follow-up if applicable;*
    - *reporting to the audit client and relevant interested parties, as appropriate.*
e. *determine and ensure provision of all necessary resources;*
f. *ensure that appropriate documented information is prepared and maintained, including audit program records;*
g. *monitor, review and improve the audit program;*
h. *communicate the audit program to the audit client and, as appropriate, relevant interested parties.*

The individual(s) managing the audit program should request its approval by the audit client.

ISO 19011, clause 7.2.3.2 Generic knowledge and skills of management system auditors (cont'd)

a.*Audit principles, processes and methods: knowledge and skills in this area enable the auditor to ensure audits are performed in a consistent and systematic manner.*

An auditor should be able to:

- *understand the types of risks and opportunities associated with auditing and the principles of the risk-based approach to auditing;*
- *plan and organize the work effectively;*
- *perform the audit within the agreed time schedule;*
- *prioritize and focus on matters of significance;*
- *communicate effectively, orally and in writing (either personally, or through the use of interpreters);*
- *collect information through effective interviewing, listening, observing and reviewing documented information, including records and data;*
- *understand the appropriateness and consequences of using sampling techniques for auditing;*
- *understand and consider technical experts' opinions;*
- *audit a process from start to finish, including the interrelations with other processes and different functions, where appropriate;*
- *verify the relevance and accuracy of collected information;*
- *confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;*
- *assess those factors that may affect the reliability of the audit findings and conclusions;*
- *document audit activities and audit findings, and prepare reports;*
- *maintain the confidentiality and security of information.*

Slide Notes Extension

ISO 19011, clause 7.2.3.2 Generic knowledge and skills of management system auditors (cont'd)

b.*Management system standards and other references: knowledge and skills in this area enable the auditor to understand the audit scope and apply audit criteria, and should cover the following:*

- *management system standards or other normative or guidance/supporting documents used to establish audit criteria or methods;*
- *the application of management system standards by the auditee and other organizations;*
- *relationships and interactions between the management system(s) processes;*
- *understanding the importance and priority of multiple standards or references;*
- *application of standards or references to different audit situations.*

c.*The organization and its context: knowledge and skills in this area enable the auditor to understand the auditee's structure, purpose and management practices and should cover the following:*

- *needs and expectations of relevant interested parties that impact the management system;*
- *type of organization, governance, size, structure, functions and relationships;*
- *general business and management concepts, processes and related terminology, including planning, budgeting and management of individuals;*
- *cultural and social aspects of the auditee.*

d.*Applicable statutory and regulatory requirements and other requirements: knowledge and skills in this area enable the auditor to be aware of, and work within, the organization's requirements. Knowledge and skills specific to the jurisdiction or to the auditee's activities, processes, products and services should cover the following:*

- *statutory and regulatory requirements and their governing agencies;*
- *basic legal terminology;*
- *contracting and liability.*

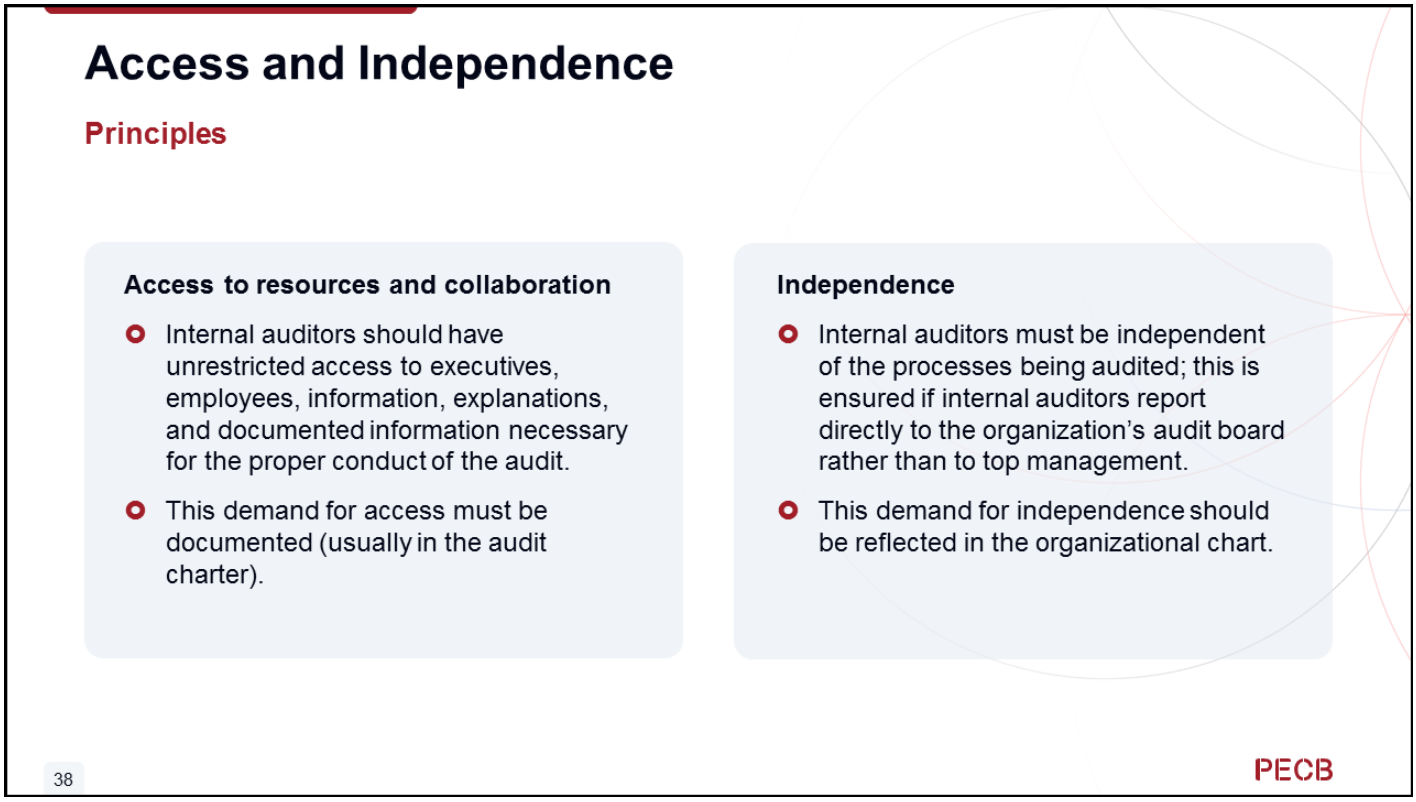
NOTE: Awareness of statutory and regulatory requirements does not imply legal expertise and a management system audit should not be treated as a legal compliance audit.

While internal auditors are not independent of the organizations that employ them, independence, objectivity, and impartiality are the cornerstone of the internal audit profession. This independence enables unrestricted evaluation of management activities and personnel and allows internal auditors to perform their role successfully.

To ensure the objectivity and impartiality of the internal audit function, auditors should not undertake operational roles related to the management system. If a person has assumed such a role, a reasonable period of time (usually one year) should pass before the person can occupy the position of the internal auditor. A person may undertake operational roles and conduct an audit only if the two spheres of activities involved are not related. In this case, there have to be well-documented job descriptions to avoid potential conflicts of interest and violations of the principle of independence.

The internal audit charter is a way of describing how the organization will benefit from the internal audit especially in achieving its objectives. The top management should approve the internal audit charter.

Important note: Smaller organization may find it better to outsource the internal audit function to a third party. It is indeed easier to demonstrate the independence and impartiality of a person who has no connection with the implementation and operations of the ISMS.



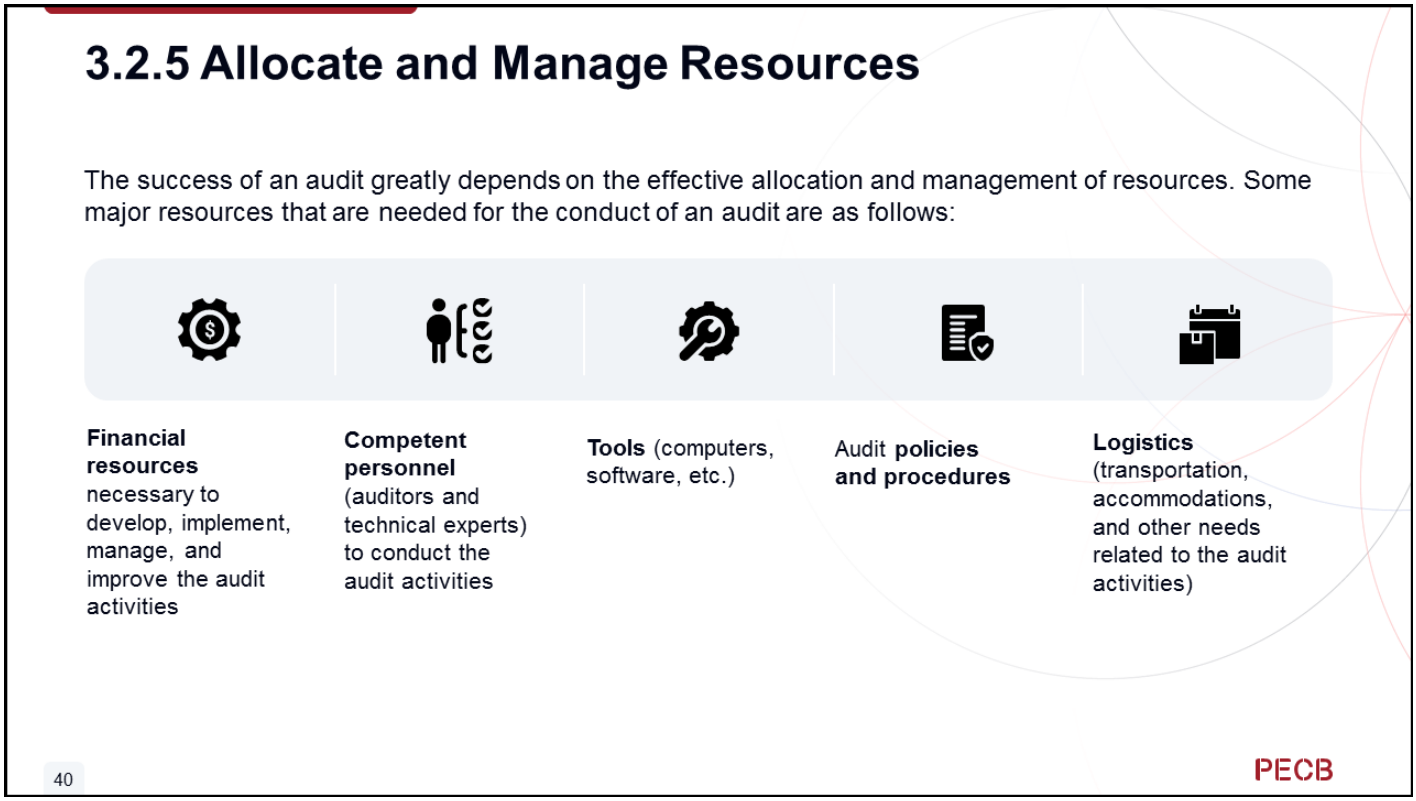
In order to ensure that the mission of the internal auditor is successfully completed, the organization must demonstrate their availability and collaboration.

3.2.4 Plan Audit Activities

The main activities that an internal auditor must plan beforehand include:

- Reviewing the application of internal policies and procedures
- Reviewing the effectiveness and efficiency of operations
- Reviewing the use of resources in the organization
- Evaluating the degree of conformity to laws, regulations, and standard requirements
- Reviewing the information security risk assessment process
- Reviewing the organization's documented information to verify the allocation of the roles and responsibilities for information security

PECB



ISO 19011, clause 5.4.4 Determining audit program resources

When determining resources for the audit program, the individual(s) managing the audit program should consider:

a. *the financial and time resources necessary to develop, implement, manage and improve audit activities;*
b. *audit methods;*
c. *the individual and overall availability of auditors and technical experts having competence appropriate to the particular audit program objectives;*
d. *the extent of the audit program and audit program risks and opportunities;*
e. *travel time and cost, accommodation and other auditing needs;*
f. *the impact of different time zones;*
g. *the availability of information and communication technologies (e.g. technical resources required to set up a remote audit using technologies that support remote collaboration);*
h. *the availability of any tools, technology and equipment required;*
i. *the availability of necessary documented information, as determined during the establishment of the audit program;*
j. *requirements related to the facility, including any security clearances and equipment (e.g. background checks, personal protective equipment, ability to wear clean room attire).*

ISO 19011, clause 3.9 Audit evidence

Records, statements of fact or other information, which are relevant to the audit criteria and verifiable

ISO 19011, clause 3.10 Audit findings

Results of the evaluation of the collected audit evidence against audit criteria

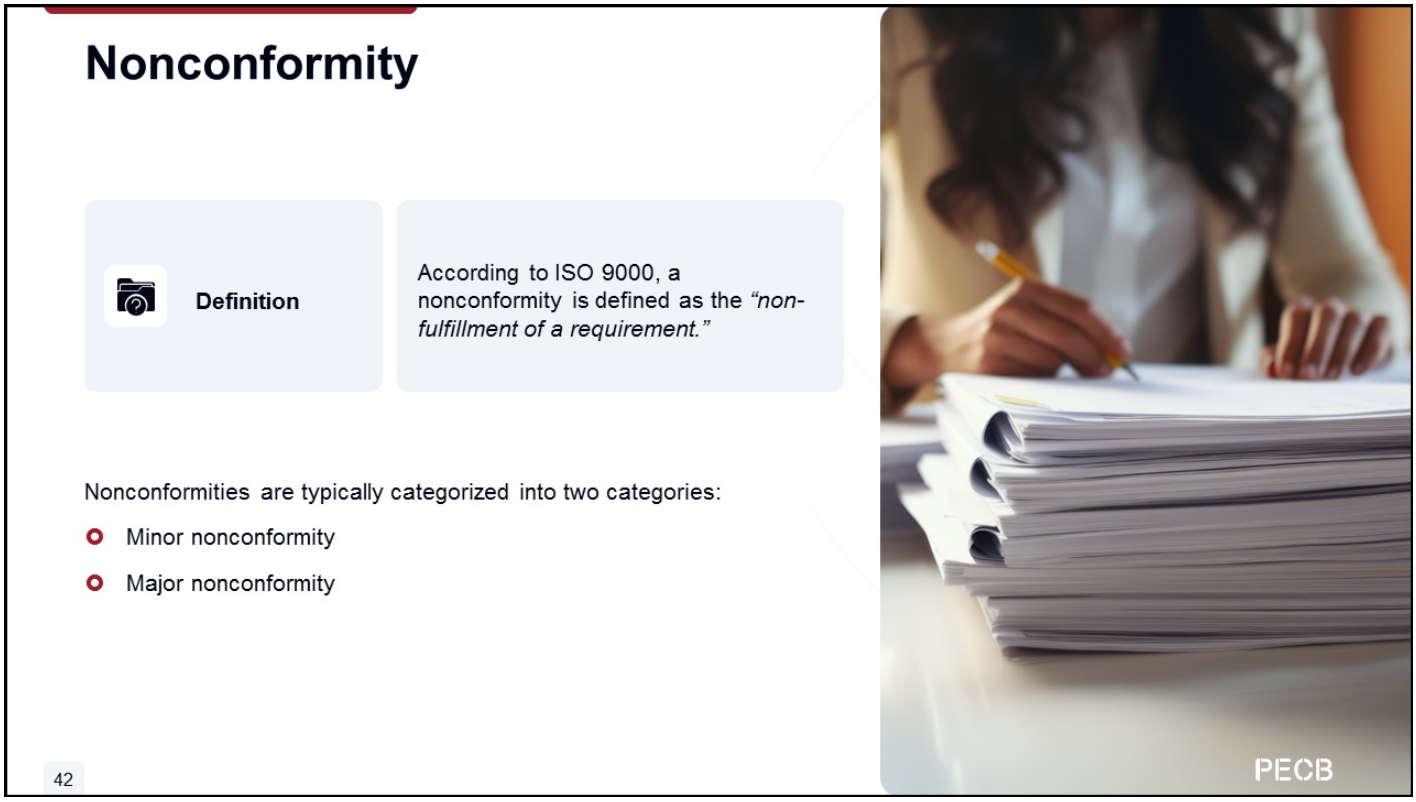
- *Note 1 to entry: Audit findings indicate conformity or nonconformity.*
- *Note 2 to entry: Audit findings can lead to the identification of risks, opportunities for improvement or recording good practices.*
- *Note 3 to entry: In English if the audit criteria are selected from statutory requirements or regulatory requirements, the audit finding is termed compliance or non-compliance.*

ISO 19011, clause 3.11 Audit conclusion

Outcome of an audit, after consideration of the audit objectives and all audit findings

To ensure the relevance of an audit procedure, the auditor must collect evidence from different sources of information and evaluate them objectively. The evidence-collection process can be carried out by using different audit procedures and methods, including sampling, when and if required.

After evaluating the audit evidence against the audit criteria, the auditor drafts the audit findings. Finally, following the analysis of all the audit findings and reviewing them, the auditor issues the audit conclusion(s).



Requirements can derive from several sources: national or international standards, internal rules and policies of the organization, laws and regulations of the country in which the organization operates, contracts signed with clients or partners.

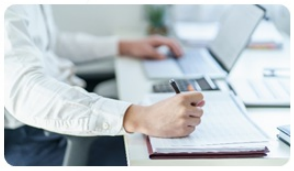
ISO 9000, clause 3.6.11 Conformity

Fulfillment of a requirement

Common examples of nonconformities include:

- The documentation is not complete.
- The control is not implemented or is ineffective.

3.2.7 Document Nonconformities



If an audit finding indicates a nonconformity, the auditor must document it in the nonconformity report.

An adequate documentation of a nonconformity includes three items:

→

01 Description of the requirements for which the nonconformity was detected (audit criteria)

02 Description of the observed nonconformity (including evidence supporting the findings)

03 Type of nonconformity (minor or major)

43

PECB

Once a nonconformity has been identified, the auditor must document it. The recording of the nonconformity can be as simple as a description of the observation and the reference to the audit criteria.

A nonconformity report should be explicit, unambiguous, linguistically correct, and as concise as possible.

Nonconformity Report

Example

NONCONFORMITY REPORT

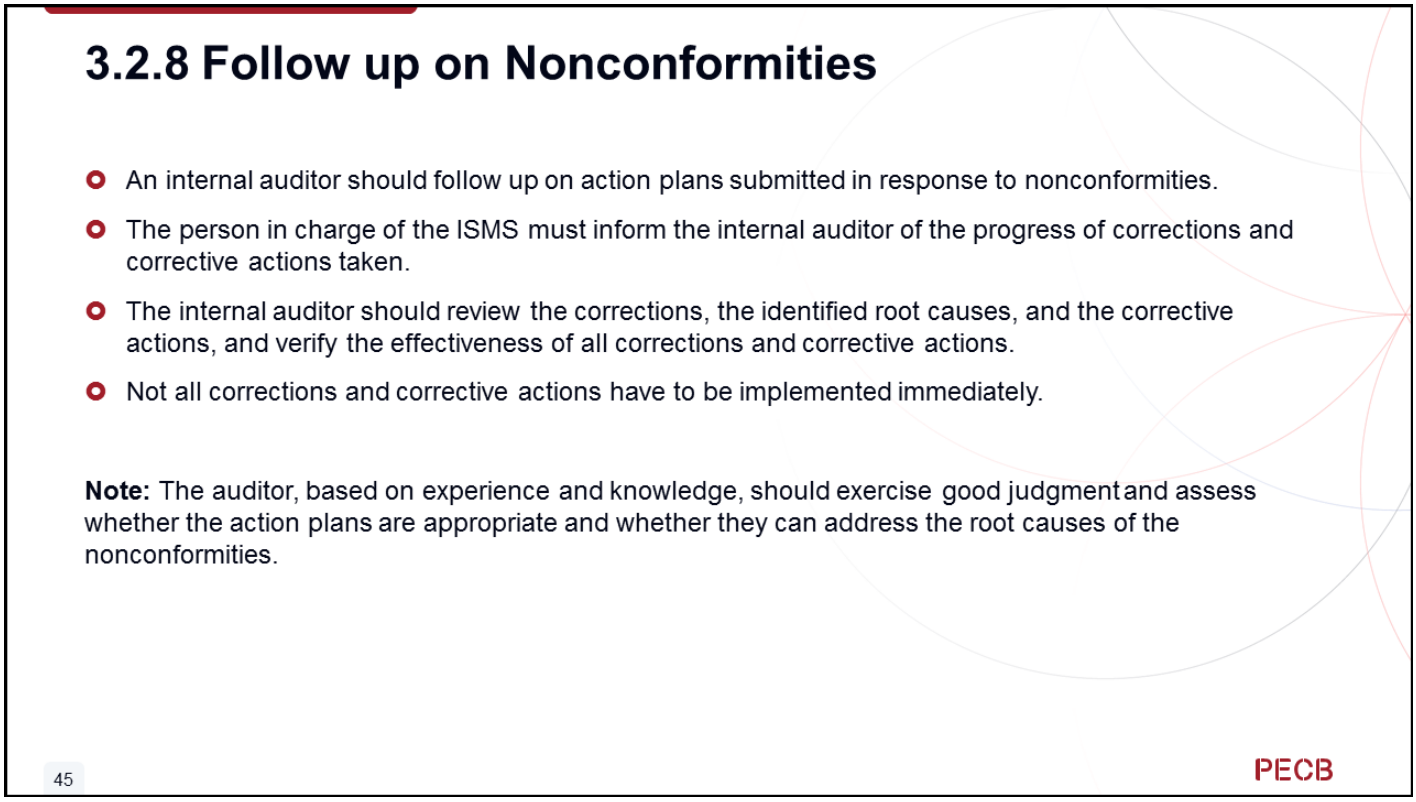
Nonconformity number: 3	**Client:** Thalia Technologies	**File number:** 34527
Process: Assets management	**Clause/control number:** 5.3	**Site:** Montreal

Audit criteria: *Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.*

Description of the observed nonconformity: In a sample of 30 interviewed employees, it was found that only 5 of them are aware of their responsibilities regarding information security.

Auditor: J. Rogers	**Acknowledgment by auditee representative:** Nonconformity presented to Mr. R. Smith and confirmed on March 21, 2022	Nonconformity
		Major
Date: March 20, 2020		Minor

PECB



The auditor must always remember that it is highly unlikely for an organization to correct all nonconformities simultaneously. Every correction or corrective action requires the use of resources and time for implementation. Action plans can be arranged in order of priority by the management, especially for those that require investment. Therefore, the auditor must ensure that the objectives regarding the correction of nonconformities are realistic.

The auditor should request or receive a periodic update from the organization to assess the progress that has been made regarding the correction of nonconformities. The monitoring of action plans is particularly important with respect to the high risk problems and corrective actions with long lead times.

