Version 7.1

Document number: ISMSLID4V7.1

Schedule of the Day

- Section 21: Monitoring, measurement, analysis, and evaluation
- Section 22: Internal audit
- Section 23: Management review
- Section 24: Treatment o nonconformities
- Section 25: Continual improvement
- Section 26: Preparing for the certification audit
- Section 27: Certification process and closing of the training course

PECB

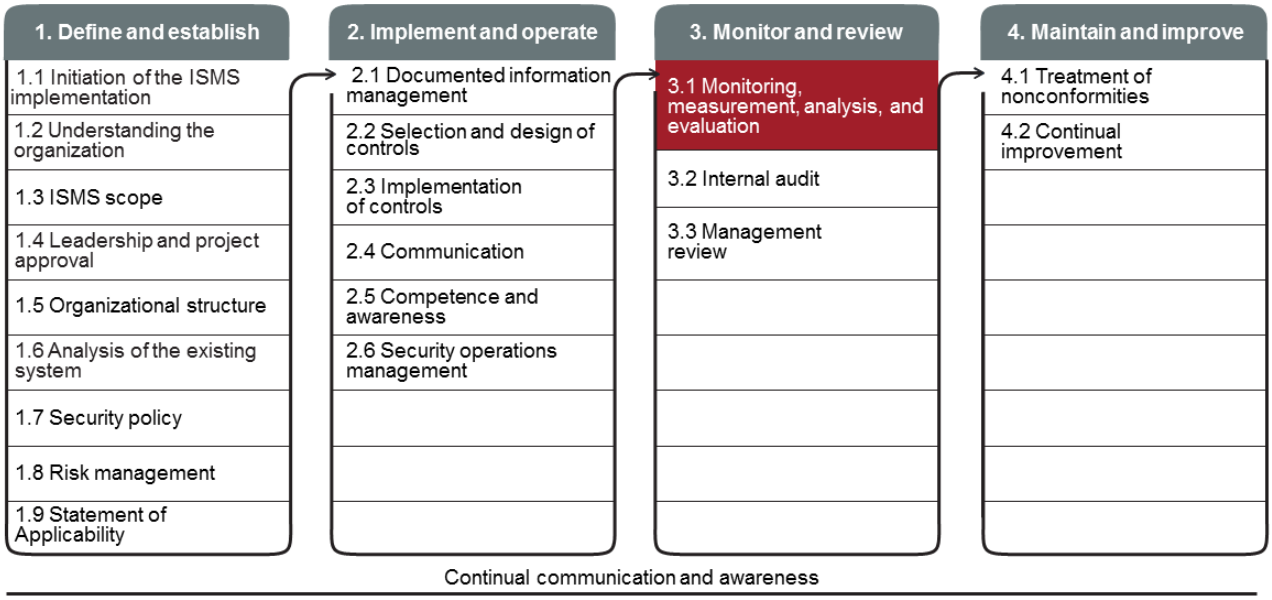
Learning Objectives of the Day

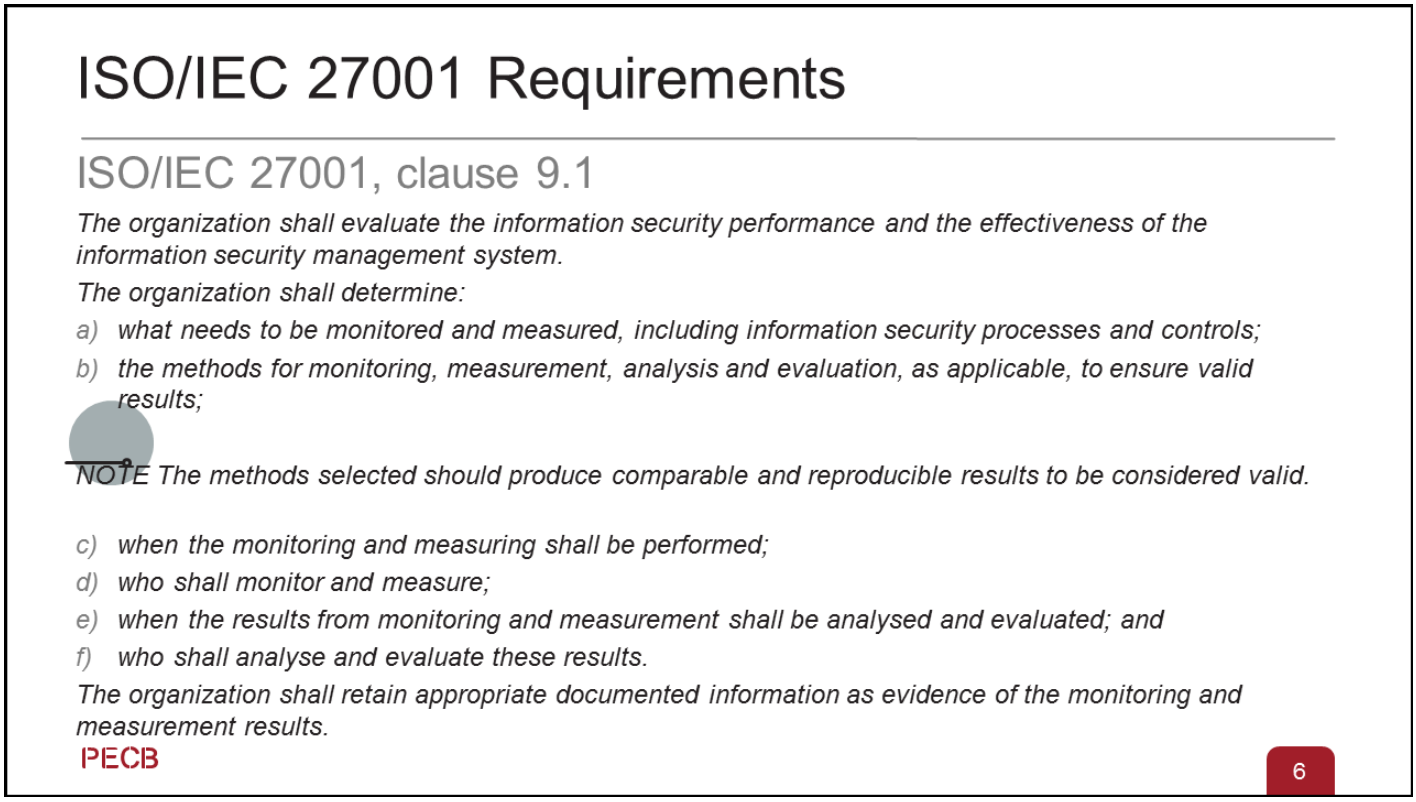
1. Acquire knowledge on how to monitor, measure, analyze, and evaluate the ISMS
2. Acquire knowledge on how to establish ISMS performance indicators
3. Acquire knowledge on how to create an internal audit program, plan and perform audit activities, and follow up on nonconformities
4. Acquire knowledge on how to prepare, conduct, and close a management review
5. Acquire knowledge on how to treat problems and nonconformities
6. Acquire knowledge on how to maintain and continually improve the ISMS
7. Acquire knowledge on how to prepare for the certification audit, stage 1 and stage 2 audit, and audit follow-up

PECB

This section aims at providing the 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.

3.1 Monitoring, Measurement, Analysis, and Evaluation





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

1. Determine what needs to be measured and monitored in the ISMS
2. Define the methods for monitoring, measurement, analysis, and evaluation
3. Gather the data for monitoring, measurement, analysis, and evaluation
4. Perform an analysis and evaluation of results

ISO/IEC 27003, clause 9.1 Monitoring, measurement, analysis and evaluation

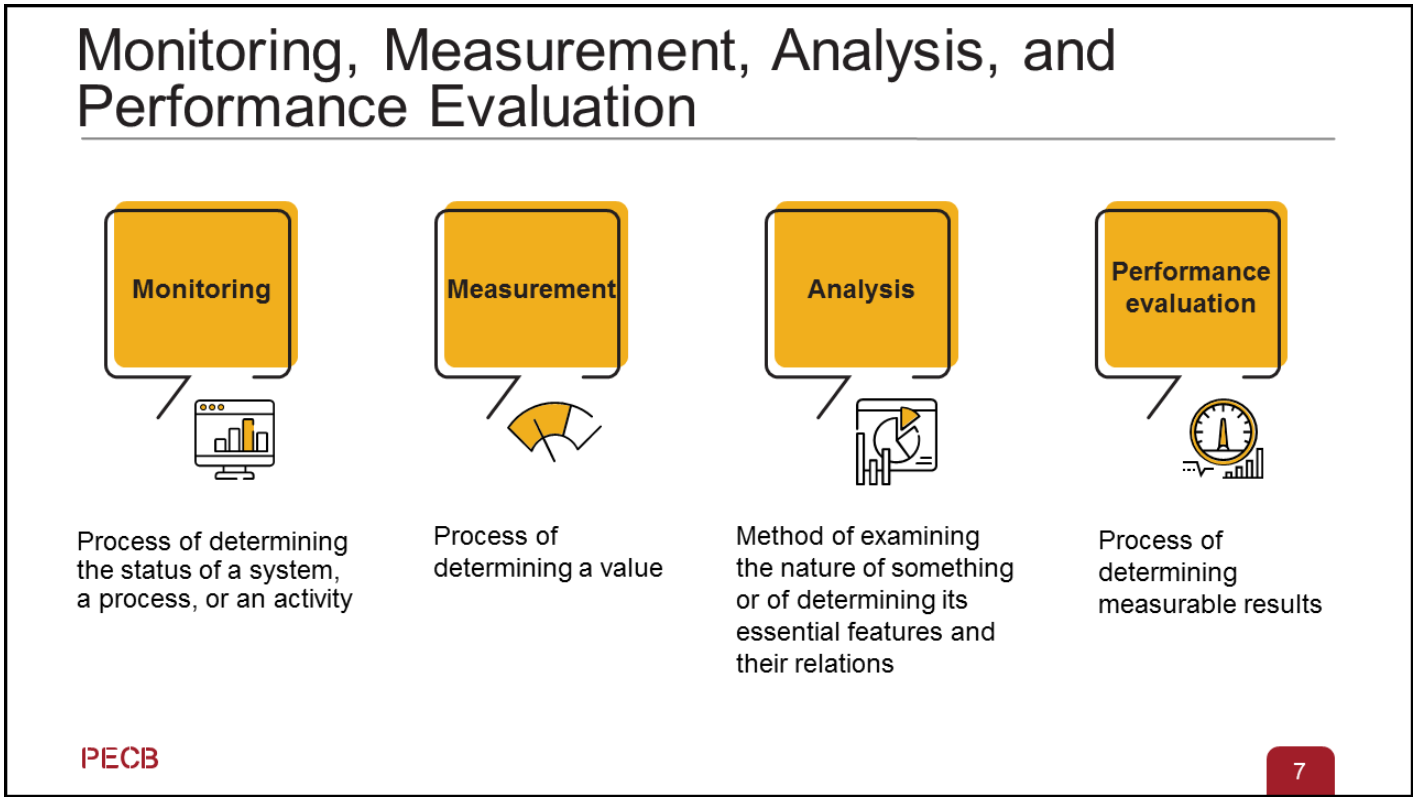
A good practice is to define the 'information need' when planning the monitoring, measurement, analysis and evaluation. An information need is usually expressed as a high level information security question or statement that helps the organization evaluate information security performance and ISMS effectiveness. 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, analysing 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.*

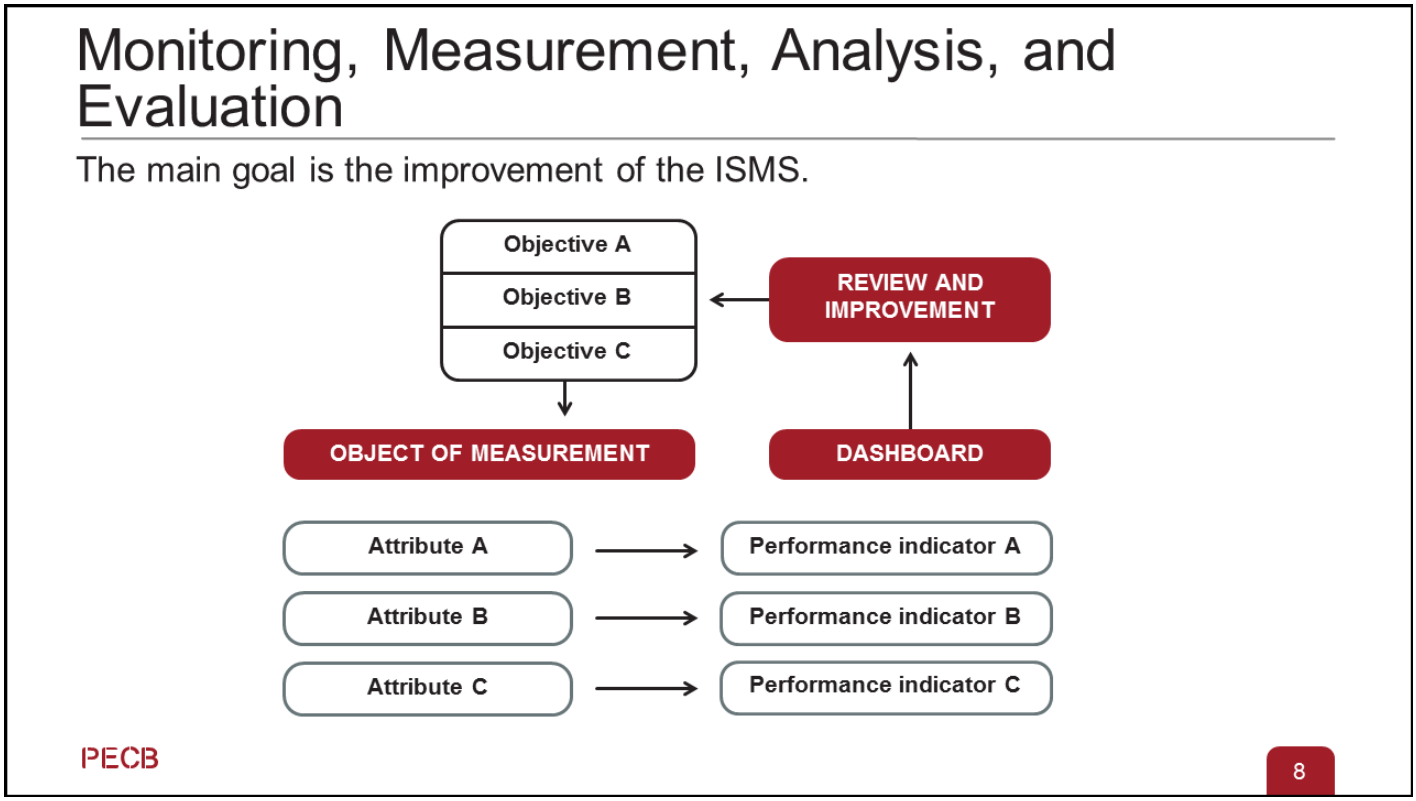


Measurement is the process of determining a value. Performance measurement can be defined as a systematic way of assessing an organization's current achievements against its objectives. Performance measures are of little value per se, unless they are viewed within the context of organizational strategies and objectives.

This holds true for management systems also, which cannot exist in a vacuum and must contribute to the objectives of the organization if they are to be effective. Measuring performance in this context should be a high priority on the agenda of individuals who are responsible for the implementation and maintenance of the management system.

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

- Implementing a systematic control to ensure the realization of processes
- Identifying deviations on a timely manner and treating them accordingly
- Allowing the users of the ISMS to make decisions regarding process results
- Determining the effectiveness and efficiency of processes
- Identifying opportunities for continual improvement



In summary, the monitoring and measuring process involves:

- Identifying the measurement objectives
- Selecting the attribute objects that can be measured
- Establishing the performance indicators
- Evaluating if the objectives are achieved and improving the management system

Example:

1. **Measurement objectives:** Ensure that 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:** % of the employees that have attended the awareness session

ISO/IEC 27004

Guidelines for measuring the performance and effectiveness of an ISMS

- The standard provides guidelines to help organizations in evaluating the ISMS performance in order to satisfy the requirements of ISO/IEC 27001.
- The standard exclusively addresses clause 9.1 *Monitoring, measurement, analysis and evaluation* of ISO/IEC 27001.
- Its elaborates on what and when to monitor and measure, establishing procedures, analyzing results, and reviewing and improving the processes of monitoring, measurement analysis, and evaluation.

PECB

9

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 fulfil the requirements of ISO/IEC 27001:2013, 9.1: monitoring, measurement, analysis and evaluation.

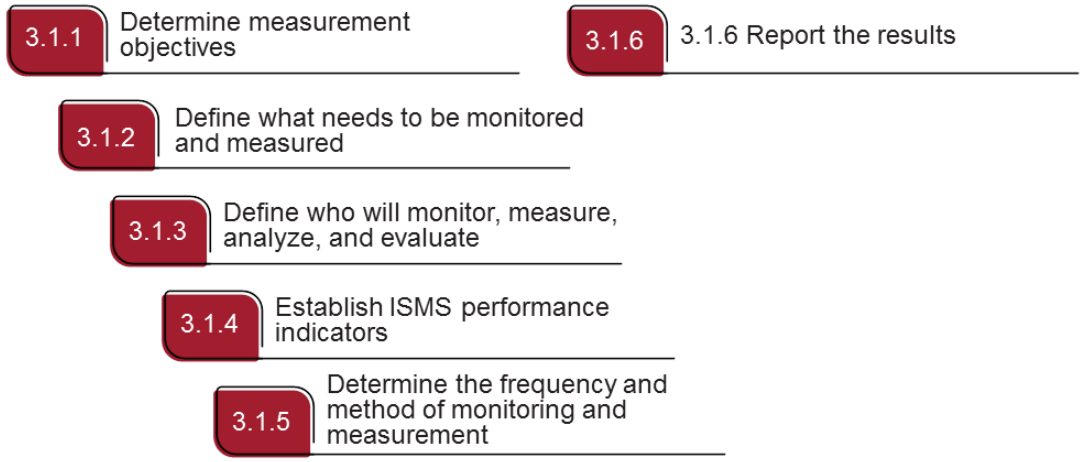
The results of monitoring and measurement of an information security management system (ISMS) can be supportive of decisions relating to ISMS governance, management, operational effectiveness and continual improvement.

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



PECB

3.1.1 Determine Measurement Objectives

- The organization should evaluate its management system in order to ensure its continual suitability, adequacy, and effectiveness.
- It is recommended to focus on monitoring and measuring activities that are linked to critical processes that enable the organization to achieve its information security performance objectives.
- Too many measures can distort an organization's focus and blur what is truly important.

PECB

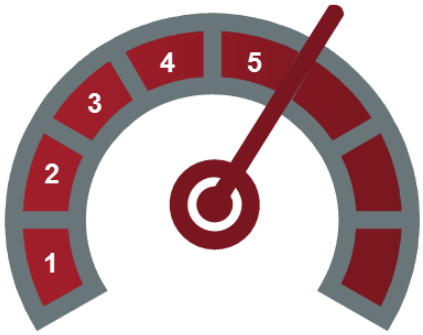
11

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

- Evaluating the effectiveness of the ISMS processes and procedures in place
- Verifying the extent to which standard requirements have been met
- Providing input for management reviews to facilitate decision-making and justify the needed improvements of the ISMS

3.1.2 Define What Needs to be Monitored and Measured

1. The extent to which the organization's information security objectives are met
2. The critical processes, procedures, and functions
3. Historical evidence of poor ISMS performance (e.g., nonconformities, near misses, false alarms, failures, incidents)



4. Compliance with applicable legal and regulatory requirements, industry best practices
5. Corrective and preventive actions used to treat nonconformities

PECB

12

ISO/IEC 27004, clause 6.1 General

In order to determine what to monitor and measure, the organization should first consider what it wishes to achieve in evaluating information security performance and ISMS effectiveness. This can allow it to determine its information needs.

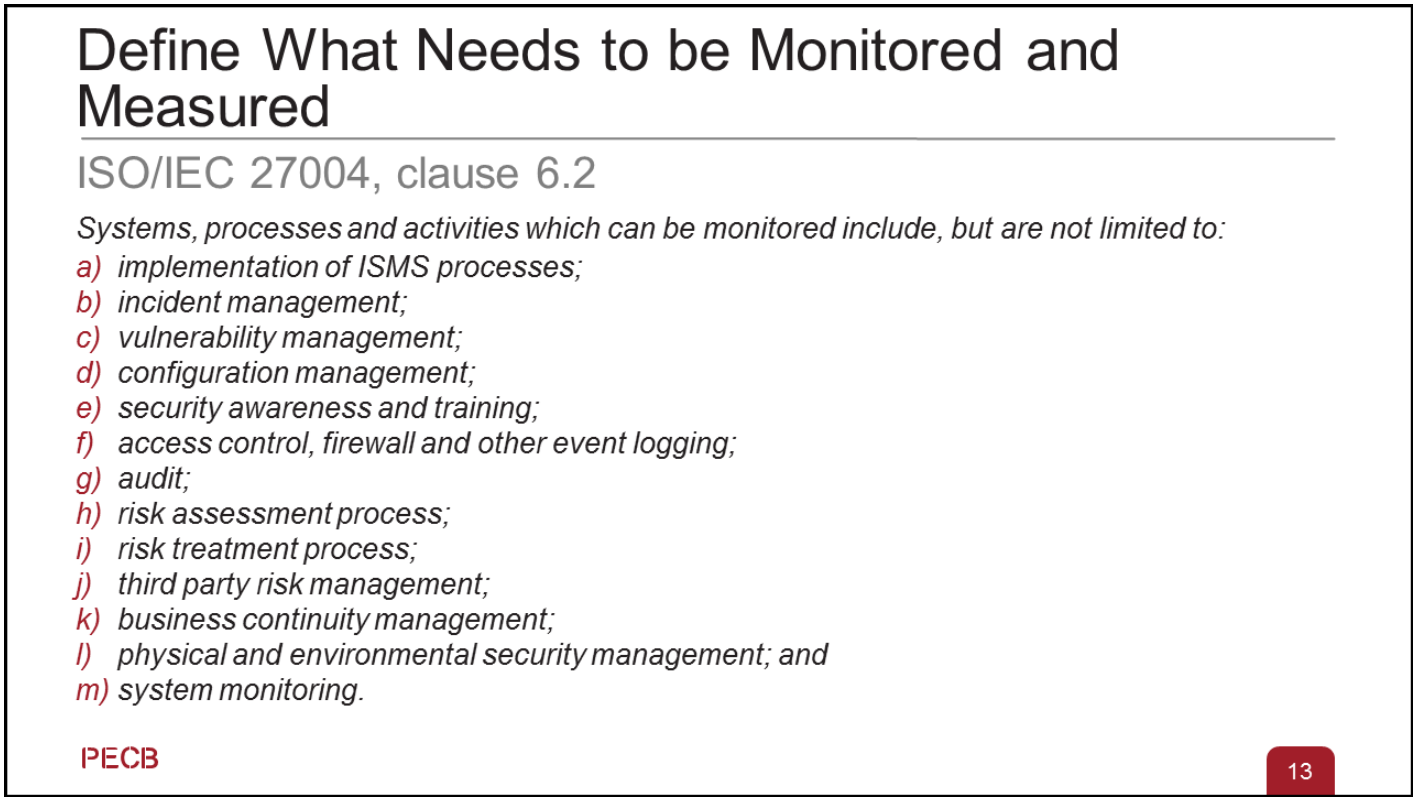
Organizations should next decide what measures are needed to support each discrete information need and what data are required to derive the requisite measures. Hence, measurement should always correspond to the information needs of the organization.

A minimum number of meaningful performance measures are far more preferable than a plethora of measures that do not relate to organizational objectives. Many organizations use the SMART (Specific-Measurable-Attainable-Realistic-Timely) methodology when developing their performance measures.

- **Specific:** Clear and focused to avoid misconception
- **Measurable:** Can be quantified and compared to other data
- **Attainable:** Achievable, reasonable, and acceptable in a particular context
- **Realistic:** Fits into the organization's culture and is cost-effective within the available resources
- **Timely:** Achievable within the set time frame

No singular set of generic measures will be effective for all organizations, and may not even be effective for organizations in similar environments. The final mix of measures will be a product of operational, legislative, and cultural context.

There are a number of performance measurement levels ranging from strategic high-level measures to more specific operational-or program-level measures. It is crucial for an organization to measure the activities that truly matter, and not waste time and resources on measuring activities simply because they can be measured. In terms of efficiency, an organization needs meaningful measures that will indicate what is really happening so that it can decide to either let an activity continue or intervene to take corrective action. In terms of effectiveness, an 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.

Define What Needs to be Monitored and Measured

ISO/IEC 27004, clause 6.3

ISMS processes and activities that are candidates for measurement include:

a) *planning;*
b) *leadership;*
c) *risk management;*
d) *policy management;*
e) *resource management;*
f) *communicating;*
g) *management review;*
h) *documenting; and*
i) *auditing.*

PECB

14

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.*

3.1.3 Define Who Will Monitor, Measure, Analyze, and Evaluate

ISO/IEC 27004, clause 6.5

Whether the measurement is performed manually or automatically, organizations can define the following measurement-related roles and responsibilities:

a) *measurement client: the management or other interested parties requesting or requiring information about the effectiveness of an ISMS, controls or group of controls;*
b) *measurement planner: the person or organizational unit that defines the measurement constructs that links measurable attributes to a specified information need;*
c) *measurement reviewer: the person or organizational unit that validates that the developed measurement constructs are appropriate for evaluating information security performance and the effectiveness of an ISMS, controls or group of controls;*
d) *information owner: the person or organizational unit that owns the information that provides input into measures. This person is responsible for providing the data and is also frequently (but not always) responsible for conducting measurement activities;*
e) *information collector: the person or organizational unit responsible for collecting, recording and storing the data;*
f) *information analyst: the person or organizational unit responsible for analysing data; and*
g) *information communicator: the person or organizational unit responsible for communicating the results of analysis.*

PECB

15

ISO/IEC 27004, clause 6.5 Who will monitor, measure, analyse 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.

3.1.4 Establish ISMS Performance Indicators

Examples

- Percentage of false alarms through event detection
- Average cost of an incident

- Percentage of employees who have received training
- No. of training hours per employee

- Percentage of systems tested for vulnerabilities in the last three months
- No. of days to close known vulnerabilities

- Percentage of nonconformity not corrected on time
- The average number of days required to fix a nonconformity

Incidents

Training

Vulnerabilities

Nonconformities

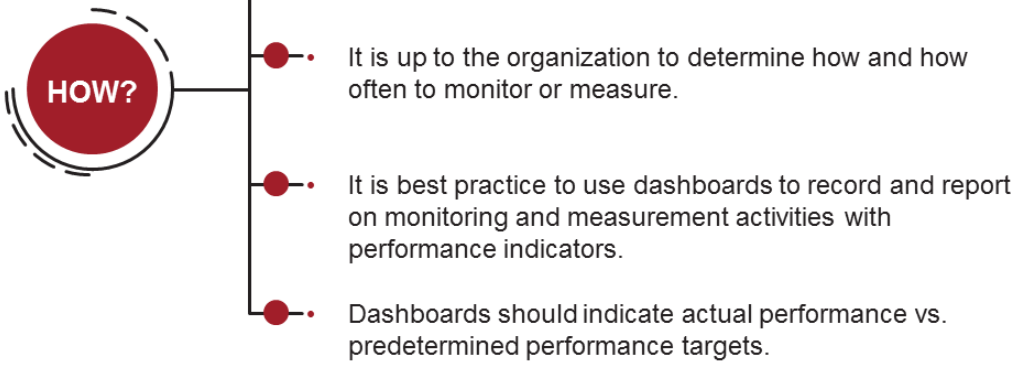
PECB

16

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

3.1.5 Determine the Frequency and Method of Monitoring and Measurement

How and when to monitor and measure?

