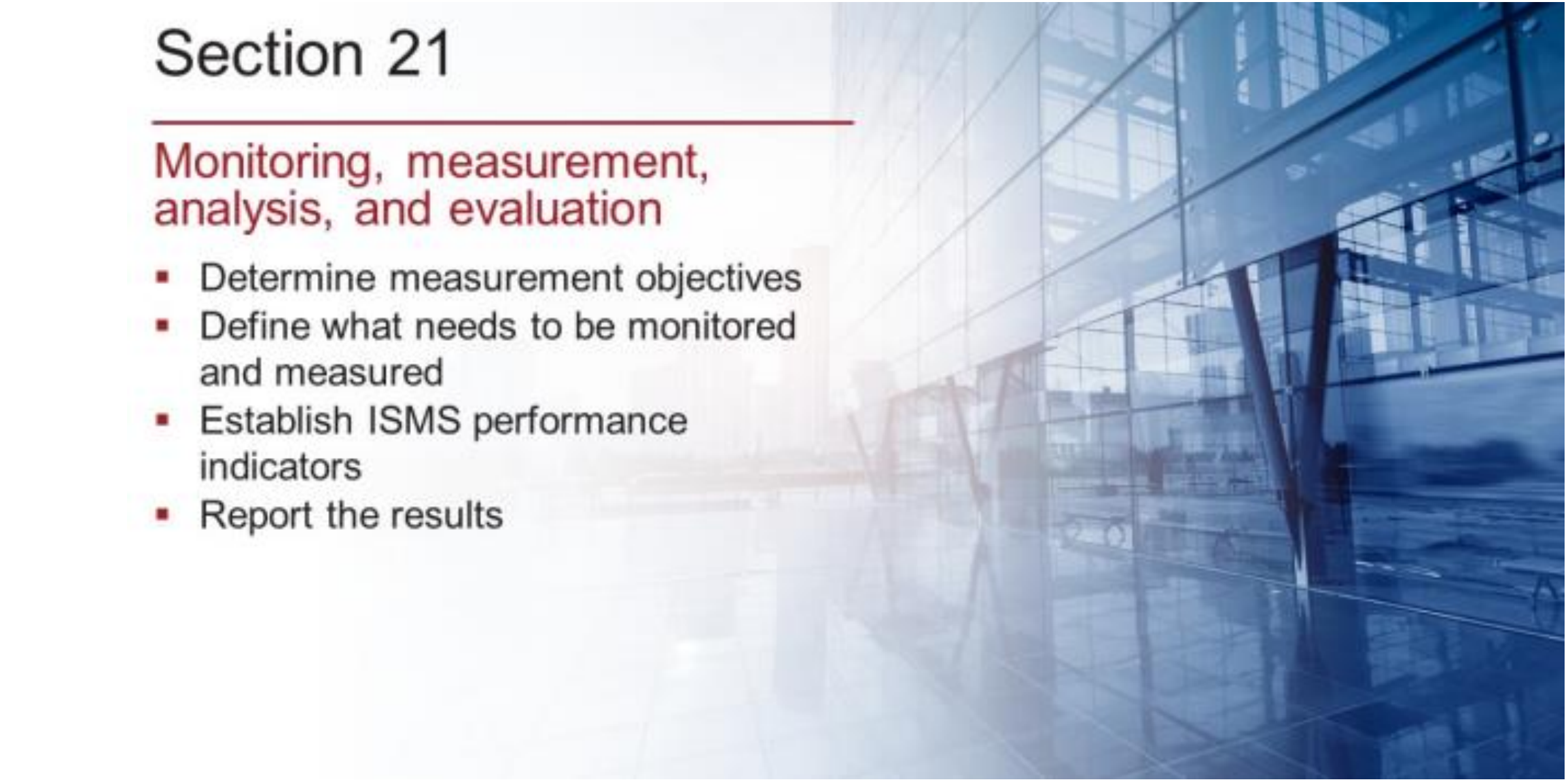
Section 21

Monitoring, measurement, analysis, and evaluation

- Determine measurement objectives
- Define what needs to be monitored and measured
- Establish ISMS performance indicators
- Report the results