Section 22 Summary

- Internal audits help organizations determine if their ISMS is effective efficient, and if it fulfills the requirements of ISO/IEC 27001.
- Internal audit results are used as input for continual improvement.
- The internal auditor is responsible for developing an internal audit program, planning the audit activities, drafting audit reports, managing the resources, establishing the criteria for the internal audit, monitoring, reviewing, and improving the internal audit program, following up on nonconformities, and preparing the organization for external audits.
- Major resources needed to conduct an internal audit include: financial resources, competent personnel, tools, audit policies and procedures, and logistics.
- The auditor should follow up on nonconformities by reviewing the corrections and corrective actions, and by verifying their effectiveness.

Questions?

Quiz 23

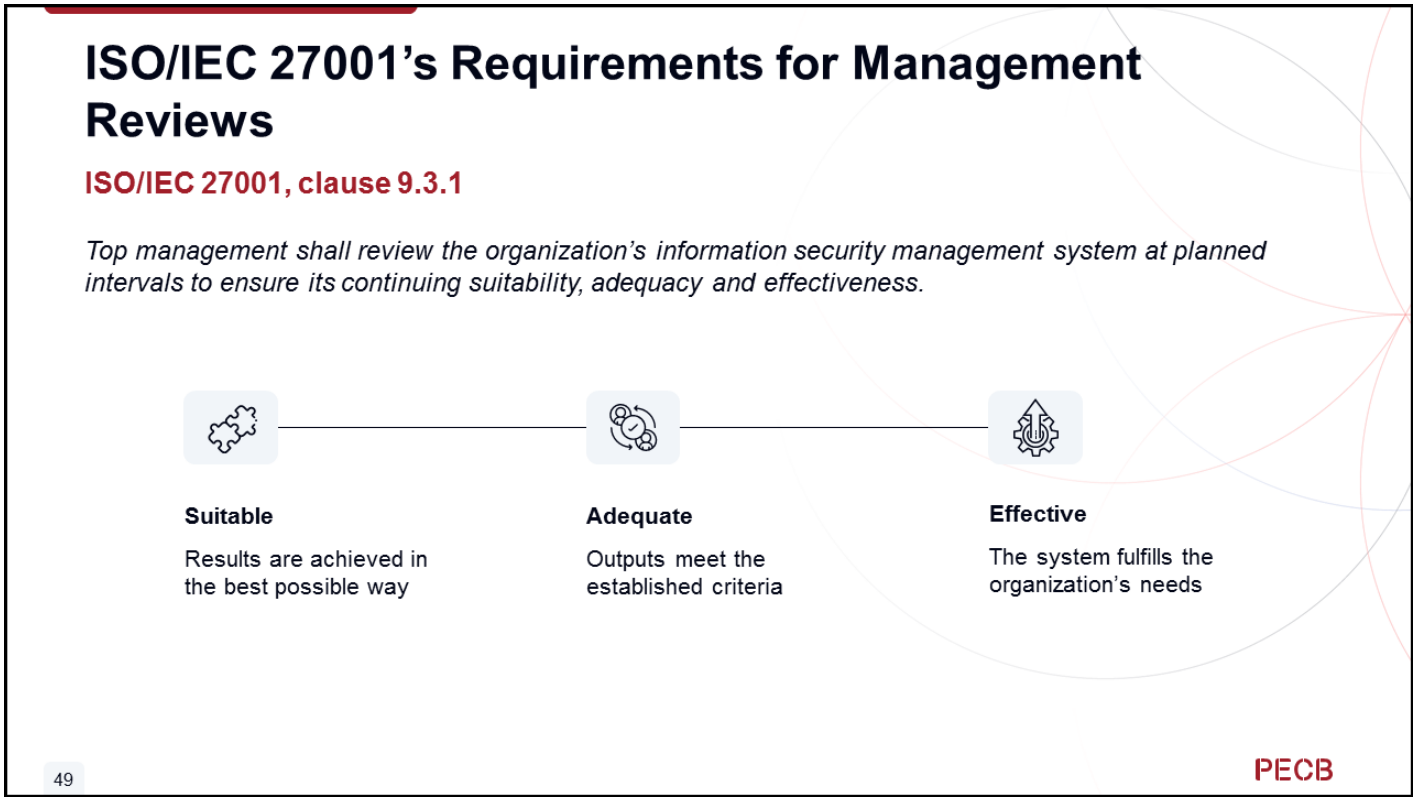
Note: To complete Quiz 23, please go to the Quizzes Worksheet.

This section will help the participant gain knowledge on preparing and conducting a management review. In addition, the participant will be able to understand the process of closing the review and the follow-up activities of the management review.

Management Review

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 9.3 Management review

The purpose of management review is to ensure the continuing suitability, adequacy and effectiveness of the ISMS. Suitability refers to continuing alignment with the organization's objectives. Adequacy and effectiveness refer to a suitable design and organizational embedding of the ISMS, as well as the effective implementation of processes and controls that are driven by the ISMS.

Overall, management review is a process carried out at various levels in the organization. These activities could vary from daily, weekly, or monthly organizational unit meetings to simple discussions of reports. Top management is ultimately responsible for management review, with inputs from all levels in the organization.

3.3 Management Review

List of activities

PECB

3.3.1 Prepare for the Management Review

Management reviews must be conducted at planned intervals (e.g., monthly, quarterly semi-annually, or annually). Although ISO/IEC 27001 does not provide specific requirements regarding the frequency of management review meetings, it is common practice to conduct management review each quarter.

Management reviews can be included in a regular management meeting and discussed as a topic on the agenda.

It is good practice to send all related documentation to the attendees (e.g., audit report, results of reviews, action plans) before the management review meeting.

3.3.2 Conduct the Management Review

ISO/IEC 27001, clause 9.3.2

The management review shall include consideration of:

a) *the status of actions from previous management reviews;*

b) *changes in external and internal issues that are relevant to the information security management system;*

c) *changes in needs and expectations of interested parties that are relevant to the information security management system;*

d) *feedback on the information security performance, including trends in:*
   1) *nonconformities and corrective actions;*
   2) *monitoring and measurement results;*
   3) *audit results;*
   4) *fulfilment of information security objectives;*

e) *feedback from interested parties;*

f) *results of risk assessment and status of risk treatment plan;*

g) *opportunities for continual improvement.*

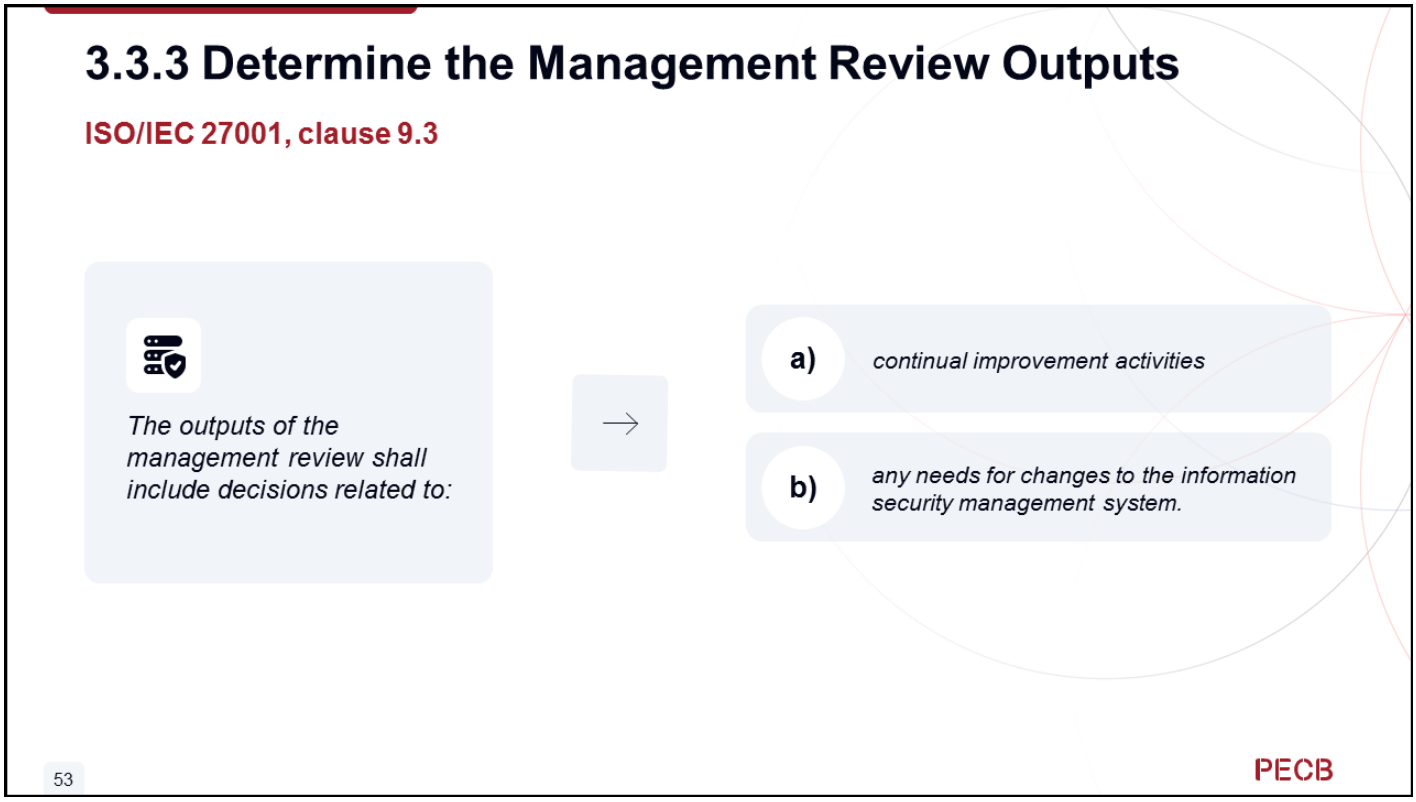
52

PECB

The input needed for each of the topics mentioned in the slide must be prepared in advance. The aim of the review will be to verify whether the defined objectives by management are being accomplished and whether the ISMS is meets the requirements of the standard. For each point, the management review will decide what (if any) actions to take.

ISO/IEC 27003, clause 9.3 Management review

Inputs to the management review should be at the appropriate level of detail, according to the objectives established for the management involved in the review. For example, top management should evaluate only a summary of all items, according to the information security objectives or high level objectives.



ISO/IEC 27003, clause 9.3 Management review

The outputs from the management review process should include decisions related to continual improvement opportunities and any needs for changes to the ISMS. They can also include evidence of decisions regarding:

a. *changes of the information security policy and objectives, e.g. driven by changes in external and internal issues and requirements of interested parties;*
b. *changes of the risk acceptance criteria and the criteria for performing information security risk assessments;*
c. *actions, if needed, following assessment of information security performance;*
d. *changes of resources or budget for the ISMS;*
e. *updated information security risk treatment plan or Statement of Applicability; and*
f. *necessary improvements of monitoring and measurement activities.*

3.3.4 Follow Up on the Management Review

ISO/IEC 27001, clause 9.3

The organization shall retain documented information as evidence of the results of management reviews.

Information from management reviews that should be documented includes:

- The date and location of review
- Contributors and their role to the review
- The criteria against which the ISMS has been reviewed
- Current performance of the ISMS
- Any changes identified in the internal and external environment
- Decisions and actions to be taken
- Responsibilities and timescales for the agreed actions

PECB

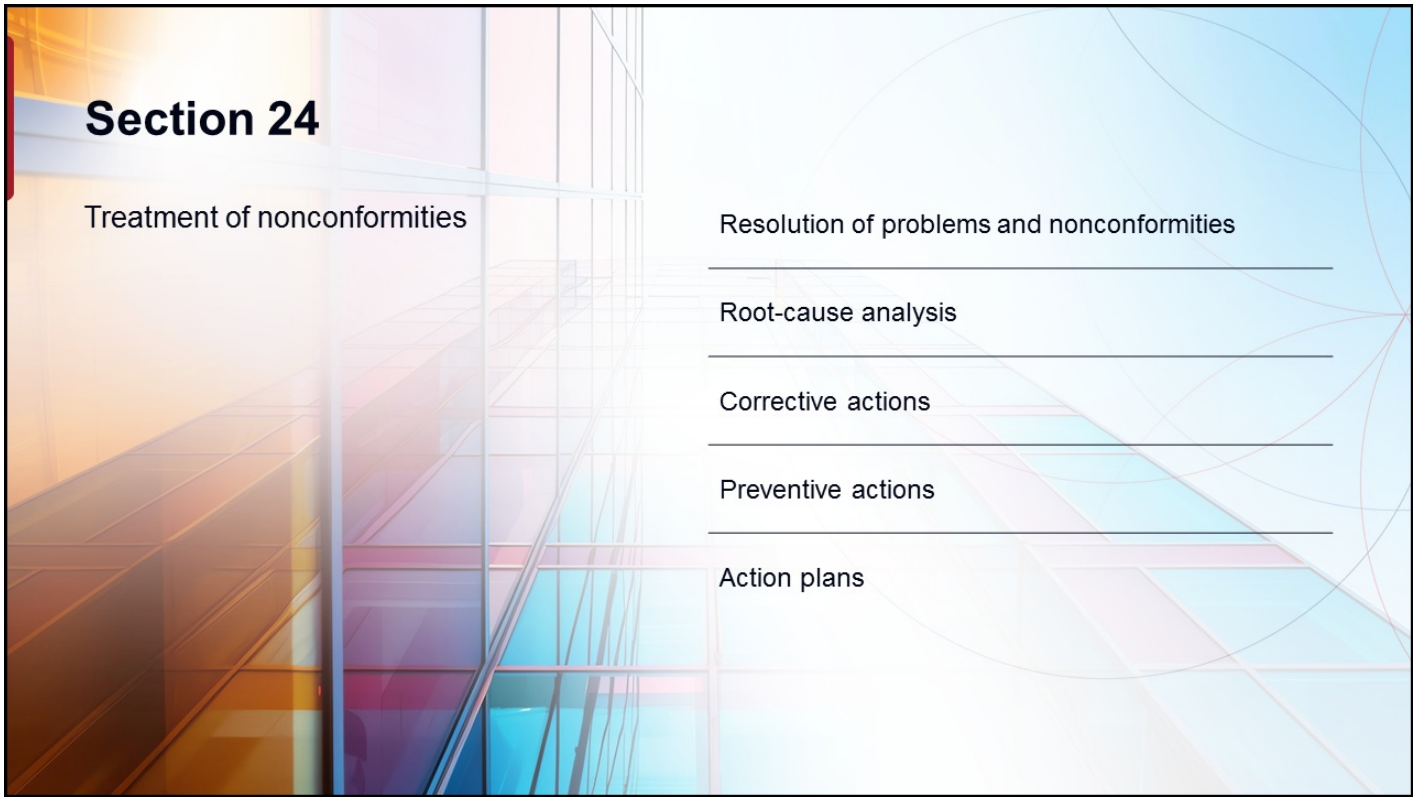
Section 23 Summary

- Management review is conducted by the top management to analyze the suitability, adequacy, and effectiveness of the information security management system. Management reviews must be conducted at planned intervals.
- Management review should include, among others, information on audit results, nonconformities and corrective actions, review of new and ongoing actions, results of monitoring and measurement, risks assessment, and status of risk treatment plan.
- Management review outputs include decisions in regard to continual improvement opportunities and changes to the ISMS.

Questions?

Quiz 24

Note: To complete Quiz 24, please go to the Quizzes Worksheet.

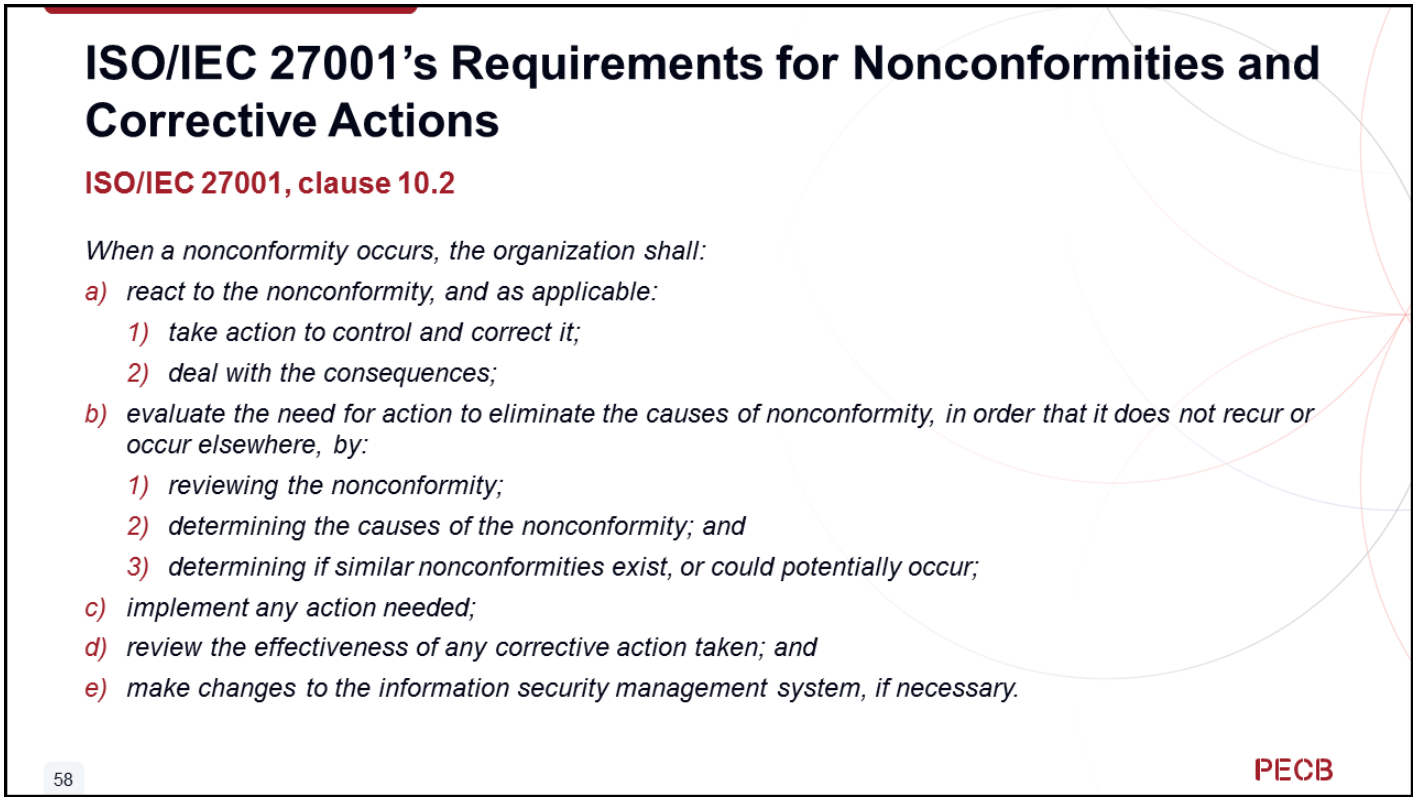


This section aims to help participants gain knowledge on treating nonconformities and understand the importance of corrective and preventive actions. Moreover, participants will learn how to draft an action plan and review the effectiveness of the actions taken.

Treatment of Nonconformities

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

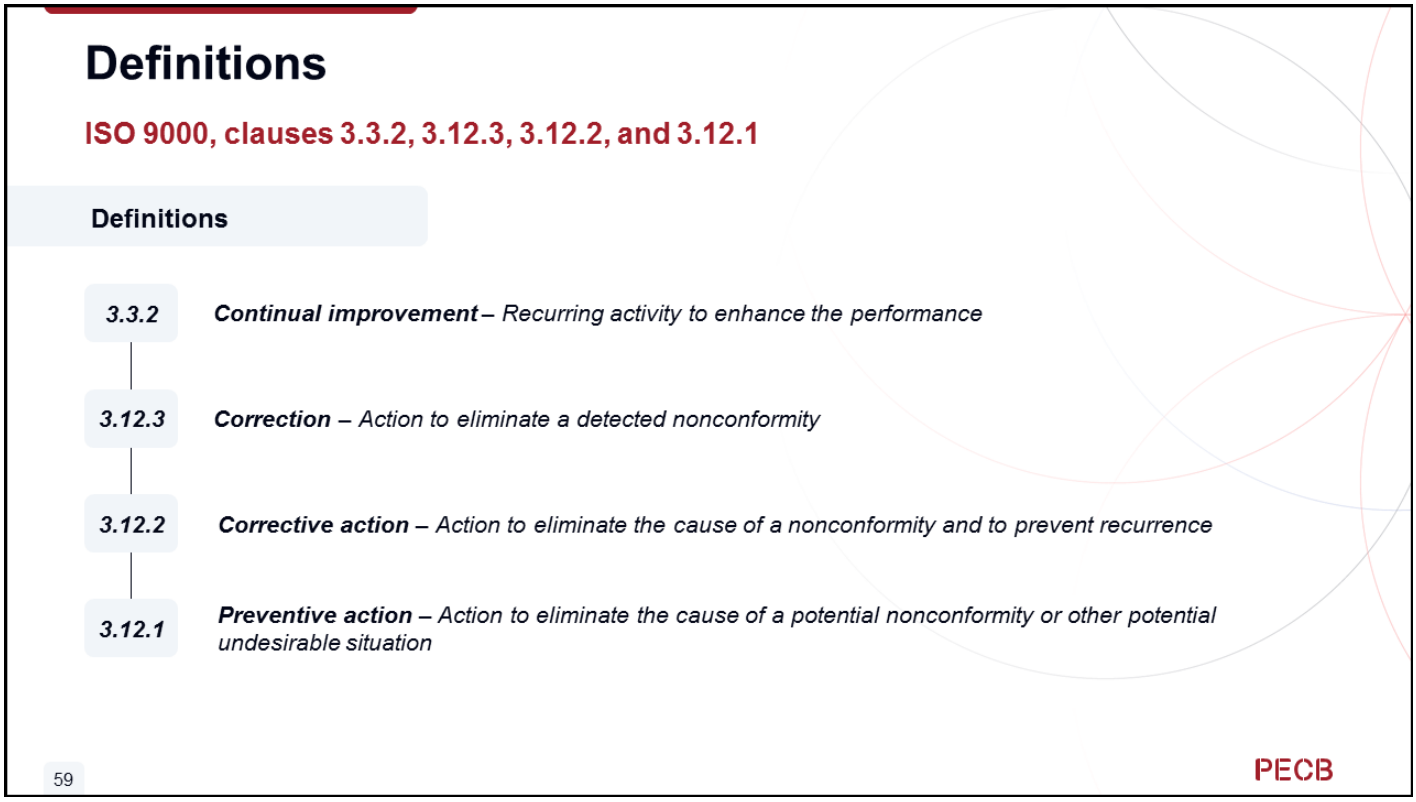


ISO/IEC 27003, clause 10.1 Nonconformity and corrective action

Explanation

A nonconformity is a non-fulfilment of a requirement of the ISMS. Requirements are needs or expectations that are stated, implied or obligatory. There are several types of nonconformities such as:

a. *failure to fulfill a requirement (completely or partially) of ISO/IEC 27001 in the ISMS;*
b. *failure to correctly implement or conform to a requirement, rule or control stated by the ISMS; and*
c. *partial or total failure to comply with legal, contractual or agreed customer requirements.*
    - *Nonconformities can be for example:*
d. *persons not behaving as expected by procedures and policies;*
e. *suppliers not providing agreed products or services;*
f. *projects not delivering expected outcomes; and*
g. *controls not operating according to design.*
    - *Nonconformities can be recognized by:*
h. *deficiencies of activities performed in the scope of the management system;*
i. *ineffective controls that are not remediated appropriately;*
j. *analysis of information security incidents, showing the non-fulfilment of a requirement of the ISMS;*
k. *complaints from customers;*
l. *alerts from users or suppliers;*
m. *monitoring and measurement results not meeting acceptance criteria; and*
n. *objectives not achieved.*



Notes on terminology:

1. By definition, information security improvement is the part of information security management focused on increasing the ability to fulfill information security requirements. The requirements can be related to any aspect, including effectiveness, efficiency, or traceability.
2. The process of establishing objectives and finding opportunities for improvement is a continual process that uses audit findings and audit conclusions, analysis of data, management reviews, or other means. It generally leads to corrective action or preventive action.
3. Preventive action is taken to prevent occurrence, whereas corrective action is taken to prevent recurrence.
4. A correction can be made in conjunction with a corrective action.