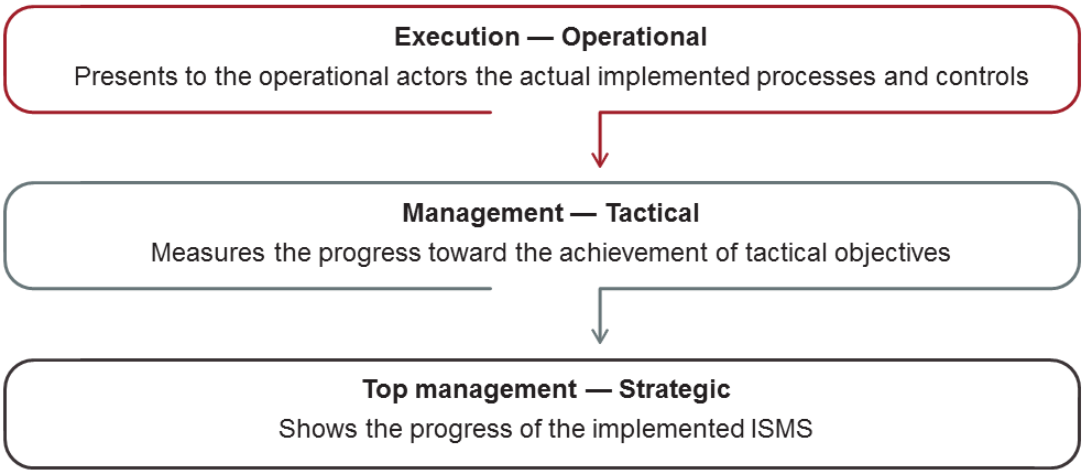


PECB

17

3.1.6 Report the Results

Examples of dashboards



PECB

18

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

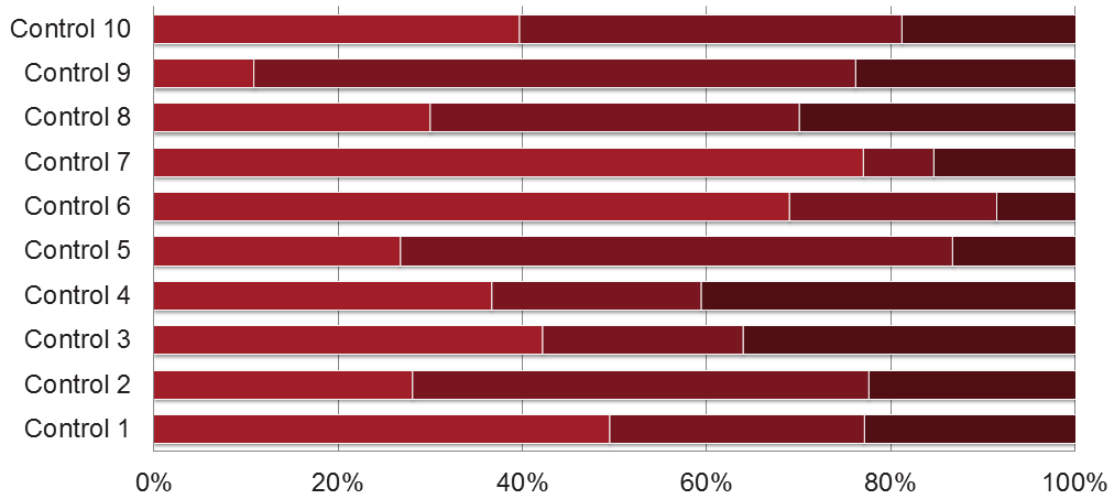
- **Tactical and operational dashboards** are less focused on strategic objectives and more tied to the effectiveness of specific controls or processes.
- **Scorecards or strategic dashboards** provide strategic information by integrating high-level indicators.
- **Reports** (from simple and static in 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



PECB

19

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	Control of documented information				X						
5	Information security risk assessment										X
6	Information security risk treatment								X		
7	Monitoring, measurement, analysis and evaluation					X					
8	Internal audit						X				
9	Management review								X		
10	Corrective action									X	
Overall assessment									X		

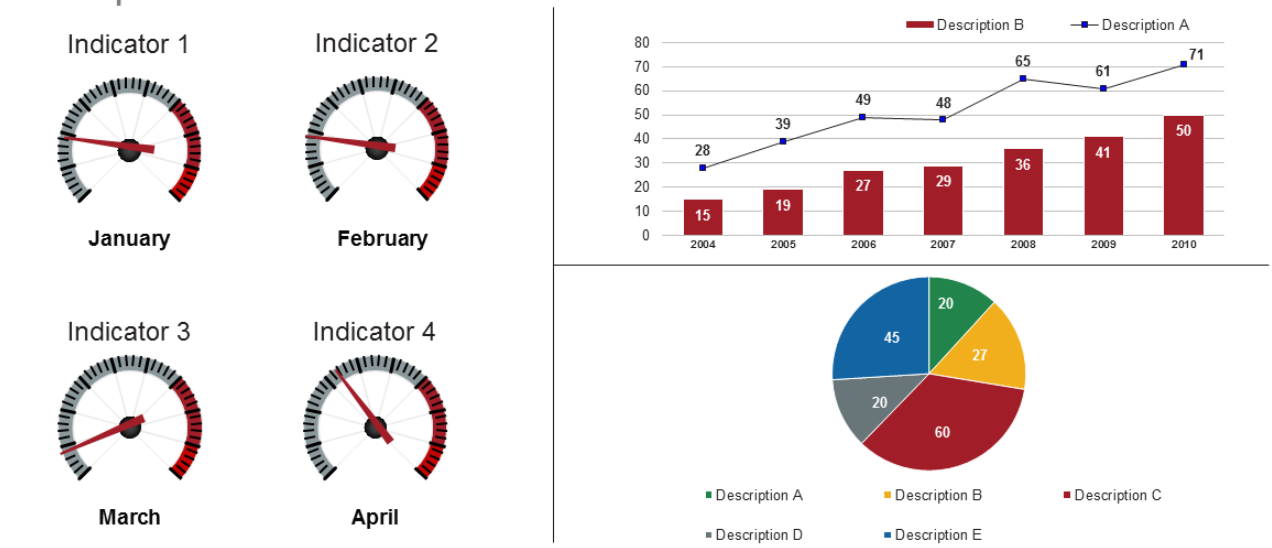
PECB

20

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

III. Strategic Dashboard

Example



PECB

21

Strategic dashboards 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.

Exercise 14: Development of information security indicators

Provide at least two examples of metrics that would be sufficient to measure the level of conformity to the following clauses and controls of ISO/IEC 27001.

Example: Clause 5.1 Leadership and commitment

- *The number of management review meetings completed to date*
- *The average participation rate in management review meetings to date*

1. Clause 10.1 d) Review the effectiveness of any corrective action taken
2. Clause 5.3 Organizational roles, responsibilities and authorities
3. Control A.8.1.2 Ownership of assets
4. Control A.8.1.4 Return of assets
5. Control A.9.3.1 Use of secret authentication information

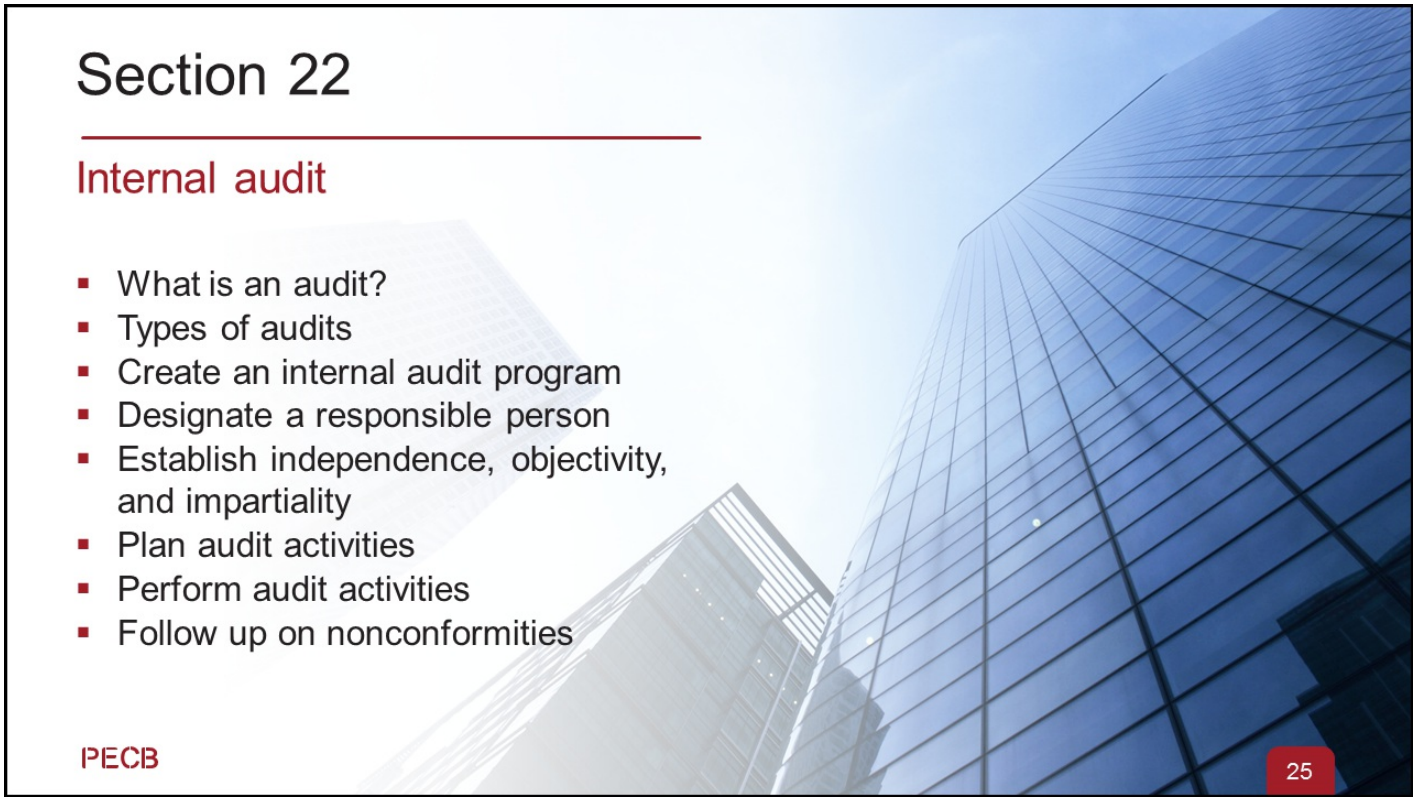
Duration of the exercise: 30 minutes

Comments: 15 minutes

1. **Monitoring, measurement, analysis, and evaluation should define 'information needs,' which are usually expressed as a high-level information security question or statement that helps the organization evaluate information security performance and ISMS effectiveness.**
   A. True
   B. False
2. **What is performance evaluation?**
   A. Process of determining the status of a system, process, or activity
   B. Process of determining measurable results
   C. Process of determining a value
3. **ISO/IEC 27004 provides guidelines to help organizations in evaluating the ISMS performance in order to satisfy the requirements of ISO/IEC 27001.**
   A. True
   B. False
4. **What does "SMART" stand for?**
   A. Sophisticated, Measurable, Adversary, Realistic, and Timely
   B. Specific, Measurable, Attainable, Realistic, and Timely
   C. Specialized, Maintainable, Attainable, Realistic, and Timely
5. **According to ISO/IEC 27004, which of the options below is not included in ISMS processes and activities that are candidates for measurement?**
   A. Financing and business management
   B. Communicating and documenting
   C. Planning and leadership
6. **What is the aim of monitoring, measurement, analysis, and evaluation in an ISMS?**
   A. To begin the ISMS implementation
   B. To improve the ISMS implementation
   C. To prohibit the ISMS implementation

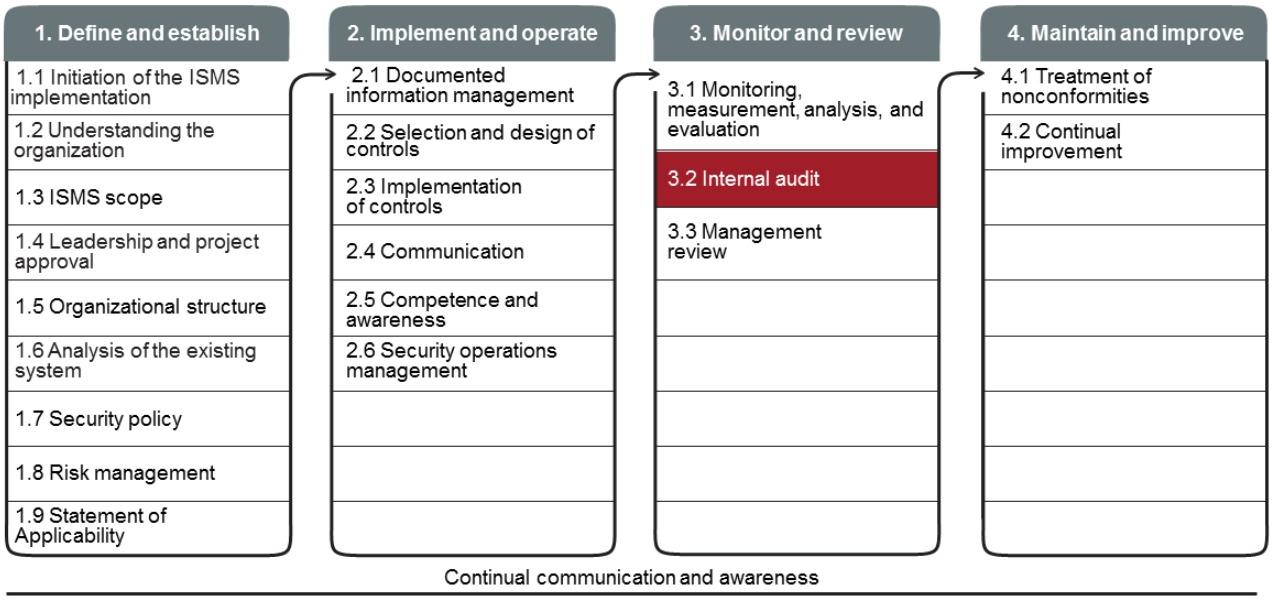
Section summary

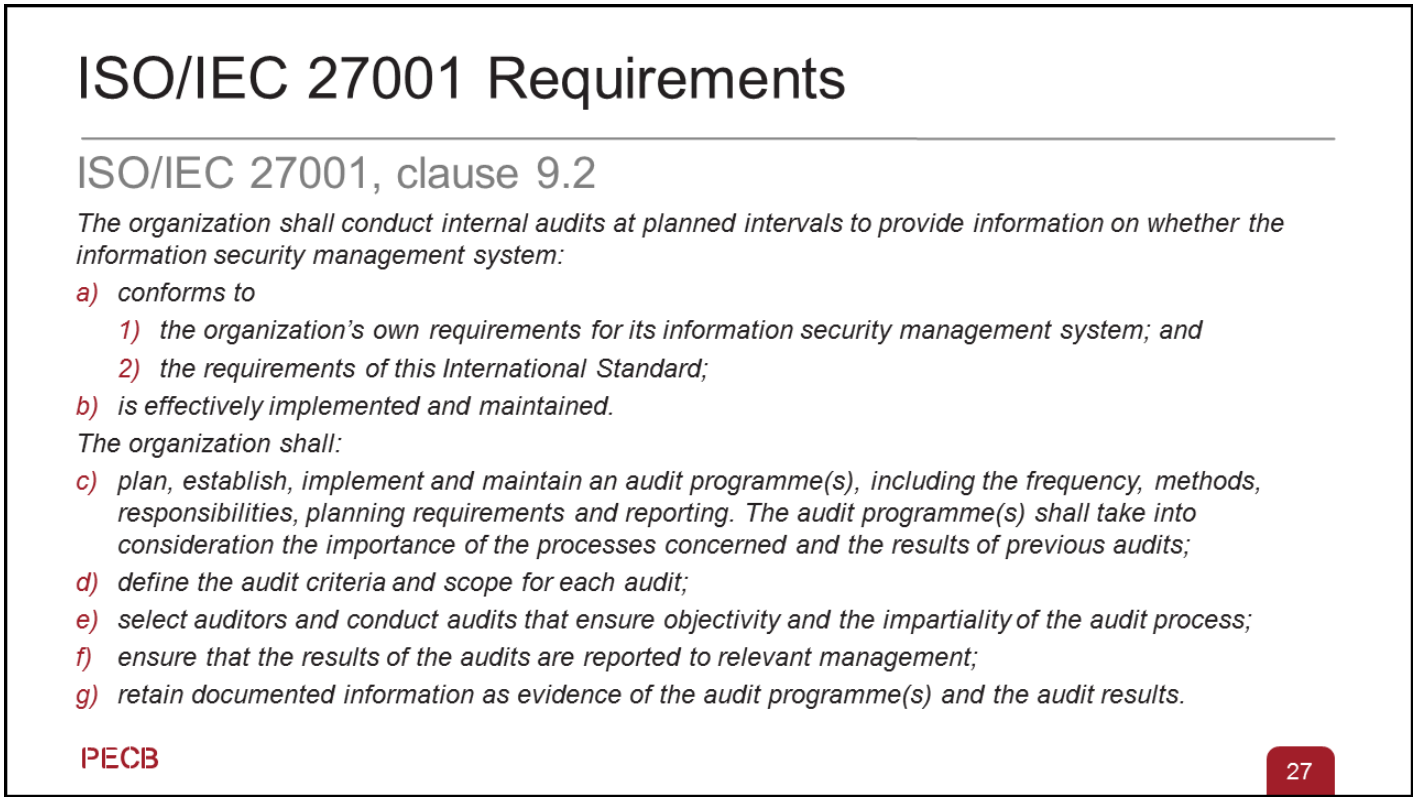
- Monitoring, measurement, analysis, and evaluation aim to improve the ISMS.
- The organization should identify measurement objectives, select attribute objects to be measured, create performance indicators, and evaluate whether the objectives have been met.
- The organization should determine how and how often to monitor or measure the ISMS.



This section provides information that will help the participant comprehend the role of an audit function and identify the differences between internal and external audits. Moreover, the participant will be able to define the audit planning activities, and allocate and manage the necessary resources to conduct either an internal or external audit program.

3.2 Internal audit





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

1. Conduct internal audits
2. Ensure the independence, objectivity, and impartiality of the audit function
3. Plan and perform audit activities

ISO/IEC 27003, clause 9.2 Internal audit

Auditors also evaluate whether the ISMS is effectively implemented and maintained. An audit programme 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 programme adjusted to better manage areas experiencing higher risks due to nonconformity.

What is an Audit?

ISO 19011, clause 3.1

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

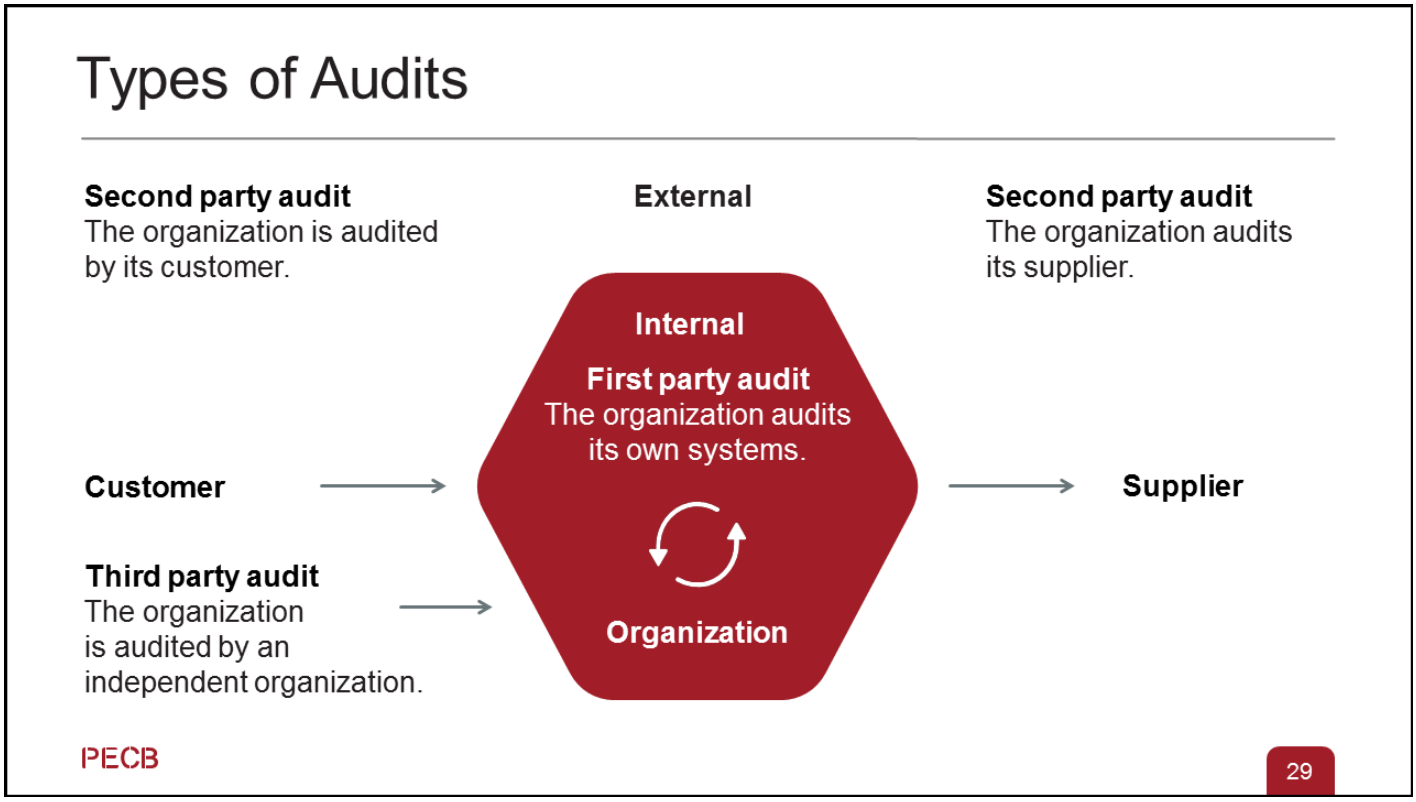
In short: Auditing means asking the auditee what they do and how they do it, in order to check whether the practices are in compliance with the organization's policies, procedures, and processes.

PECB

28

An audit is an assessment based on evidence and facts. This assessment points out the strengths and weaknesses of the audited organization or the audited system. Audit results are then communicated to the management, who then undertake the required and appropriate measures. The same principles and techniques apply to management system audits.

- 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.
- An **information security audit** determines if the information assets are protected appropriately.



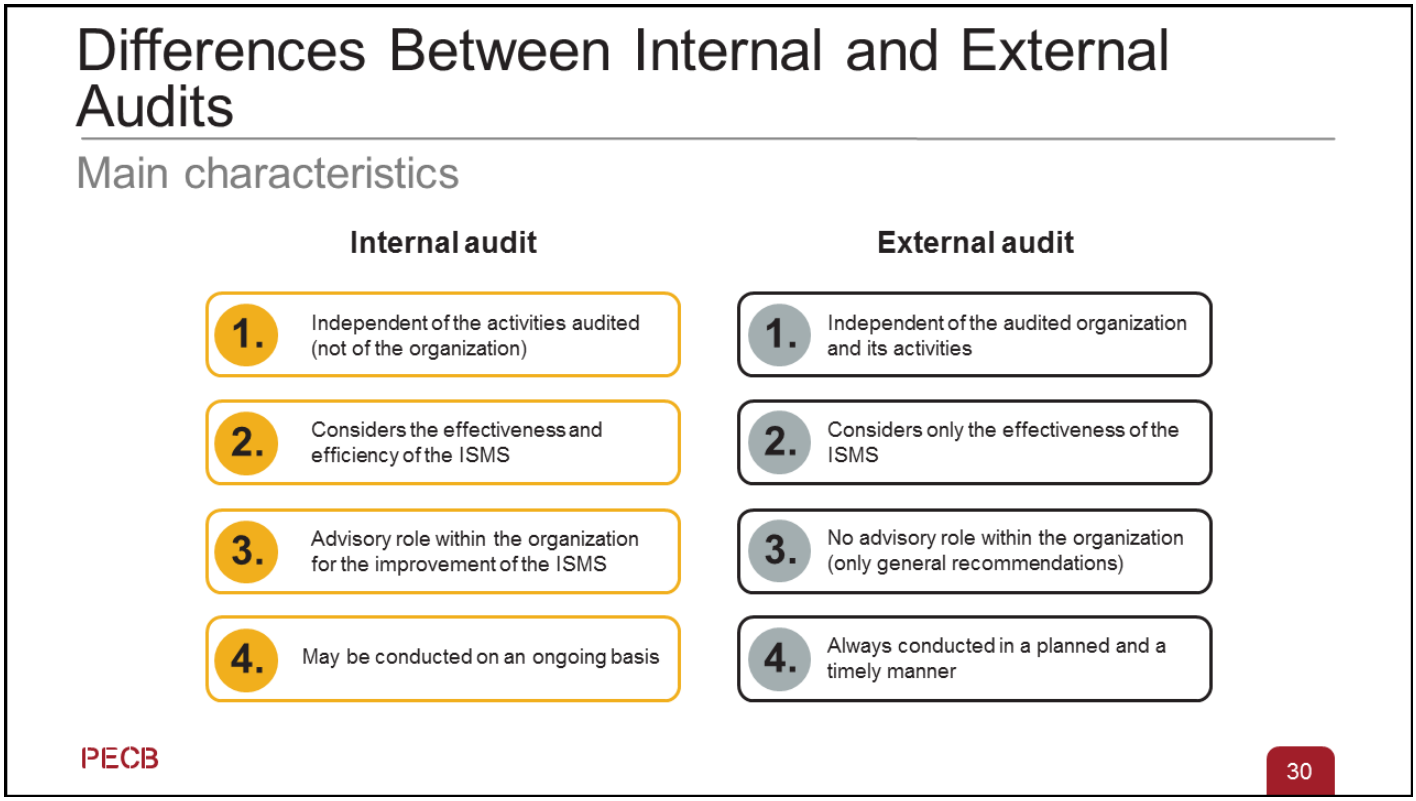
Internal audits:

The internal audit, also known as the **first party audit**, is an independent and objective activity that gives the organization an assurance on the level of control over operations, gives recommendations to improve operations, and contributes to creating added value. Internal audits are conducted by or for the organization itself for the purpose of management reviews and other internal needs. Independence must be demonstrated by the absence of responsibility in the activities to be audited.

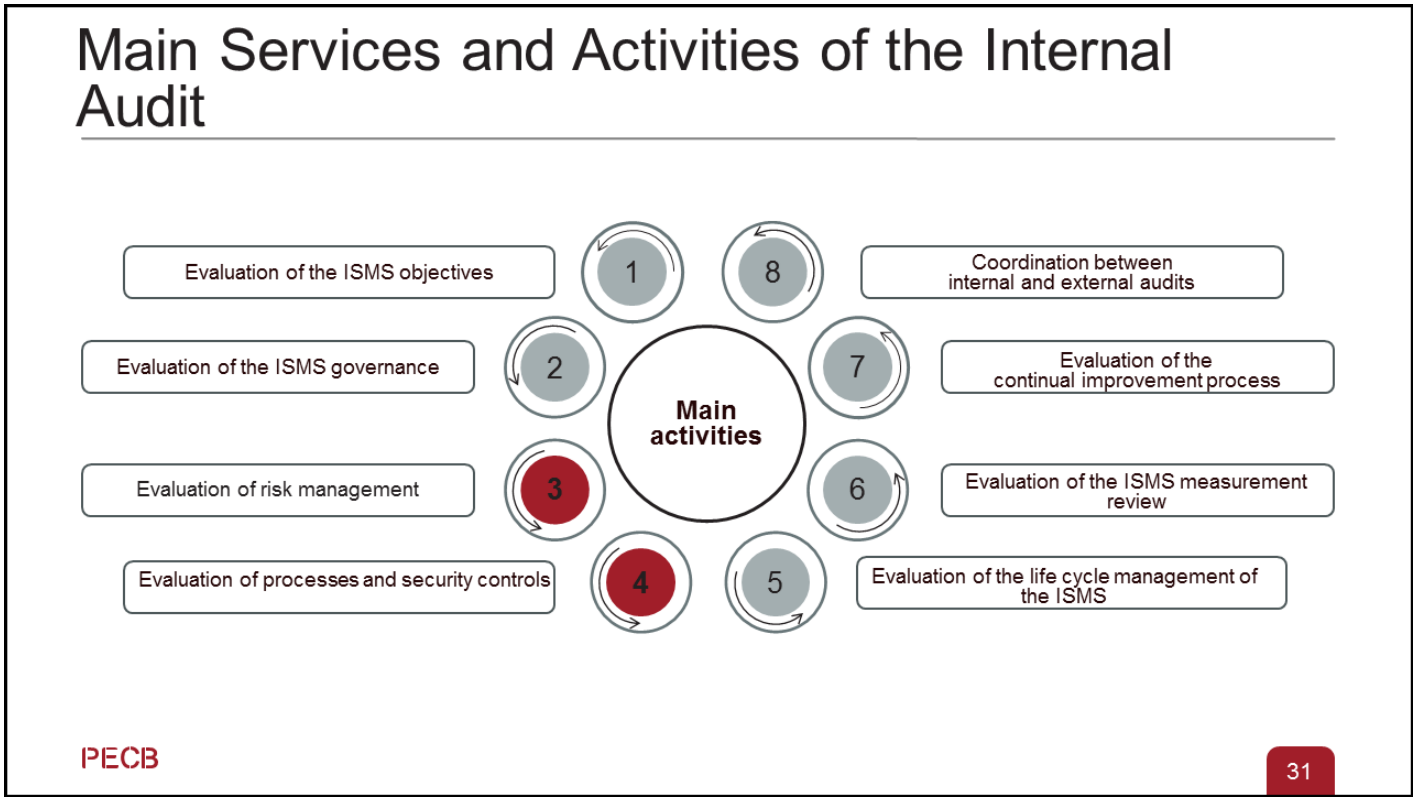
External audits include audits known as second and third party audits:

- **Second party audits** are conducted by parties that have an interest in the audited organization such as customers or other individuals acting on their behalf.
- **Third party audits** are conducted by external and independent audit organizations such as those providing certification and registration of conformity or governmental agencies.

Important note: Third party audits are performed by auditors who are external to and independent of the auditee.



Internal auditing is an independent, objective, and advisory activity designed to upgrade and improve the organization's functions. It also contributes 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.



The objectives of the internal audit function should be reviewed and approved by the organization's 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 function 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 ISMS objectives:** The internal auditor should evaluate whether the organization is able to achieve its information security objectives.
2. **Evaluation of the ISMS governance:** The internal auditor should validate if the organization's management supports activities related to the ISMS and whether the roles and responsibilities of interested parties are clearly defined.
3. **Evaluation of risk management:** 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 processes and controls:** The internal auditor should evaluate the adequacy, effectiveness, and efficiency of ISMS processes or 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.