3.1 Monitoring, Measurement, Analysis, and Evaluation

1. Define and establish		2. Implement and operate		3. Monitor and review		4. Maintain and improve	
1.1	Initiation of the ISMS implementation	2.1	Documented information management	**3.1**	Monitoring, measurement, analysis, and evaluation	4.1	Treatment of nonconformities
1.2	Understanding the organization and its context	2.2	Selection and design of controls	3.2	Internal audit	4.2	Continual improvement
1.3	ISMS scope	2.3	Implementation of controls	3.3	Management review		
1.4	Leadership and project approval	2.4	Communication				
1.5	Organizational structure	2.5	Competence and awareness				
1.6	Analysis of the existing system	2.6	Security operations management				
1.7	Security policy						
1.8	Risk management						
1.9	Statement of Applicability						

Continual communication and awareness

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 9.1

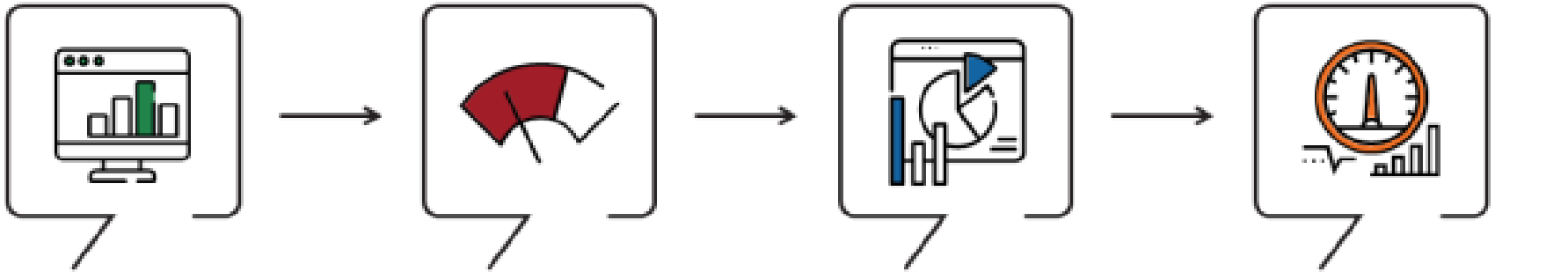
The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

a) *what needs to be monitored and measured, including information security processes and controls;*
b) *the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;*
c) *when the monitoring and measuring shall be performed;*
d) *who shall monitor and measure;*
e) *when the results from monitoring and measurement shall be analysed and evaluated;*
f) *who shall analyse and evaluate these results.*

Documented information shall be available as evidence of the results.

Monitoring, Measurement, Analysis, and Performance Evaluation



Monitoring
Process of determining the status of a system, a process, or an activity

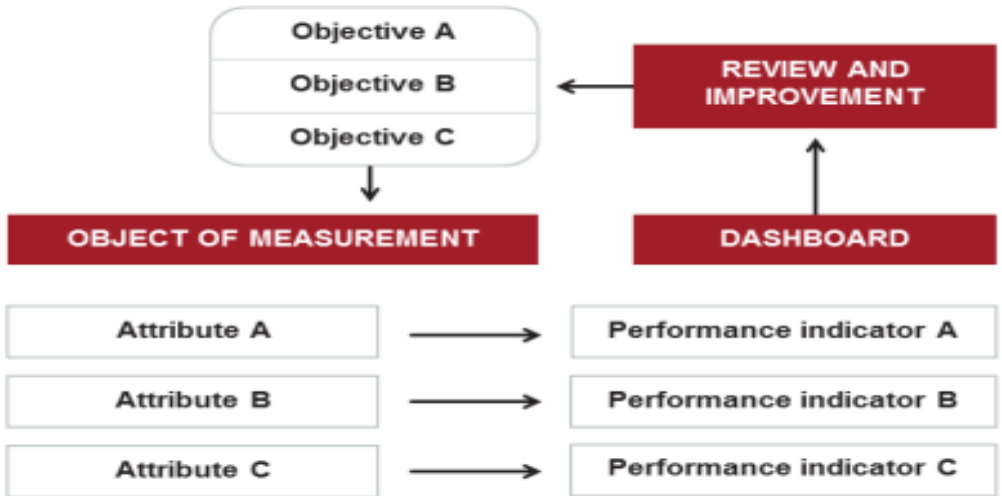
Measurement
Process of determining a value

Analysis
Method of examining the nature of something or of determining its essential features and their relations

Performance evaluation
Process of determining measurable results

Monitoring, Measurement, Analysis, and Evaluation

The main goal is the improvement of the ISMS.



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.
- It 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.

3.1 Monitoring, Measurement, Analysis, and Evaluation

List of activities

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.