ISO 9000, clause 3.7.11 Effectiveness

Extent to which planned activities are realized and planned results are achieved

ISO 9000, clause 3.7.10 Efficiency

Relationship between the result achieved and the resources used

4.1 Treatment of Nonconformities

List of activities

4.1.1 Define a process to resolve problems and nonconformities

4.1.2 Determine the corrective actions

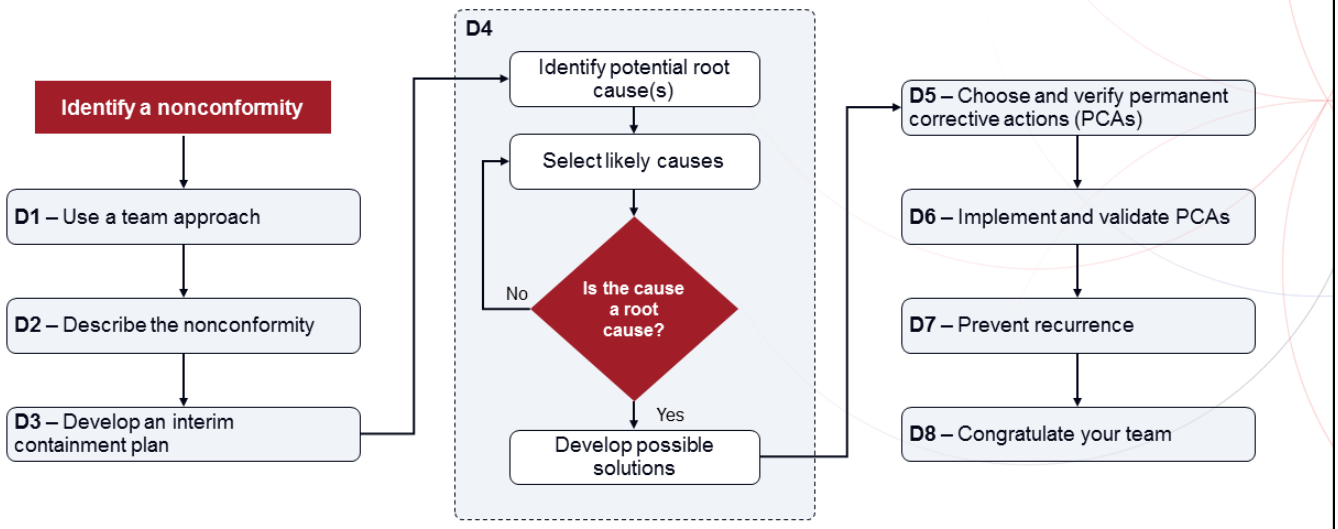
4.1.3 Determine the preventive actions

4.1.4 Draft an action plan

PECB

4.1.1 Define a Process to Resolve Problems and Nonconformities

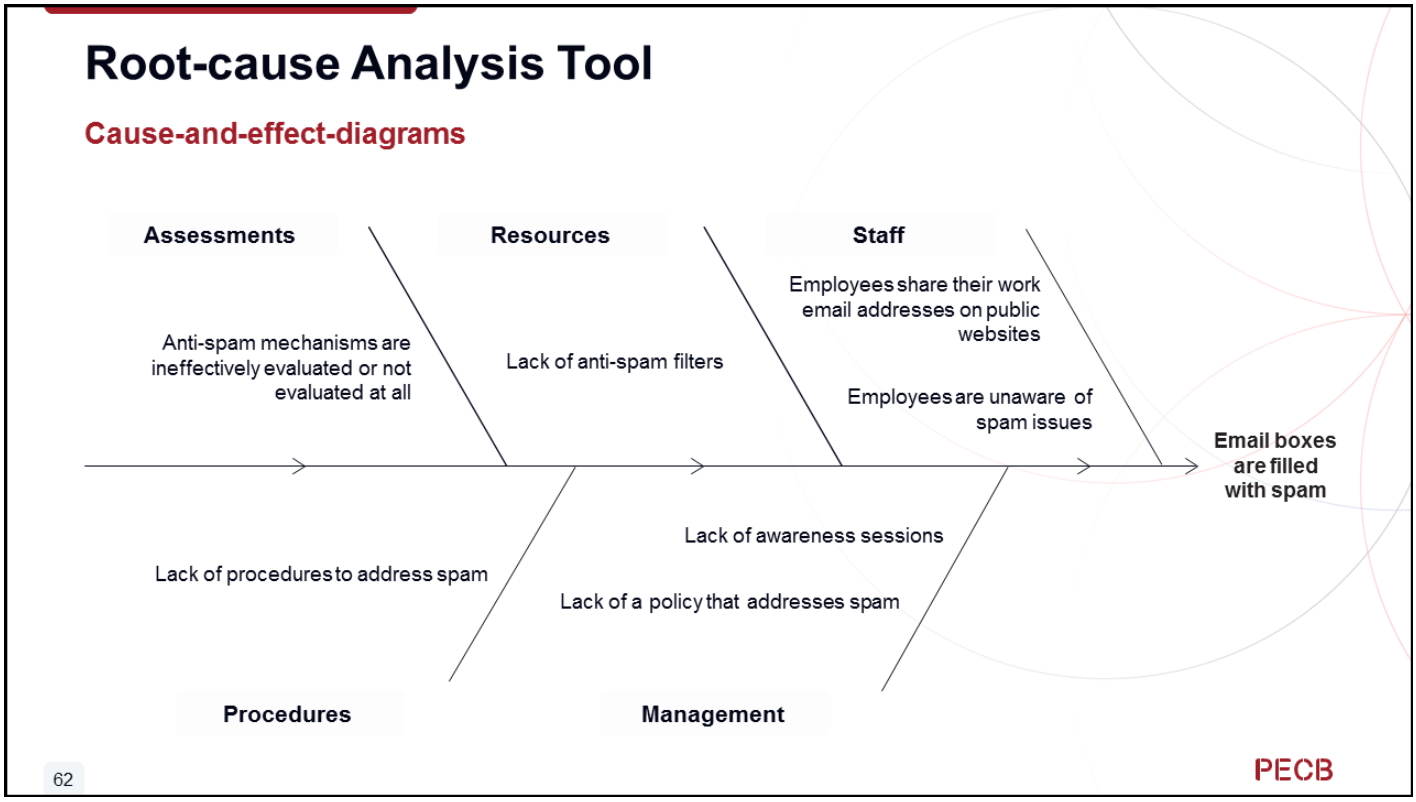
Example of the eight disciplines problem-solving method:



The Eight Disciplines Problem Solving (8Ds) is a method used to approach and resolve problems and nonconformities. Its purpose is to identify, correct, and eliminate recurring problems. Moreover, it is useful to improve processes and controls. It establishes a permanent corrective action based on a statistical analysis of the problem and focuses on the origin of the problem by determining its root causes.

The steps include:

- **D1 – Use a team approach:** establish a team consisting of professionals with thorough knowledge of processes and controls
- **D2 – Describe the nonconformity:** define the problem by breaking it down into measurable items (The 5W2H [who, what, where, when, why, how and how many] can be used as a tool in this step.)
- **D3 – Develop an interim containment plan:** determine and implement the respective containment actions in order to confine the problem and thus prevent it from affecting the interested parties
- **D4 – Identify potential root cause(s):** identify and analyze all possible reasons for the occurrence of the problem in the first place; seek an explanation as to why the problem has not been detected at the time it occurred (The root causes must be properly verified and, if required, proven, and not simply determined by a brainstorming session.)
- **D5 – Choose and verify permanent corrective actions (PCAs):** make sure, quantitatively, that the chosen corrective action will resolve the problem by means of pre-production programs.
- **D6 – Implement and validate PCAs:** determine and implement the best corrective actions
- **D7 – Prevent recurrence:** in order to avoid the repetition of the same problems or similar ones, take actions by modifying the management systems, operation systems, practices, and procedures
- **D8 - Congratulate your team:** acknowledge the collective efforts of the team members and officially thank them for their work



Root cause analysis is a method used to resolve nonconformities by identifying the root causes of the problem. This practice is based on the theory that problems are better resolved when the root causes are corrected or eliminated, as opposed to simply treating the immediate and obvious symptoms.

By addressing the root causes, the possibility of the nonconformity to recur is reduced. To be effective, root cause analysis must be performed systematically and conclusions must be supported by evidence. For each problem analyzed, there is generally more than one root cause.

A cause-and-effect diagram, also known as a fishbone diagram, is a root-cause analysis tool that maps the causes and the effects visually. It sorts possible causes of a problem into different smaller categories to get closer to the root cause of the problem. It is vital to choose the categories wisely in order to identify the root cause of the problem and find the appropriate solution.

Asking the Right Questions

The questions needed for the analysis of any problem

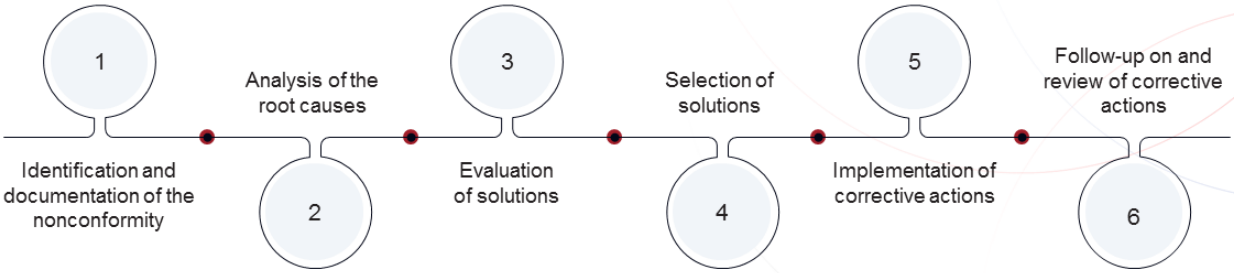
Current situation	What has been done?	How is it done?	Who did it?	Where is it done?	When is it done?
Questioning	Why is this necessary?	Why is it done this way?	Why this person?	Why is it done at this place?	Why is it done at that moment?
Solution tracking	What else could we do?	How to do it differently?	Who else could do it?	Where else could we do it?	Could we do it another time?
Remaining option(s)	What will be done?	How will it be done?	Who will do it?	Where will it be done?	When will it be done?

PECB

4.1.2 Determine the Corrective Actions

ISO/IEC 27001, clause 10.2

Corrective actions shall be appropriate to the effects of the nonconformities encountered.



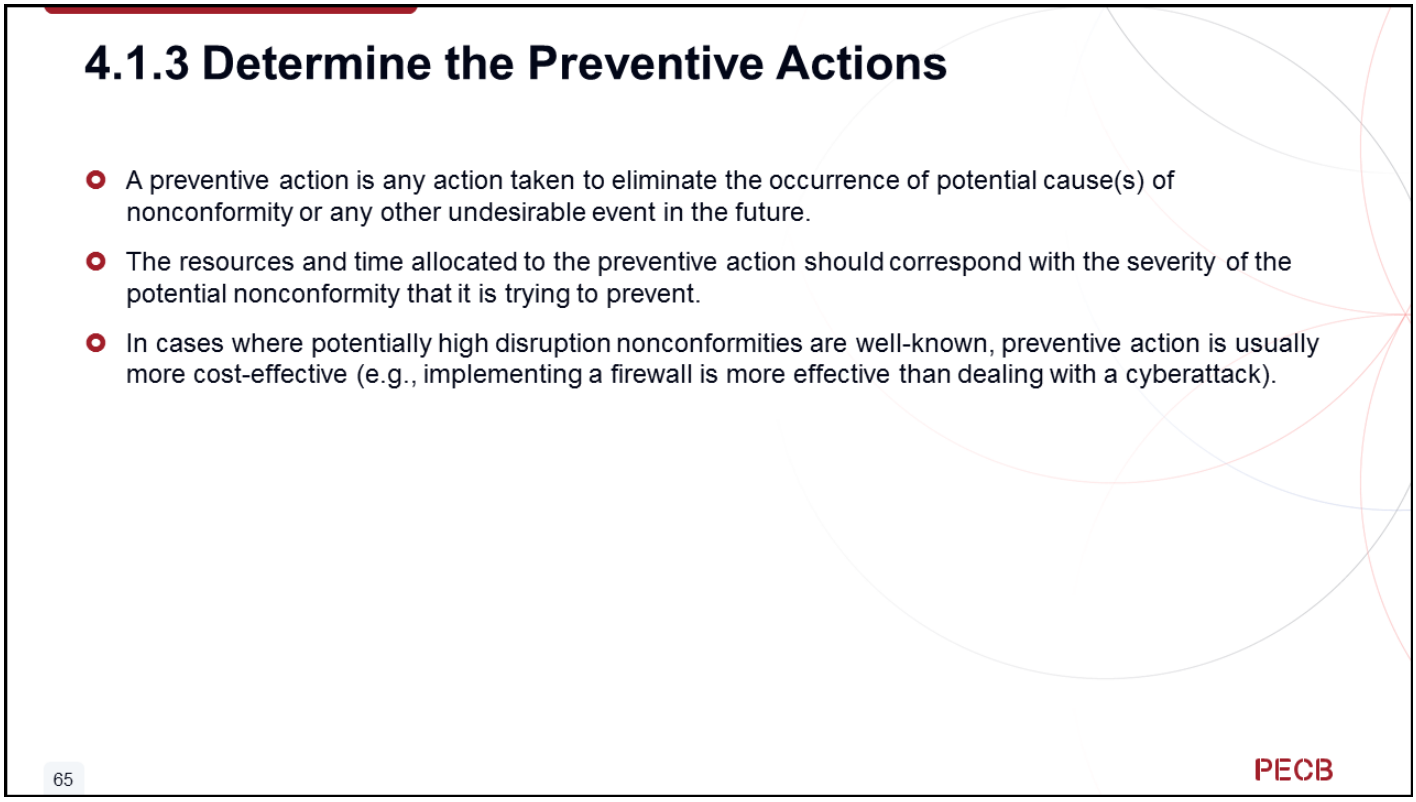
64

PECB

A corrective action is an action taken to permanently eliminate the root cause(s) of a nonconformity or of any other existing undesirable event and to prevent its reoccurrence. A corrective action is, thus, a term that includes the reaction to a problem related to a system or process, security incidents, obstacles in achieving objectives, nonconformities, etc.

The corrective action process should include:

1. **Identification and documentation of the nonconformity:** the person(s) responsible define and document the nonconformity and analyze its impact on the organization.
2. **Analysis of the root cause(s):** the person(s) responsible determine the source of the nonconformity and analyze its root cause(s).
3. **Evaluation of options:** the possible corrective actions are listed. At this stage, if the problem is significant, or if the probability that the problem will reoccur is high, temporary corrective actions can be implemented.
4. **Selection of solutions:** one or more corrective actions are selected to correct the problem and the improvement objectives are determined. The selected solution must correct the problem and should also ensure that the problem will not reoccur.
5. **Implementation of corrective actions:** the approved corrective action plan is implemented and all the taken actions described in the plan are documented.
6. **Follow-up on and review of corrective actions:** the person(s) responsible must monitor the effectiveness of the implanted corrective actions. This can be done by periodically assessing whether the organization is achieving its information security objectives through the corrective actions implemented.

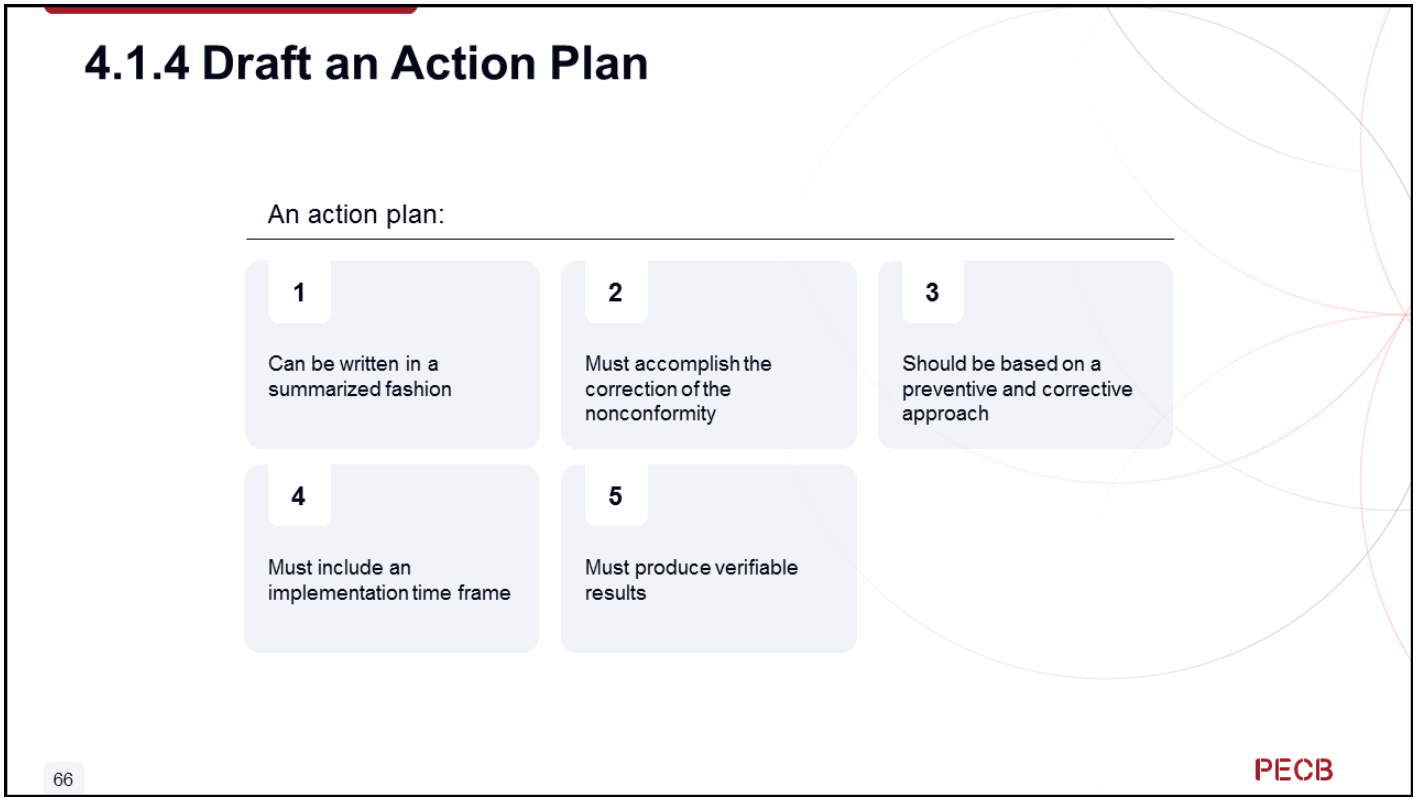


By establishing a continual risk management process, the organization is more likely to detect a change in the risk factors that concern the organization. Information security threats and vulnerabilities can change abruptly, so the organization should continuously monitor them to detect these changes and take actions to prevent information security incidents.

To determine if there is a need for preventive actions, the organization should, among others, monitor the following:

- New assets in the ISMS
- Modifications to the value of assets, for example, because of the evolution in operational needs
- New threats (internal or external) that have not been evaluated
- New vulnerabilities identified that have not been evaluated
- Identified vulnerabilities to determine those exposed to new threats
- Security incidents

Similarly to the corrective action process, a preventive action process includes: identifying a potential problem, evaluating options, selecting solutions, implementing preventive actions, and reviewing preventive actions.



Implementation dates must be realistic and based on the nonconformities observed and the costs of the corrective measures to be taken. The deadlines set must be reasonable.

Submission of Action Plans Following an Audit

- An action plan must be submitted to address each nonconformity separately. A general action plan devised to address all nonconformities is unacceptable.
- Action plans must be approved by the top management.
- The auditor analyzes the cause(s) and evaluates if the specific correction and corrective actions taken or planned can eliminate the detected nonconformities within a defined timeframe.

67

PECB

The top management may decide to accept the risk instead of implementing corrective, preventive, or improvement actions; however, they must document the justification for their decision.

The action plans must be submitted within specified deadlines. Most certification bodies (in the case of a certification audit) set a deadline between 10 and 60 days for the submission of action plans. If the action plan is not received within the specified time period, the auditee will not be recommended for certification.

Action Plans

Examples

1. A new data system must be installed to manage clients' accounts in the network, and to separate the confidential data from other databases (time frame: within three weeks).

2. A new version of the information security policy must be published to include legal and regulatory statements, and contract requirements (time frame: within two months).

3. Establish and communicate a formal disciplinary process to take action against employees and other relevant interested parties who have committed an information security policy violation (time frame: within three months).

PECB

Documented Information

ISO/IEC 27001, clause 10.2 and ISO/IEC 27003, clause 10.1

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.

Sufficient documented information is required to be retained to demonstrate that the organization has acted appropriately to address the nonconformity and has dealt with the related consequences.

All significant steps of nonconformity management (starting from discovery and corrections) and, if started, corrective action management (cause analysis, review, decision about the implementation of actions, review and change decisions made for the ISMS itself) should be documented.