Slide Notes Extension

PECB

32

5.Evaluation of the life cycle management of the ISMS: 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 ISMS.
6.Evaluation of the ISMS measurement review: The internal auditor should make sure that the organization periodically conducts a review of the measurement of the ISMS 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 measures to address the detected nonconformities and enhance the effectiveness and efficiency of the ISMS.
8.Coordination between internal and 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 function is to ensure that the organization performs adequate monitoring of external audit reports and action plans that they have established and approved.

ISO 19011

Guidelines for auditing management systems

The standard provides guidance on:

- The concepts of management system audits
- The main auditing and auditor characteristics and audit principles
- The key elements of the audit process
- The key aspects of an audit program
- The qualifications of auditors

PECB

33

ISO 19011 provides guidelines and support for audit methods but its application is not prescriptive. 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 (always being in accordance with the auditor's own work methods).

It should be noted that ISO 19011 was developed as a guideline for management system audits.

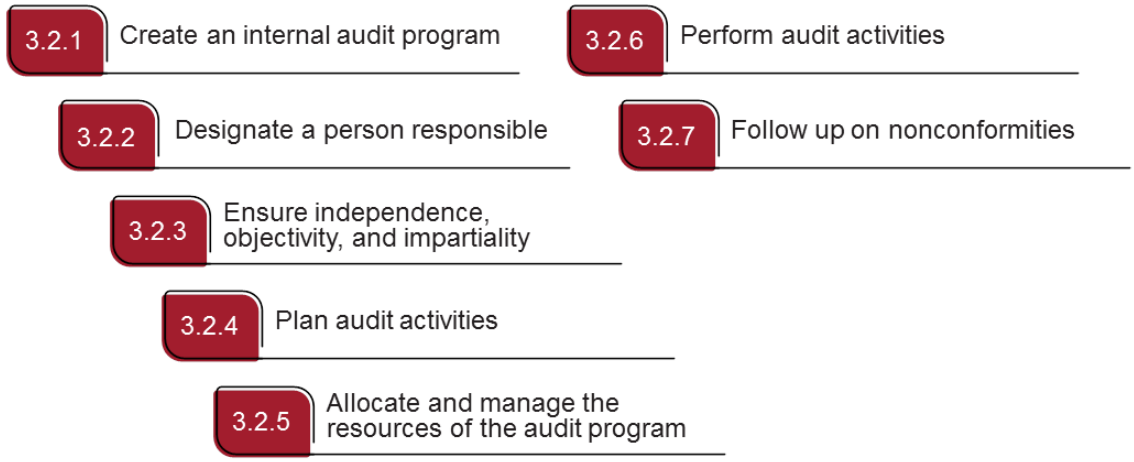
The content of the ISO 19011:2018 standard:

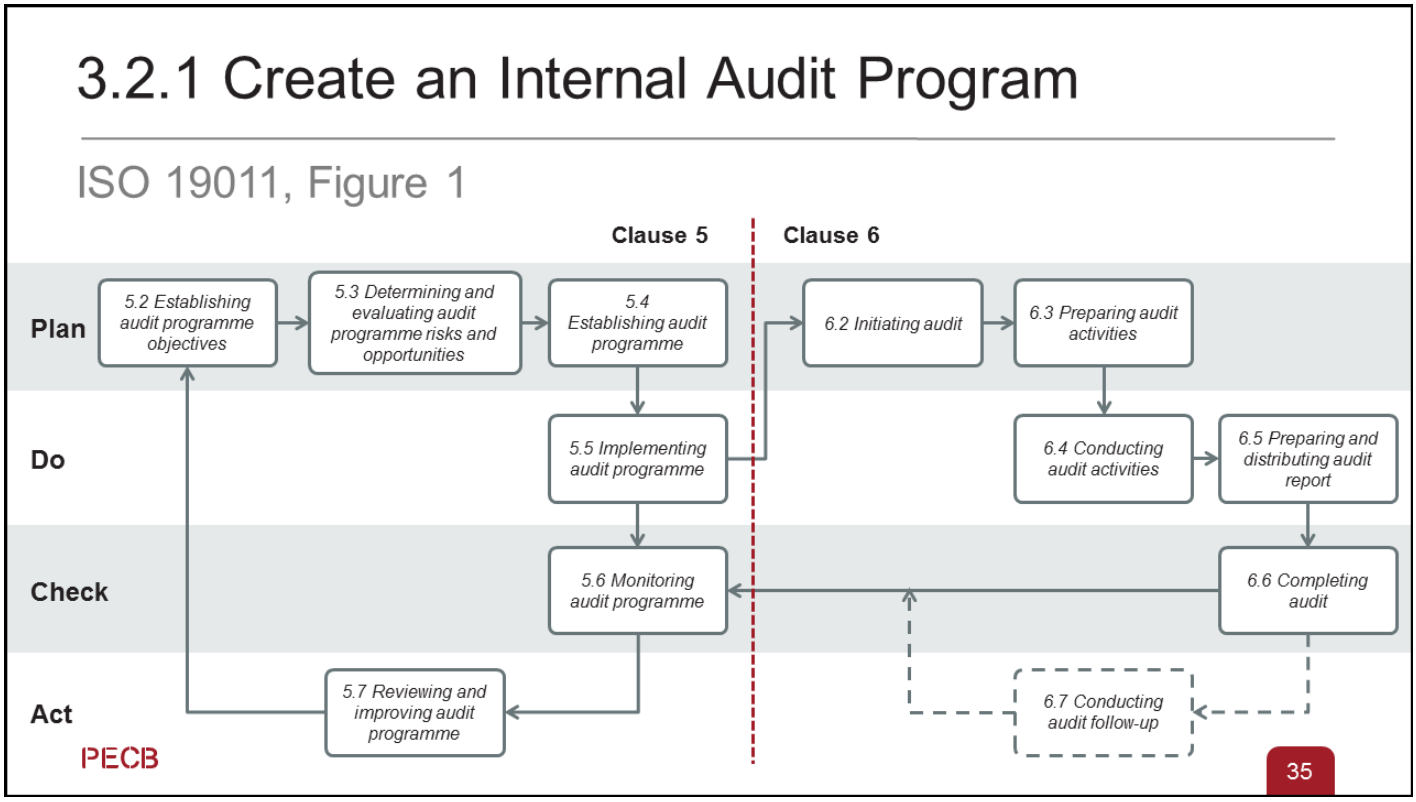
1. Scope
2. Normative references
3. Terms and definitions
4. Principles of auditing
5. Managing an audit programme
6. Conducting an audit
7. Competence and evaluation of auditors

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

3.2 Internal Audit

List of activities



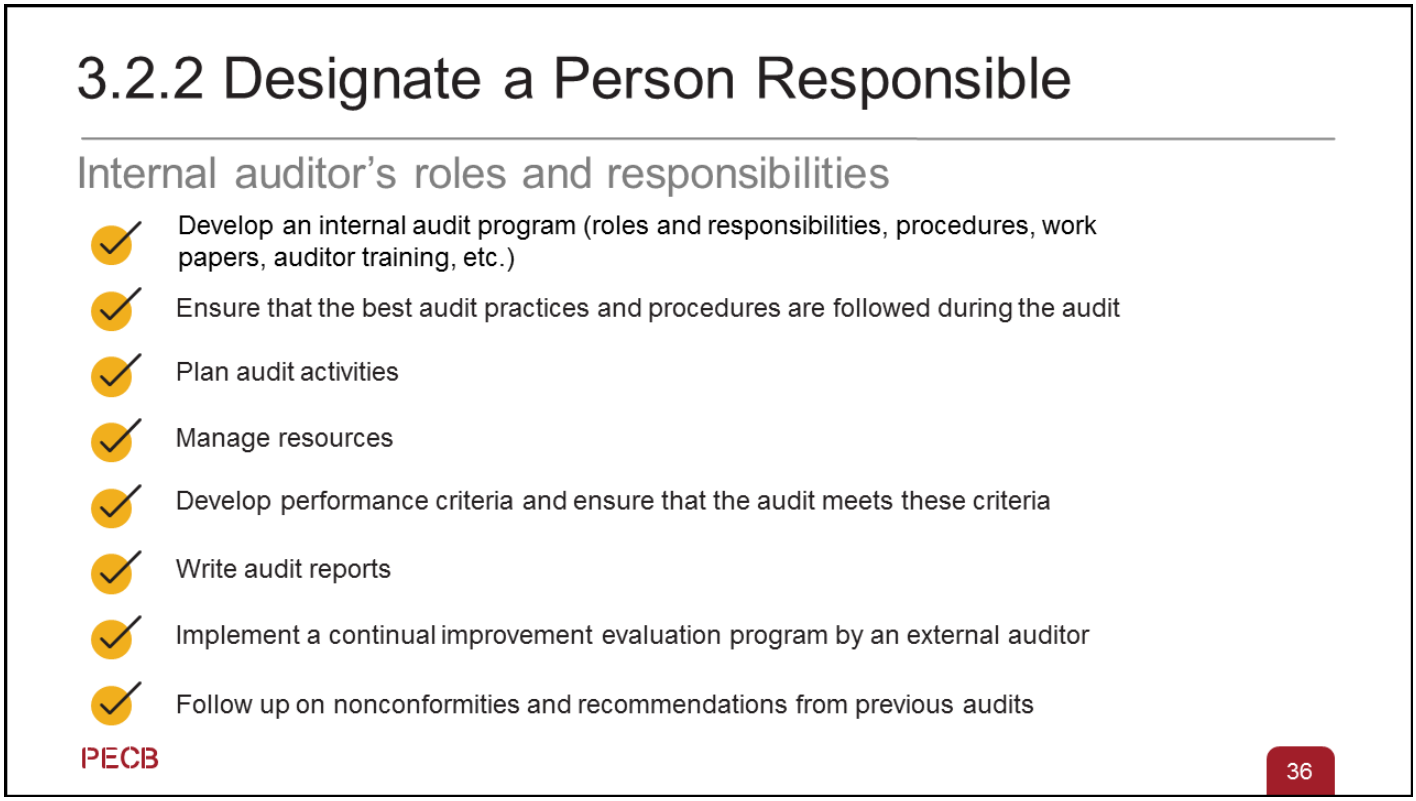


ISO 19011, clause 3.4 Audit programme

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

An audit program should follow the steps described in the PDCA model. An audit program can include more than one audit depending on the size and complexity of the organization to be audited. Joint or combined audits can be conducted as well. An organization can establish more than one audit program.

The audit program includes all the activities required for planning and organizing the type and number of audits, along with the measures to provide the resources needed to carry out an effective audit within the indicated time frame.

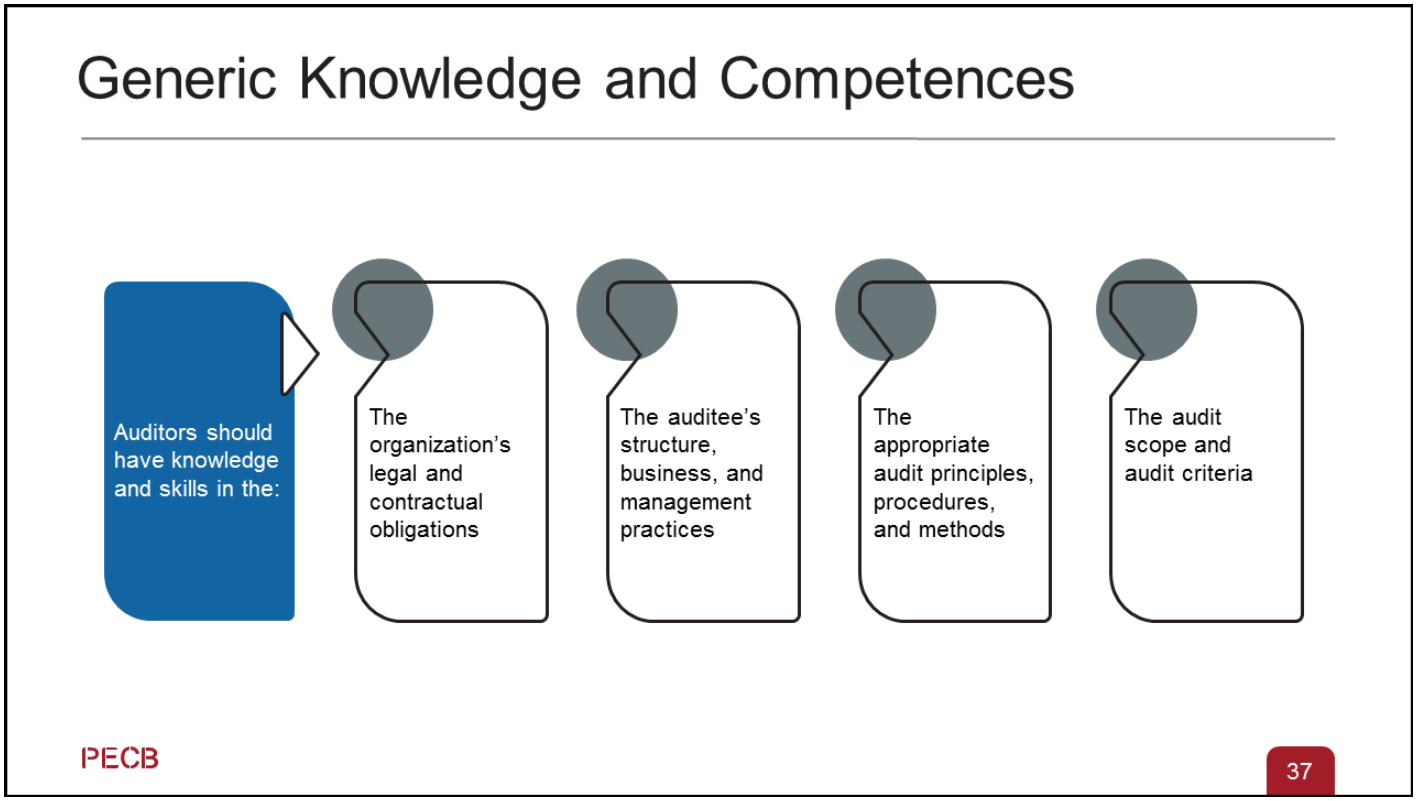


ISO 19011, clause 5.4.1 Roles and responsibilities of the individual(s) managing the audit programme

The individual(s) managing the audit programme should:

a. *establish the extent of the audit programme 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 programme, 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 programme;*
    - *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 programme records;*
g. *monitor, review and improve the audit programme;*
h. *communicate the audit programme to the audit client and, as appropriate, relevant interested parties.*

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



ISO 19011, clause 7.2.3.2 Generic knowledge and skills of management system auditors

Auditors should have knowledge and skills in the areas outlined below.

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

PECB

38

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.*

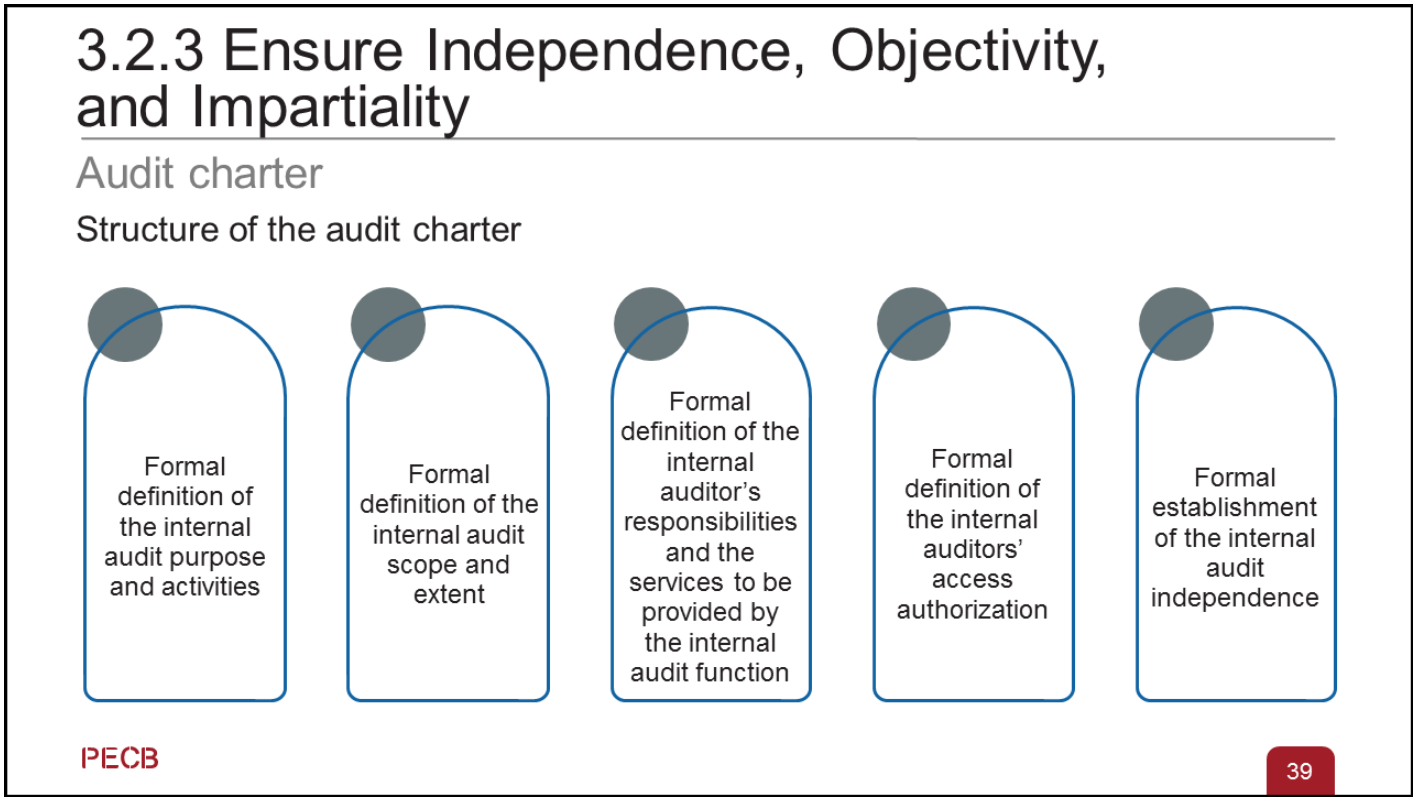
c)The organization and its context: knowledge and skills in this area enable the auditor to understand the auditee's structure, purpose and management practices and should cover the following:

- *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.*

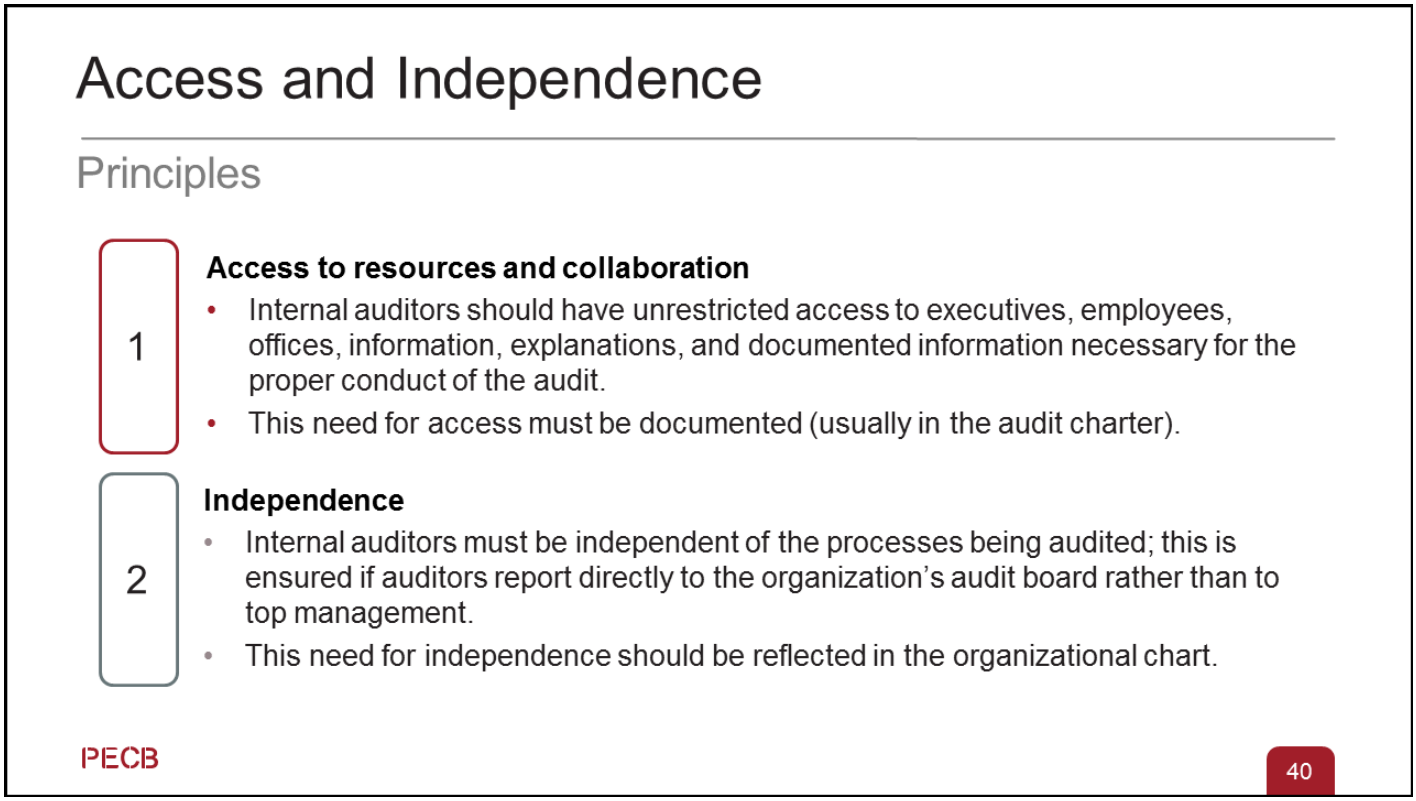
NOTE Awareness of statutory and regulatory requirements does not imply legal expertise and a management system audit should not be treated as a legal compliance audit.



The internal audit charter is an official document that outlines the internal audit activities, objectives, and roles and responsibilities of the internal audit team. The internal audit charter settles the position of the internal audit inside the organization, including the nature of the auditor's reporting relationship with the top management; permits access to documents and records, personnel, and physical properties relevant to the performance of activities; and, lastly, defines the scope of internal audit activities. The top management should approve the internal audit charter.

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 a violation of the principle of independence.

Important note: In case of a small organization, it is often 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 management system.



In order to ensure that the mission of the internal auditor is successfully completed, the audited entities must demonstrate their availability and collaboration. As such, auditors should not experience, from the audited entities, limits to their interventions or be subject to interference.

3.2.4 Plan Audit Activities

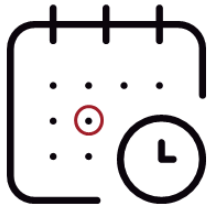
Short- and long-term planning

A high-level planning of audit activities over three years

This plan must take into account that the overall information security management system should be audited every three years.

A more detailed annual planning

This plan must take into account that there is no requirement for the auditor to audit all the processes and controls of the information security management system during that year.



PECB

41

The internal auditor is in charge of planning and conducting the internal audit mission.

An organization that implements an audit program (internally or externally) must provide the resources necessary for its operation including:

1. **Financial resources** necessary to develop, implement, manage, and improve the audit activities
2. **Competent personnel** (auditors and technical experts) to conduct the audit activities
3. **Tools** (computers, software, etc.)
4. **Audit policies and procedures**
5. **Logistics** (transportation, accommodations, and other needs related to the audit activities)

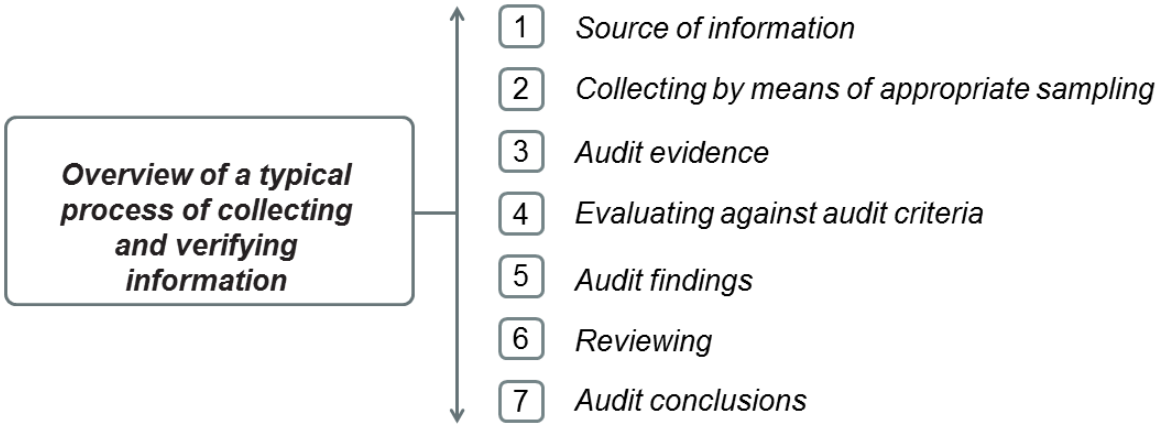
ISO 19011, clause 5.4.4 Determining audit programme resources

When determining resources for the audit programme, the individual(s) managing the audit programme 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 programme objectives;*
d. *the extent of the audit programme and audit programme 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 programme;*
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).*

3.2.6 Perform Audit Activities

ISO 19011, Figure 2



PECB

43

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 (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 the quality review, the audit team issues the audit conclusion(s).

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

Perform Audit Activities

Audit procedures should include information on how to:

1. Plan and schedule audits
2. Manage the audit risks
3. Ensure the competence of audit team members
4. Assign the roles and responsibilities of audit team members
5. Select and use suitable sampling methods
6. Conduct follow-up audit, if applicable
7. Report the audit conclusions to the auditee
8. Maintain audit records
9. Monitor the effectiveness of the audit

PECB

Nonconformity

Definition

- According to the ISO 9000 standard, a nonconformity is defined as the "*non-fulfilment of a requirement.*"
- There are two types of nonconformities:
  - Minor nonconformity
  - Major nonconformity

PECB

45

Requirements can originate from several sources; they can be specified in a standard, be part of an internal requirement of the organization, originate from a law or regulation, or be part of a contract signed with a client or partner.

ISO 9000, clause 3.6.9 Nonconformity

Non-fulfilment of a requirement

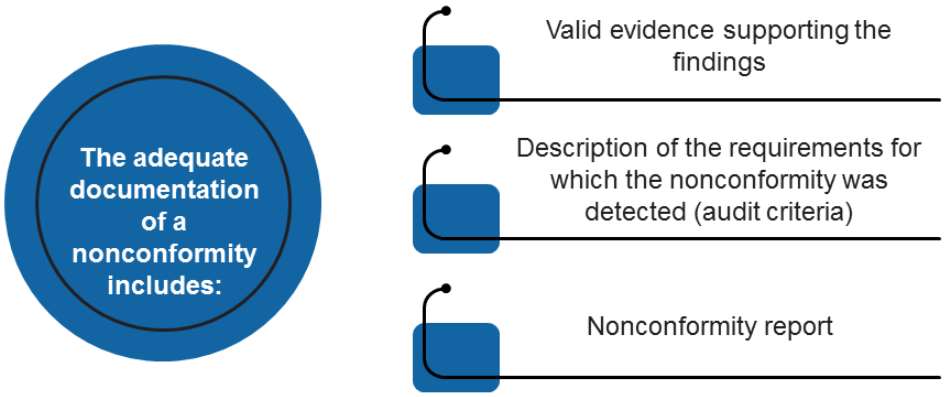
ISO 9000, clause 3.6.11 Conformity

Fulfilment of a requirement

Common examples of nonconformities:

- The documentation is not complete.
- The control is not implemented or does not function properly.
- The control does not provide the expected results.

Document the Nonconformities



PECB

46

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

It is to be noted that ISO/IEC 27001 contains several clauses that include more than one requirement. It is important that the auditor documents the specific conditions of the nonconformity (e.g., by writing the exact text and requirement associated to the audit criteria).

A nonconformity report should be:

- Explicit and related to an ISMS requirement
- Unambiguous, linguistically correct, and as concise as possible

Nonconformity Report

Example

NONCONFORMITY REPORT		
Nonconformity N°: 3	**Client:** Thalia Technologies	**File N°:** 34527
Process: Assets Management	**clause number:** A.8.1.1	**Site:** Montreal
Audit criteria: Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.		
Description of the observed nonconformity: In a sample of 25 assets analyzed originating from the assets list, only 5 assets were correctly identified. **Recommendation:** Establish an inventory of all important assets and clearly identify the assets including, for example, its type, owner, size, location, the information related to its backup, as well as its value to the organization.		
Auditor: John Doe	**Acknowledgment by auditee representative:** Nonconformity presented to Mr. R. Smith and confirmed on June 3, 2007	**Nonconformity**
Date: June 5, 2019		Major* Minor*

PECB

47

The final part (and the most important) of the documentation of a nonconformity is writing a nonconformity report. **The report must specify the audit criteria, the description of the nonconformity, and the audit findings. Recommendations are optional, and can be included.**

If the three parts of the nonconformity are well documented, the auditee will be able to understand and recognize the nonconformity. This will also serve as a useful record for a future report.