PECB

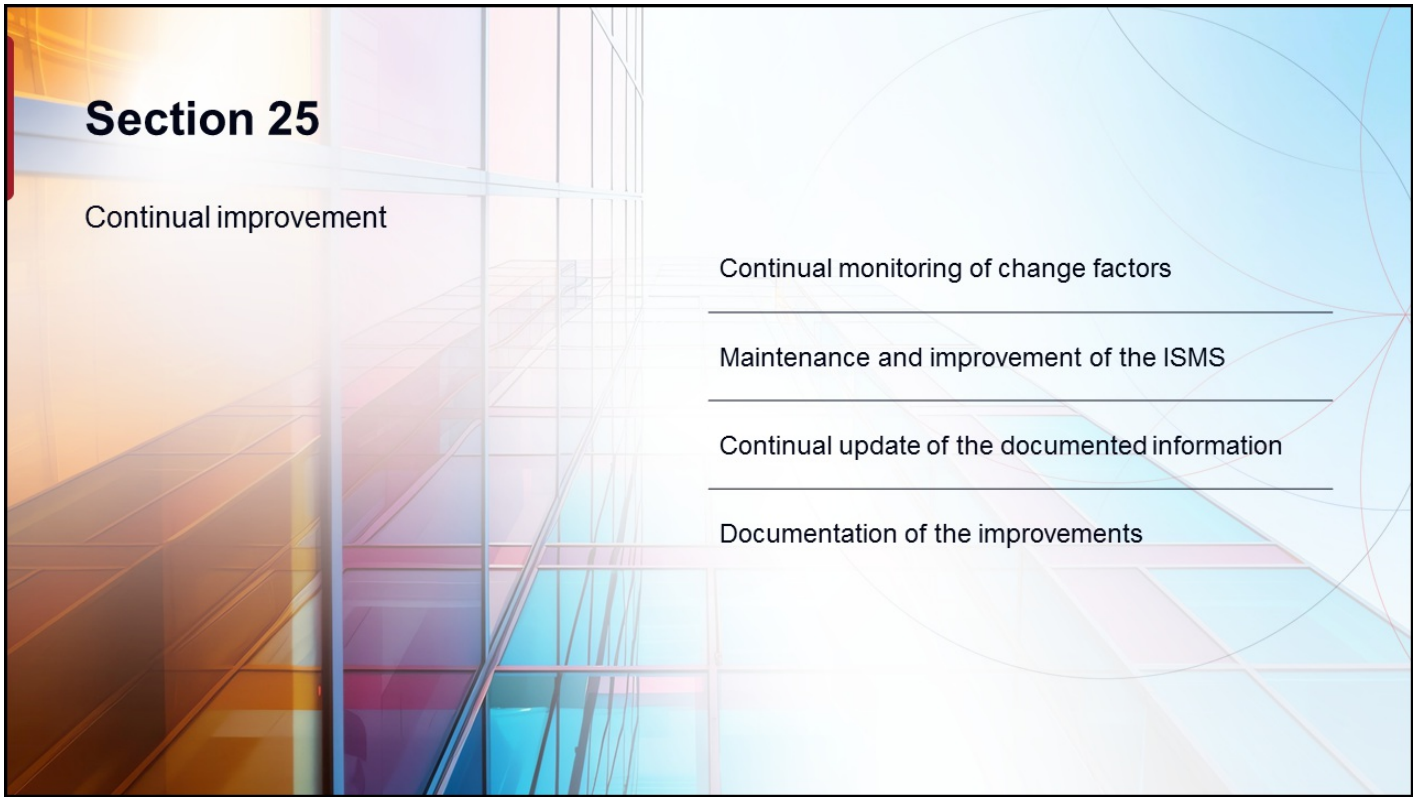
Section 24 Summary

- A corrective action is an action taken to permanently eliminate the root cause(s) of a nonconformity or of any other existing undesirable event and to prevent its reoccurrence.
- A preventive action is any action taken to eliminate a potential nonconformity or any other undesirable event and to prevent their occurrence in the future.
- An action plan must be submitted to address each nonconformity separately. A general action plan to address all nonconformities is unacceptable.
- Action plans must be approved by the top management and they must have a time frame.

Questions?

Quiz 25

Note: To complete Quiz 25, please go to the Quizzes Worksheet.

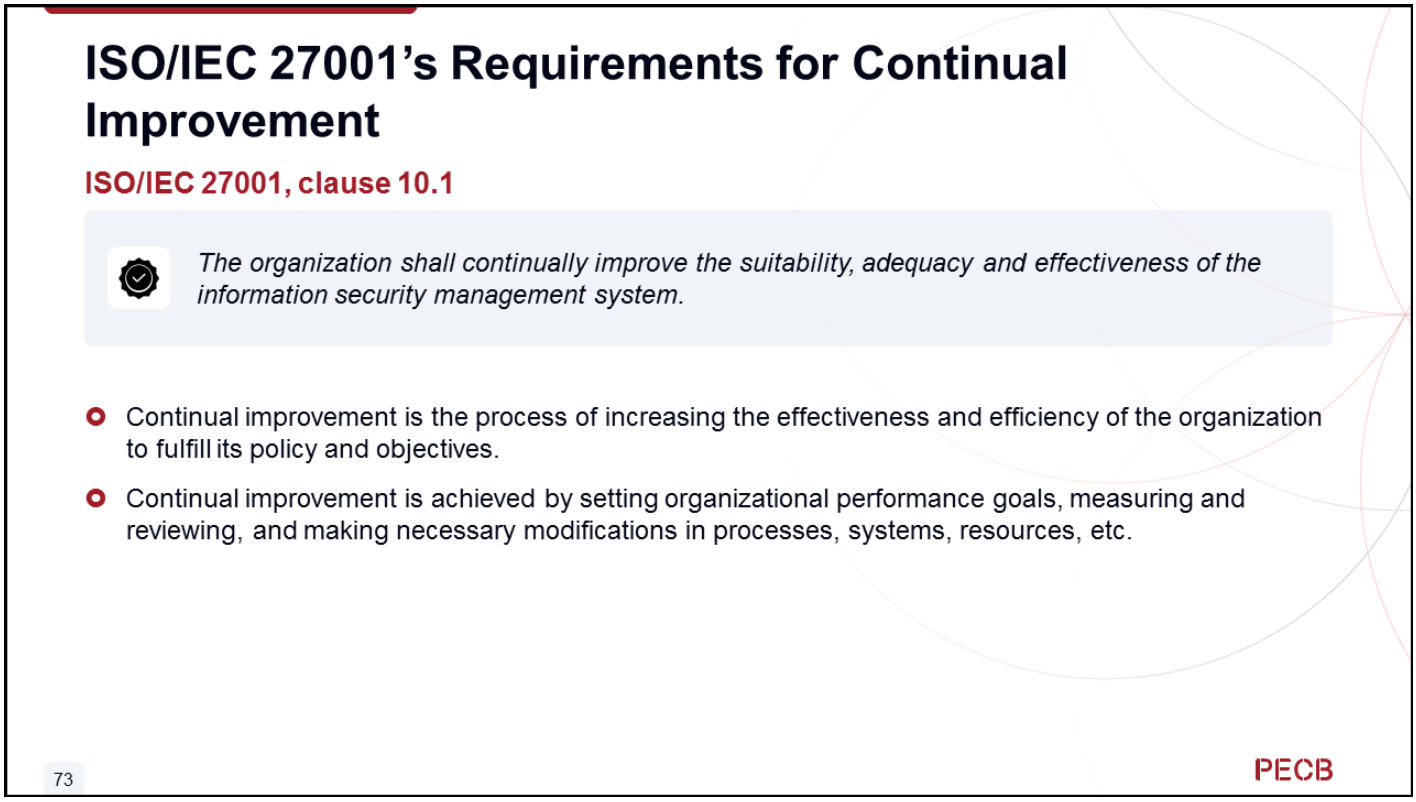


This section provides information that will help participants gain knowledge on the continual improvement of the information security management system through the monitoring of change factors, the update of documented information, the maintenance and improvement of the ISMS, and so on.

Continual Improvement

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 10.2 Continual improvement

Explanation

A systematic approach using continual improvement will lead to a more effective ISMS, which will improve the organization's information security. Information security management leads the organization's operational activities in order to avoid being too reactive, i.e. that most of the resources are used for finding problems and addressing these problems. The ISMS is working systematically through continual improvement so that the organization can have a more proactive approach. Top management can set objectives for continual improvement, e.g. through measurements of effectiveness, cost, or process maturity.

Guidance

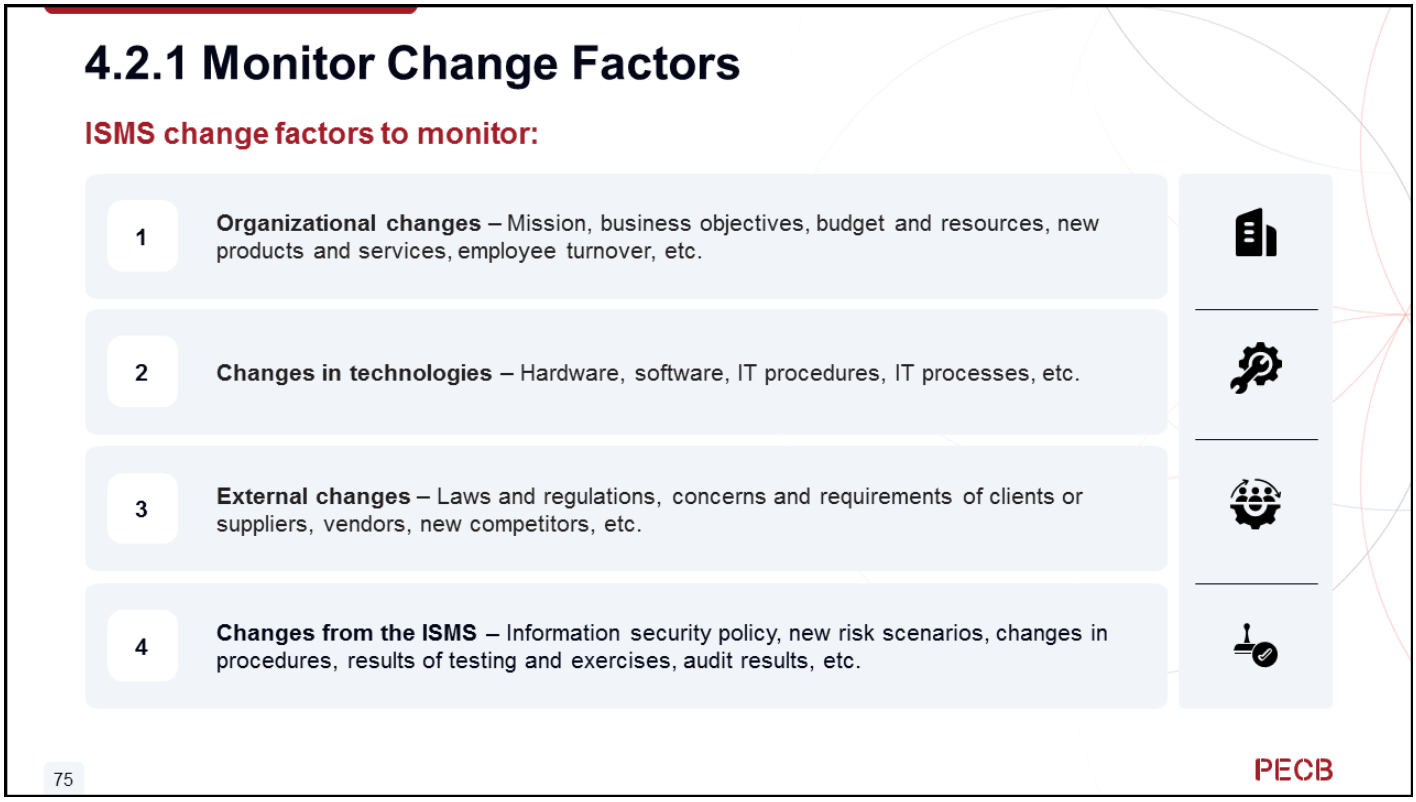
Continual improvement of the ISMS should entail that the ISMS itself and all of its elements are assessed considering internal and external issues, requirements of the interested parties and results of performance evaluation. The assessment should include an analysis of:

a. *suitability of the ISMS, considering if the external and internal issues, requirements of the interested parties, established information security objectives and identified information security risks are properly addressed through planning and implementation of the ISMS and information security controls;*
b. *adequacy of the ISMS, considering if the ISMS processes and information security controls are compatible with the organization's overall purposes, activities and processes; and*
c. *effectiveness of the ISMS, considering if the intended outcome(s) of the ISMS are achieved, the requirements of the interested parties are met, information security risks are managed to meet information security objectives, nonconformities are managed, while resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS are commensurate with those results.*

4.2 Continual Improvement

List of activities

PECB



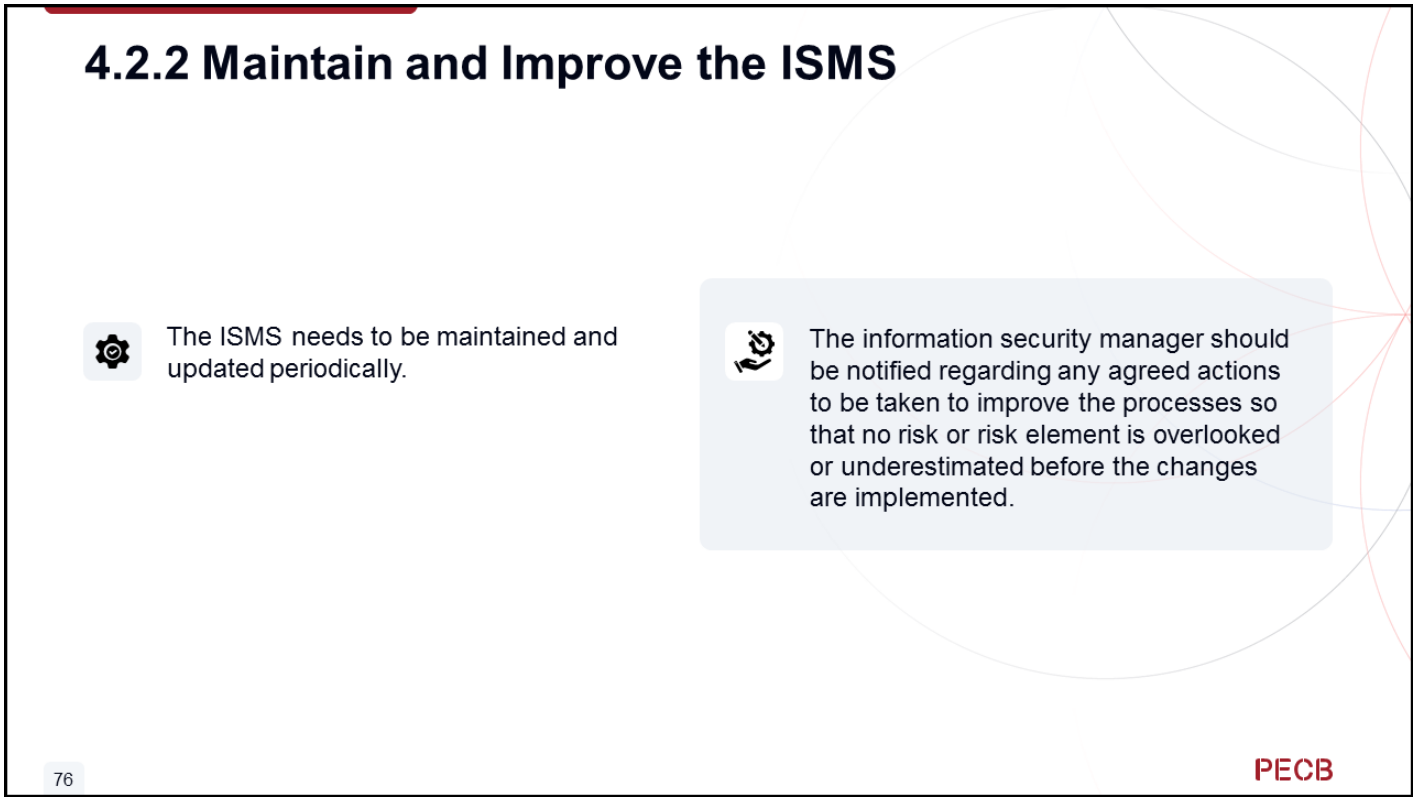
To be effective, the management system should accurately reflect the business requirements, organizational structure, and internal policies and procedures.

As part of the continual improvement process, activities and procedures undergo changes because of the changes in business needs, technology advancements, or new internal and external policies. Therefore, it is essential that the management system is reviewed and updated regularly as part of the organization's change management process to ensure that the new information is documented and controls are revised, if required.

As a general rule, the plan should be reviewed for accuracy and completeness at a defined frequency or whenever significant changes occur to any element of the plan. Some elements may require more frequent reviews.

While all strategies should be reviewed on an ongoing basis, the frequency that an organization's ISMS should be reviewed depends on the nature, scale, and complexity of the organization, its business risk profile, and the environment in which it operates. Good practice indicates that the organization's strategy should be reviewed at least every 12 months, unless:

- It is the initial development and documented evidence of the strategy.
- It undergoes a significant change in the key technology, including systems or networks.
- The pace of business change is particularly aggressive.



Another way for an organization to demonstrate that it continuously strives to improve its ISMS is by publishing their performance. This can be done in two ways.

1. Informing the employees of what has been achieved (e.g., monthly): The benefits are manifold: employees become aware of where the organization stands in the market; they can see the result of their contribution and better tie their personal goals to organization's growth.
2. Publishing a report on organizational performance over a period of time (e.g., annually): This practice allows organizations to present their accomplishments to the customer and other interested parties.

4.2.3 Maintain and Update Documented Information – Examples

ISMS documentation

- Information security policy
- Information security objectives and targets
- Awareness and training programs
- Risk analysis
- Documented information control procedure
- Incident management plans
- Internal audit program
- Management review plans

Factors of change

- Organizational changes
- New rules
- Changes in the business scope
- Incidents
- Faulty operations
- Failures
- Risk management reports
- Test results
- Internal and external audits reports

77

PECB

Documented information is the cornerstone of the proper functioning of the information security management system. In the event of a crisis, it is important to have complete and up-to-date documented information in order to allow the actors involved to follow a guide of actions instead of taking decisions based on improvisation or intuition.

The proper maintenance of documented information eliminates to a great degree the possibility of taking spontaneous decisions. In addition, it makes the principal actors ready to act when the situation requires it, giving guidance, and avoiding as many mistakes as possible.

The ISMS is a dynamic system and continual change is imperative. As a consequence, the ISMS documented information must be adapted on each and every trigger of change.

The Benefits of Continual Improvement

- **Increased efficiency –** Continual improvement increases productivity as the changes may lead to long-term positive outputs.
- **Collaborative teams –** Working continuously toward a common goal will help in building new relationships within teams and reinforcing the existing ones.
- **Increased customer satisfaction –** While actively improving processes, organizations simultaneously increase the quality of the products and services that they offer.
- **Error reduction –** With the continual improvement of processes, the number of errors in those processes will also be reduced.

PECB

4.2.4 Document the Improvements

It is good practice to document continual improvement activities in a register. This register can take the form of a spreadsheet or a database in which activities are collected, prioritized, and tracked to completion.

Continual Improvement Register					
No.	Change description	Priority	Date of initiation	Date of completion	Signature

79

PECB

The improvements or modifications made to the ISMS should be recorded by using a record of changes, which lists a special identifier (e.g., change number or any specific code), description of the change being made, priority (which can be classified as high, medium, low or based on numbers of 1 to 5), dates of change initiation and completion, and the signature of the person overseeing the change.

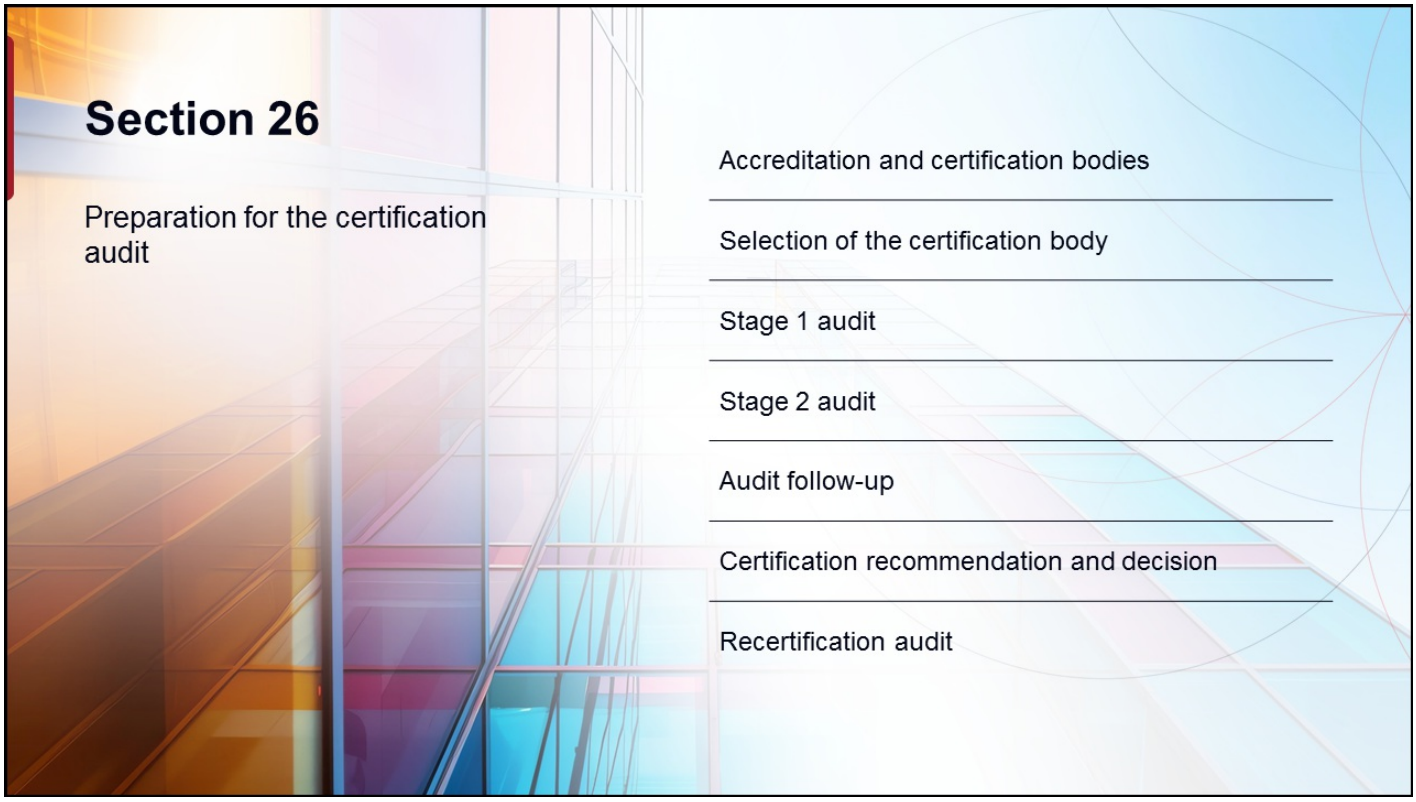
Section 25 Summary

- The organization must continually improve the suitability, adequacy, and effectiveness of the ISMS.
- Continual improvement refers to the process of increasing the effectiveness and efficiency of the organization to fulfill its policy and objectives.
- The ISMS needs to be maintained and updated periodically.
- Continual improvement helps organizations fulfill their policies and objectives.
- The organization should maintain and update its ISMS documentation, including the information security policy, information security objectives, awareness and training programs, ISMS risk analyses, incident management plans, management review plans, and the internal audit program.
- Continual improvement helps organizations increase efficiency and customer satisfaction, reduce errors, and build teamwork.