To support traceability and facilitate the follow-up of action plans, it is crucial that nonconformities be recorded and documented systematically. A simple way to do this would be to use a standard nonconformity report (NCR).

3.2.7 Follow up on Nonconformities

Guidelines

- An internal auditor should follow up on action plans submitted in response to nonconformities (resulting from internal and external audits).
- The person in charge of the ISMS must inform the internal auditor of the progress of corrections and corrective actions.
- The internal auditor should review the corrections, identified causes, and corrective actions, and verify the effectiveness of all corrections and corrective actions.
- Not all corrections and corrective actions have to be implemented immediately.

Note: Based on experience and knowledge, the auditor should exercise good judgment and assess whether action plans are appropriate and can address the intrinsic causes of nonconformities.

PECB

48

An auditor must always remember that it is highly unlikely that the organization is able to complete the improvements simultaneously. Every improvement requires resources and time to implement. Action plans can be arranged in order of priority by the management, especially actions that require investments. Therefore, the auditor must try to ensure that improvement objectives are realistic in the specific context of the auditee.

Verbal responses may be received by the auditor. In this case, the auditor should register them in writing thereafter.

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

1.What is an audit?

A. A systematic, independent, and documented process
B. A symmetric and objective documents
C. A subjective opinion on the state

2.What audit type determines whether the organization's accounting practices are compliant with legal requirements?

A. A financial audit
B. An administrative audit
C. An information security audit

3.Internal audits include audits known as second and third party audits.

A. True
B. False

4.Which of the following is NOT a characteristic of internal audits?

A. They provide general recommendations and not an advisory role within the organization
B. They consider the effectiveness and efficiency of the ISMS
C. They are independent of the activities audited (not of the organization)

5.Auditors should possess knowledge and skills in audit principles, processes, and methods.

A. True
B. False

6.A nonconformity report should NOT be _____.

A. Ambiguous
B. Explicit
C. Correct

7.How many types of nonconformities are there?

A. One: Minor nonconformities
B. One: Major nonconformities
C. Two: Minor and major nonconformities

8.An auditor must always remember that it is highly unlikely that the organization is able to complete all the improvements simultaneously.

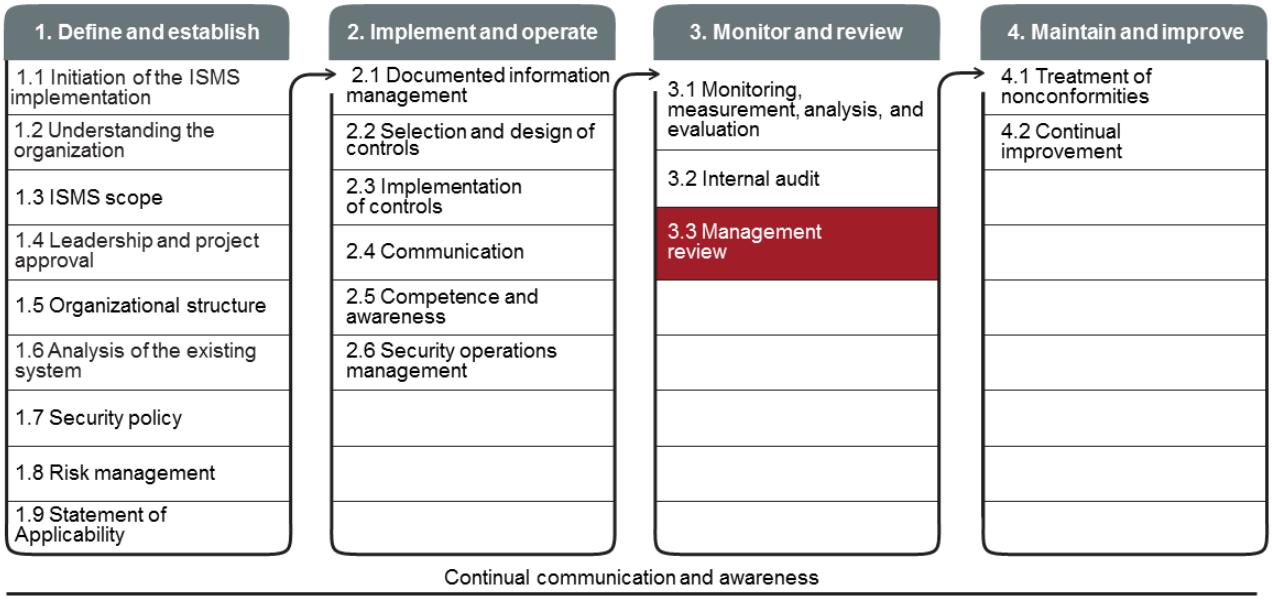
A. True
B. False

Section summary

- Internal audits help organizations evaluate if their ISMS is effectively implemented and maintained, as well as their compliance with the ISO/IEC 27001 requirements.
- Internal audit is a type of audit where organizations audit their own systems.
- Internal audit results are used as input for continual improvement. Their goal is improving the functioning of the organization.
- The internal auditor is responsible for developing an internal audit program, planning the audit activities, writing audit reports, developing performance criteria and ensuring that the audit meets them, implementing continual improvement program, following up on nonconformities, and analyzing recommendations obtained from previous audits.
- To conduct an internal audit, the auditor needs access to the organization’s workplaces and documentation.
- The auditor collects information from different sources and evaluates whether requirements are met.
- The auditor should follow up on nonconformities by reviewing the corrections and corrective actions, and by verifying their effectiveness.

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

3.3 Management Review



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 9.3

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

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) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results; and

4) fulfilment of information security objectives;

d) feedback from interested parties;

e) results of risk assessment and status of risk treatment plan; and

f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

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

PECB

54

An organization wishing to comply with ISO/IEC 27001 shall at least perform a management review every year and maintain records

Management Review

Definition

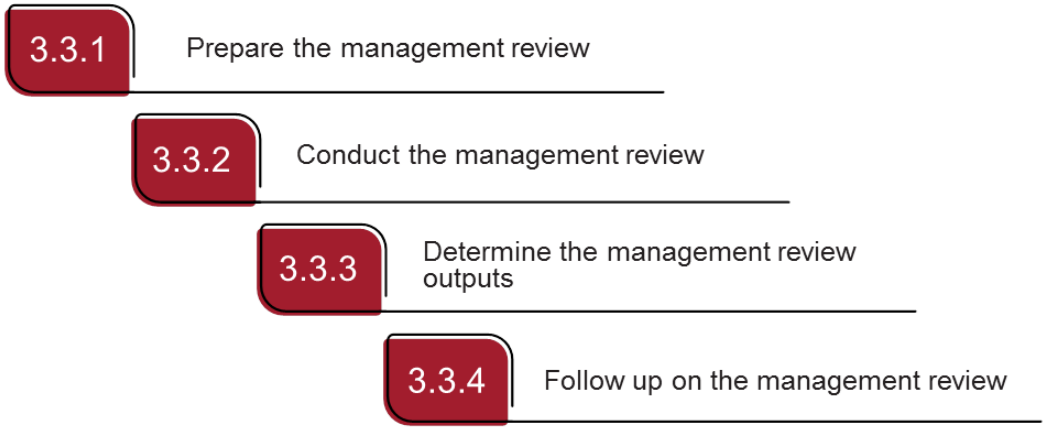
A management review is a periodic review of the management system performed by the top management to analyze the system's continuing suitability, adequacy, and effectiveness.

Term	Concept
Suitability	Results are achieved in the best possible way
Adequacy	Outputs fulfill established criteria
Effectiveness	The system fulfills the organization's needs

PECB

3.3 Management Review

List of activities



PECB

3.3.1 Prepare the Management Review

- Management reviews must be conducted at planned intervals.
- Management reviews can be included in a management meeting and be a topic on the agenda.
- It is good practice to send all documentation related to the management committee (audit report, results of reviews, action plans) before the review.

PECB

57

There is no specific requirement for frequency of management review meetings. The common practice is quarterly meetings. With annual meetings, the organization may not be able to prevent or resolve issues in a timely manner.

3.3.2 Conduct the Management Review

The input to a management review should include information on:

1. The status of actions from previous management reviews
2. Changes in external and internal issues that are relevant to the ISMS
3. Nonconformities and corrective actions
4. Monitoring and measurement results
5. Audit results
6. The fulfillment of information security objectives
7. The feedback from interested parties
8. The results of risk assessment and the status of risk treatment plan
9. Opportunities for continual improvement
10. The review of new or ongoing actions

PECB

58

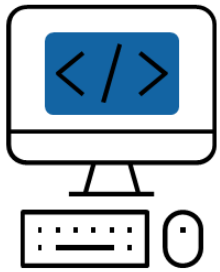
For the sake of efficiency, the input needed for each of these topics must be prepared in advance by the ISMS coordinator. The role of the review will be to verify whether the defined objectives by management are being accomplished, and whether the ISMS is in compliance with the standard. For each point, the management review will decide what, if any, actions to take.

3.3.3 Determine the Management Review Outputs

Decisions and resolutions

The output from the management review shall include any decisions and actions related to the following:

1. Continual improvement opportunities
2. Any needs for changes to the ISMS



PECB

3.3.4 Follow Up on the Management Review

- Management reviews must be documented.
- The organization should provide reports on the management review to those who are part of it.
- The ISMS coordinator and the internal audit team have the responsibility to ensure that follow-up action plans are approved by management.

Exercise 15: Management review

Explain the purpose of a management review with regard to the ISMS implementation and the points that should be taken into account when performing such a review.

Duration of the exercise: 30 minutes

Comments: 15 minutes

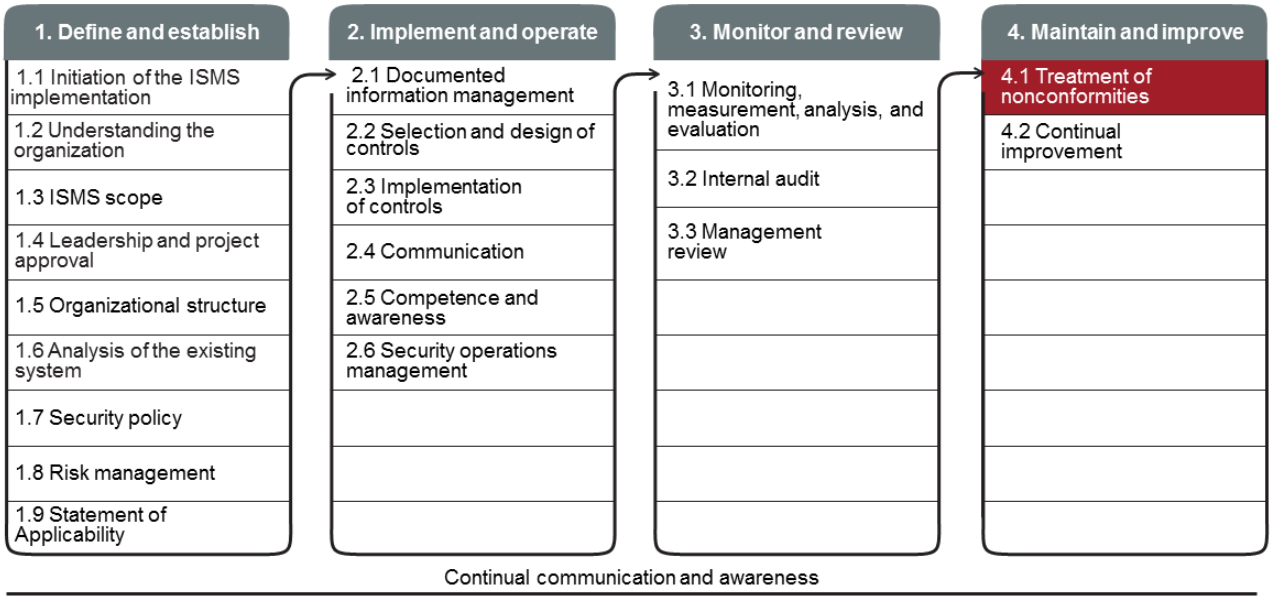
1. **What is accomplished when the implemented management system fulfills the organization's needs?**
   A. Suitability
   B. Adequacy
   C. Effectiveness
2. **An organization wishing to comply with ISO/IEC 27001 should at least perform annual management reviews and maintain records.**
   A. True
   B. False
3. **Who is responsible for ensuring that follow-up action plans are approved by the top management?**
   A. The ISMS coordinator and the internal audit team
   B. The top management
   C. The information security manager
4. **What should be included in the management review output?**
   A. Decisions related to risk opportunities
   B. Decisions related to continual improvement opportunities
   C. Decisions related to outsourcing opportunities
5. **Since there is no specific requirement regarding the frequency of management review meetings, annual meetings are enough to prevent or resolve issues.**
   A. True
   B. False

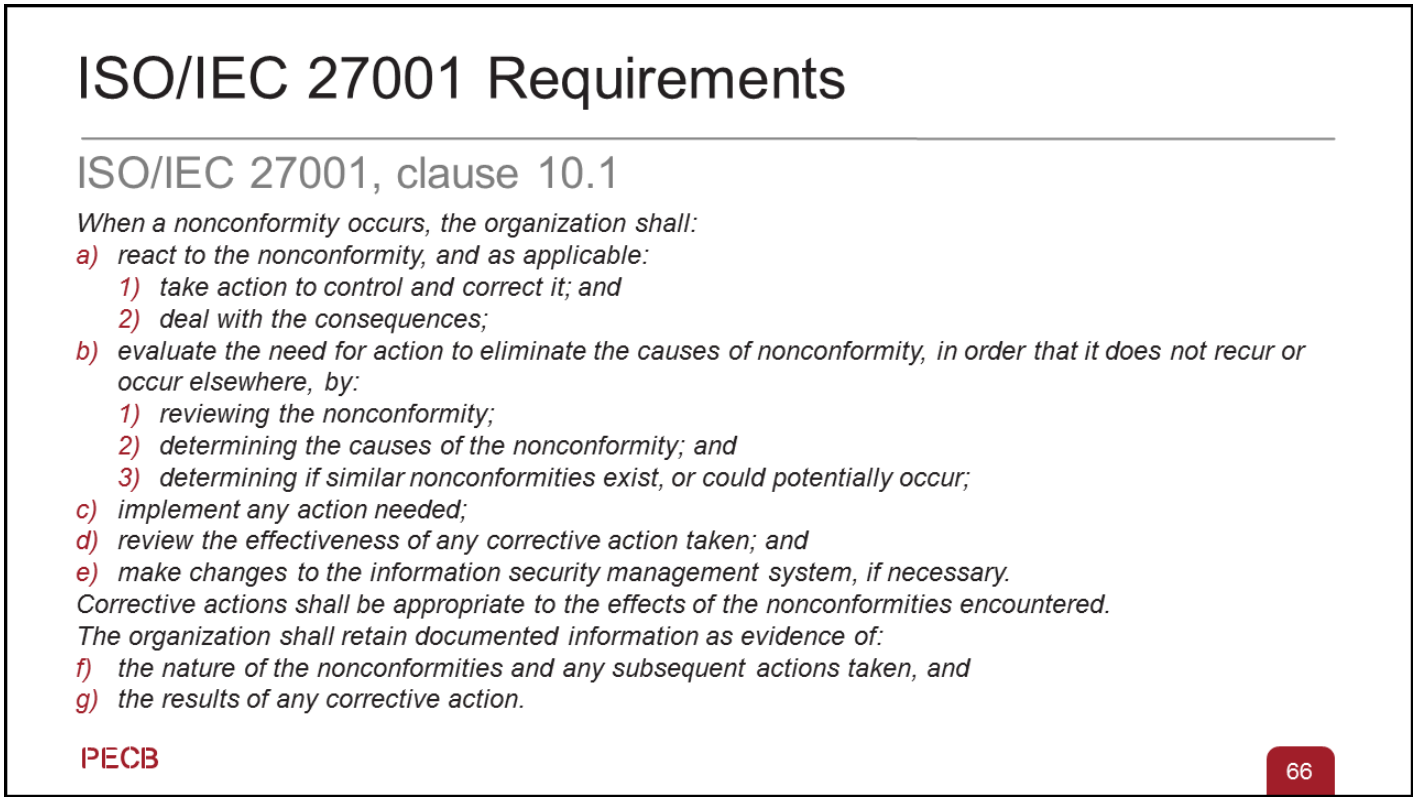
Section summary

- Management review is conducted by the top management to analyze the suitability, adequacy, and effectiveness of the information security management system.
- 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 makes decisions in regard to continual improvement opportunities and changes to the ISMS.

This section will help the participant comprehend the importance of treating problems and nonconformities. Moreover, the participant will acquire knowledge about the root-cause analysis process and tools, as well as the corrective and preventive action procedures.

4.1 Treatment of Nonconformities





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

1. Define a process to review, evaluate, and treat nonconformities
2. Identify nonconformities and react effectively

ISO/IEC 27003, clause 10.1 Nonconformity and corrective action

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:

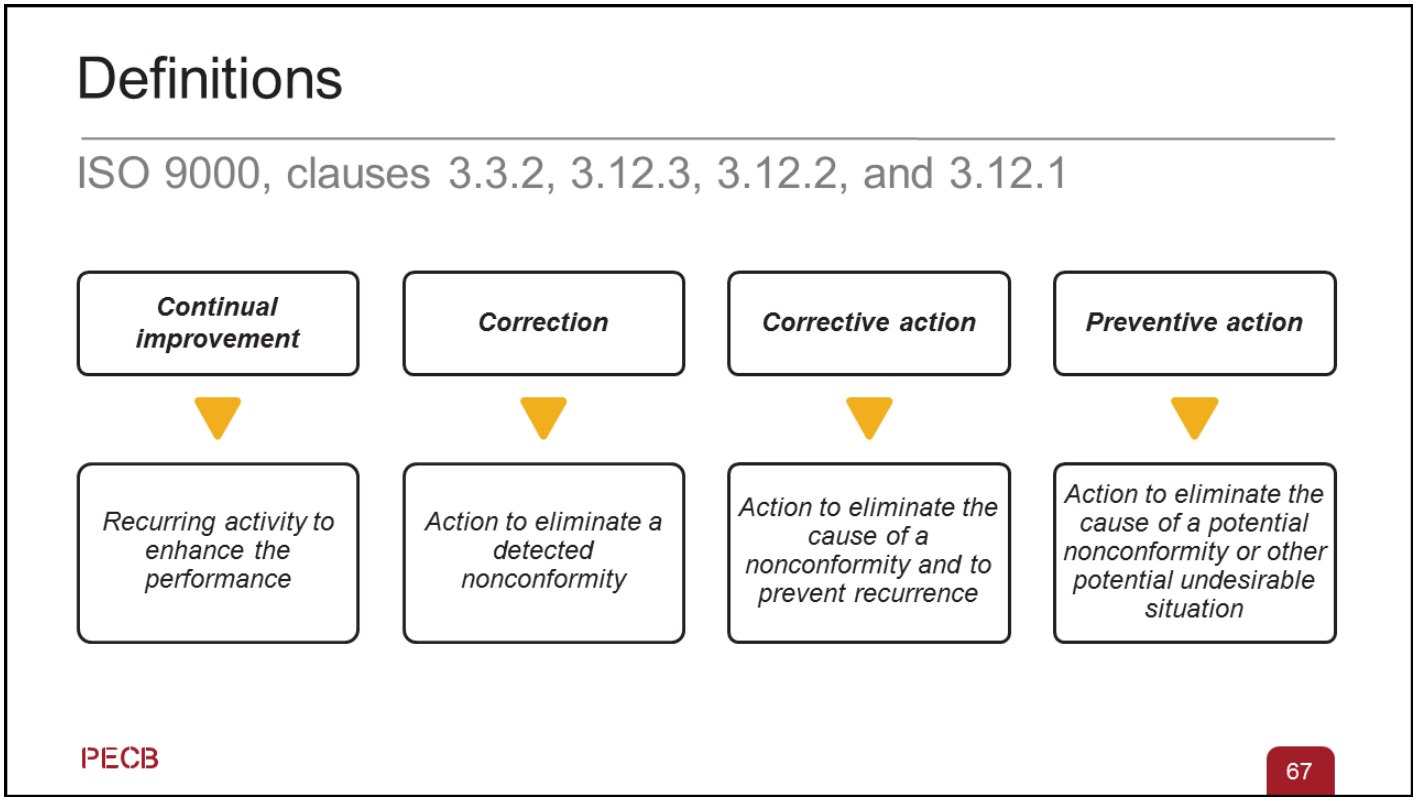
a. *failure to fulfil a requirement (completely or partially) of ISO/IEC 27001 in the ISMS;*
b. *failure to correctly implement or conform to a requirement, rule or control stated by the ISMS; and*
c. *partial or total failure to comply with legal, contractual or agreed customer requirements.*

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 recognised 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

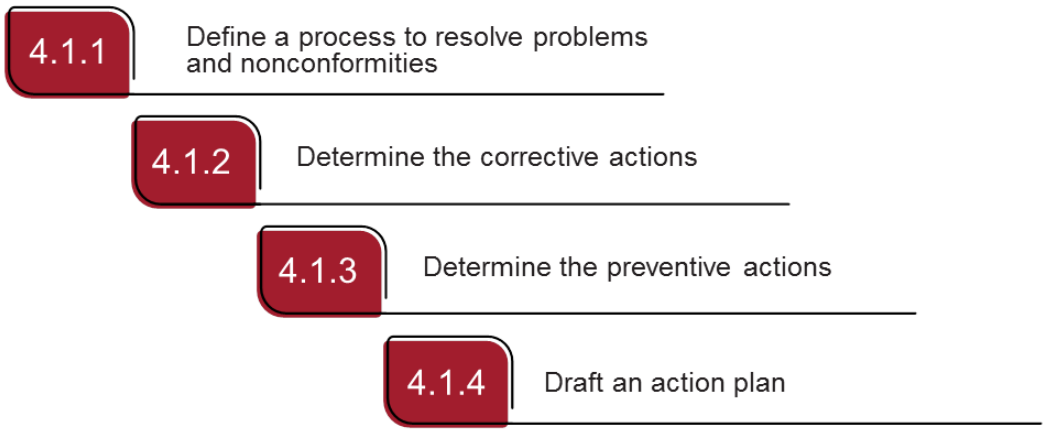
Extent to which planned activities are realized and planned results are achieved

ISO 9000, clause 3.7.10 Efficiency

Relationship between the result achieved and the resources used

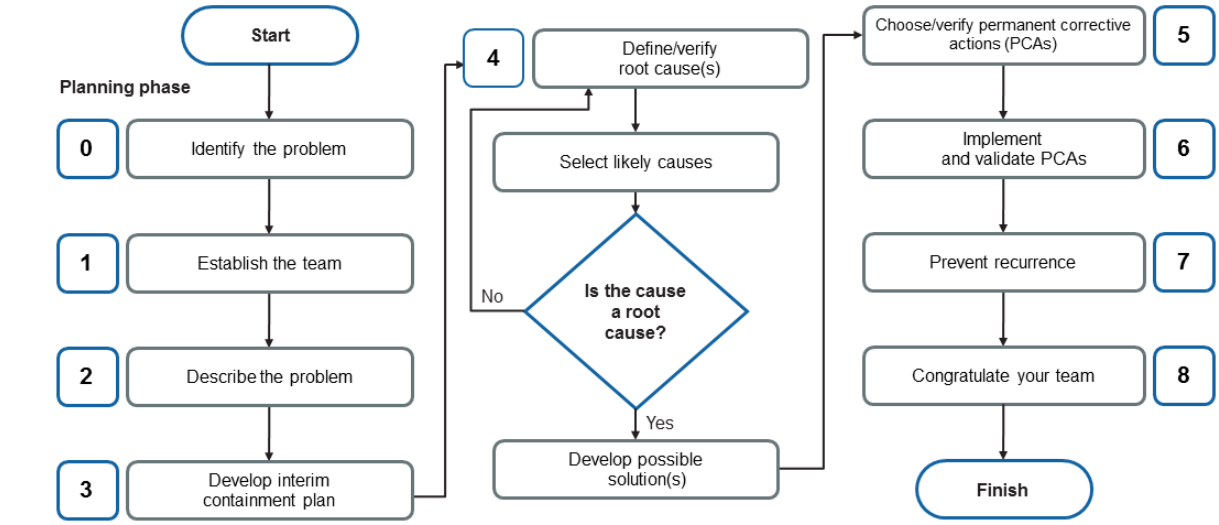
4.1 Treatment of Nonconformities

List of activities



4.1.1 Define a Process to Resolve Problems and Nonconformities

Example of the eight disciplines problem solving method:



PECB

69

Eight disciplines problem solving is a method used to approach and resolve problems and nonconformities. Its purpose is to identify, correct, and eliminate recurring problems, and it is useful in product and process improvement. 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. Originally, it was composed of eight stages or disciplines. Later on, an initial planning stage was added.

The steps are:

0. Plan: Plan for solving the problem and determine the prerequisites

1.Use a team: Establish a team consisting of professionals with thorough knowledge of products and processes.

2.Define and describe the problem: 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.

3.Develop interim containment plan: Implement and verify interim actions; determine and implement the respective containment actions in order to confine the problem, thus preventing it from reaching the customer.

4.Determine, identify, and verify root causes and escape points: Identify and analyze all of the possible reasons for the occurrence of the problem in the first place. Additionally, seek for an explanation as to why the problem has not been detected at the time of its occurrence. The root causes must be properly verified and, if required, proven and not simply determined by a brainstorming session. The tools that can be used to map the root-cause analysis include the Five WHYs or Ishikawa Diagrams.

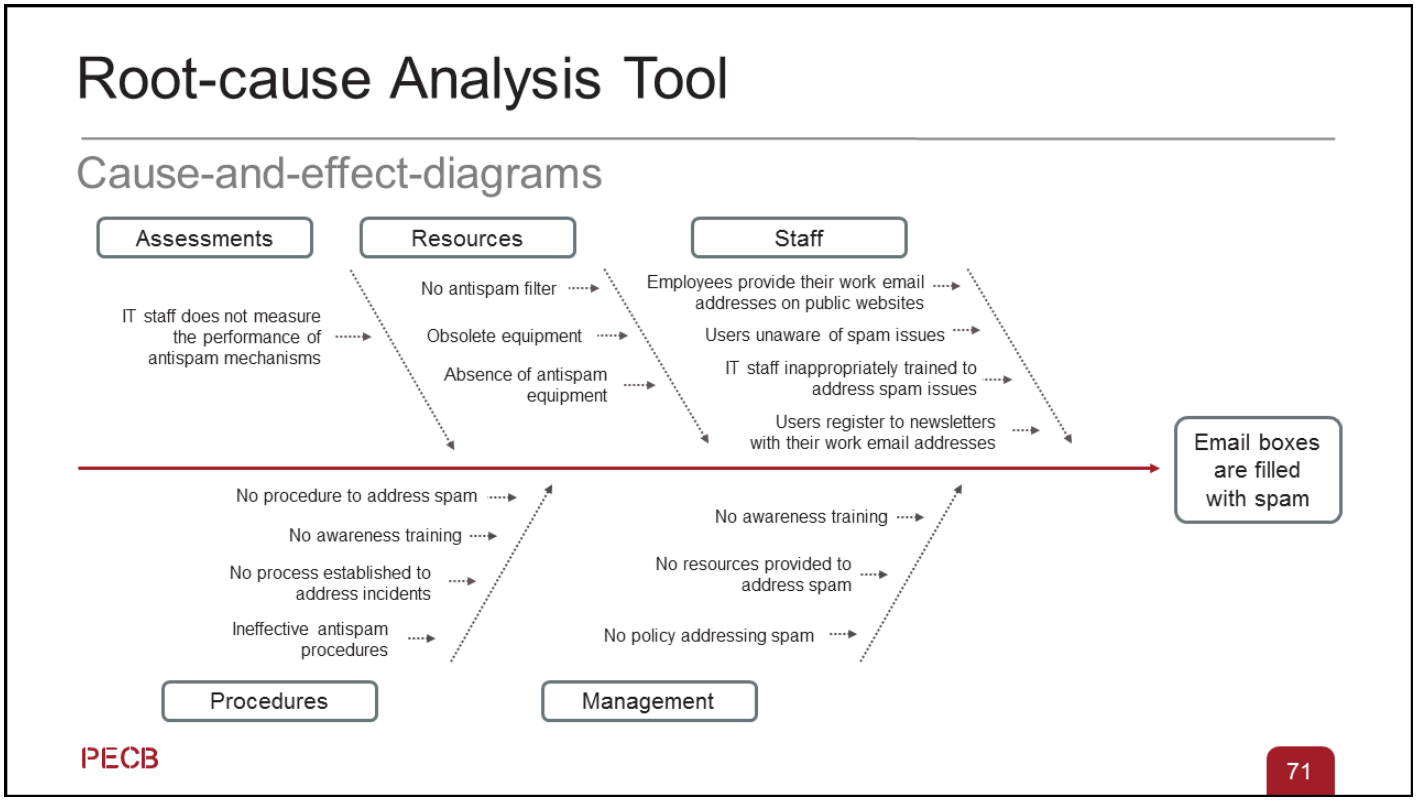
5.Choose and verify permanent corrections (PCs) for problem/nonconformity: Make sure that the chosen corrective action will resolve the problem for the client by means of pre-production programs.

Slide Notes Extension

PECB

70

6.Implement and validate corrective actions: Determine and implement the best corrective actions.
7.Take preventive measures: In order to avoid the repetition of the same or similar problems, take actions to modify the management systems, operation systems, practices, and procedures.
8.Congratulate your team: The organization should acknowledge the collective efforts of the team members and officially thank them for their work.



Root cause analysis is a method of resolving nonconformities based on identifying their root causes. This practice is based on the conviction that problems are best resolved when we correct or eliminate the root causes, as opposed to simply treating the immediate and obvious symptoms.

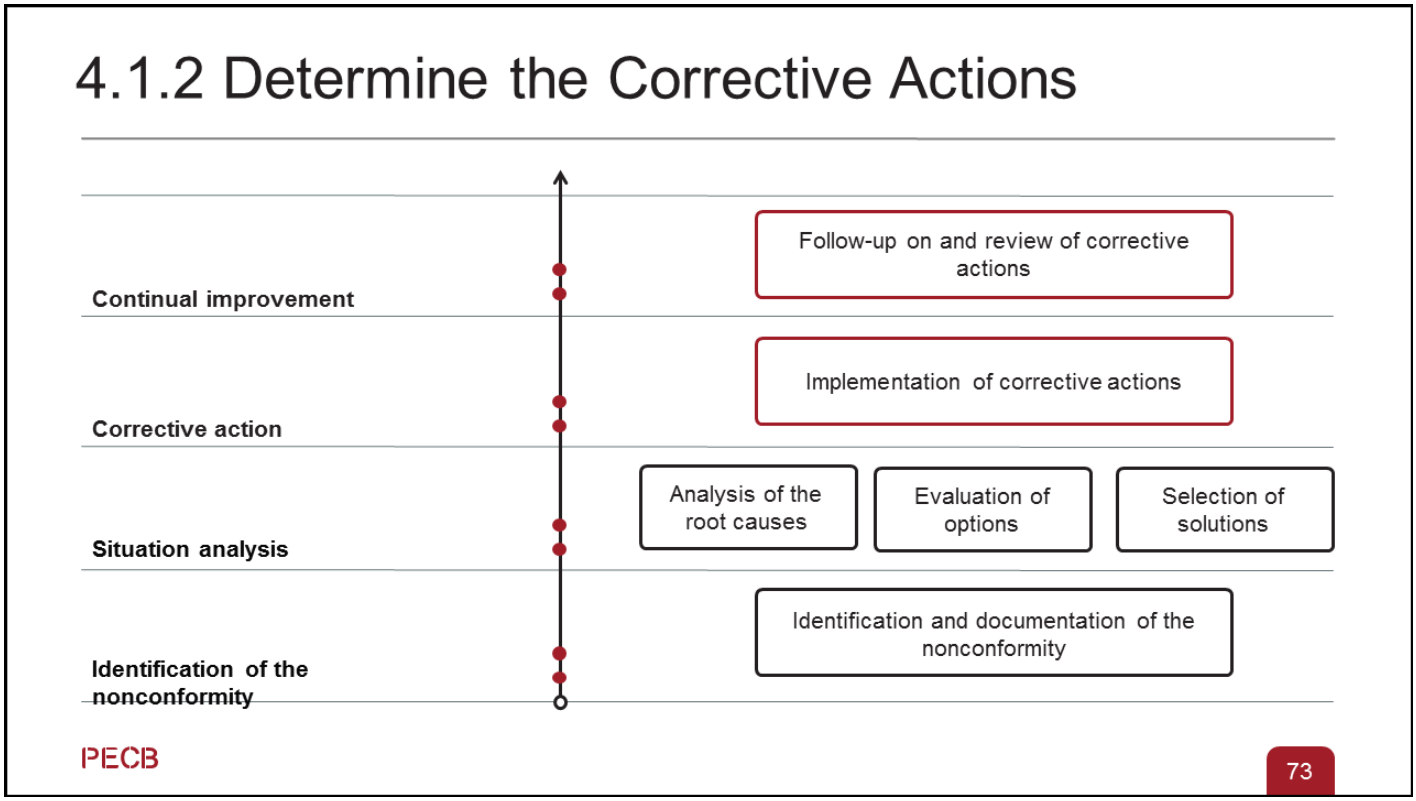
By putting in place measures to correct the root causes, the nonconformity recurrence is reduced to a minimum. Putting in place measures that treat root causes directly is more effective than treating the symptoms of problems. To be effective, the root cause analysis must be performed systematically and conclusions must be supported by evidence. For each problem analyzed, there is generally more than one root cause.

A cause-and-effect diagram is also known as a fishbone diagram, or the Ishakawa diagram. It is a root-cause analysis tool that maps the causes and the effects visually. Typically, it starts with the problem in the middle of the diagram (the spine of the fish skeleton). In our example, the problem is email boxes filled with spam. Then, it continues with sorting possible causes into different categories that branch from the original problem. In our example, these categories include assessments, resources, staff, procedures, and management. We can continue with breaking the categories into smaller parts to get closer to the root cause of the problem. It is vital to choose the categories wisely in order to identify the root and find the appropriate solution.

Asking the Right Questions

The questions needed for the analysis of any problem

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



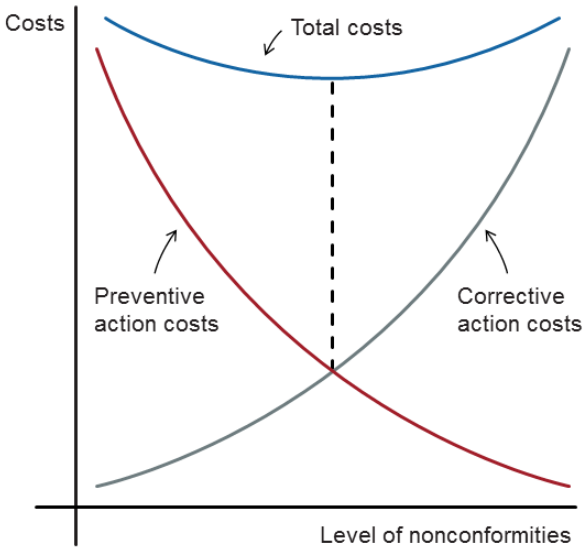
A corrective action is an action taken to **eliminate once and for all the root causes** of a nonconformity or of any other **existing** undesirable event, and to **prevent its recurrence.** A corrective action is, thus, a term that includes the reaction to a system problem process, to security incidents, to gaps in reaching objectives, to nonconformities, etc.

The corrective action process should include:

1. **Identification of the nonconformity:** The initial step in the process is to clearly define and document the nonconformity and analyze its impacts on the organization.
2. **Analysis of the root causes:** Determine the source of the nonconformity and analyze the root causes.
3. **Evaluation of solutions:** A list of possible corrective actions is elaborated. At this stage, if the problem is important, or if there is a considerably high probability that the problem will be repeated, temporary corrective actions can be set in place.
4. **Selection of solutions:** One or more corrective actions are selected to correct the situation and the contemplated improvement objectives are determined. The selected solution must correct the problem and should also contribute to the avoidance of the recurrence of similar situations.
5. **Implementation of corrective actions:** The corrective action plan approved is implemented and all the actions described in the plan are documented.
6. **Follow-up on corrective actions:** One must check that the new corrective controls are in place and effective. The follow-up is usually performed by the person responsible for the project and the audit department.
7. **Review of corrective actions:** To perform a review of the effectiveness of the corrective actions, it is periodically evaluated whether the organization has reached its security objectives using corrective actions, and if they remain effective over time.

4.1.3 Determine the Preventive Actions

The organization shall determine the actions to **eliminate the potential nonconformity causes** in accordance with the conditions of the ISMS.



PECB

74

A preventive action is any action taken to **eliminate the causes of a nonconformity** or any other **potentially** undesirable event, and to prevent their realization in future. Monitoring and adequate controls must be implemented in the ISMS to ensure that the potential problems are identified and eliminated before they occur.

It is to be noted that an action aiming to prevent nonconformities is often more cost-effective than a corrective action. **An organization should aim for cost/effectiveness balance between the implementation of corrective and preventive actions.**

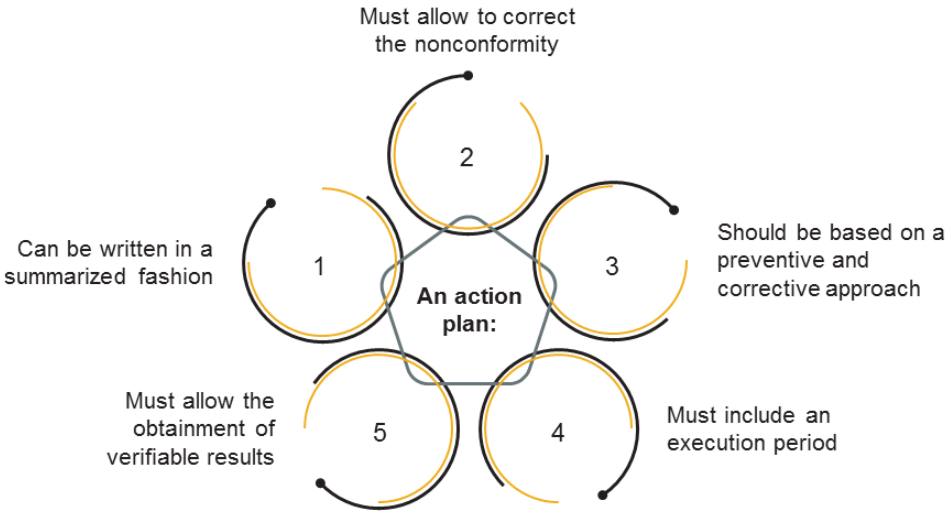
By establishing a continual risk management process, the organization is, usually, more likely to detect a change in the risk factors that concern the organization, because risks are not static. Threats, vulnerabilities, probability, or consequences can change abruptly. Consequently, constant monitoring is necessary to detect these changes and take preventive actions before a risk occurs.

The organization can ensure, for example, that the following are monitored:

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

The preventive actions process is similar to the corrective actions process: identifying a potential problem, evaluating solutions, choosing solutions, implementing preventive actions, and follow-up and review of preventive actions.

4.1.4 Draft an Action Plan



PECB

75

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

Submission of Action Plans Following an Audit

- Every nonconformity requires its own action plan; it is impermissible to include all nonconformities in a single inclusive action plan.
- Action plans must be approved by management.
- The auditor analyzes the cause and evaluates if the specific correction and corrective actions taken or planned to be taken allow the elimination of the detected nonconformities within a defined timeframe.

PECB

76

If, following the analysis, the management decides to accept the risk instead of implementing corrective, preventive, or improvement actions, 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

Example

1. A new system dedicated to the management of the client account data must be installed in the network to separate the confidential data from other databases (2nd quarter of 2019).

2. A new version of the security policy must be published to include legal and regulatory statements, as well as contract requirements (within 2 months).

3. The names of the persons to be contacted in case of disaster must be explicitly mentioned in the business continuity plan (immediately) and the procedures to contact these persons must be documented and communicated.

Exercise 16: Corrective action plan

An internal audit has been conducted in *e-Scooter* and several nonconformities have been detected. Propose corrective actions for each nonconformity and justify such actions.

1. After the internal audit, a nonconformity has been issued regarding the lack of a business continuity plan and the criteria for its activation during a disaster. In an interview with the company's CEO, it was claimed that he is planning on establishing a business continuity plan, but was first working on some other priorities. However, the interviews conducted with employees revealed that, despite the lack of a documented business continuity plan, they are required to report any potential interruption or crisis to the CEO.
2. The company did not process an incident within the time frame determined in its incident management policy. This policy explicitly points out that, as a target, all incidents should be closed within five days and that 100% of incidents must be closed within 15 days from the time being reported. For this incident, a customer who rented an e-Scooter reported to have fallen victim of a credit card fraud and wanted a full refund. The person in charge of managing this incident was absent and returned to the office after 12 days. By the time they started to process the incident, there was plenty of work to be done and the credit card fraud case was so complex that it took another five days to deal with this issue, investigate, and close the incident. Nobody else in the company took care of the incidents during the employee's absence.
3. According to the internal audit conclusions, when e-Scooter's application went down last week, the third-party (cloud provider) responsible for maintaining the application did not intervene for 72 hours. This has caused a financial damage of approximately $35,000 during the application's unavailability, an amount considered unacceptable to the company.

Duration of the exercise: 30 minutes

Comments: 15 minutes

1.An action taken to eliminate the cause of a potential nonconformity or other potential undesirable situation is known as:

A. Correction
B. Corrective action
C. Preventive action

2.What does the root-cause analysis involve?

A. Determining the source of the nonconformity
B. Defining and analyzing the impacts of the nonconformity
C. Selecting the solutions

3.An organization has integrated the identification of interruptions for business continuity in their annual ISMS risk assessment. How would you assess the situation?

A. Conformity
B. Major nonconformity
C. Minor nonconformity

4.Which step should be taken first, according to the eight disciplines problem solving method?

A. Plan
B. Define and describe the problem
C. Use a team

5.All nonconformities should be included in a single inclusive action plan.

A. True
B. False

6.The auditee has not submitted the action plans within the specified deadline. What follows?

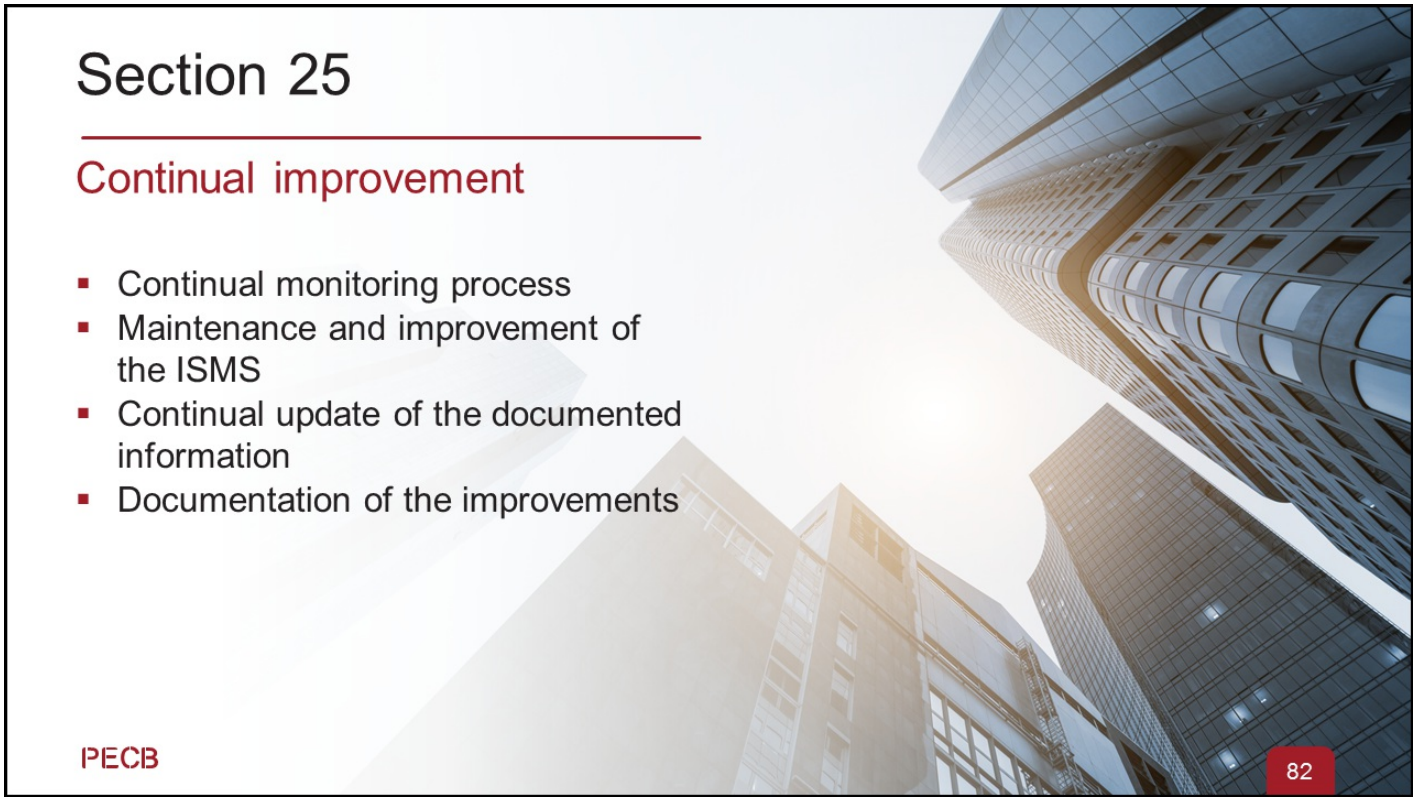
A. The certification body will be involved
B. The auditor will issue a minor nonconformity
C. The organization will not be recommended for certification

7.What are the activities that should be included in the situation analysis phase of the corrective action process?

A. Identification and documentation of the nonconformities
B. Follow- up on and review of corrective actions
C. Evaluation of options and selection of solutions

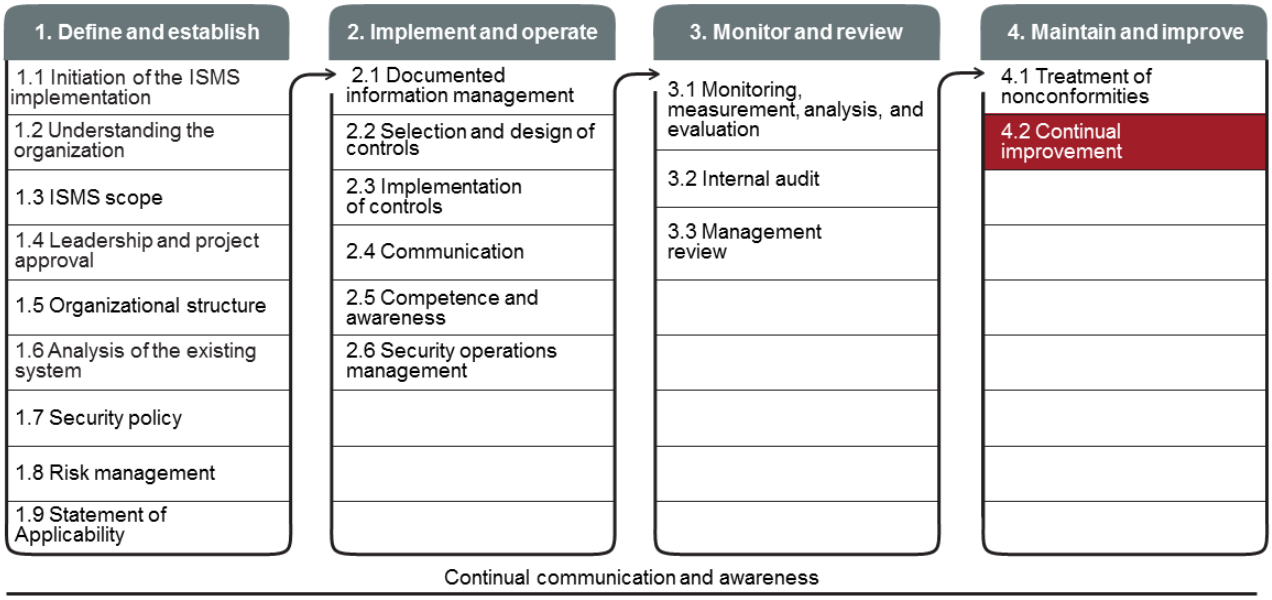
Section summary

- Organizations should define a process to react effectively to nonconformities and review, evaluate, and treat them.
- The treatment of nonconformities requires defining a process to resolve them, determining the corrective and preventive actions, and drafting the action plan.
- Drafting an action plan should include the correction of nonconformities, the execution period, and the obtainment of verifiable results.
- An action plan should be submitted for each nonconformity within specified deadlines.



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

4.2 Continual Improvement



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 10.2

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

PECB

84

An organization wishing to comply with ISO/IEC 27001 shall at least demonstrate that actions are taken to continually improve the effectiveness of the ISMS

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.

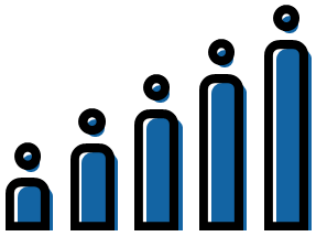
Guidance

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.*

Continual Improvement

Continual improvement is the process of increasing the effectiveness and efficiency of the organization to fulfill its policy and objectives.



In small but **certain** steps

PECB

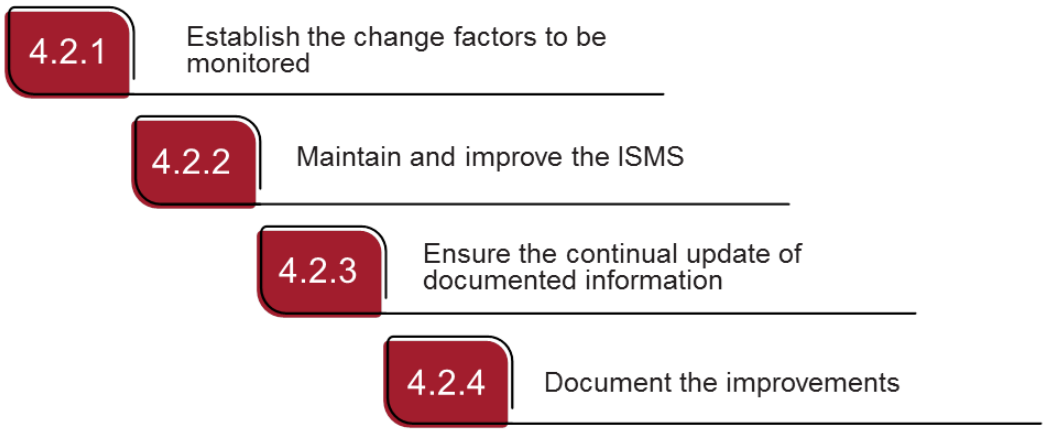
85

Emphasis is placed on continual improvement through the setting of organizational performance goals, measurement, and review, and the subsequent modification of processes, systems, resources, capability, and skills.

This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there should be at least one annual review of performance and a revision of processes, followed by the setting of revised performance objectives for the following period.

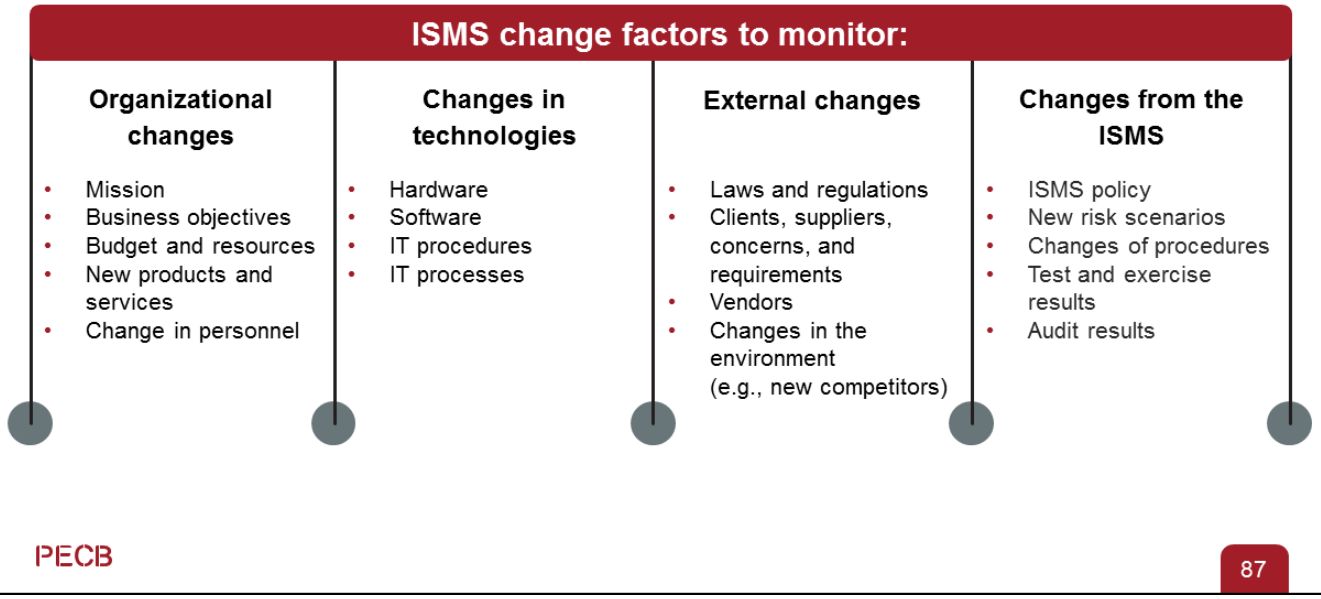
4.2 Continual Improvement

List of activities



PECB

4.2.1 Establish the Change Factors to Be Monitored



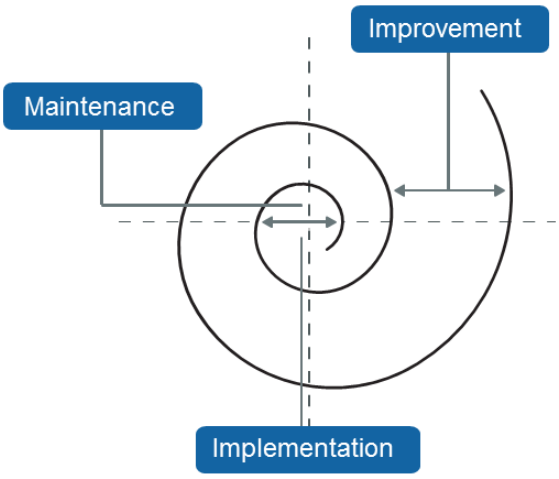
To be effective, the management system should accurately reflect the business requirements, procedures, organizational structure, and policies. During the continual improvement phase, the processes and procedures undergo frequent changes because of shifting business needs, technology upgrades, or new internal or 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 new information is documented and controls are revised, if required.

As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency, or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will 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 upon 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:

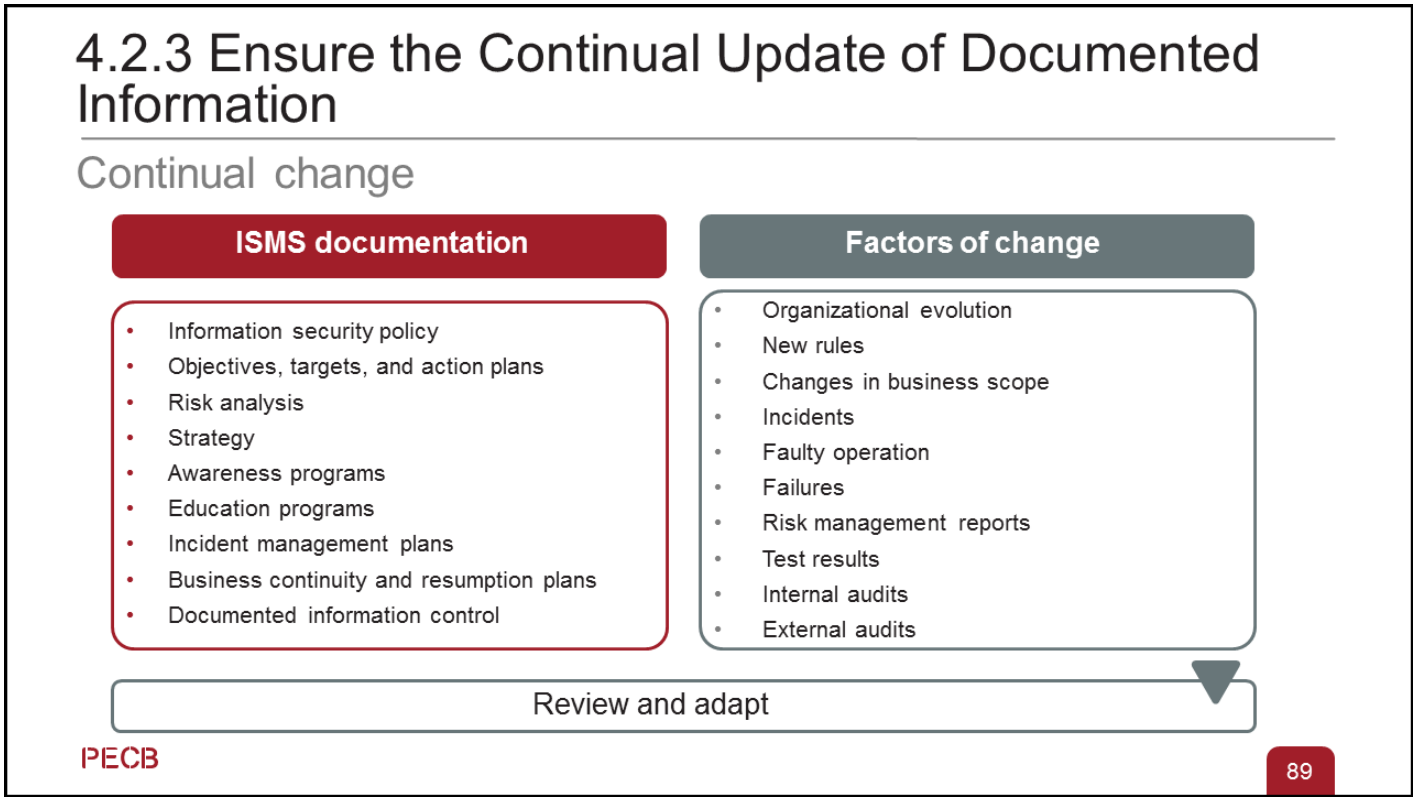
- It is the initial development and documented evidence of the strategy.
- It undergoes a significant change in the key technology or telecommunications, including systems or networks.
- The pace of business change is particularly aggressive.