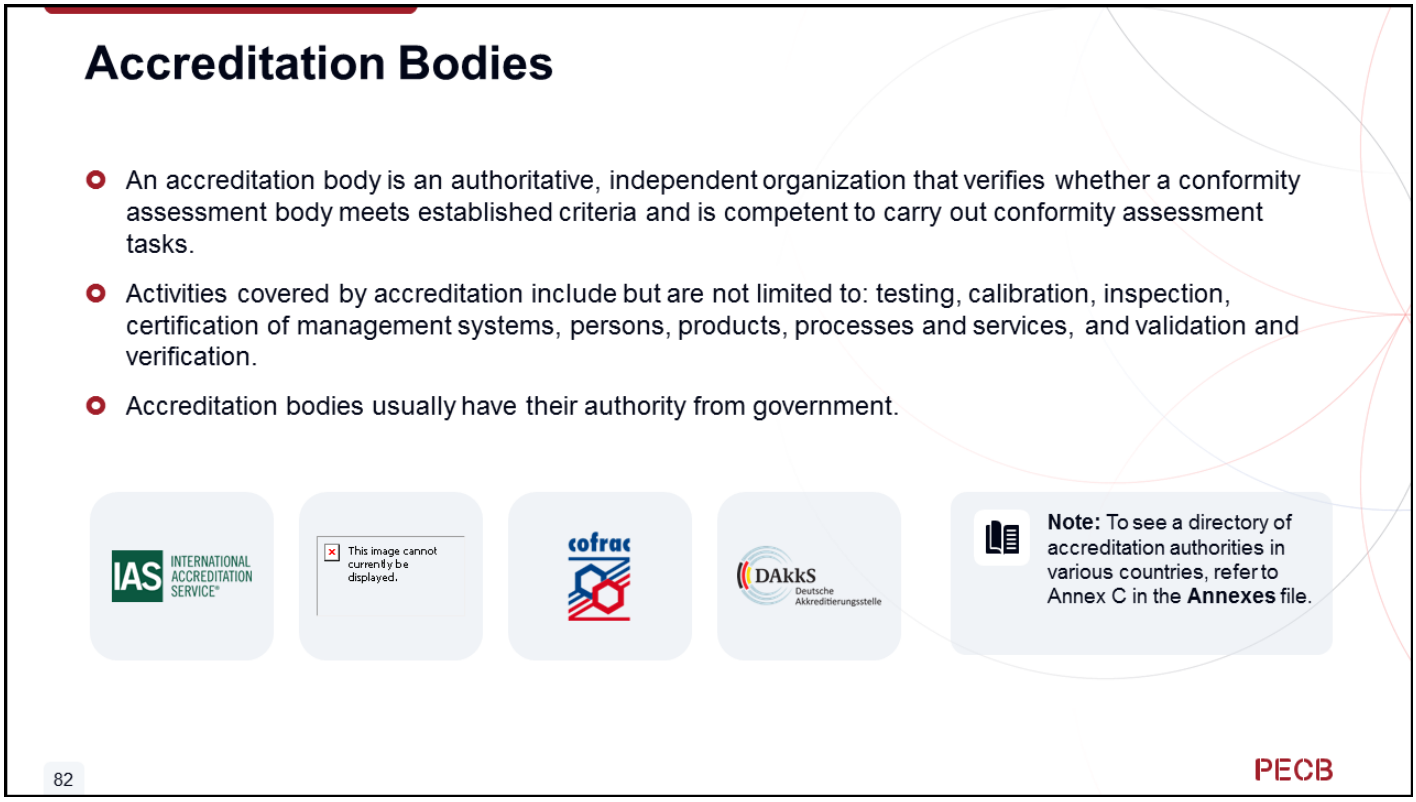
Questions?

Quiz 26

Note: To complete Quiz 26, please go to the Quizzes Worksheet.



This section provides information that will help participants gain knowledge about accreditation and certification bodies. In addition, participants will be able to understand the certification process, including the selection of the certification body, the stage 1 and 2 audit, the audit follow-up, the certification recommendation and decision, and the recertification audit.



ISO/IEC 17011 provides general requirements for accreditation bodies in assessing and accrediting certification bodies. Compliance with the requirements of ISO/IEC 17011 proves that the accreditation bodies are competent and reliable in offering accreditation services.

Commonly, there is only one accreditation authority in each country. However, in the United States, there are several accreditation bodies: IAS and ANAB.

- The **International Accreditation Service (IAS)** accredits certification programs for persons, products, and management systems according to ISO/IEC 17024, ISO/IEC 17065, and ISO/IEC 17021-1.
- **The ANSI National Accreditation Board (ANAB)** supervises the certification bodies accredited against ISO/IEC 17021-1.

Accreditation authority groups:

- **European co-operation for Accreditation (EA)** is the European network of accreditation organizations based in Europe. The members include UKAS, COFRAC, BNAC, ENAC, etc.

Source: https://european-accreditation.org

- **International Accreditation Forum (IAF)** is the international association of accreditation organizations for systems in management, product, services, individuals, and other programs. The objective of IAF is to ensure that the member organizations only certify competent organizations and establish agreements of mutual recognition among its members.

Source: https://www.iaf.nu

Certification Bodies

Certification bodies certify management systems, persons, products, processes, and services.

Certification bodies are always third-party, impartial conformity assessment bodies.

A certification body can be a governmental or nongovernmental organization, with or without regulatory authority.

While the term "certification body" may be used to refer to organizations that provide certification of persons (ISO/IEC 17024) and products, processes, and services (ISO/IEC 17065), in this training course it is used only to refer to organizations that certify management systems (as specified in ISO/IEC 17021-1).

83

PECB

ISO/IEC 17021-1, Introduction

Certification of a management system provides independent demonstration that the management system of the organization:

a. *conforms to specified requirements;*
b. *is capable of consistently achieving its stated policy and objectives;*
c. *is effectively implemented.*

ISO/IEC 17024, Introduction

This International Standard has been developed with the objective of achieving and promoting a globally accepted benchmark for organizations operating certification of persons. Certification for persons is one means of providing assurance that the certified person meets the requirements of the certification scheme.

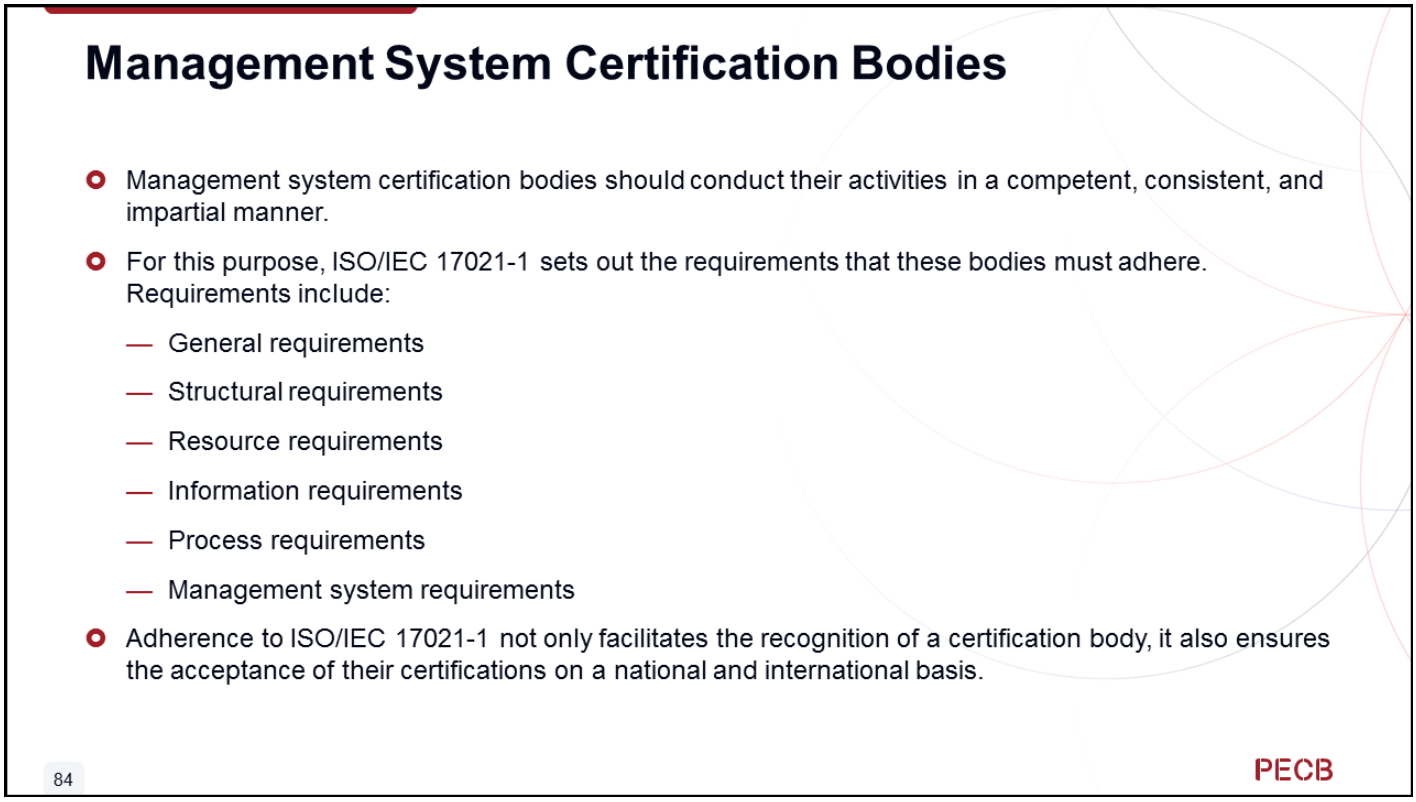
In either case, this International Standard can serve as the basis for the recognition of the certification bodies for persons and the certification schemes under which persons are certified, in order to facilitate their acceptance at the national and international levels.

ISO/IEC 17065, Introduction

The overall aim of certifying products, processes or services is to give confidence to all interested parties that a product, process or service fulfils specified requirements.

Parties that have an interest in certification include, but are not limited to:

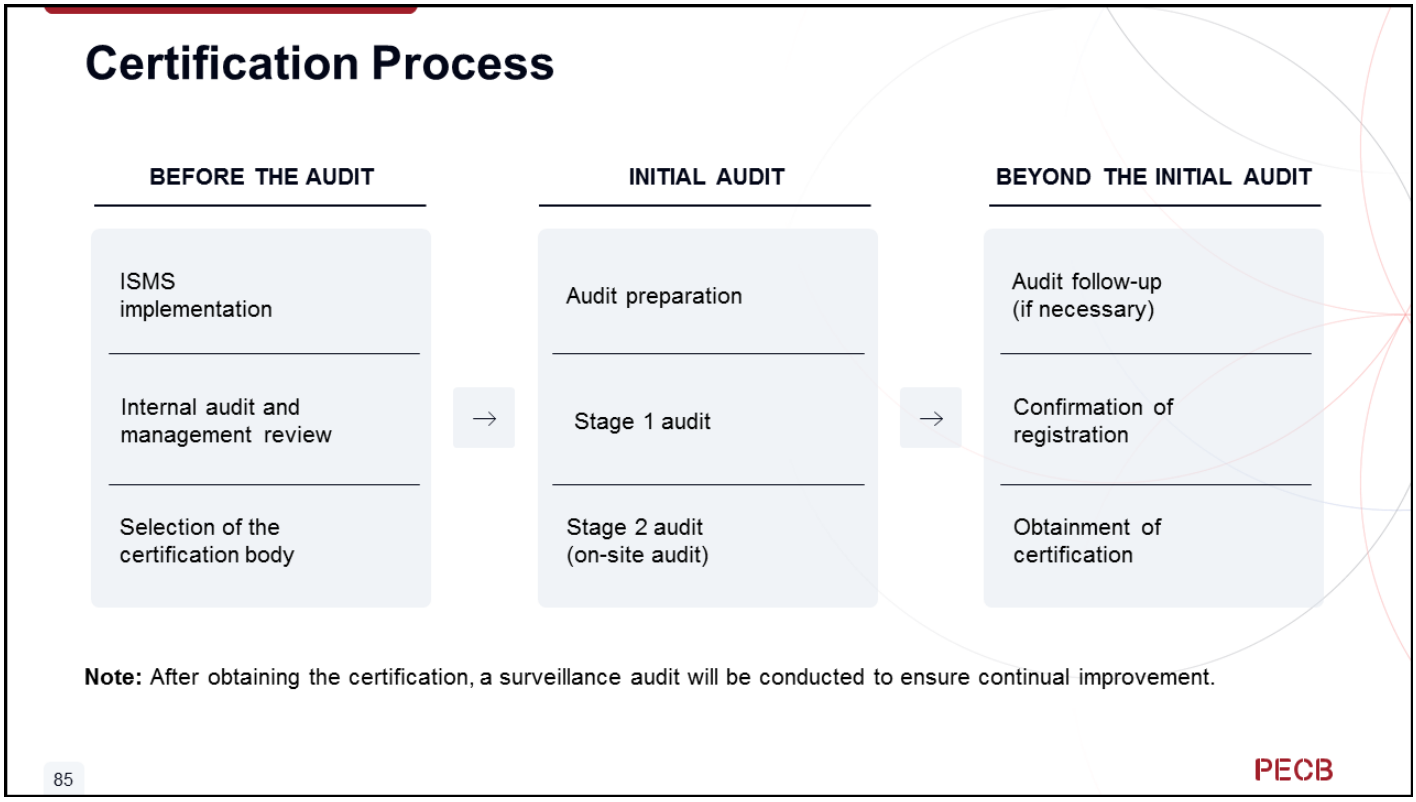
a. *the clients of the certification bodies;*
b. *the customers of the organizations whose products, processes or services are certified;*
c. *governmental authorities;*
d. *non-governmental organizations; and*
e. *consumers and other members of the public.*



Apart from the aforementioned requirements, ISO/IEC 17021-1 acknowledges the fact that varying competences are needed for auditing different management systems. This acknowledgement is reflected in the fact that ISO has developed a series of parts of the main ISO/IEC 17021 standard that deal with auditor competence for different types of management systems.

The following standards specify competence requirements for auditing and certification in the following areas:

- ISO/IEC 17021-2: Environmental management systems
- ISO/IEC 17021-3: Quality management systems
- ISO/IEC TS 17021-4: Event sustainability management systems
- ISO/IEC TS 17021-5: Asset management systems
- ISO/IEC TS 17021-6: Business continuity management systems
- ISO/IEC TS 17021-7: Road traffic safety management systems
- ISO/IEC TS 17021-8: Management systems for sustainable development in communities
- ISO/IEC TS 17021-9: Anti-bribery management systems
- ISO/IEC TS 17021-10: Occupational health and safety management systems
- ISO/IEC TS 17021-11: Facility management systems
- ISO/IEC TS 17021-12: Collaborative business relationship management systems



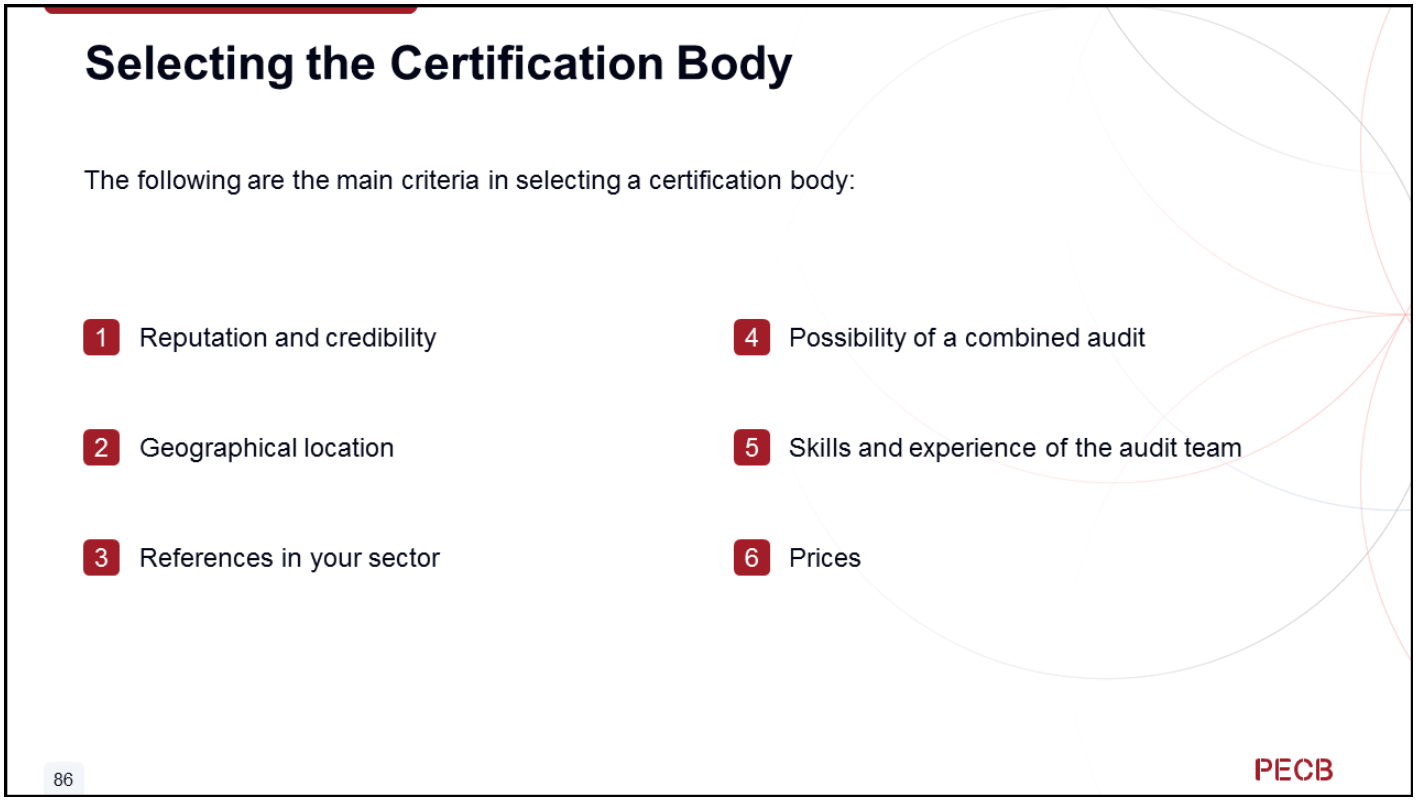
Note:

- Continual improvement refers to the ongoing process that an organization undergoes in order to improve their procedures, processes, and products or services.
- Surveillance audit refers to the activity that is performed once a year (sometimes more, based on the organization's needs) to ensure that their management system is in conformity to the respective management system standard.

1. **Selection of the certification body (registrar):** Organizations are free to select the certification body. When doing so, they should keep in mind that more renowned certification bodies offer greater recognition.
2. **Pre-assessment audit (optional):** Pre-assessment audit allows organizations to measure any gaps between their existing management system and the requirements of the standard.
3. **Stage 1 audit:** The main objective of stage 1 audit is to verify whether the management system is designed to meet the requirements of the standard and the objectives of the organization. It is recommended to perform at least some portion of the stage 1 audit on-site (at the organization's premises).
4. **Stage 2 audit (on-site visit):** The objective of stage 2 audit is to evaluate whether the management system conforms to all the requirements of the standard, is being implemented, and can support the organization in achieving its objectives. Stage 2 audit is conducted at the premises of the organization.
5. **Audit follow-up:** If nonconformities have been detected, the auditor will perform a follow-up visit to validate only the action plans associated with those nonconformities (which usually takes up to one day).
6. **Confirmation of registration:** If the organization complies with the requirements of the standard, the certification body confirms the registration and publishes the certificate.

Definitions:

- **Certification –** Certification is a formal procedure which attests to a status or a level of achievement by providing an official document.
- **Attestation –** Attestation is a method used to check, confirm, and authenticate the validity of a document.



1. **Reputation and credibility:** The value of certification depends on the reputation and credibility of the certification body that issues the certificate. As a result, it is important to select a credible certification body.
2. **Geographical location:** Choosing a certification body that operates in your area or that the audit team members speak the local language and are familiar with the local customs is advisable.
3. **References in your sector:** If the industry you operate in has specific regulatory requirements, selecting a certification body that already has clients in your business sector is preferable.
4. **Possibility of a combined audit:** If you consider certifying your organization against several standards (e.g., ISO 9001 and ISO 14001), you may want to ensure that the certification body can provide combined audits.
5. **Skills and experience of the audit team:** It is best practice to contact the certification body to ensure that the audit team has the necessary competencies and skills to perform the audit.
6. **Prices:** Prices vary between certification bodies, but you may want to request a few bids, as the number of days per audit proposed by the certification body may differ, influencing audit costs.