4.2.2 Maintain and Improve the ISMS



- The ISMS needs to be maintained and updated periodically.
- The respective information security managers should be notified regarding any agreed actions to be taken to improve the processes so that no risk or risk element is overlooked or underestimated before the changes are implemented.

PECB



The ISMS documentation is the cornerstone of a properly functioning 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 in an emergency to follow a guide of actions instead of taking ad hoc decisions based on improvisation or intuition.

Proper maintenance of documented information by no means eliminates spontaneous decisions since one should not expect that it is entirely up to date. It simply 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 documented information must be adapted on each and every trigger of change.

The Benefits of Continual Improvement

Continual change

PECB

4.2.4 Document the Improvements

Usually by the change management procedure

Record of changes			
Page no.	Change comment	Date of change	Signature

PECB

91

The ISMS coordinator should record plan modifications using a record of changes, which lists the page number, change comment, and date of change. The record of changes, depicted in the slide, should be integrated into the different documents included in the ISMS.

1. **Which of the following is an activity taken toward continual improvement?**
   A. Determining measurement objectives
   B. Establishing the ISMS performance indicators
   C. Establishing the change factors to be monitored
2. **The continual _____ ensures continual improvement.**
   A. Changes in laws and regulations
   B. Alterations in the business scope
   C. Update of documented information
3. **What should be reviewed and updated on a continual basis?**
   A. The information security incidents
   B. The information security policy
   C. The information security failures
4. **What is the correlation between continual improvement and information security errors?**
   A. Continual improvement helps reduce the number of errors
   B. Continual improvement helps increase the number of errors
   C. Continual improvement introduces new errors
5. **An action taken to eliminate the causes of a nonconformity helps in the creation of a continual improvement culture.**
   A. True
   B. False

Section summary

- Continual improvement helps organizations fulfill their policies and objectives.
- An organization should continually improve the effectiveness of the ISMS by establishing the change factors to be monitored, ensuring the continual update of documented information, and documenting the improvements.
- Continual improvement helps organizations increase efficiency and customer satisfaction, reduce errors, and build teamwork.

This section provides information that will help the participant gain knowledge about certification audits, selecting the certification body, preparing for the audit, and conducting the stage 1 and 2 audits. Moreover, the participant will acquire knowledge on the follow-up audit and the certification decision.

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 1

The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

PECB

95

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

1. Conform to clauses 4 to 10 and to all applicable security controls
2. Have an ISMS that is operational since at least three months

Accreditation Body

National organizations which supervise certification programs (organizations and professionals) of certification bodies and assess their competence to perform certification activities.

PECB

96

ISO/IEC 17011 specifies the general requirements for accreditation bodies that aim at assessing and accrediting certification bodies. It consists of requirements that support the peer evaluation process for mutual recognition arrangements between accreditation bodies.

Usually, there is only one accreditation authority in each country. However, in the United States, there are different accreditation bodies, including IAS, ANSI, 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 American National Standards Institute (ANSI) supervises the certification bodies accredited against ISO/IEC 17024.
- The ANSI-ASQ 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 nationally recognized based in the European geographic sector. The members include UKAS, COFRAC, BNAC, ENAC, etc.
Source: www.european-accreditation.org

International Accreditation Forum (IAF) is the international association of accreditation organizations for systems in management, product, services, individuals, and other programs of this type. Their objective is to ensure that the member national certification organizations only certify competent organizations and establish agreements of mutual recognition among its members. You can find a list of accreditation authorities for several countries on the IAF official website.
Source: www.iaf.nu

Slide Notes Extension

PECB

97

The following is a list of accreditation authorities for several countries (see the complete list on the IAF website: www.iaf.nu):

Argentina: Organismo Argentino de Acreditación (OAA), www.oaa.org.ar

Australia and New Zealand: Joint Accreditation System of Australia and New Zealand (JAS-ANZ), www.jas-anz.org

Austria: Federal Ministry of Economy, Family and Youth (BMWFJ), www.en.bmdw.gv.at

Belgium: Belgian Accreditation Body (BELAC), www.belac.fgov.be

Brazil: General Coordination for Accreditation (CGCRE), www.inmetro.gov.br

Canada: Standards Council of Canada (SCC), www.scc.ca

Chile: Instituto Nacional de Normalizacion (INN), www.inn.cl

China: China National Accreditation Service for Conformity Assessment (CNAS), https://www.cnas.org.cn/english/index.shtml

Egypt: Egyptian Accreditation Council (EGAC), www.egac.gov.eg

Finland: Finnish Accreditation Service (FINAS), www.finas.fi

France: Comité Français d'Accréditation (COFRAC), www.cofrac.fr

Germany: Deutsche Akkreditierungsstelle GmbH (DAkkS), www.dakks.de

Hong Kong, China: Hong Kong Accreditation Service (HKAS), www.itc.gov.hk/hkas

India: National Accreditation Board for Certification Bodies (NABCB), www.qcin.org

Iran: National Accreditation Center of Iran (NACI), http://www.naci.isiri.org

Ireland: Irish National Accreditation Board (INAB), www.inab.ie

Japan: International Accreditation Japan (IAJapan), www.jab.or.jp

Korea: Korea Accreditation System (KAS), www.iaf.nu/articles/IAF_MEM_Korea_Republic_of_/86

Malaysia: Standards Malaysia (DSM), www.jsm.gov.my

Mexico: Mexican Accreditation Entity (EMA), www.ema.org.mx

Netherlands: Dutch Accreditation Council (Raad Voor Accreditatie) (RvA), www.rva.nl

Norway: Norwegian Accreditation (NA), www.akkreditert.no

Pakistan: Pakistan National Accreditation Council (PNAC), www.pnac.org.pk

Philippines: Philippine Accreditation Office (PAB), www.dti.gov.ph

Portugal: Portuguese Institute for Accreditation (IPAC), www.ipac.pt

Romania: Romanian Accreditation Association (RENAR), www.renar.ro

Russian Federation: Scientific Technical Center on Industrial Safety (STC-IS), www.oaontc.ru/en/

Singapore: Singapore Accreditation Council (SAC), www.sac-accreditation.gov.sg

Slovenia: Slovenska Akreditacija (SA), www.slo-akreditacija.si

South Africa: South African National Accreditation System (SANAS), www.sanas.co.za

Spain: Entidad Nacional de Acreditacion (ENAC), www.enac.es

Sweden: Swedish Board for Accreditation and Conformity Assessment (SWEDAC), www.swedac.se/?lang=en

Switzerland: State Secretariat for Economic Affairs, Swiss Accreditation Service (SAS), www.sas.ch

Thailand: National Standardization Council of Thailand (NSC), www.tisi.go.th

Tunisia: Tunisian Accreditation Council (TUNAC), www.tunac.tn

Turkey: Turkish Accreditation Agency (TURKAK), www.turkak.org.tr

Slide Notes Extension

PECB

98

United Arab Emirates: Emirates International Accreditation Center (EIAC), www.eiac.gov.ae

United Kingdom: United Kingdom Accreditation Service (UKAS), www.ukas.com

United States: ANSI-ASQ National Accreditation Board (ANAB), www.anab.org

United States: American National Standards Institute (ANSI), www.ansi.org

United States: International Accreditation Services (IAS), www.iasonline.org

Uruguay: Organismo Uruguayo de Acreditacion (OUA)

Vietnam: Bureau of Accreditation (BoA), www.boa.gov.vn/en

Certification Bodies

ISO/IEC 17021-1

- **Certification body:** Third party that performs the assessment of conformity of management systems
- **Certification:** Procedure in which a third party attests in writing that a product, process, or service conforms to the specified criteria

PECB 99

ISO/IEC 17021-1, clause 1 Scope

This part of ISO/IEC 17021 contains principles and requirements for the competence, consistency and impartiality of bodies providing audit and certification of all types of management systems.

Certification bodies operating to this part of ISO/IEC 17021 do not need to offer all types of management system certification.

Certification of management systems is a third-party conformity assessment activity and bodies performing this activity are therefore third-party conformity assessment bodies.

NOTE 1 Examples of management systems include environmental management systems, quality management systems and information security management systems.

NOTE 2 In this part of ISO/IEC 17021 certification of management systems is referred to as "certification" and third-party conformity assessment bodies are referred to as "certification bodies".

NOTE 3 A certification body can be non-governmental or governmental, with or without regulatory authority.

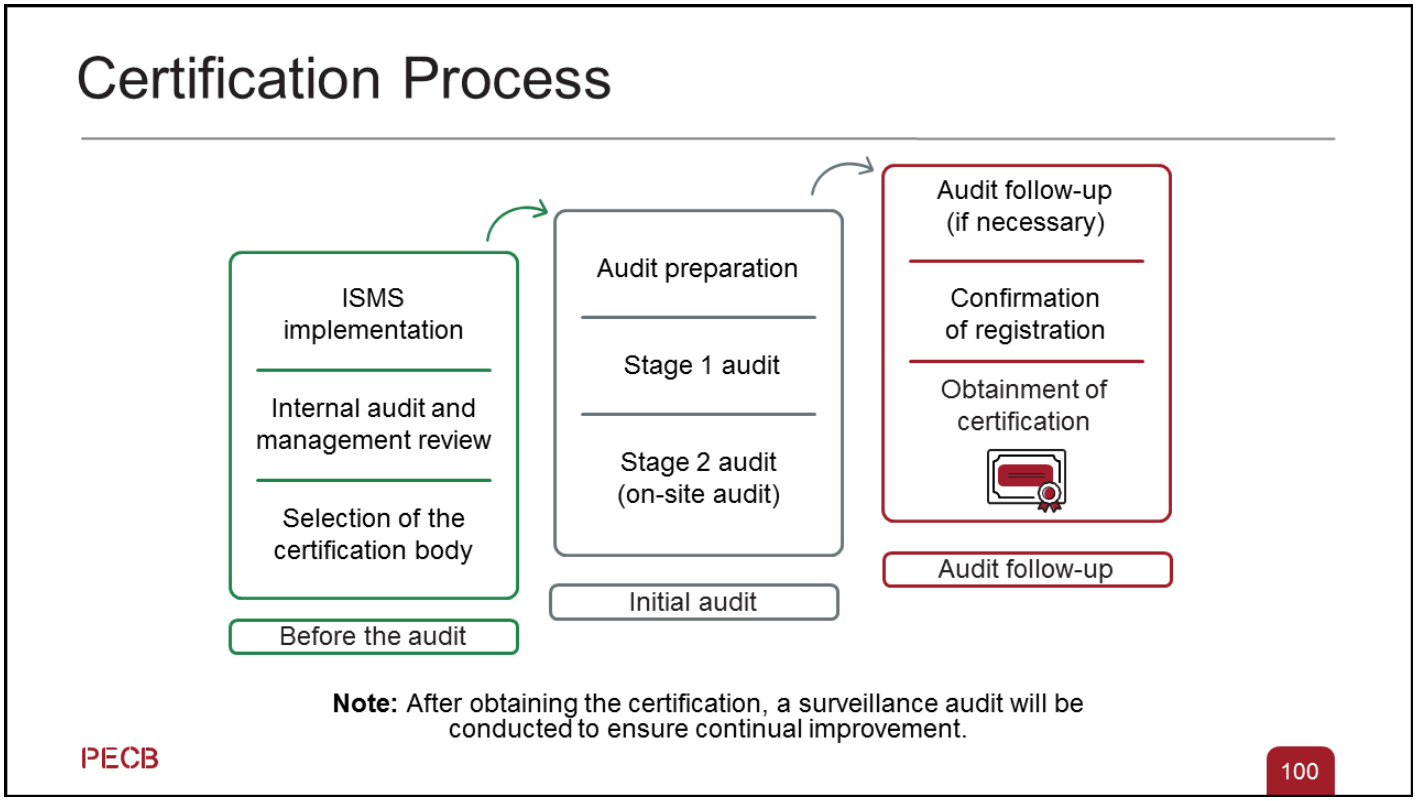
NOTE 4 This part of ISO/IEC 17021 can be used as a criteria document for accreditation, peer assessment or other audit processes.

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.*

Certification activities involve the audit of an organization's management system. The form of attestation of conformity of an organization's management system to a specific management system standard or other normative requirements is usually a certification document or a certificate.



Obtaining a certification for the organization:

1. Implement the ISMS
2. Conduct an internal audit and a management review
3. Select the certification body
4. Prepare the certification audit
5. Conduct the stage 1 audit
6. Conduct the stage 2 audit (on-site audit)
7. Conduct the audit follow-up
8. Confirm the registration
9. Obtain the ISO/IEC 27001 certification

Important note: Continual improvement can be described as an ongoing process to improve procedures, processes, and the organization's products or services in general.

The surveillance audit is an activity that is performed once a year (or more), based on the organization's needs to maintain confidence that the organization's management system fulfills the requirements of the particular management system (standard).

Slide Notes Extension

PECB

101

1. **Selection of the certification body (registrar):** Each organization can select the certification body of its choice.
2. **Pre-assessment audit (optional):** An organization can choose to perform a pre-audit to measure the gap between its 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 auditee's premises).
4. **Stage 2 audit (on-site visit):** The objective of stage 2 audit is to evaluate whether the declared management system conforms to all the requirements of the standard, is actually being implemented in the organization, and can support the organization in achieving its objectives. Stage 2 audit takes place at the auditee's premises where the management system is actually implemented.
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.

Note: The terms "organization" and "auditee" have been used interchangeably in this page.

Certification and Attestation

Differences

Certification

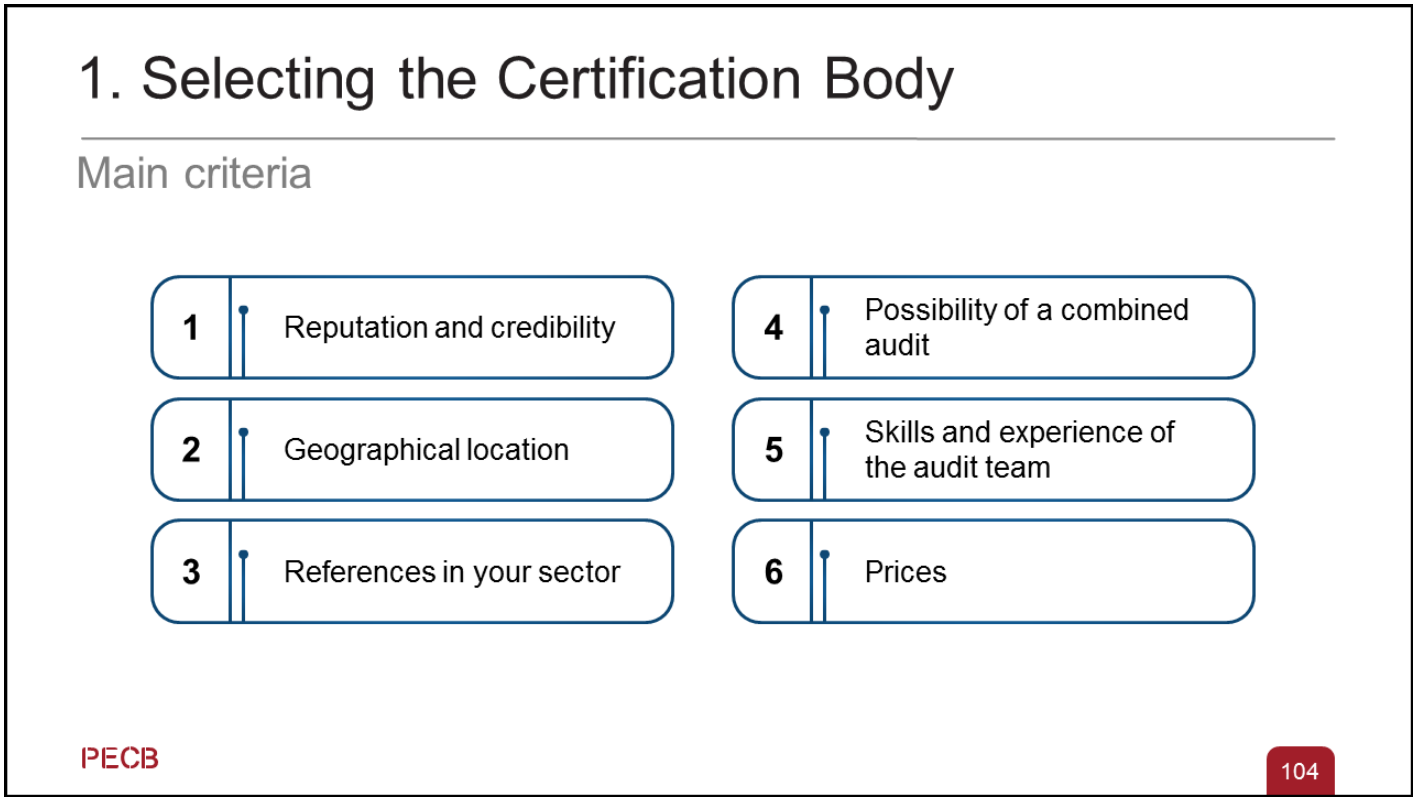
Certification is a formal procedure which attests to a status or a level of achievement by providing an official document.

Attestation

Attestation is a method used to check, confirm, and authenticate the validity of a document.

Before the Audit

- Before being audited, an ISMS must be in operation for at least three-months.
- In addition, at least an internal audit and a management review must have been conducted.



The following are the main criteria in selecting a certification body:

1. **Reputation and credibility** — The value of the 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** — It is advisable to choose 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.
3. **References in your sector** — If the industry you operate in has specific regulatory requirements, it is desirable to select a certification body that already has clients in your business sector.
4. **Possibility of a combined audit** — If you consider certifying your organization against several standards (e.g., ISO 9001 or 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 Lead Auditor of the certification body to ensure that the audit team has the necessary competences and skills to perform the audit.
6. **Prices** — Prices vary lightly 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, which influences audit costs.

Model: How Long Should the Audit Last?

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

Number of employees	Audit time (day/person) ISO 9001	Audit time (day/person) ISO/IEC 27001
1 to 10	1.5 – 2	5
11 to 15	2.5	6
16 to 25	3	7
26 to 45	4	8.5
46 to 65	5	10
66 to 85	6	11
86 to 125	7	12
126 to 175	8	13
176 to 275	9	14

PECB

105

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

Model: How Long Should the Audit Last?

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

Number of employees	Audit time (day/person) ISO 9001	Audit time (day/person) ISO/IEC 27001
276 to 425	10	15
426 to 625	11	16.5
626 to 875	12	17.5
876 to 1175	13	18.5
1176 to 1550	14	19.5
1551 to 2025	15	21
2026 to 2675	16	22
2676 to 3450	17	23
3451 to 4350	18	24

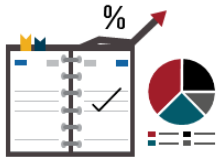
PECB

Rejection of an Auditor

- The auditee can request the replacement of audit team members for valid reasons.
- The audit team could withdraw if it deems that the reasons cited are not valid.

Examples of valid reasons:

- The auditor is in a conflict of interest situation (real or potential).
- The auditor has previously displayed unprofessional conduct.
- The auditor does not hold the security clearance required by the auditee.



PECB

107

The audit client or the auditee can request the replacement of an audit team member for valid reasons. Alternately, the audit team could withdraw if it considers that the reasons are not valid.

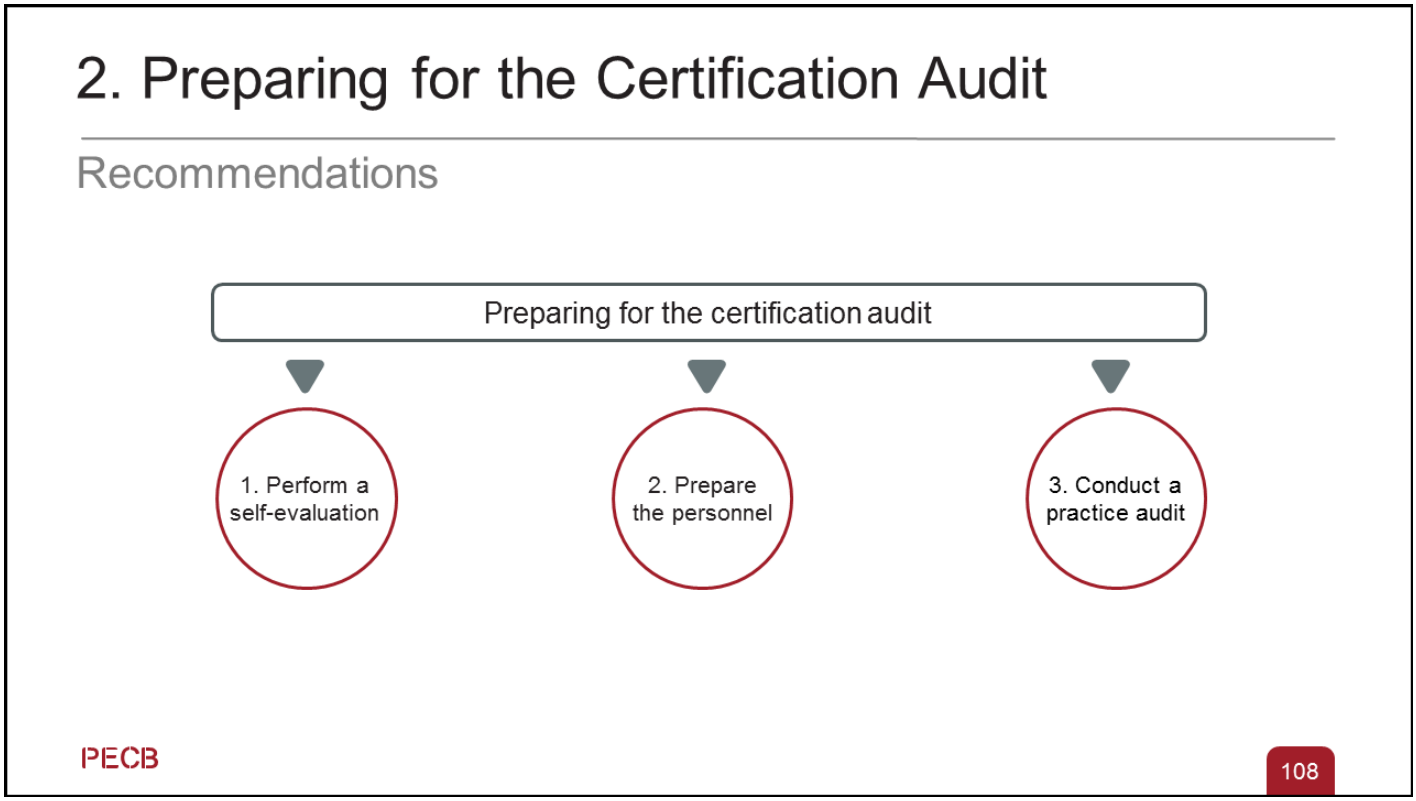
A valid reason would be the case of an auditor having previously displayed unprofessional conduct. Other examples of valid reasons are situations with real (a member of the audit team has worked for the auditee) or perceived (an auditee could ask to replace an auditor who has worked for one of its major competitors) conflict of interest.

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 making a decision concerning the replacement of an audit team member.

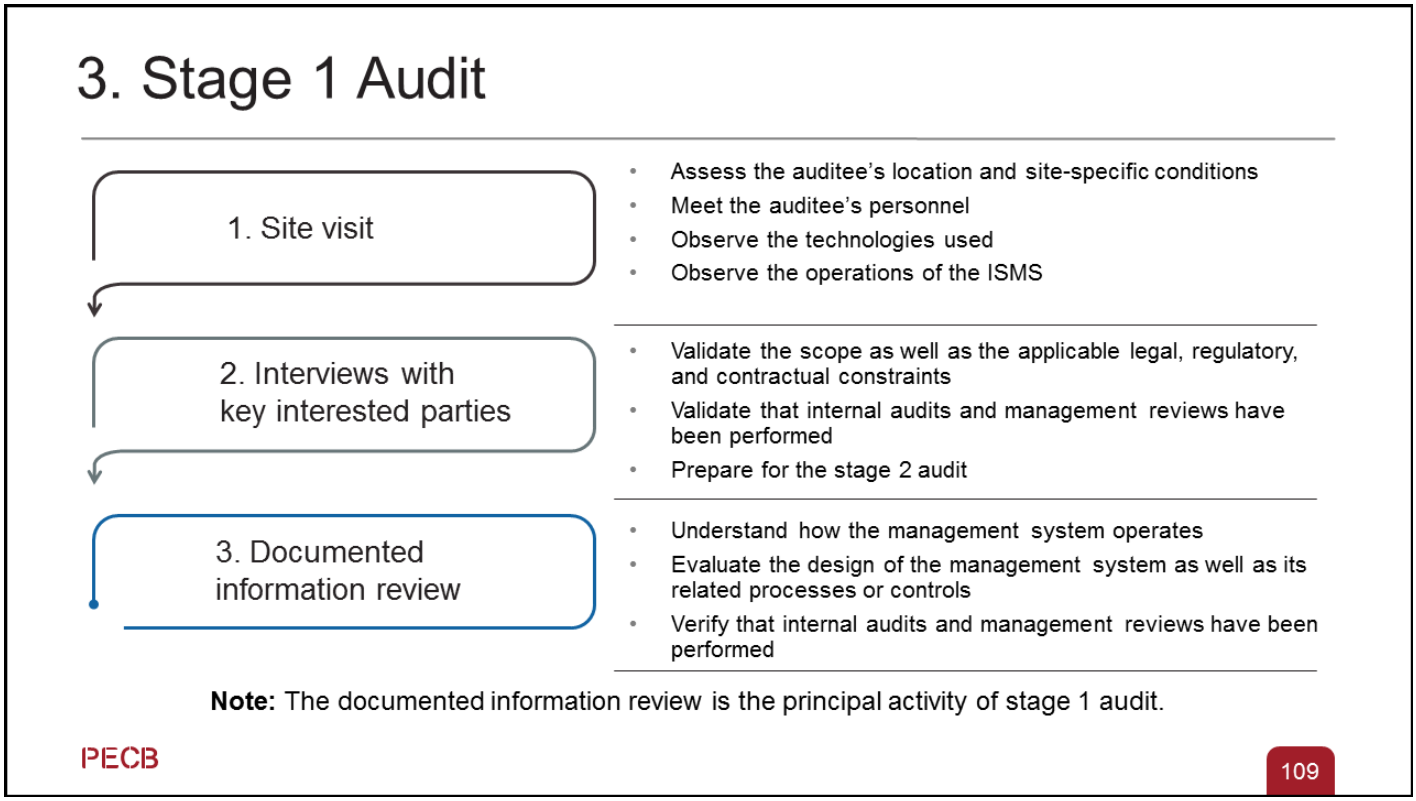
ISO/IEC 17021-1, clause 9.2.3.5 Communication concerning audit team members

The certification body shall provide the name of and, when requested, make available background information on each member of the audit team, with sufficient time for the client to object to the appointment of any particular audit team member and for the certification body to reconstitute the team in response to any valid objection.



Before the external auditors come to audit the organization, it is recommended to:

1. **Perform a self-evaluation** — Review the requirements of clauses 4 to 10 and address the following questions:
    - Is the process appropriately defined?
    - Have the responsibilities been defined?
    - Is documented information maintained?
    - Is the process effective in obtaining the required results?
2. **Prepare the personnel** — Prepare the employees for the audit by:
    - Organizing training sessions
    - Conducting practice interviews
    - Preparing “cheat sheets”
    - Reviewing documented information
3. **Conduct a practice audit —** Make sure during the practice audit to:
    - Review the documented information
    - Prepare the personnel
    - Advise the management regarding the audit
    - Accompany the organization during the audit



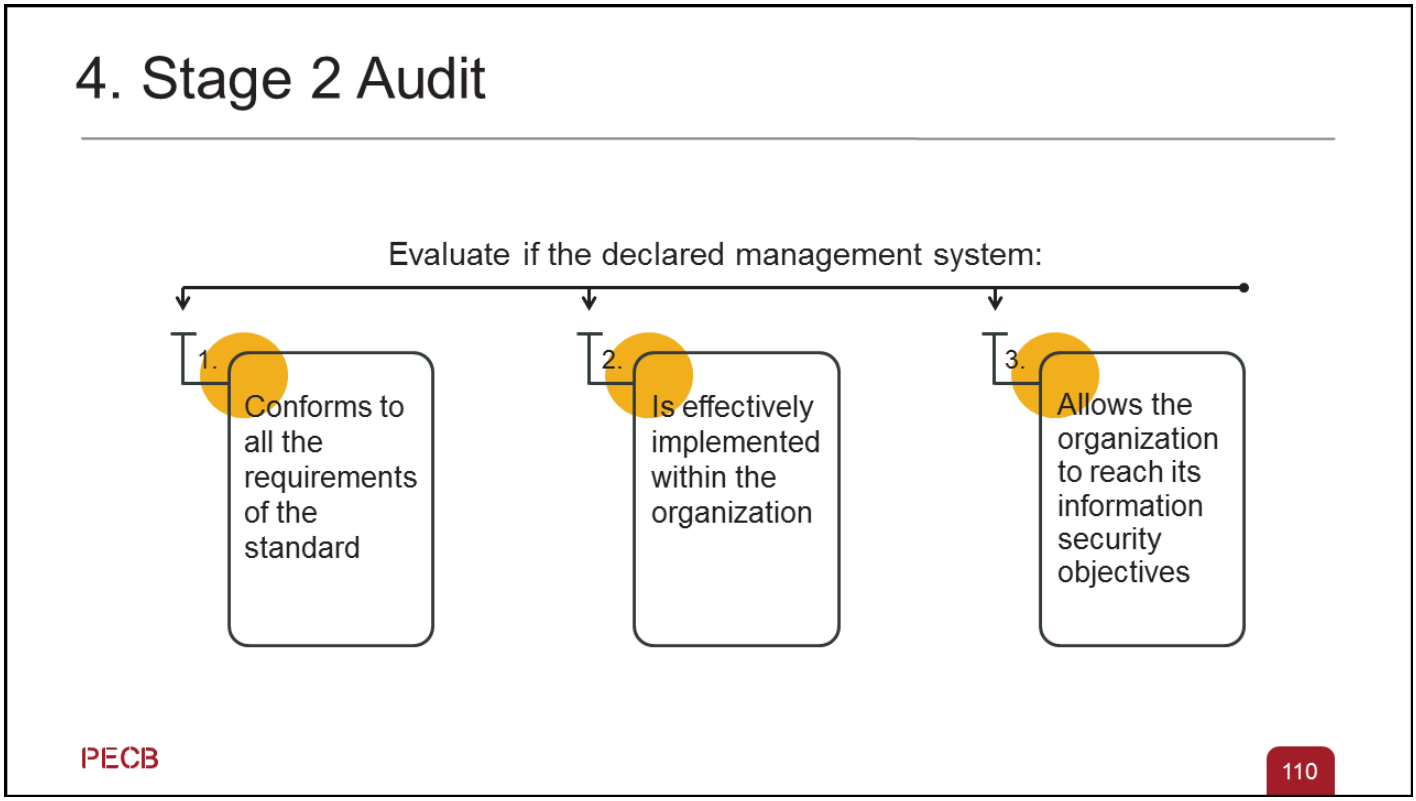
During the stage 1 audit, the auditor does not verify the effectiveness of the management system in place, but verifies the "design" of the management system. The auditor will check the effectiveness of the management system during the stage 2 audit (on-site audit) to validate whether the documented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

The stage 1 audit ideally takes place two to four weeks before the stage 2 audit (on-site).