Audit Time Calculation

ISO/IEC 27006, Table B.1 (excerpt)

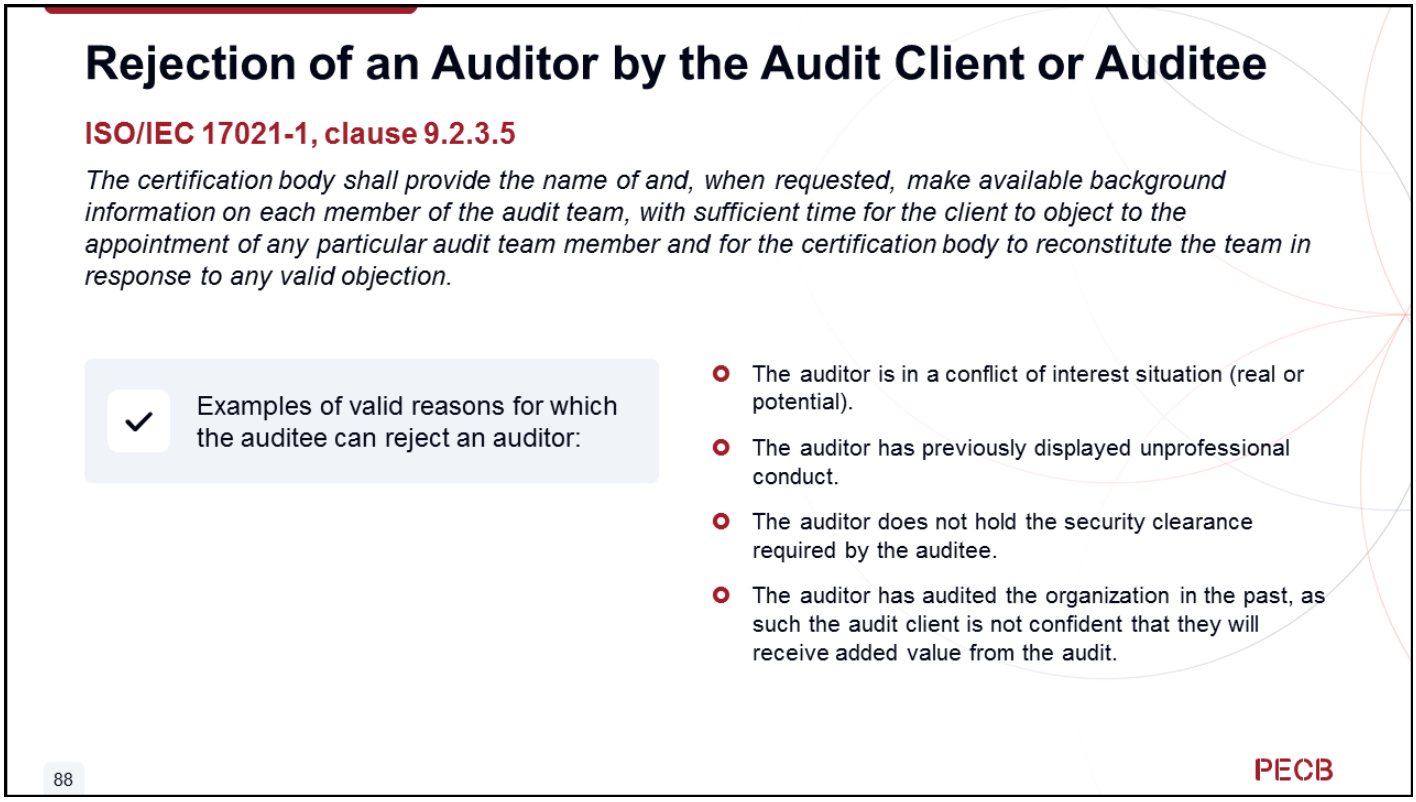
Number of employees	Audit time (day/person) ISO/IEC 27001	Number of employees	Audit time (day/person) ISO/IEC 27001
1 to 10	5	276 to 425	15
11 to 15	6	426 to 625	16.5
16 to 25	7	626 to 875	17.5
26 to 45	8.5	876 to 1175	18.5
46 to 65	10	1176 to 1550	19.5
66 to 85	11	1551 to 2025	21
86 to 125	12	2026 to 2675	22
126 to 175	13	6801 to 8500	27
176 to 275	14	8501 to 10700	28

87

PECB

Certification bodies must give auditors enough time to complete the audit. The time available to complete an audit can vary depending on the following:

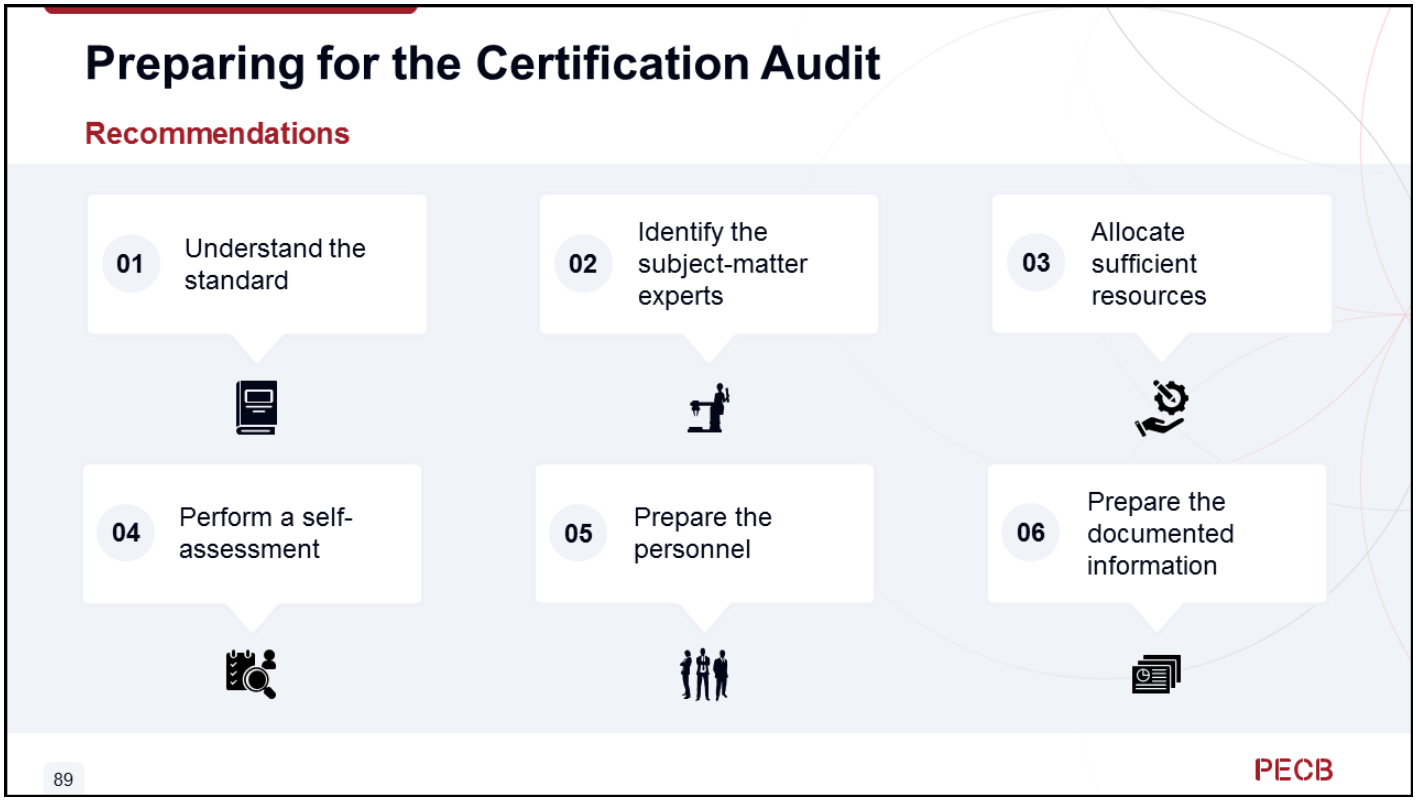
- Scope of the management system
- Complexity of the processes of the management system
- Field of activity of the auditee
- Complexity and diversity of the technologies in use
- Number of sites to audit
- Previous audits
- Agreements related to outsourced services
- Regulations, laws, and contract agreements



The audit client or the auditee can request the replacement of an audit team member for valid reasons. A valid reason would be the case of an auditor having previously displayed unprofessional conduct. Other examples of valid reasons are situations with real conflict of interest (an auditor has previously worked for the auditee) or perceived conflict of interest (an auditor has worked for one of the auditee's major competitors).

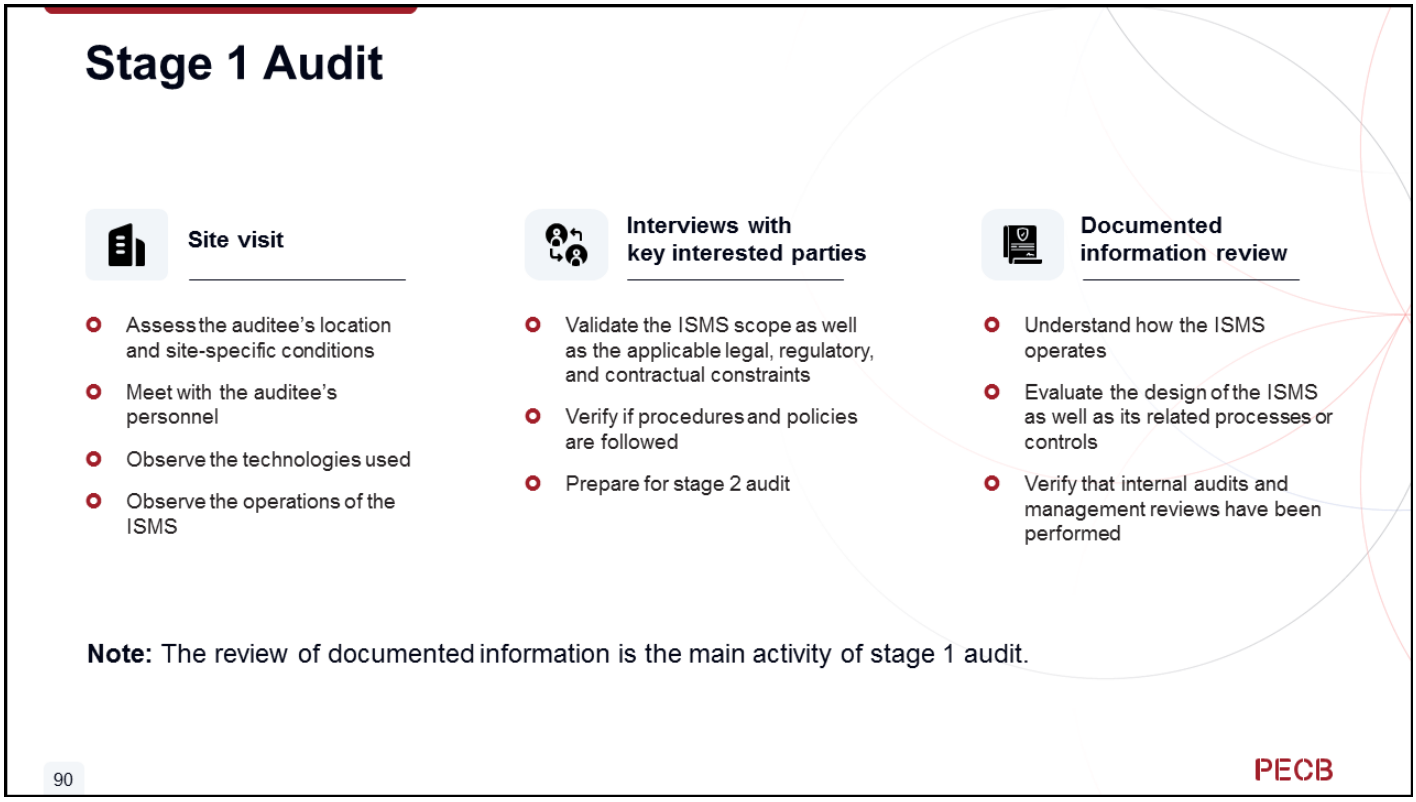
In some industries and sectors (arms industry, nuclear power, information services, etc.), an auditee can request that each member of the audit team holds a security clearance or that a background check on each member is conducted before being admitted on-site.

It is recommended to communicate these reasons to the persons responsible for the audit team and to the persons responsible for the audit program before requesting the replacement of an audit team member.



To be well prepared for a certification audit, the organization can take the following actions prior to the commencement of the audit:

1. **Understand the standard:** The whole audit will center around the standard against which the organization is seeking certification. A general understanding of the standard can help the organization efficiently manage the external audit.
2. **Identify the subject-matter experts:** The organization must determine which of their employees have the knowledge to help the external auditor understand and evaluate the processes. If the organization has already assigned a person or team to manage the ISMS, this step is unnecessary.
3. **Allocate sufficient resources:** An external audit requires time and effort from the organization.
4. **Perform a self-assessment:** The organization should review its compliance with the requirements of ISO/IEC 27001 and address the following questions:
    - Are the processes clearly defined?
    - Have the roles and responsibilities been segregated?
    - Do we maintain documented information?
    - Are the processes effective in producing the desired results?
5. **Prepare the personnel:** The organization should prepare its employees for the external audit by:
    - Informing them about the audit
    - Organizing training sessions
6. **Prepare the documented information:** Because external auditors will ask for evidence that procedures are in place, it is preferable to prepare documented information in advance so as to avoid losing time.

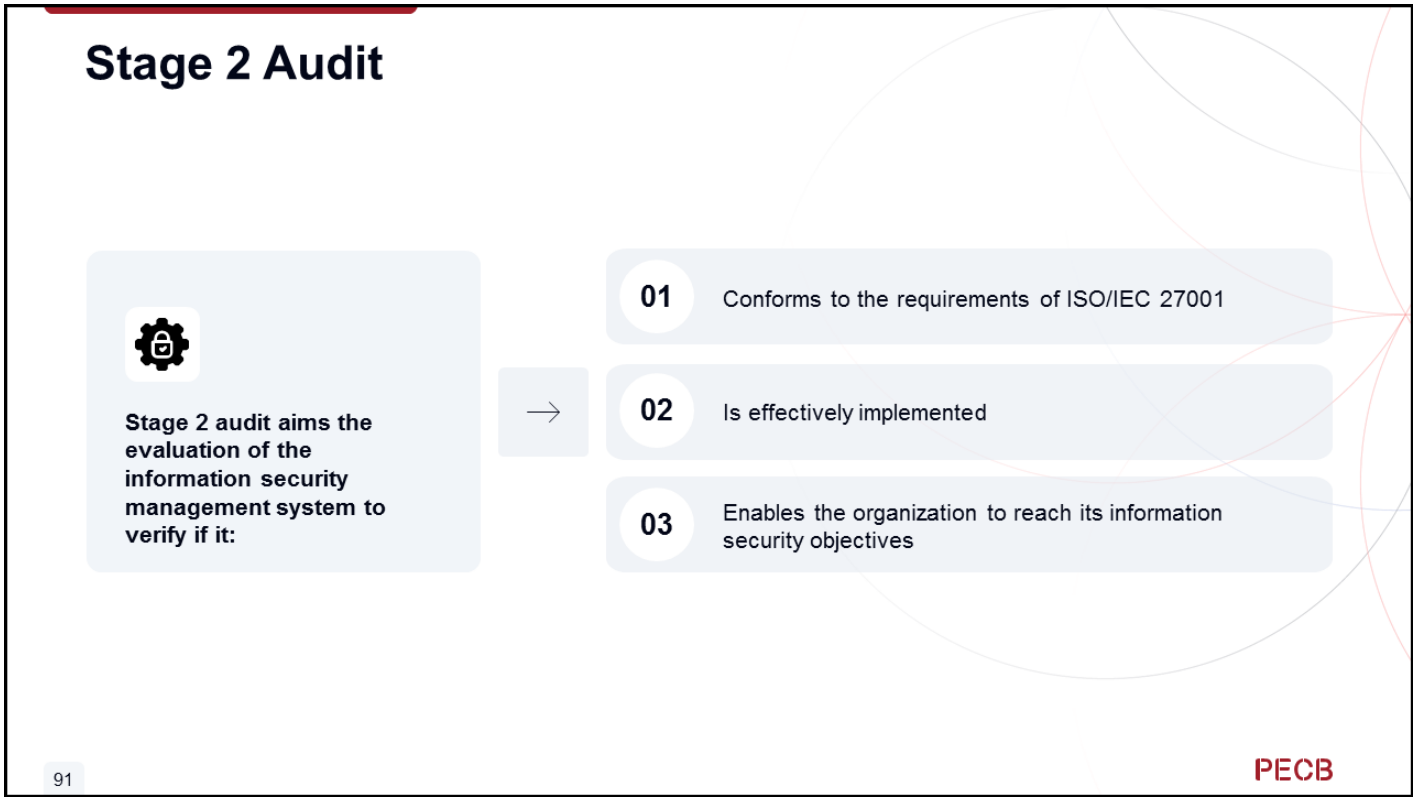


During the stage 1 audit, the auditor does not verify the effectiveness of the management system, but rather the design of the management system. The auditor will verify the effectiveness of the management system during the stage 2 audit (on-site audit) to validate whether the documented processes exist, are effective, and comply with the standard requirements.

Usually, 30% of the total time is spent on the stage 1 audit.

The stage 1 audit should not be conducted too far from the stage 2 audit, so that the management system does not change substantially between the two stages. It should, however, be conducted far enough apart to prepare the on-site audit plan. The stage 1 audit ideally takes place two to four weeks before the stage 2 audit (on-site).

It is noteworthy that although a confidentiality agreement is signed, the auditee has the right to require that the documented information review takes place on-site and that no documented information is carried off-site.



ISO/IEC 17021-1, clause 9.3.1.3 Stage 2

The purpose of stage 2 is to evaluate the implementation, including effectiveness, of the client's management system. The stage 2 shall take place at the site(s) of the client. It shall include the auditing of at least the following:

a. *information and evidence about conformity to all requirements of the applicable management system standard or other normative documents;*
b. *performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document);*
c. *the client's management system ability and its performance regarding meeting of applicable statutory, regulatory and contractual requirements;*
d. *operational control of the client's processes;*
e. *internal auditing and management review;*
f. *management responsibility for the client's policies.*

Certification Recommendation

When concluding the audit, the auditor must issue one of the four following recommendations related to certification:

1	2	3	4
Recommendation for certification	Recommendation for certification conditional upon the filing of corrective action plans **without prior visit**	Recommendation for certification conditional upon the filing of corrective action plans **with prior visit**	Unfavorable recommendation for certification

92

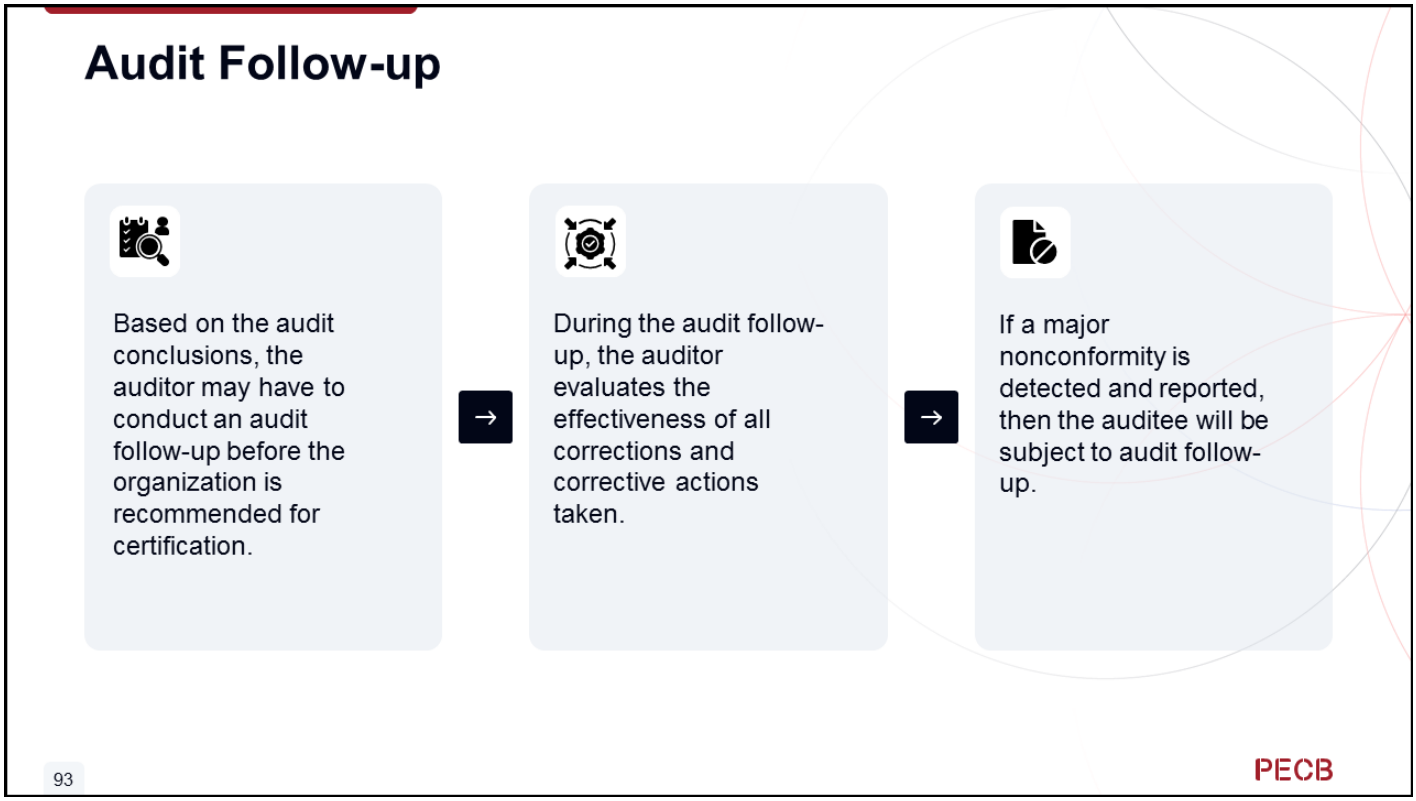
PECB

1.Recommendation for certification: Based on the evidence gathered during the audit, the auditor is confident that the auditee is in conformity to the requirements of the standard. The auditor did not detect any nonconformity during the audit.

2.and 3. Recommendation for certification conditional upon the filing of corrective action plans: The auditor is confident that the auditee is in conformity to the requirements of the standard. However, the auditor detected a few minor nonconformities. As such, the auditee is required to submit corrective actions plans for each minor nonconformity within a short period of time. If the corrective action plans are accepted, the auditee can then be certified. There are some cases when the auditor requires a new on-site visit prior to issuing a favorable certification recommendation. If there is no additional on-site visit required, the corrective action plans will be verified and validated during the surveillance audit visits.

4.Unfavorable recommendation for certification: The auditor is confident that the auditee is not in conformity to the requirements of the standard. The auditor detected one or more major nonconformities during the audit. As such, the auditor issues an unfavorable recommendation. It is worth mentioning that there are no public statements made about organizations that received unfavorable recommendation. A public statement is made for organizations that received favorable recommendation (except in some cases).

Please note that the auditor only issues a recommendation for certification. The final certification decision is made by the certification committee of the certification body.



The audit follow-up activities should be planned carefully and in detail just as the other steps included in the conduct of the audit. The audit follow-up's objective is to validate the actions plans and the implemented corrective actions submitted by the auditee. If any major nonconformity is detected, the auditee must resolve them before being recommended for certification.

The audit follow-up is usually conducted 4 to 12 weeks after the initial audit so that the auditee is given time to implement the corrective actions. The conduct of audit follow-up is usually completed within a day.

ISO 19011, clause 6.7 Conducting audit follow-up

The outcome of the audit can, depending on the audit objectives, indicate the need for corrections, or for corrective actions, or opportunities for improvement. Such actions are usually decided and undertaken by the auditee within an agreed timeframe. As appropriate, the auditee should keep the individual(s) managing the audit program and/or the audit team informed of the status of these actions.

The completion and effectiveness of these actions should be verified. This verification may be part of a subsequent audit. Outcomes should be reported to the individual managing the audit program and reported to the audit client for management review.

Certification Decision

The certification body must take the certification decision based on:

- An evaluation of the results and conclusions of the audit
- Other relevant information (for example, public information or client comments on the audit report)

Note: Auditors that take part in the audit never take part in the certification decision.

94

PECB

ISO/IEC 17021-1, clause 9.5.1.1

The certification body shall ensure that the persons or committees that make the decisions for granting or refusing certification, expanding or reducing the scope of certification, suspending or restoring certification, withdrawing certification or renewing certification are different from those who carried out the audits. The individual(s) appointed to conduct the certification decision shall have appropriate competence.

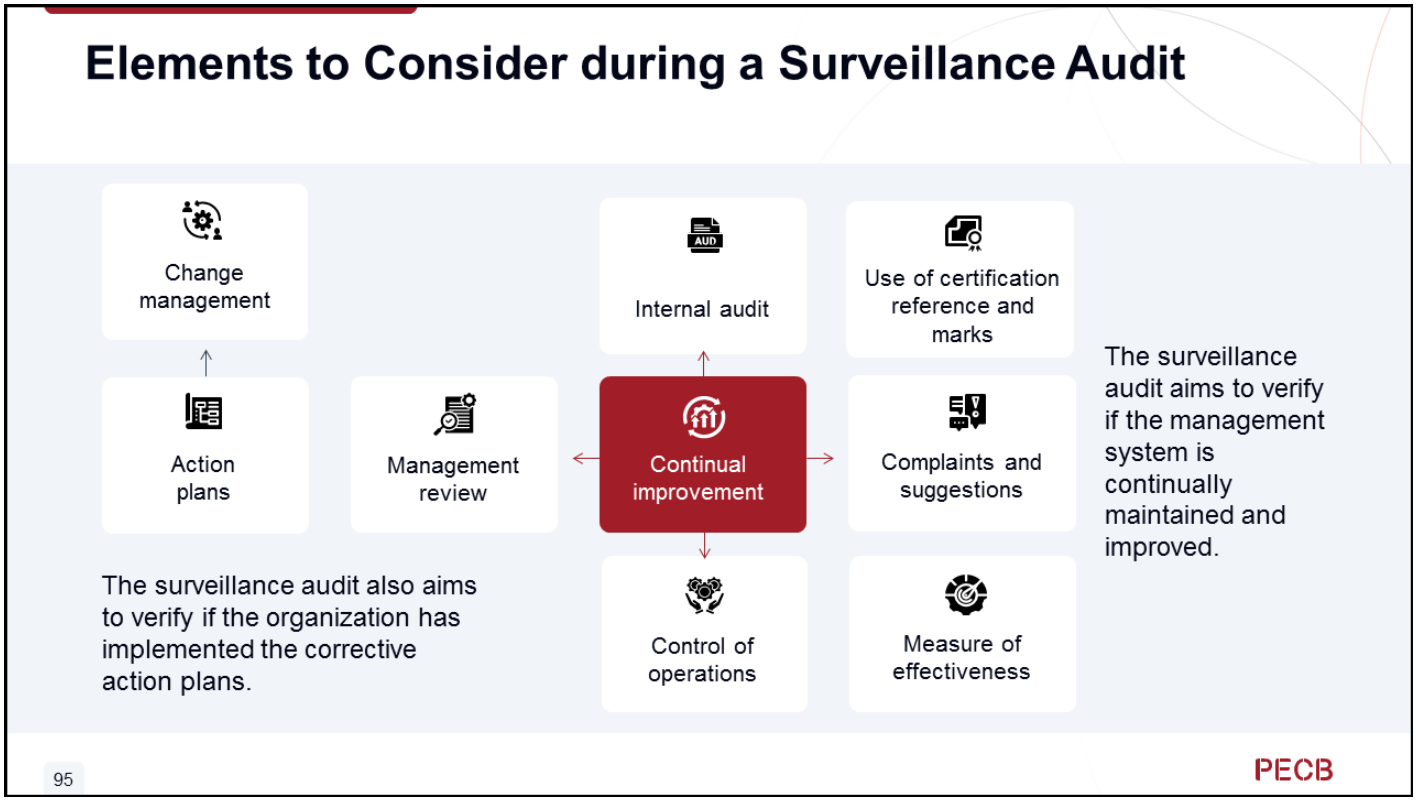
ISO/IEC 17021-1, clause 9.5.3.1

The information provided by the audit team to the certification body for the certification decision shall include, as a minimum:

a. *the audit report;*
b. *comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client;*
c. *confirmation of the information provided to the certification body used in the application review;*
d. *confirmation that the audit objectives have been achieved;*
e. *a recommendation whether or not to grant certification, together with any conditions or observations.*

ISO/IEC 17021-1, clause 9.5.3.2

If the certification body is not able to verify the implementation of corrections and corrective actions of any major nonconformity within 6 months after the last day of stage 2, the certification body shall conduct another stage 2 prior to recommending certification.



ISO/IEC 17021-1, clause 9.6.2.2 Surveillance audit

Surveillance audits are on-site audits, but are not necessarily full system audits, and shall be planned together with the other surveillance activities so that the certification body can maintain confidence that the client's certified management system continues to fulfill requirements between recertification audits.

Each surveillance for the relevant management system standard shall include:

a. *internal audits and management review;*
b. *a review of actions taken on nonconformities identified during the previous audit;*
c. *complaints handling;*
d. *effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system (s);*
e. *progress of planned activities aimed at continual improvement;*
f. *continuing operational control;*
g. *review of any changes;*
h. *use of marks and/or any other reference to certification.*

Recertification Audit

ISO/IEC 17021-1, clauses 9.6.3.1.1 and 9.6.3.1.2

- *The purpose of the recertification audit is to confirm the continued conformity and effectiveness of the management system as a whole, and its continued relevance and applicability for the scope of certification.*
- *A recertification audit shall be planned and conducted to evaluate the continued fulfilment of all of the requirements of the relevant management system standard or other normative document.*
- *This shall be planned and conducted in due time to enable for timely renewal before the certificate expiry date.*
- *The recertification activity shall include the review of previous surveillance audit reports and consider the performance of the management system over the most recent certification cycle.*

96

PECB

ISO/IEC 17021-1, clause 9.6.3.1.3

Recertification audit activities may need to have a stage 1 in situations where there have been significant changes to the management system, the organization, or the context in which the management system is operating (e.g. changes to legislation).

NOTE: Such changes can occur at any time during the certification cycle and the certification body might need to perform a special audit, which might or might not be a two-stage audit.

ISO/IEC 17021-1, clause 9.6.3.2.1

The recertification audit shall include an on-site audit that addresses the following:

a. *the effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification;*
b. *demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance;*
c. *the effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system(s).*

Use of ISO Trademarks

- A certified auditee is authorized to publicly display its certification and use it for marketing purposes.
- The certification cannot be displayed directly on a product or in a way that would lead to believe that the product is certified.
- The certification body will provide the auditee with a logo that can be used for marketing purposes.
- The unauthorized use of ISO trademarks could mislead, create false impressions, or cause confusion. Therefore, the ISO trademarks must not be used with the intention to express the certification of a product, person, or organization since ISO does not perform certifications.

97

PECB

ISO/IEC 17021-1, clause 8.3.1

A certification body shall have rules governing any management system certification mark that it authorizes certified clients to use. These rules shall ensure, among other things, traceability back to the certification body. There shall be no ambiguity, in the mark or accompanying text, as to what has been certified and which certification body has granted the certification. This mark shall not be used on a product nor product packaging nor in any other way that may be interpreted as denoting product conformity.

ISO/IEC 17021-1, clause 8.3.2

A certification body shall not permit its marks to be applied by certified clients to laboratory test, calibration or inspection reports or certificates.

Section 26 Summary

- Certification is a formal procedure which attests to a status or a level of achievement by providing an official document, whereas attestation refers to a method used to check, confirm, and authenticate the validity of a document.
- An accreditation body is an authoritative, independent organization that verifies whether a conformity assessment body meets established criteria and is competent to carry out conformity assessment tasks.
- Certification bodies certify management systems (ISO/IEC 17021-1), persons (ISO/IEC 17024), and products, processes, and services (ISO/IEC 17065).
- A certified auditee is authorized to publicly display its certification and use it for marketing purposes.
- ISO trademarks must not be used with the intention to express the certification of a product, person, or organization, since ISO does not perform certifications.

Questions?

Quiz 27

Note: To complete Quiz 27, please go to the Quizzes Worksheet.

Note: To complete the Scenario-based Quiz 4, please go to the Quizzes Worksheet.

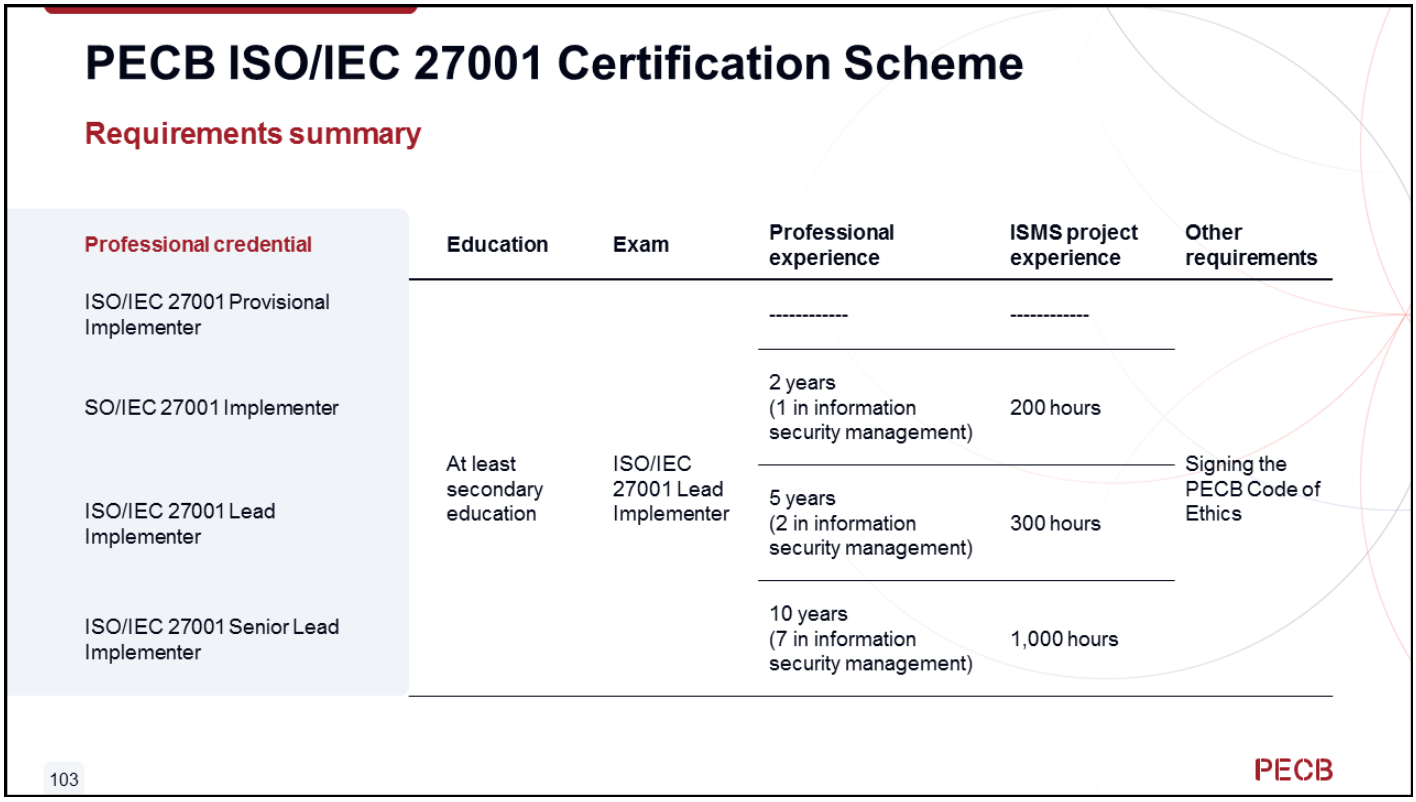
Day 4 Summary

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

- Monitoring, measurement, analysis, and evaluation
- Internal audits Types of audits, internal audits, and internal audit programs
- Management reviews
- Treatment of nonconformities, corrections, corrective actions, and preventive actions
- Maintenance and continual improvement of the ISMS
- Management system certification process

Note: To complete Homework 11-12, please go to the Exercises Worksheet.

This section provides information that will help participants gain knowledge on the PECB certification scheme and process.



The main implementer credentials:

1. The **"Certified Provisional Implementer"**credential recognizes that individuals have the basic knowledge to participate in the implementation and management of a management system.
2. The **"Certified Implementer"**credential recognizes that individuals have the necessary knowledge to participate in the implementation and management of a management system.
3. The **"Certified Lead Implementer"**credential recognizes that individuals are equipped with the skills needed to implement a management system and possess the competences of managing a team.
4. The **"Certified Senior Lead Implementer"** credential is targeted toward professionals who have extensive experience in implementation projects.

Attestation of Course Completion

After completing the training course and submitting the **Training Course Evaluation Form**, an Attestation of Course Completion will be generated at myPECB Dashboard, under the **My Courses** tab. The Attestation of Course Completion is worth 31 CPD credits.

104

PECB

Note: It is important to not confuse the Attestation of Course Completion with the actual certificate. The former is only a confirmation of having participated a training course, not gaining a certificate. To obtain a certificate, candidates will have to pass the exam, apply for certification, and get certified once the evaluation of the application is approved.

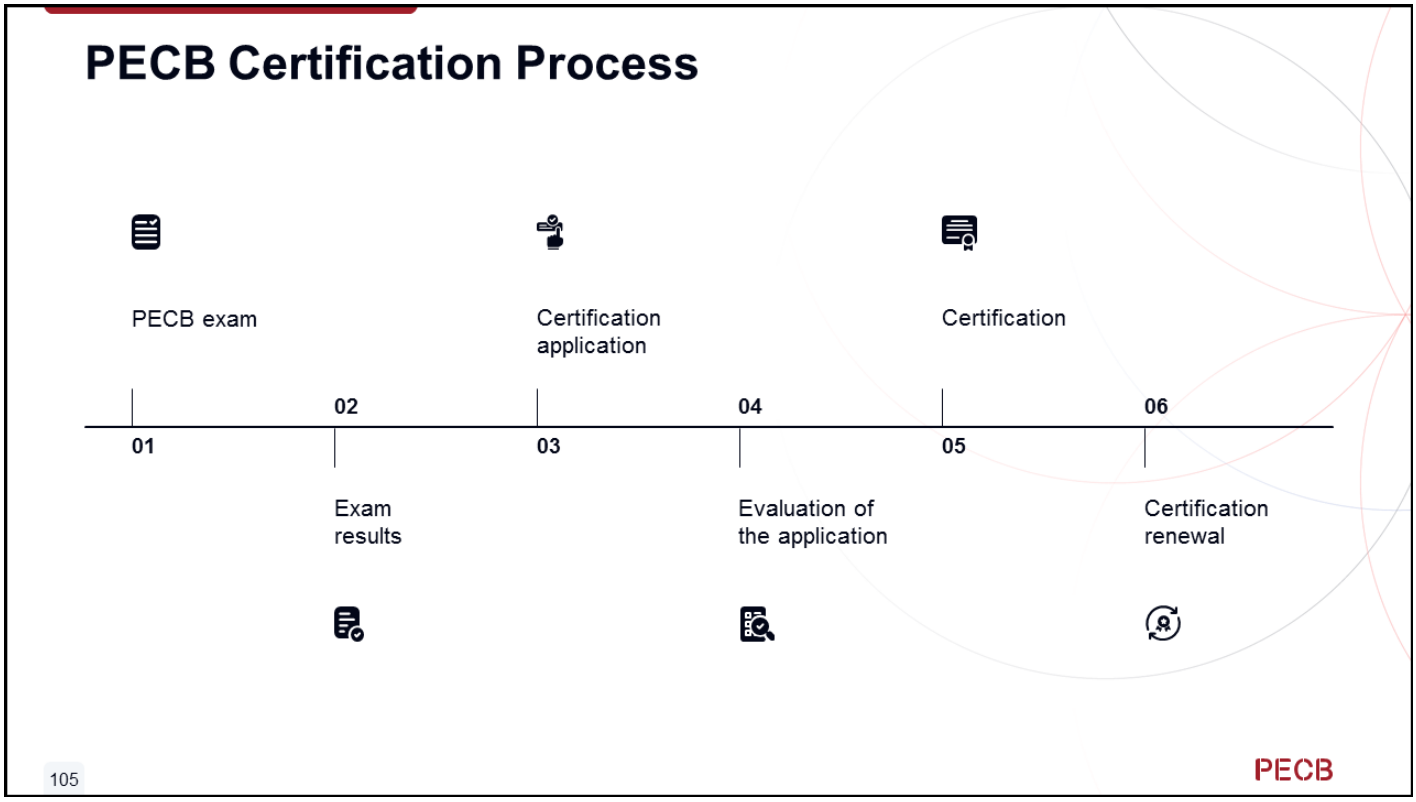
PECB Support

We are committed to continuously enhancing the quality and practical relevance of our training courses. Your feedback is invaluable in helping us achieve this goal, and we kindly invite you to share your evaluation of the training course and the trainer.

If you have suggestions for improving PECB's training course materials, we encourage you to reach out through one of the following methods:

- Open a ticket via PECB's Help Center at https://help.pecb.com/
- Send an email to support@pecb.com.
- Submit feedback through the KATE application

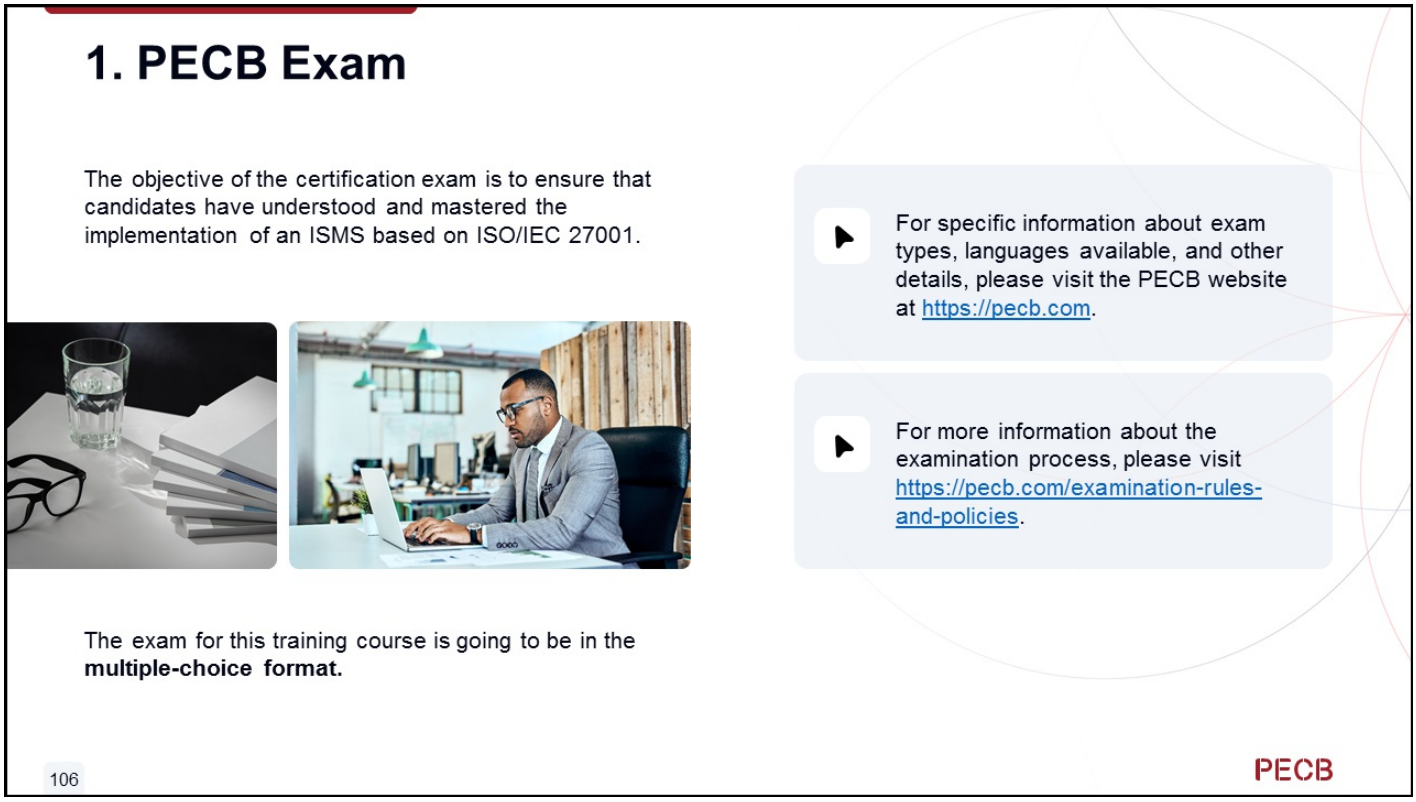
Additionally, if you experience any issues or dissatisfaction related to our partner, the training session (e.g., facilities, equipment), the exam, or the certification process, please contact us through the channels listed above. Your input helps us ensure a positive experience for all our members.



Passing the exam is not the only prerequisite to obtain the "PECB Certified ISO/IEC 27001 Lead Implementer" credential. The professional experience records will also be taken into account. If candidates have successfully passed the exam but do not have the required level of experience, they will not be able to claim the "PECB Certified ISO/IEC 27001 Lead Implementer" credential.

Important note: Candidates who have completed the training course with one of our partners, are provided with a coupon code that includes two exam attempts (first take and retake), certification application and the first year of Annual Maintenance Fee (AMF). This coupon code is valid within a 12-month period from the receive date.

For detailed information on the certification process, please go to https://pecb.com/pecb-certification-process.



The PECB Examination Committee ensures that the development and adequacy of the exam questions are maintained based upon current professional practice.

To take an exam in a particular language, please ask the trainer or contact us by sending an email to examination@pecb.com.

All competency domains are covered in the exam. To read a detailed description of each competency domain, please visit the PECB website at https://pecb.com.

For **multiple-choice,open-book exams,** candidates are allowed to use the following reference materials:

- A hard copy of the main standard
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through PECB Exams app and/or printed)
- A hard copy dictionary

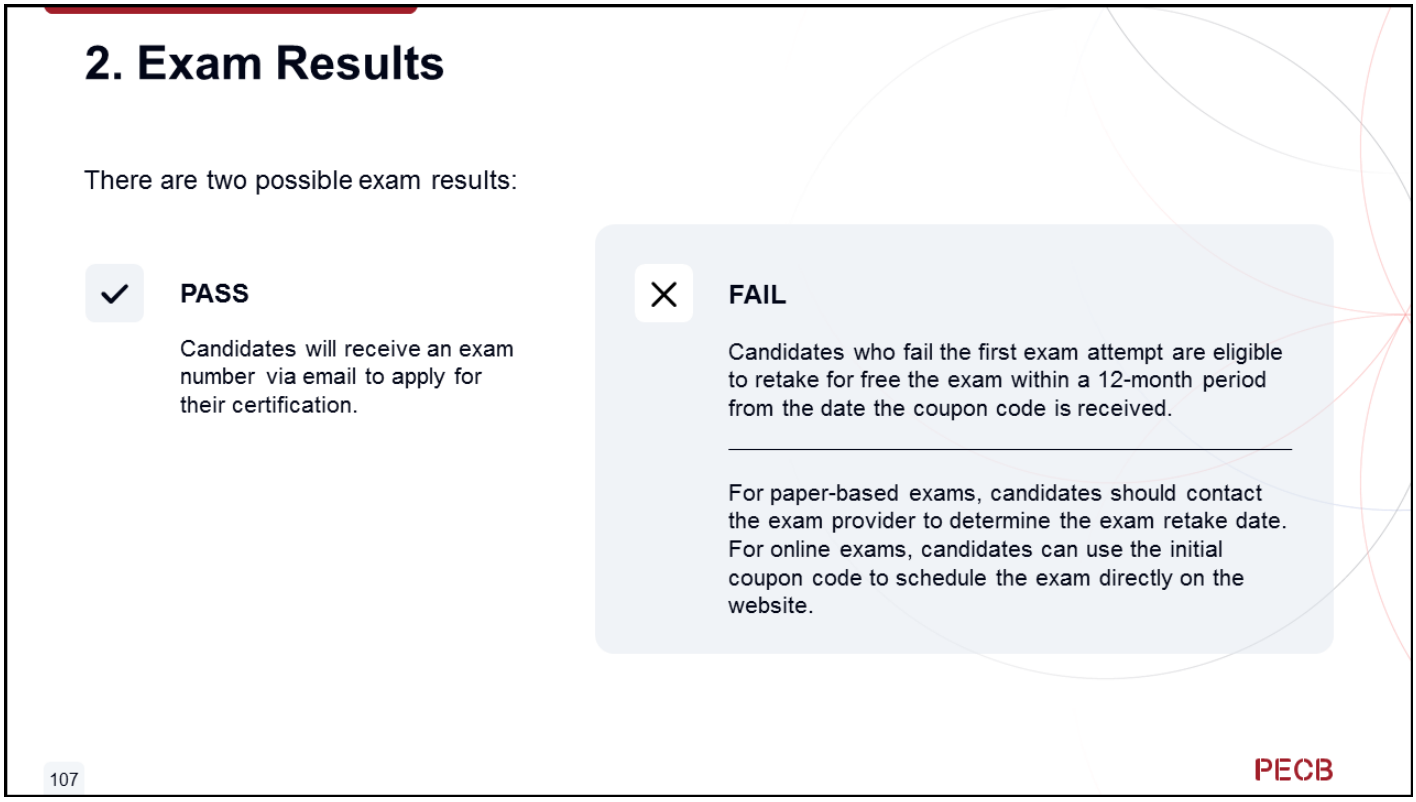
The multiple-choice, open-book exams include both stand-alone and scenario-based questions. These questions consist of a stem and three options used to evaluate the competency of a candidate in a multiple-choice exam. Only one of the options is correct.