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

In certain circumstances, the stage 1 audit can be combined (or performed at a distance) with the stage 2 audit, so as to not jeopardize the effectiveness of the audit. This is often the case when the audit team members must travel over long distances to perform the audit.

It is to be noted that, even though a confidentiality agreement is signed, **an auditee has the right to require that the documented information review takes place on-site and that no document 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. Recommendation for certification
2. Recommendation for certification conditional upon the filing of corrective action plans without prior visit
3. Recommendation for certification conditional upon the filing of corrective action plans with prior visit
4. Unfavorable recommendation

PECB

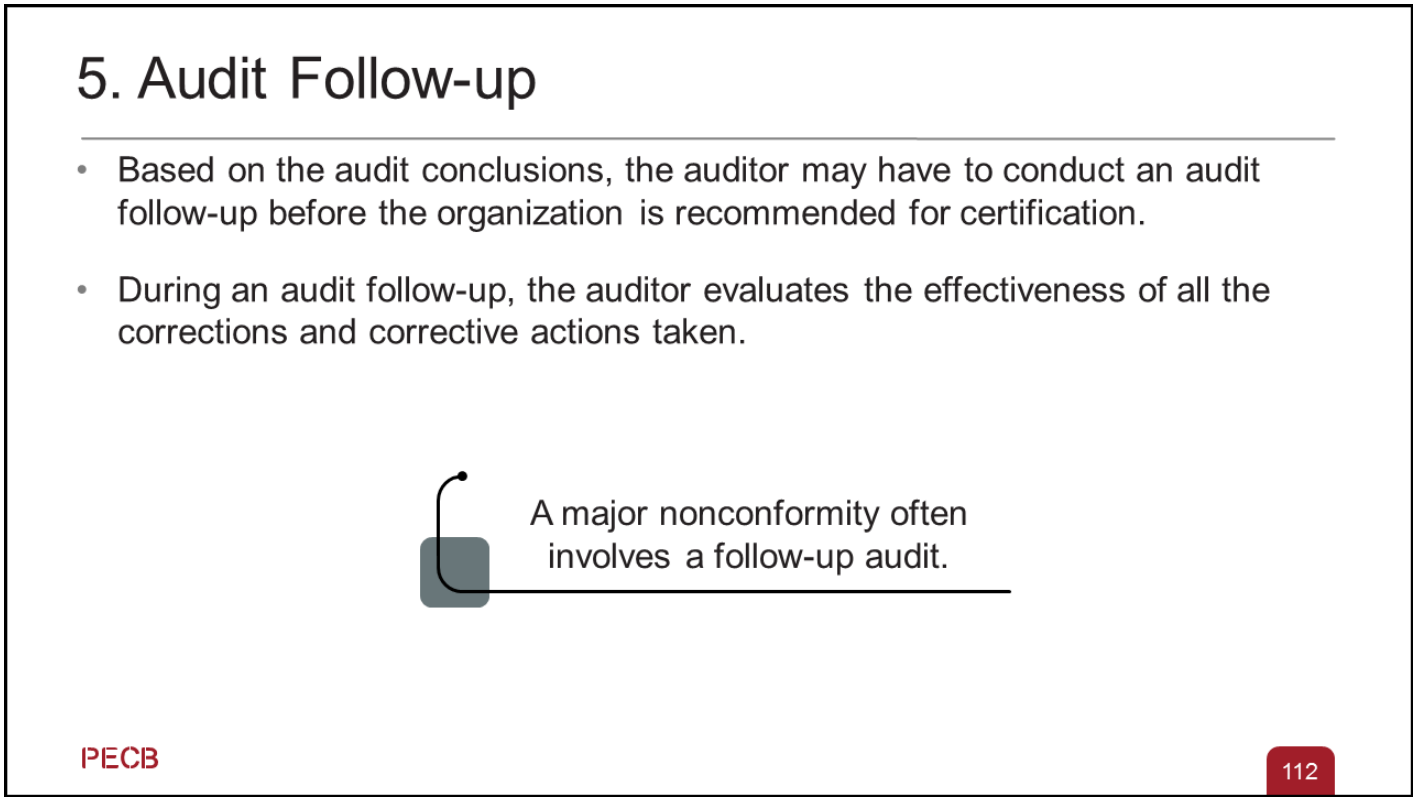
111

1.Recommendation for certification: The auditor is reasonably sure that the auditee conforms to the standard requirements. No nonconformity was observed during the audit.

2.and 3. Recommendation for certification conditional upon the submission of corrective action plans: The auditor is reasonably sure that the auditee conforms to the standard requirements; however, a certain number of minor nonconformities were detected. The auditee is required to submit an action plan of corrective measures for each minor nonconformity within a short period of time. If the action plan is accepted, the auditee can be certified. In some cases, the auditor can require a new visit on-site before issuing the certification recommendation. When there is no additional on-site visit required prior to certification, a verification of corrective measures included in the action plans will be validated during the surveillance visits.

4.Unfavorable recommendation: The auditor recommends not to issue a certificate to the auditee. A new full or partial audit is recommended. If one or more major nonconformities are reported, the auditor should issue an unfavorable recommendation. It is to be noted that there is no public statement of organizations having received negative recommendations. A public statement is only issued for certified organizations (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.



Being an integral part of the initial audit process, the audit follow-up activities should be planned with as much attention and detail as the other steps necessary for the execution of the audit.

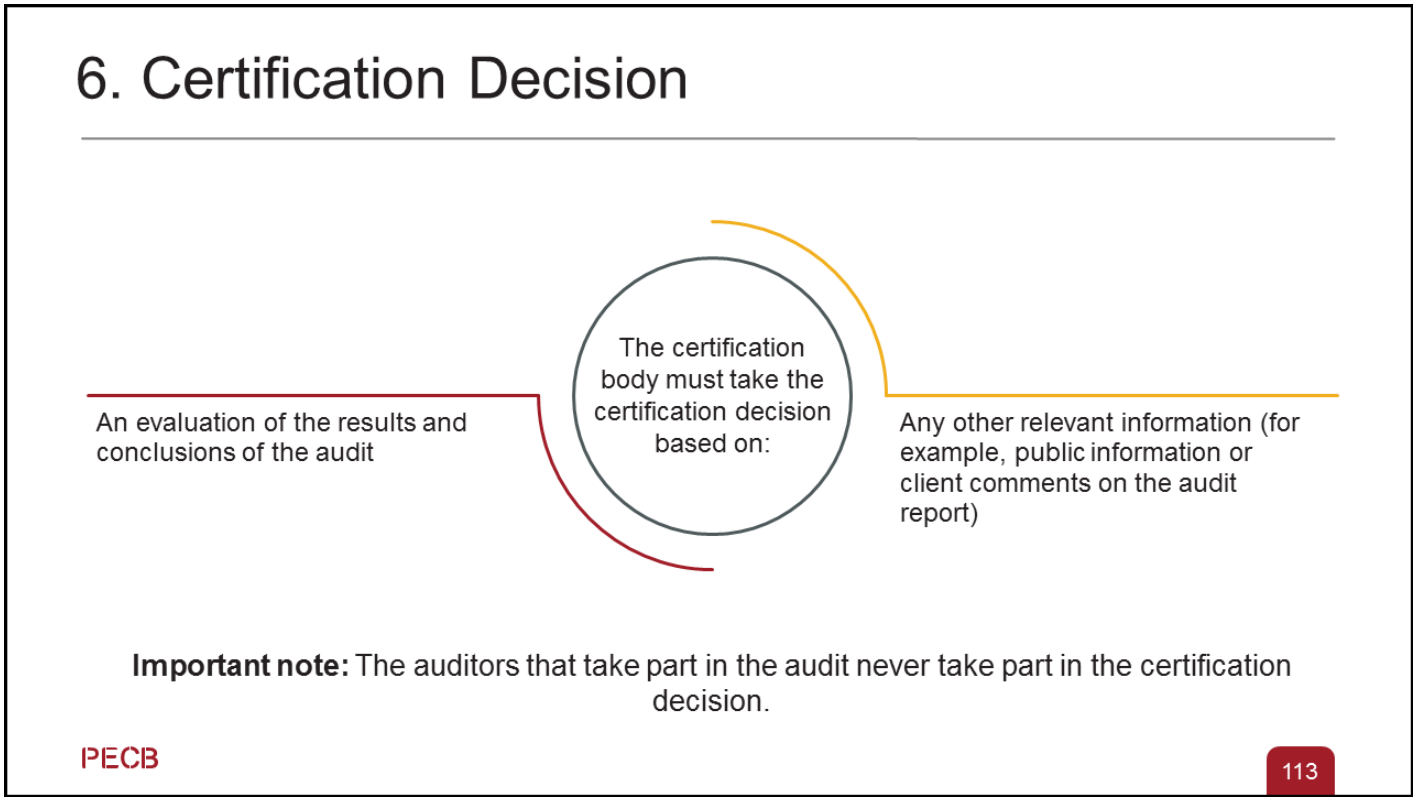
The objective of the audit follow-up is to validate the action plans submitted by the auditee and the implemented corrective actions. If any major nonconformities have been raised, the organization must resolve them before being recommended for certification.

An audit follow-up is usually performed 4 to 12 weeks after the initial audit in order to give the organization time to respond to the audit report and implement the corrective measures. The audit follow-up usually lasts only one 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 programme 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 programme and reported to the audit client for management review.



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.

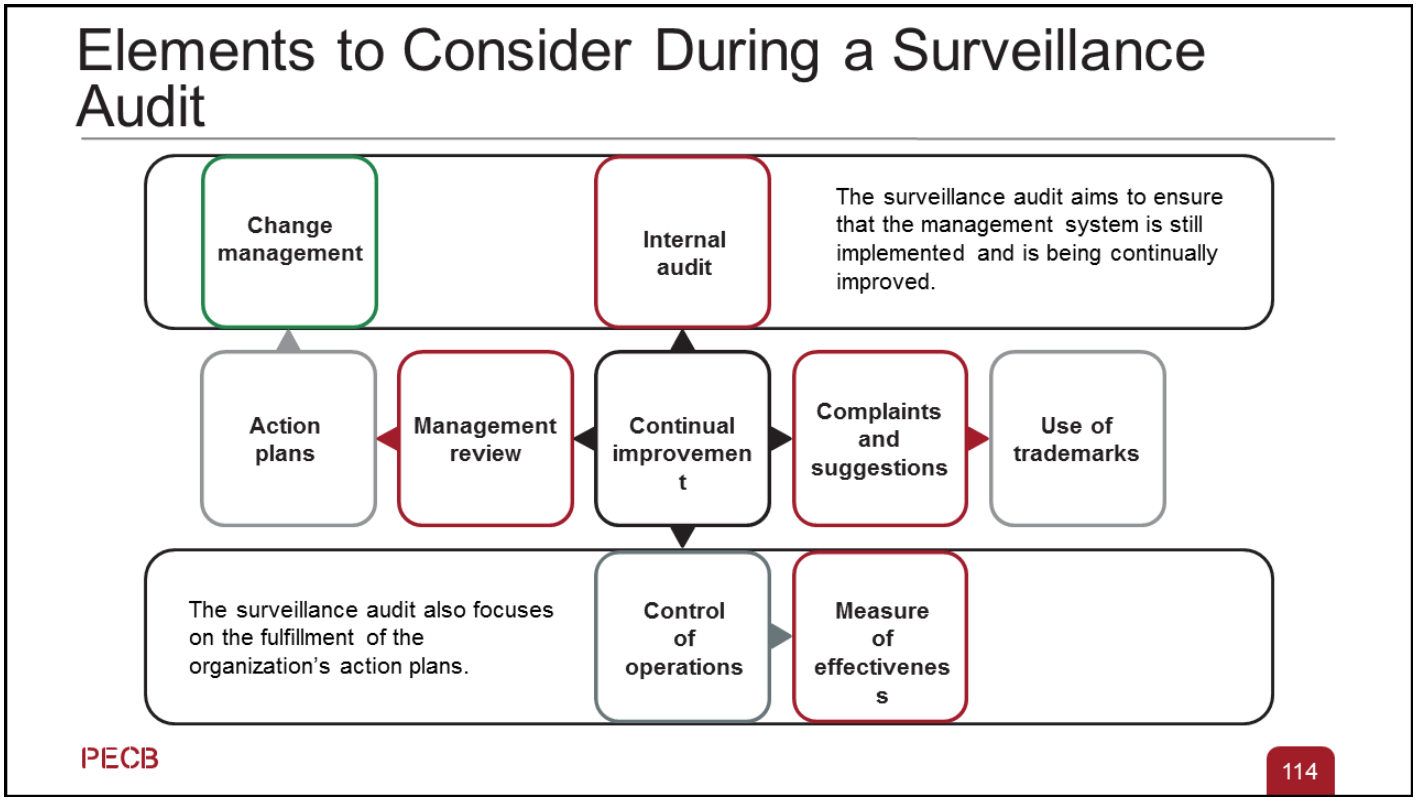
ISO/IEC 17021-1, clause 9.5.3.1

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 fulfil 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, clause 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.*

PECB

115

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.

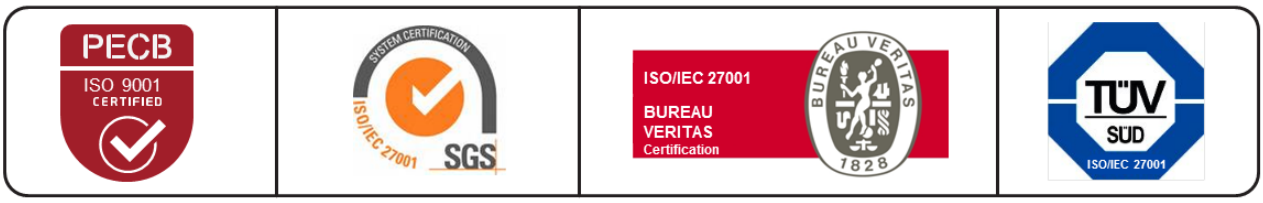
ISO/IEC 17021-1, clause 9.6.3.2.1

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 organization 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.



PECB

116

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.

NOTE ISO/IEC 17030 provides additional information for use of third-party marks.

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.

1. **Which step should be completed before the certification audit?**
   A. Selecting a certification body
   B. Preparing for audit follow-up
   C. Conducting on-site audit activities
2. **Which of these scenarios is a valid reason for rejecting an auditor?**
   A. The auditor is not familiar with the local customs of the area the organization operates in
   B. The auditor has issued an unfavorable certification recommendation
   C. The auditor has worked for one of the organization's competitors
3. **What is the main activity of stage 1 audit?**
   A. Verifying the efficiency of the management system
   B. Reviewing the documented information
   C. Evaluating compliance with the requirements of the standard
4. **The auditor issues the final certification decision upon concluding the audit.**
   A. True
   B. False
5. **What is the main objective of the audit follow-up?**
   A. To validate the operational control of the auditee processes
   B. To verify the "design" of the management system
   C. To validate the action plans and corrective actions implemented by the auditee

This section provides information that will help the participant gain knowledge about the competences and evaluation of implementers, as well as PECB certification procedures.

PECB ISO/IEC 27001 Certification Scheme

Requirements summary

Exam	Professional credential	Professional experience	ISMS audit experience	ISMS project experience
ISO/IEC 27001 Foundation	ISO/IEC 27001 Foundation	----------	----------	----------
ISO/IEC 27001 Lead Auditor	ISO/IEC 27001 Provisional Auditor	----------	----------	----------
	ISO/IEC 27001 Auditor	Two years (One in information security management)	200 hours	----------
	ISO/IEC 27001 Lead Auditor	Five years (Two in information security management)	300 hours	----------
	ISO/IEC 27001 Senior Lead Auditor	Ten years (Seven in information security management)	1,000 hours	----------
ISO/IEC 27001 Lead Implementer	ISO/IEC 27001 Provisional Implementer	----------	----------	----------
	ISO/IEC 27001 Implementer	Two years (One in information security management)	----------	200 hours
	ISO/IEC 27001 Lead Implementer	Five years (Two in information security management)	----------	300 hours
	ISO/IEC 27001 Senior Lead Implementer	Ten years (Seven in information security management)	----------	1,000 hours
ISO/IEC 27001 LA + LI (Four additional Foundation exams)	ISO/IEC 27001 Master	Fifteen years (Ten in information security management)	700 hours	700 hours

120

The **"Foundation"** credential recognizes that individuals understand the basic concepts, approaches, methods, and techniques used for the effective management of a management system.

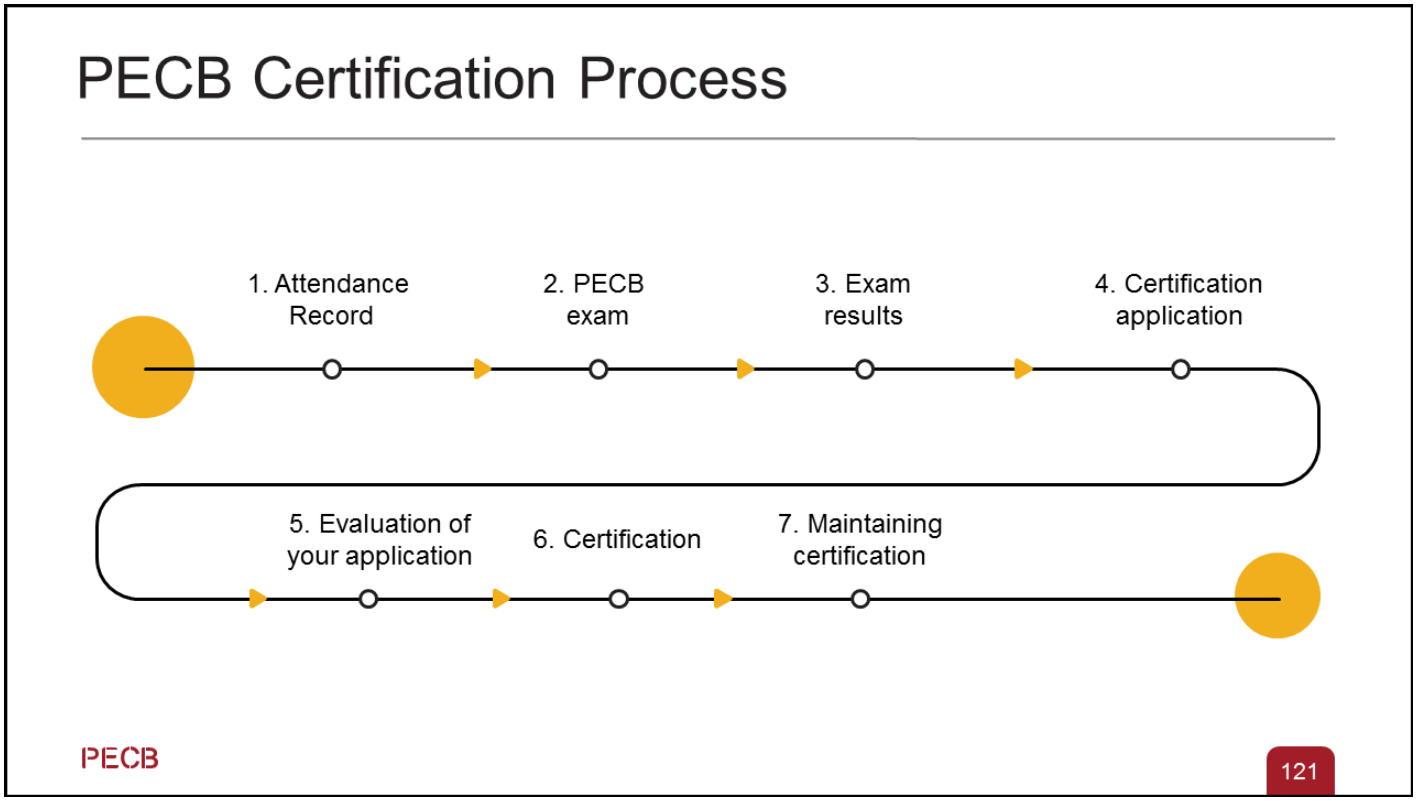
The main auditor credentials:

1. The **"Certified Provisional Auditor"** credential recognizes that individuals possess the basic knowledge about auditing and that they can be a member of an audit team.
2. The **"Certified Auditor"** credential recognizes that individuals have the necessary knowledge to participate in an audit and that they possess the basic skills to conduct a management system certification audit having already been members of an audit team.
3. The **"Certified Lead Auditor"** credential recognizes that individuals master the audit techniques and demonstrate the audit competences to manage an audit team.
4. The **"Certified Senior Lead Auditor"** credential is targeted towards professionals who have extensive experience in auditing.

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 master the skills needed to implement a management system and possess the competences in managing a team to implement a compliance framework.
4. The **"Certified Senior Lead Implementer"** credential is targeted towards professionals who have extensive experience in implementation projects.

The **"Master"** credential recognizes that individuals master the basic concepts, approaches, methods, and techniques to form and lead an audit team and to lead the implementation of a management system.

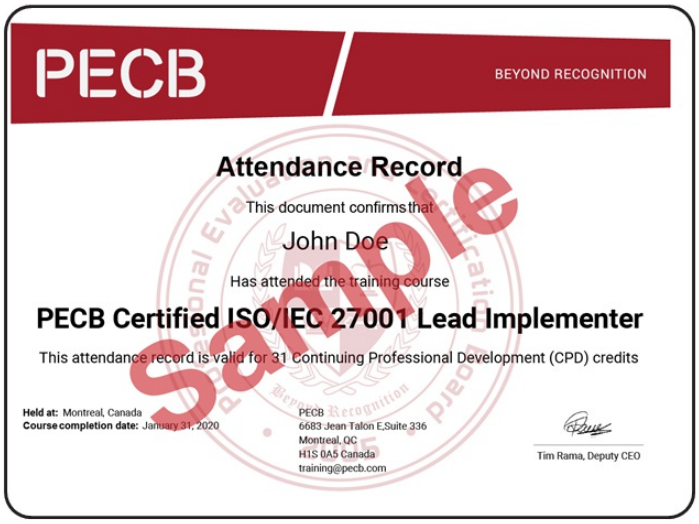


Passing the exam is not the only prerequisite to obtain the "PECB Certified ISO/IEC 27001 Lead Implementer" credential. Additionally, the validation of the professional experience records will take place. Individuals who have successfully passed the exam but do not have the required level of experience cannot claim to be ISO/IEC 27001 Lead Implementer-certified.

Important note: Certification fees are included in the exam price. Candidates therefore will not have to pay any additional fees when applying for certification at their corresponding level of experience and receive one of the professional credentials: PECB Certified ISO/IEC 27001 Provisional Implementer, PECB Certified ISO/IEC 27001 Implementer, PECB Certified ISO/IEC 27001 Lead Implementer, or PECB Certified ISO/IEC 27001 Senior Lead Implementer.

1. Attendance Record

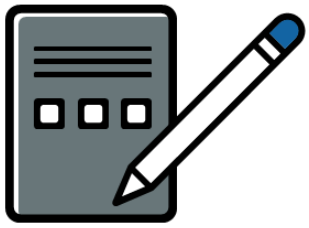
Continuing Professional Development (CPD) credits



After attending the training course and submitting the **Training Evaluation Form**, an Attendance Record will be generated at your myPECB Dashboard under the **My Courses** tab. The Attendance Record is worth 31 CPD (Continuing Professional Development) credits.

2. PECB Exam

- The objective of the certification exam is to ensure that the candidates understand and master the implementation of an information security management system based on ISO/IEC 27001.
- The exam is available in several languages.
- For more information about the examination, please visit Examination Rules and Policies.



PECB

123

The objective of the certification exam is to ensure that candidates have understood and mastered all the necessary concepts and techniques related to the ISMS so that they are able to participate in implementation projects.

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

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

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

3. Exam Results

There are two possible results:

- You will receive an exam number via email to apply for your certification.
- The exam number is important when applying for the PECB certification.

- You can retake the exam within 12 months following the initial exam for free.
- Please contact the exam provider to determine the exam retake date.

Important note: No numerical score will be sent to the candidates.

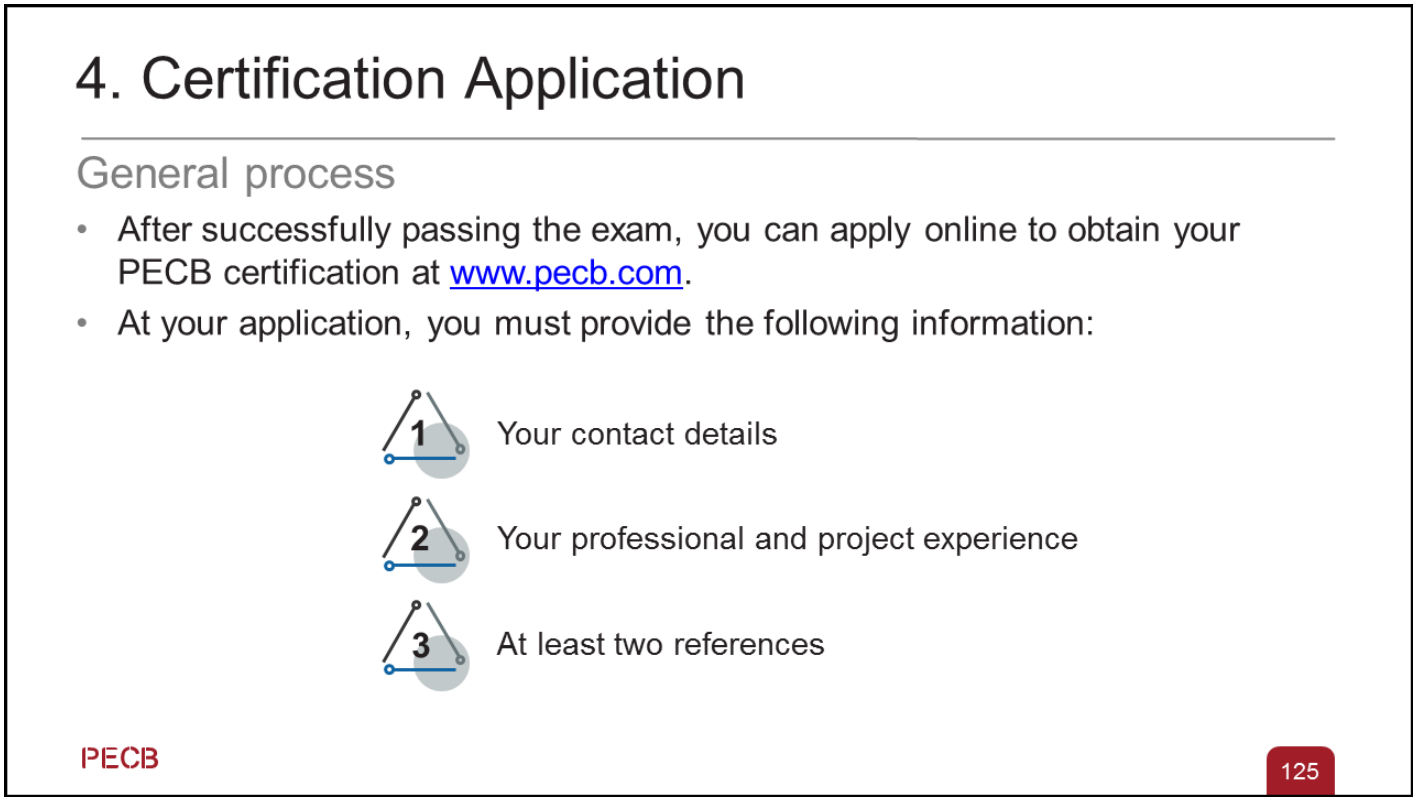
PECB

124

Exams are reviewed by qualified examiners who are assigned anonymously.

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

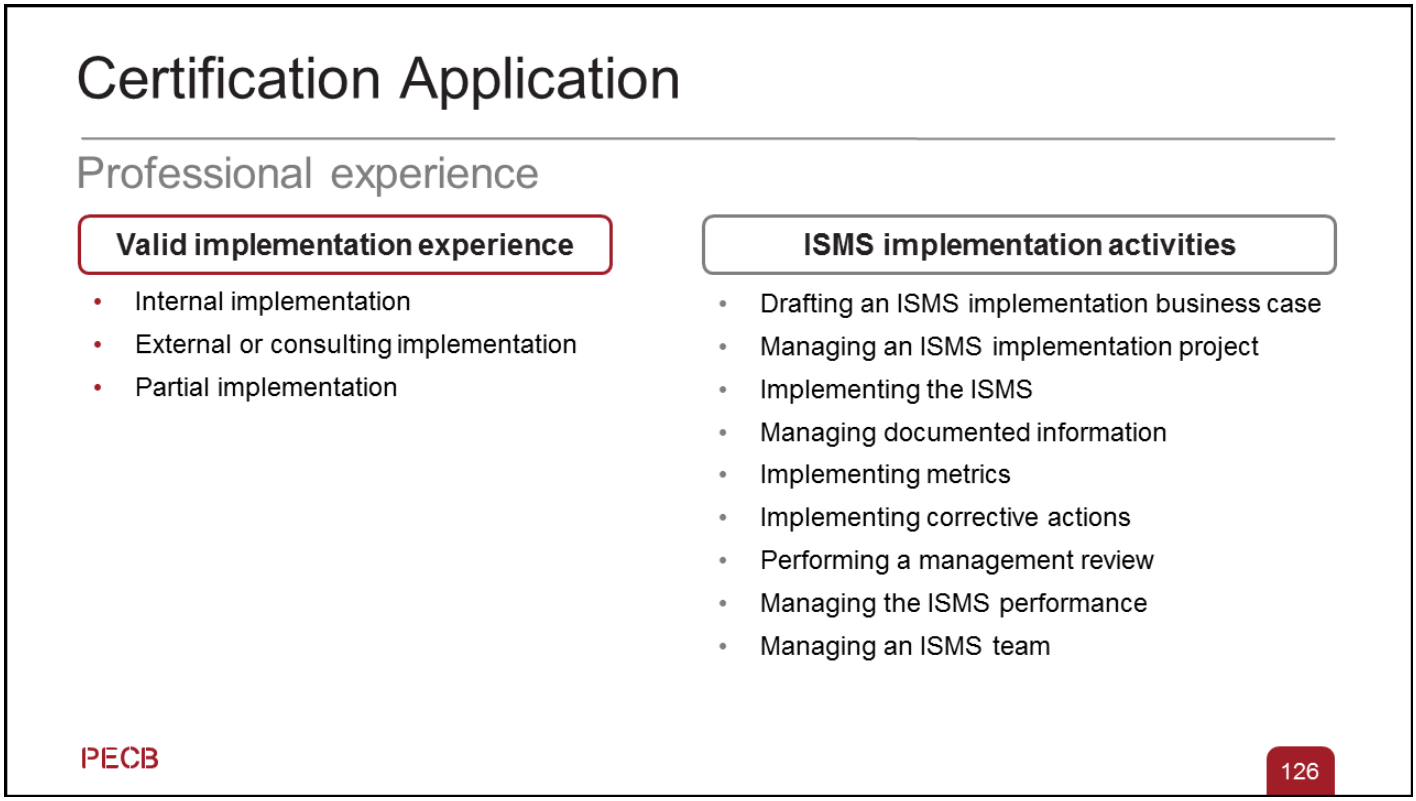
In case candidates fail the exam, an explanation will be provided to them about the domains they failed to demonstrate the required competence. Candidates have 12 months to retake the exam. To do this, they must contact the head of the training organization. Candidates can retake the exam for free. However, administrative fees may be applicable.



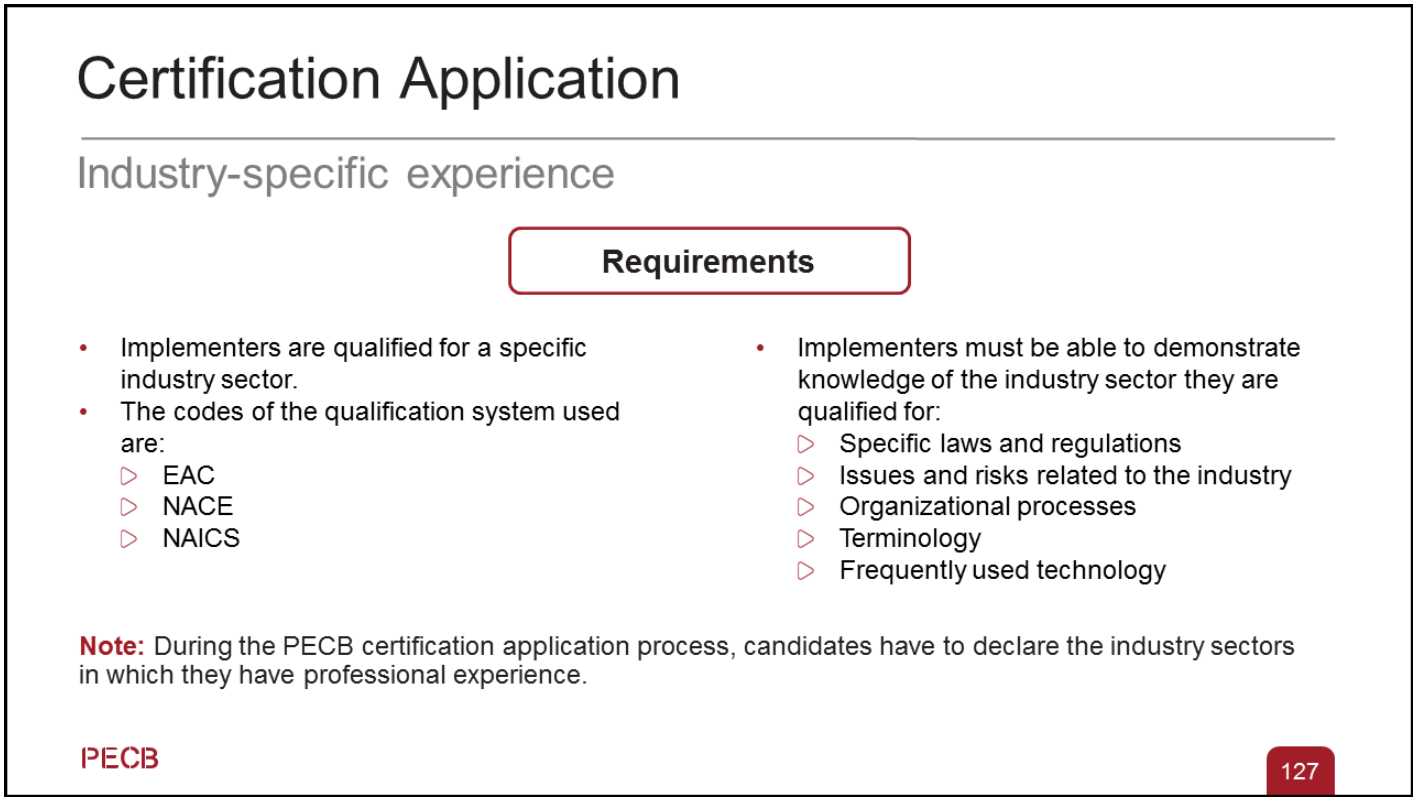
After successfully passing the exam, candidates have a maximum period of three years to submit a professional file in order to obtain a professional credential related to the ISO/IEC 27001 certification scheme. Candidates may apply at the same time for more than one professional credential related to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

At your application, you must provide the following information:

1. **Your contact details**
   - Please write your name as you wish it to appear on your certificate (in ASCII format). Before submitting your certificate application, please make sure to review the accuracy of the contact details you provided when creating your PECB Account. The certificate will be issued with the name you provided when you created the account. To update your name in your PECB Account, please contact customer@pecb.com.
2. **Your professional and audit experience**
   - You must provide a resume to present your professional experience. Work experience can be any activity showing that you have skills and general knowledge about the functioning of an organization.
   - For audit experience, please 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 must be provided by individuals who can confirm your experience (colleagues, partners, supervisors, etc.). It is important that these individuals know you enough to attest to your qualifications.
   - Your application will be assessed once the references have been submitted.



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.



An implementer's project log should contain a list of all the missions performed, including:

1. The number of days in implementing projects (on-site and off-site)
2. The number of people who took part in the implementation project
3. The roles and responsibilities of the implementer in implementation projects
4. The standards implemented
5. The client's name and contact information
6. The organization's name, contact information, and industry sector where the project was implemented
7. The project team leader's name and contact information

5. Evaluation of Your Application

Once your application is complete, PECB will conduct an evaluation:

Your references will be contacted to validate:

- Your work experience
- Your personal and professional attitude

Your application will not be evaluated until your references have been submitted.

You can validate if your references have been submitted within your **PECB Account** Dashboard under the **My Certifications** tab.

PECB

128

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

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

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

6. Certification

- Once your application is approved, PECB is going to issue a professional certificate in PDF format which can be downloaded from your PECB Account.
- This certificate contains the certification number which you can validate on the PECB website, www.pecb.com, by following the tab "Certification Verification."
- Only individuals that fulfill all the criteria for certification can hold the "PECB Certified ISO/IEC 27001 Lead Implementer" credential.
- It is also possible to hold the following credentials:
  - PECB Certified ISO/IEC 27001 LI
  - PECB ISO ISO/IEC 27001 Lead Implementer
  - PECB ISO/IEC 27001 LI
- For more information about the certification process, please visit Certification Rules and Policies.

PECB

129

When candidates are certified, they will receive a notification from the system where they can download the certificate from the PECB Account. The certificate is valid for three years. After this period, the certification will be renewed if the applicants meet the conditions for maintaining their professional designation.

7. Maintaining Certification

Maintaining and continual improvement of competences

Credential	Yearly requirements		Total (hours)
	Experience/Education		
All Foundation and Provisional	0	None	None
Implementer	20	Hours of work experience, implementation or consulting-related experience, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	60 hours
Auditor, Assessor	20	Hours of work experience, audit or assessment-related experience, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	60 hours
Lead Implementer	30	Hours of work experience, implementation or consulting-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	90 hours

PECB

130

In order to maintain a certificate, candidates must demonstrate sufficient hours of Continual Professional Development activities related to the certification scheme. Depending on the certification credential, such activities should cover audit work, implementation or projects activities, self-development, trainings, studies, seminars, conferences, publications, etc. For more information, please refer to the table above.

Professional development activities and certification maintenance

- PECB requires a minimum of 90 hours of activities for three years in order to maintain a “Lead Auditor” or “Lead Implementer” professional credential (60 hours for the “Auditor” or “Implementer” credential, 180 hours for the “Senior Lead Auditor” or “Senior Lead Implementer” credential, 270 hours for the “Master” credential).
- The submission of Continual Professional Development activities should be done on a yearly basis, specifically 20 hours per year for maintaining an “Auditor” or “Implementer” credential, 30 hours for maintaining a “Lead Auditor” or “Lead Implementer” credential, 60 hours for maintaining a “Senior Lead Auditor” or “Senior Lead Implementer” credential, and 90 hours for maintaining a “Master” credential.

Annual Maintenance Fee (AMF)

- A member will be billed for AMF according to the certificate due date.
- The annual cost of the AMF is:
  - $200 per certification for the “Master” credential
  - $100 per certification for all other credentials

Important note: No activities are required to maintain the following professional credentials: “Foundation,” “Provisional Implementer,” and “Provisional Auditor.”

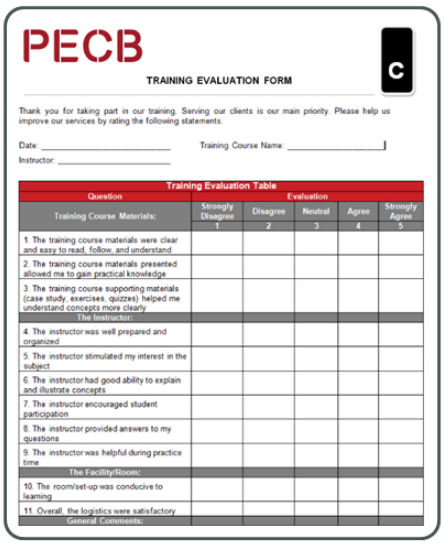
Maintaining Certification

Maintaining and continual improvement of competences

Credential	Yearly requirements		Total (hours)
	Experience/Education		
Lead Auditor, Lead Assessor	30	Hours of work experience, auditing or assessment-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	90 hours
Senior Lead Implementer	60	Hours of work experience, implementation or consulting-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	180 hours
Senior Lead Auditor	60	Hours of work experience, auditing or assessment-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	180 hours
Master	90	Hours of implementation, management or auditing-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	270 hours

Evaluation of the Training Course

Training course evaluation form



PECB

TRAINING EVALUATION FORM

C

Thank you for taking part in our training. Serving our clients is our main priority. Please help us improve our services by rating the following statements.

Date: _____ Training Course Name: _____

Instructor: _____

Training Evaluation Table

Question	Evaluation				
Training Course Materials:	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	1	2	3	4	5
1. The training course materials were clear and easy to read, follow, and understand					
2. The training course materials presented allowed me to gain practical knowledge					
3. The training course supporting materials (case study, exercises, quizzes) helped me understand concepts more clearly					
The Instructor:					
4. The instructor was well prepared and organized					
5. The instructor stimulated my interest in the subject					
6. The instructor had good ability to explain and illustrate concepts					
7. The instructor encouraged student participation					
8. The instructor provided answers to my questions					
9. The instructor was helpful during practice time					
The Facility/Room:					
10. The room/set-up was conducive to learning					
11. Overall, the logistics were satisfactory					
General Comments:					

PECB

132

We strive to constantly improve the quality and the practical relevance of our trainings. Therefore, your opinion on the training is of great value to us.

We would be very grateful if you could provide us with your evaluation of the training course and the instructor(s).

Moreover, if you have any suggestions for improving PECB's training course materials, we would like to hear from you. Please open a ticket directed to the Training Development Department on PECB's website (www.pecb.com) in the **Contact Us** section. We thoroughly read and evaluate the input we get from our members.

In case of dissatisfaction with the training (trainer, training room, equipment, etc.), the examination, or the certification processes, please open a ticket under the **Make a complaint** category on PECB's website (www.pecb.com) in the **Contact Us** section.

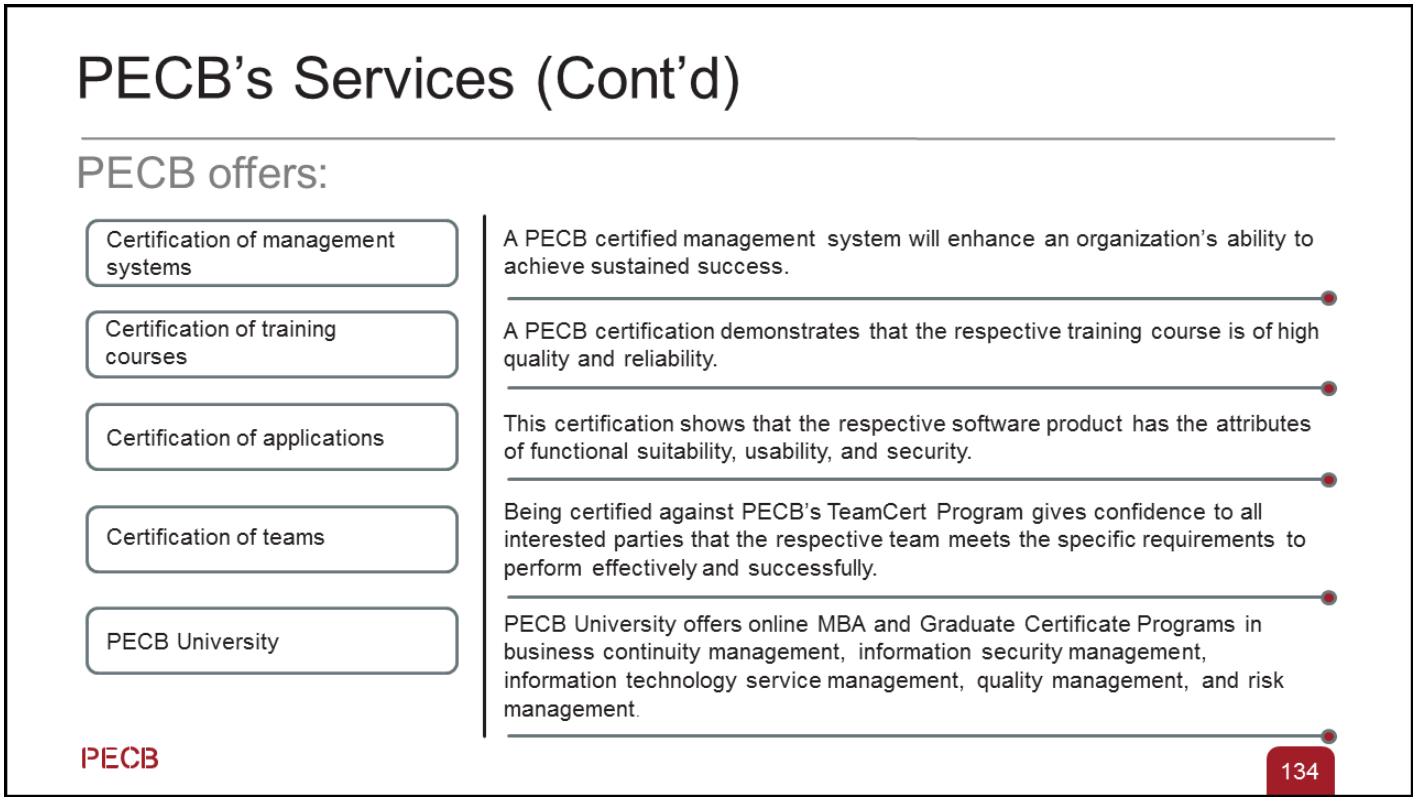
PECB's Services

PECB offers:

Certification of persons

- A personal certification is a formal recognition by PECB which states that the individual has proficiency within, and a comprehension of, a specified body of knowledge.
- Individuals can apply for various professional credentials in the PECB certification schemes. Each PECB certification has specific education and a set of experience requirements.

For example:
PECB Certified ISO/IEC 27001 Lead Implementer



Certification of management systems:

While organizations continuously seek for ways to gain competitive advantage in the market, having a certified management system in place is the best solution. The benefits are manifold: improved quality of products and services, increased international recognition, reduced costs, enhanced customer satisfaction, and so on.

Certification of training courses:

Organizations or individuals seeking to certify their training courses (also referred to as "training developers") must comply with the requirements of the training course certification program established by PECB.

Certification of applications:

Considering the tremendous increase in the number of software application users worldwide, PECB has developed a Software Certification Program. This program aims to define the common, qualitative, and quantitative rules, characteristics, and minimum conditions applicable for the software products to be used by software development organizations to assess their conformity.

Certification of teams:

PECB offers team certifications that help organizations enhance the effectiveness and productivity of their teams. Teams seeking to get certified will be subject to evaluation and assessment in order to verify the fulfillment of the requirements and criteria.

All the above-mentioned certifications are valid for three years. PECB will periodically review the performance of the individuals, teams, management systems, products, and applications to ensure that they are satisfying the requirements and ensure that continual improvement is taking place.

PECB University:

The objective of PECB University is to provide high quality graduate level education and comprehensive services that inspire continual improvement, demonstrate recognition, and benefit an organization, a community, a state, and the society as a whole.

Slide Notes Extension

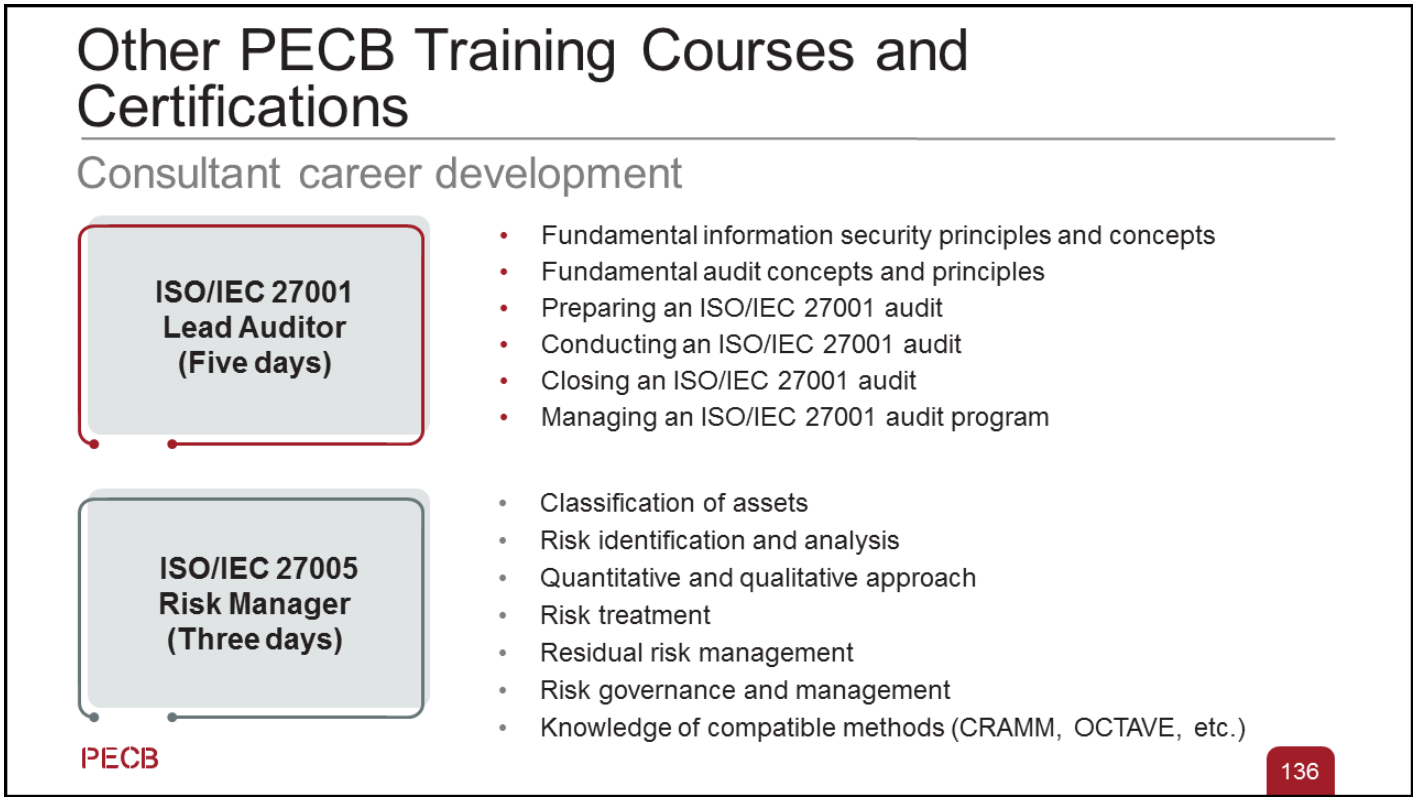
PECB

135

Important notes:

1. To complete any of the MBA programs, the candidates must receive a total of 48 credits. The programs are composed of three sets of courses, categorized as Business Core, Specialization, and Elective — plus the MBA thesis. Each course within the abovementioned categories is worth three credits, while the thesis is worth 12 credits.
2. Each of the Graduate Certificate programs is a twelve-credit worth program. Candidates will have to complete four courses that fall within the respective portfolios. Should a candidate decide to carry on with academic endeavors and progress toward an MBA degree, the candidate can complete two Graduate Certificate programs of choice combined with the Graduate Certificate in Business Administration, submit the thesis and graduate with a degree as a result.

Candidates who hold valid PECB certificates that fall under the course requirements of the university program of interest may transfer those credits to receive full credits for the respective course at the university. For more information about the PECB University or the transfer of certificate credits, please contact university@pecb.com.



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

The ISO/IEC 27001 Lead Auditor training course enables the participants to develop the necessary expertise to perform an information security management system (ISMS) audit by applying widely recognized audit principles, procedures, and techniques. During this training course, the participants will 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. The exercises will enable the participants to master the audit techniques and become competent to manage an audit program and audit team.

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

The ISO/IEC 27005 Risk Manager training course enables the participants to become proficient in the fundamentals of information security risk management including the planning of a risk management program, analysis, evaluation, risk treatment, risk communication, and surveillance. Through a variety of activities, readings, exercises based on real cases, discussions and demonstrations with risk modeling tools, the participants will be able to perform an optimal risk evaluation and to manage risks. During this training course, the participants will also gain a thorough understanding of best practices of risk assessment methods such as OCTAVE, EBIOS, MEHARI, and harmonized TRA. This training course corresponds with the implementation process of the ISMS framework presented in the ISO/IEC 27001 standard.

Markt is a recruiting corporate that works towards finding suitable employees for various positions that companies need. Upon the successful implementation of the ISMS, *Markt* has decided to hire Lisa as an internal auditor to determine the extent to which their audit criteria are fulfilled. Lisa has over 15 years of IT experience but little to no experience in auditing. The internal audit results, the treatment of nonconformities, and the corrective actions were to be discussed during the annual management review meeting.

The meeting showed that Lisa had missed out on several easily identifiable nonconformities. The audit documented information presented sufficient evidence that no logs were preserved for user access control other than the ones in the active directory. The program functions of maintaining records were either non-configured or not enabled due to the lack of storage capacity. Lisa did not include this in the internal audit report.

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

1.Despite her accomplishments on the IT sector, should *Markt* have hired Lisa as an internal auditor, even though she had no audit experience?

A. Yes, she is an IT experienced individual that would quickly learn the process
B. No, because she lacks the skills and experience to perform an internal audit
C. Yes, because even if a minor issue would arise, it would be quickly recuperated after the annual meeting

2.In the context of *Markt*, is it sufficient that management review meetings are held on an annual basis?

A. Yes, annual management reviews enable the company to review the effectiveness of the ISMS
B. No, annual management reviews are not enough for the company to resolve issues in a timely manner
C. No, annual management reviews do not contribute to the continual improvement of the ISMS

3.What action could *Markt* have taken to detect the issues with the access control logs before the occurrence of a potential risk?

A. Focus on recruiting more trained internal auditors
B. Establish a continual risk management process
C. Prioritize investment on detective controls rather than other controls

4.What is the root cause of the nonconformity with regard to the access control logs?

A. Lack of security measures for protecting the stored data logs
B. Lack of logs preserved for user access control on the active directory
C. Lack of storage capacity and mechanisms for keeping records

5.Which of the following corrective actions is the most suitable to treat the access control logs nonconformity?

A. Outsource the audit findings to an expert
B. Have the organization hire a trained person with hands-on experience to train Lisa on the spot
C. Analyze the information systems to identify records that have to be maintained and generate a records retention schedule

Slide Notes Extension

PECB

140

Summary of Day 4

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

- The process of determining the measurement objectives and defining what needs to be monitored and measured
- Internal audit, types of audit, planning, and performing audit activities
- The establishment of independence, objectivity, and impartiality
- Management review preparation and follow-up activities
- Treatment of incidents and nonconformities
- Root-cause analysis process and tools
- Continual improvement
- Maintenance and improvement of the ISMS
- The process of preparing for the certification audit and selecting the certification body
- Stage 1 and stage 2 audit
- Certification process

Follow us on Social Media Platforms

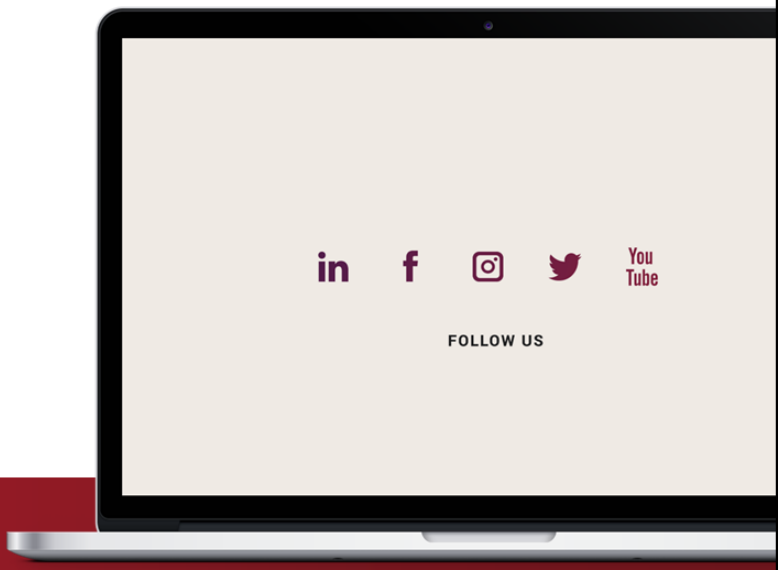
www.pecb.com/facebook

www.pecb.com/linkedin

www.pecb.com/twitter

www.pecb.com/youtube

www.instagram.com/pecb.official



PECB

Blank Page for Note Taking

Blank Page for Note Taking