What is the difference between stand-alone and scenario-based questions?

Stand-alone questions stand independently within the exam and are not context-depended, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario which a candidate is asked to read and is expected to provide answers to one or more questions related to that scenario.

Important note: Any candidate found cheating during the exam, including but not limited to the use of external tools such as ChatGPT or other AI applications, recording the exam, or taking screenshots of exam questions, will have their exam immediately terminated. The invigilator holds the authority to terminate the exam without prior notice if such actions are detected.

Furthermore, regardless of whether the candidate is sitting for their first attempt, they will not be granted a second attempt, even if it is offered free of charge.



Exams are reviewed by qualified examiners who are assigned anonymously.

To ensure independence and impartiality and to avoid conflicts of interest, trainers, training course organizers, and invigilators do not participate in the exam review process or the certification process.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

After successfully passing the exam, candidates have a period of one year to submit a professional file in order to obtain a professional credential related to the ISO/IEC 27001 certification scheme. Candidates may apply at the same time for more than one professional credential related to the ISO/IEC 27001 certification scheme (e.g., Lead Implementer, Senior Lead Implementer) if all requirements are met.

When applying, candidates must provide the following information:

1. **Their contact details**
   - Candidates should write their name as they wish it to appear on their certificate (in ASCII format). Before submitting their certificate application, candidates should make sure to review the accuracy of the contact details they have provided when creating their PECB Account. The certificate will be issued with the name that they provided when they created the account. To update the name in their PECB Account, candidates should contact support@pecb.com.
2. **Their professional and project experience records**
   - Candidates must provide a resume to present their professional experience. Work experience can be any activity showing that they have skills and general knowledge about the functioning of an organization.
   - For project experience, candidates should make sure to indicate the number of hours completed.
   - Educational degrees or the like do not replace work experience.
3. **At least two references**
   - References (colleagues, partners, supervisors, etc.) that candidates provide must confirm their experience. It is important that the references (those individuals) know the candidate enough to prove their qualifications.
   - The candidate's application will be assessed once the references have been submitted.
   - **Note:** Providing references is not required for credentials such as Foundation, Transition, and Provisional.

Certification Application

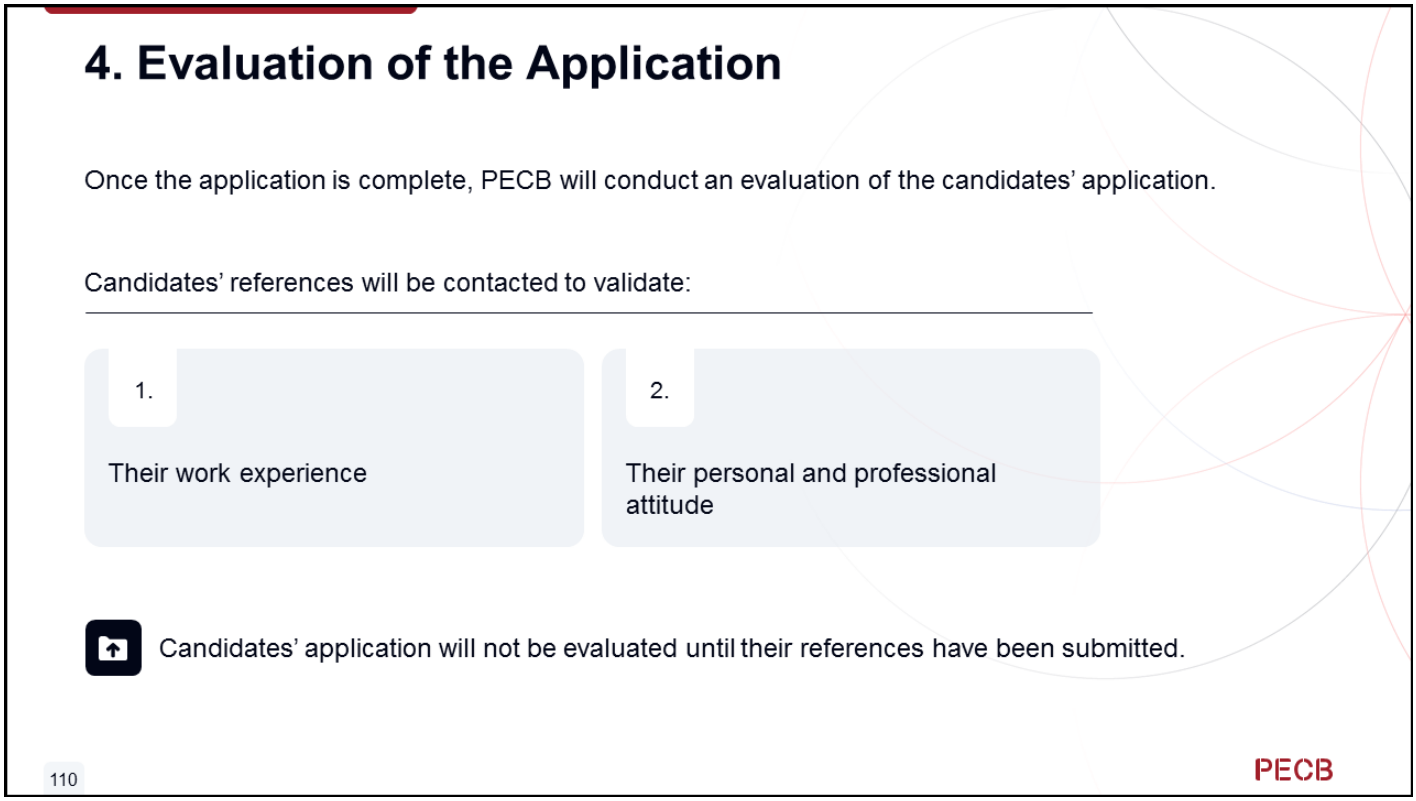
Professional experience records

ISMS implementation activities

- Drafting an ISMS implementation business case
- Managing an ISMS implementation project
- Implementing the ISMS
- Managing documented information
- Implementing corrective actions
- Monitoring the ISMS performance
- Managing an ISMS implementation team

For example, a consultant who has conducted a risk assessment for a client to accompany the implementation of its compliance framework will be considered as having relevant experience.

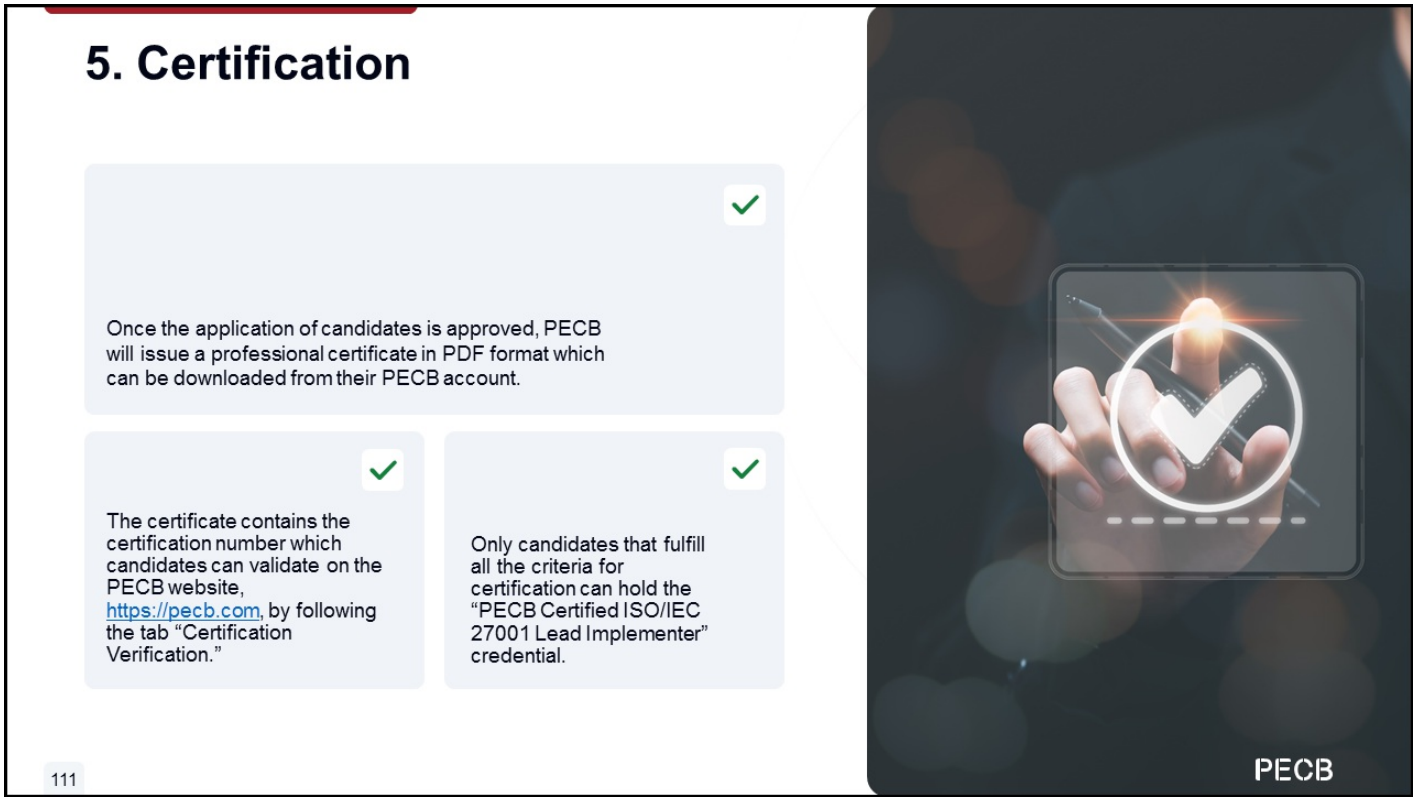
PECB



References will be contacted to complete a short questionnaire in order to attest to candidates' experience and evaluate their personal and professional qualities (according to the 13 Professional Behavioral Skills defined by ISO 19011).

Candidates can validate if their references have been submitted within their PECB Account under the **My Certifications** tab. If their respondents are late, candidates should follow up with them to ensure that they have received the reference request.

In case PECB is unable to contact one of the references or the questionnaires were not answered, candidates will be asked to provide further references.



When candidates are certified, they receive a notification from the system to download the certificate from their PECB account.

PECB has partnered with Credly to offer you the chance to claim a digital badge. You can share the badges online safely and easily. For more information, please go to https://pecb.com/pecb-digital-badges.

6. Certification Renewal

PECB Certifications are valid for three years. In order to maintain and renew a certification, PECB certified professionals must:

- Submit CPDs (Continuing Professional Development)
- Pay AMFs (Annual Maintenance Fee)
- Adhere to the PECB Code of Ethics

To renew their certification, PECB certified professionals must demonstrate sufficient hours of CPD activities related to the certification scheme. It is not mandatory to fulfill the required hours of CPD activities each year; they can instead be fulfilled within the three-year certification cycle.

In addition to CPDs, PECB Certified professionals will have to pay the AMFs (discussed on the following slides).

112

PECB

PECB certification(s) can be renewed online through the PECB Dashboard, by logging into the dashboard (https://pecb.com/en/login), clicking **My Certifications**, and then the **Renew** button. If after three years the recertification requirements are met, the certification will be renewed.

Continuing Professional Development

- Continuing Professional Development (CPD) is a portfolio structure for demonstrating, documenting, and tracking the skills, knowledge, and experience acquired by professionals after their initial certification. CPDs are important for updating professional experience, acknowledging achievements, and demonstrating professional activities conducted.
- PECB certified professionals will need to provide PECB with the required hours of auditing-related tasks they have performed and/or other CPD activities that are considered eligible. CPDs can be submitted at any time, by logging into your PECB Dashboard, and clicking on **My Certifications > CPD Info > Submit CPD.**

Certification	Annual CPD hours	3-year/Total CPD hours	Activities
Implementer	20 hours	60 hours	Hours of project experience, implementation, or consulting-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities
Lead Implementer	30 hours	90 hours	
Senior Lead Implementer	60 hours	180 hours	

113

PECB

To support certified professionals earn CPD credits, PECB continually organizes webinar sessions, provides opportunities for writing articles, participating in trainings and events, and more.

To learn more about CPDs obtained with PECB or other means, the CPD categories, their descriptions, the evidence required, the number of CPD credits awarded, and how to calculate CPDs, please visit our published CPD policy at https://pecb.com/pdf/brochures/cpd-policy.pdf.

Annual Maintenance Fee

- A PECB certification requires the payment of Annual Maintenance Fees (AMF). The annual reporting begins with the initial certification date; however, the maintenance fee for the first year is included in the certification application payment.
- The annual maintenance fee can be paid online through your PECB dashboard, clicking ***My Certifications***, and then the ***Submit AMF*** button. If CPDs have not been submitted, certified professionals will be required to do so before the AMF payment.
- For the last year of the certification cycle, the button to pay the AMF will be changed from ***Submit AMF*** to ***Renew***.

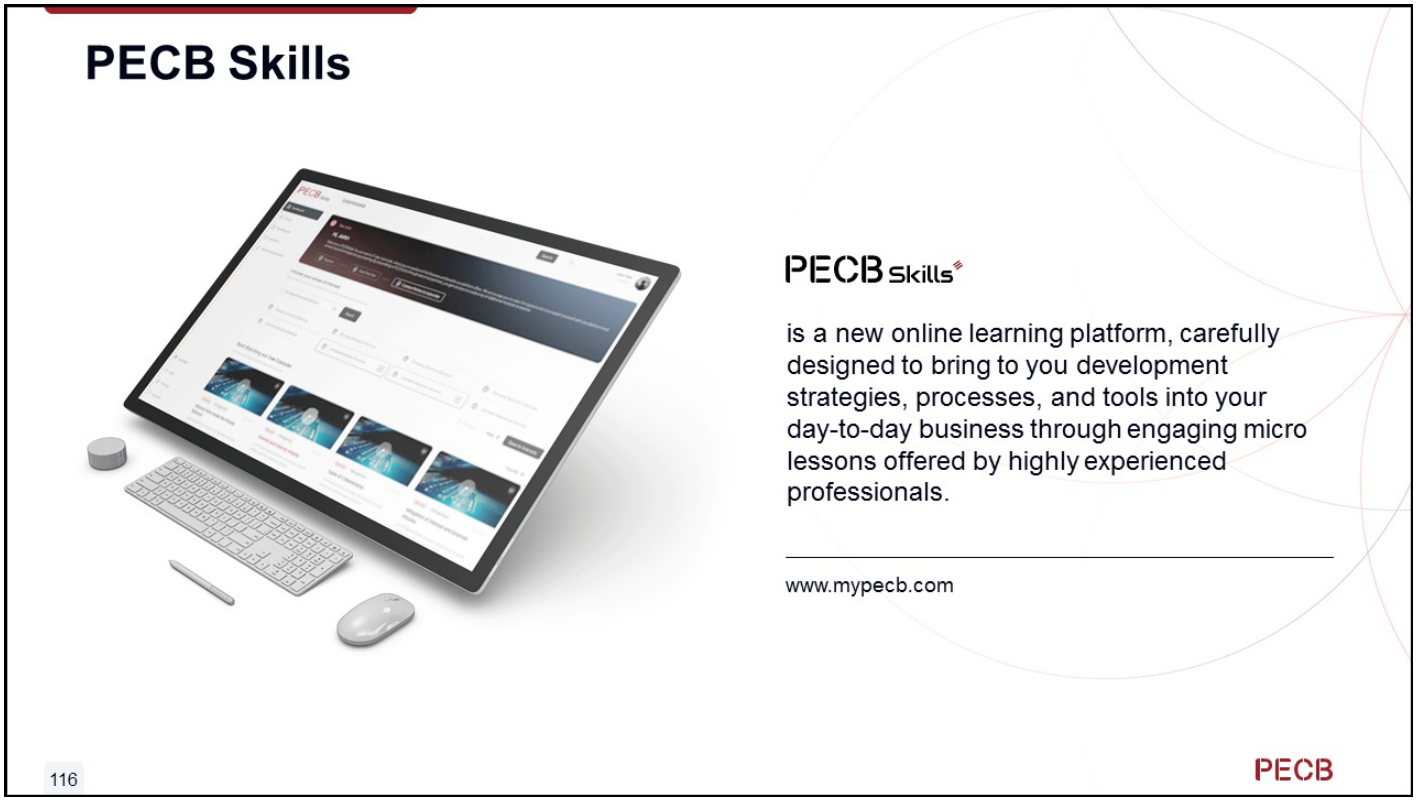
Certification	AMF (rate per year)
Foundation, Provisional, and Transition	None
All other certifications	$120

114

For example, if a certification was issued on 2019-01-15 and is valid until 2022-01-15, the following requirements apply:

- **First AMF:** 2019-01-15 until 2020-01-15 – No payment of AMF required
- **Second AMF:** 2020-01-15 until 2021-01-15 – Payment of AMF required
- **Third AMF:** 2021-01-15 until 2022-01-15 – Payment of AMF required

If the certified professional fails to fulfill either of these CPD or AMF requirements, the certification will be downgraded.



PECB Skills offers interactive micro lessons for all core content areas and more, thus providing professionals with a plethora of choices.

- **Information security:** Equip yourself with the skills to protect vital data and maintain the integrity of information systems
- **Cybersecurity:** Stay vigilant and ahead of cyber threats with best practices and advanced techniques
- **Privacy and data protection:** Delve into the critical aspects of safeguarding personal data and ensuring privacy in an interconnected world
- **Risk management:** Navigate through uncertainties with confidence, identifying and mitigating potential risks
- **Continuity, resilience, and recovery:** Learn to build robust systems, ensuring business continuity even in unforeseen circumstances
- **CMMC (Cybersecurity Maturity Model Certification):** Familiarize yourself with the defense standard for ensuring cybersecurity throughout the Defense Industrial Base (DIB)
- **GDPR (General Data Protection Regulation):** Master the European Union's benchmark regulation on data protection and privacy
- **NIST (National Institute of Standards and Technology):** Engage with guidelines and standards for ensuring cybersecurity and privacy, backed by one of the most reputable institutions in the field

With PECB Skills, you're not just learning; you are future-proofing your career and making strides in the dynamic digital ecosystem. For more information, please visit www.mypecb.com or contact us at marketing@pecb.com.

PECB Skills Certificates

Elevate your profile and unlock new opportunities through these recognitions which will further enhance your professional standing and growth:

- **Attestation of module completion:** Demonstrate proficiency in specific modules and receive 1 CPD credit.
- **Essentials certificate:** Demonstrate your competencies through a comprehensive 4-hour program, earning 4 CPD credits.

117

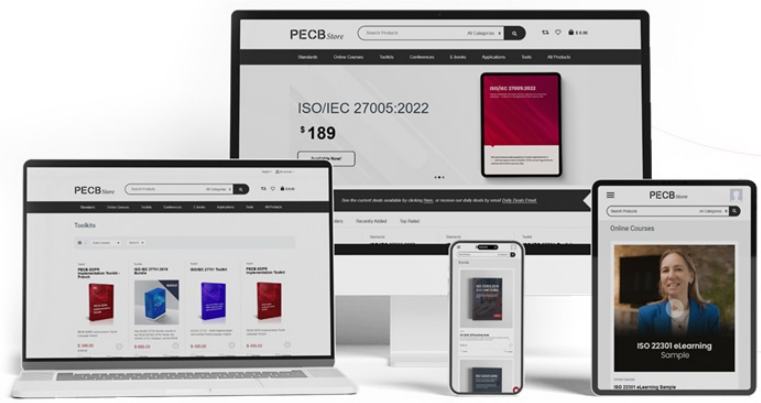
PECB

Our micro-courses are accredited by the ANSI National Accreditation Board (ANAB), a testament to their quality and adherence to rigorous educational standards.

Note: Modules comprise four short video capsules.

PECB Store

- Join PECB's online store and become part of our global network.
- Explore the wide range of standards, toolkits, and more.
- Advance your career from the comfort of your home through our digital platforms
- Buying online has never been easier!



https://store.pecb.com

118

PECB

PECB Store is PECB's online store where clients can purchase various ISO and IEC international standards, PECB Toolkits and eBooks, and many other related products and services that will be added in the future.

Standards mentioned on this training course are all available on PECB Store. We are committed to support the growth of our customers, which is why we offer you the opportunity to buy qualitative products on PECB Store and advance your professional career by applying the knowledge gained.

For more information, please visit https://store.pecb.com or contact us at store@pecb.com.

PECB Certified ISO/IEC 27005 Risk Manager (three days)

This training course helps participants become proficient in the fundamental concepts of the management of risks related to information security: planning of a risk management program, analysis, evaluation, risk treatment, risk communication, and surveillance. Through readings, exercises based on real cases, and discussions in class, the participants will be able to perform an optimal risk evaluation and manage risks through time by knowing its life cycle. Please note that this training course follows the framework of an ISO/IEC 27001 implementation process.

PECB Certified ISO/IEC 27001 Lead Auditor (five days)

The ISO/IEC 27001 Lead Auditor training course enables participants to develop the necessary ability to perform an information security management system (ISMS) audit by applying widely recognized audit principles, procedures, and techniques. During this training course, participants acquire the knowledge and skills to plan and carry out internal and external audits in compliance with ISO 19011 and the certification process according to ISO/IEC 17021-1.

Thank You!

 linkedin.com/company/pecb

 facebook.com/PECBInternational/

 instagram.com/pecb.official

 x.com/pecb

 youtube.com/pecbgroup

PECB