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

Define What Needs to be Monitored and Measured

ISO/IEC 27004, clause 6.2

Systems, processes and activities which can be monitored include, but are not limited to:

a) *implementation of ISMS processes;*
b) *incident management;*
c) *vulnerability management;*
d) *configuration management;*
e) *security awareness and training;*
f) *access control, firewall and other event logging;*
g) *audit;*
h) *risk assessment process;*
i) *risk treatment process;*
j) *third party risk management;*
k) *business continuity management;*
l) *physical and environmental security management; and*
m) *system monitoring.*

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.*

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

ISO/IEC 27004, clause 6.5

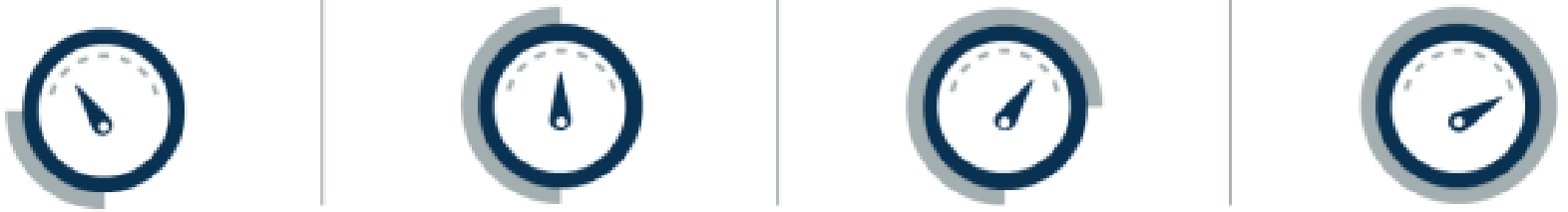
Whether the measurement is performed manually or automatically, organizations can define the following measurement-related roles and responsibilities:

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.*

3.1.4 Establish ISMS Performance Indicators

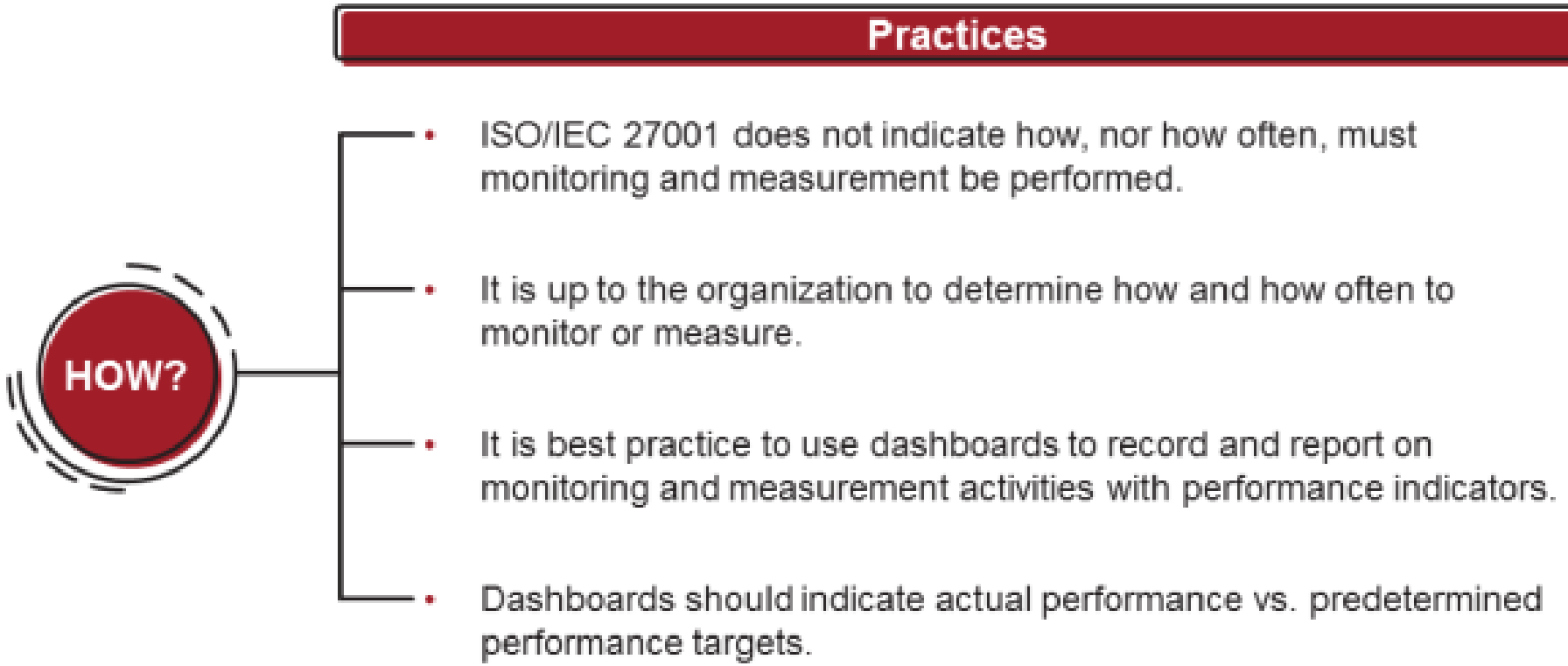
Examples

Incidents	Training	Vulnerabilities	Nonconformities
• 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



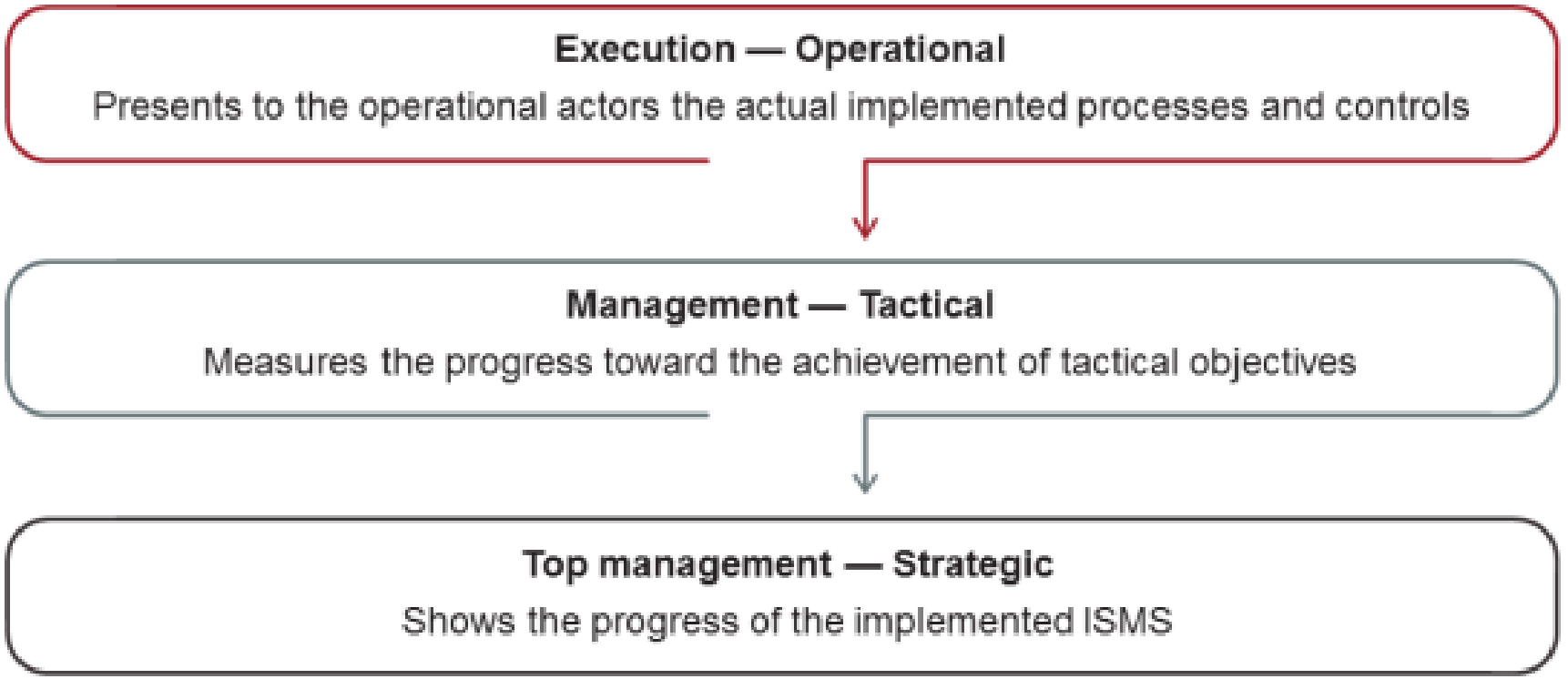
3.1.5 Determine the Frequency and Method of Monitoring and Measurement

How and when to monitor and measure?



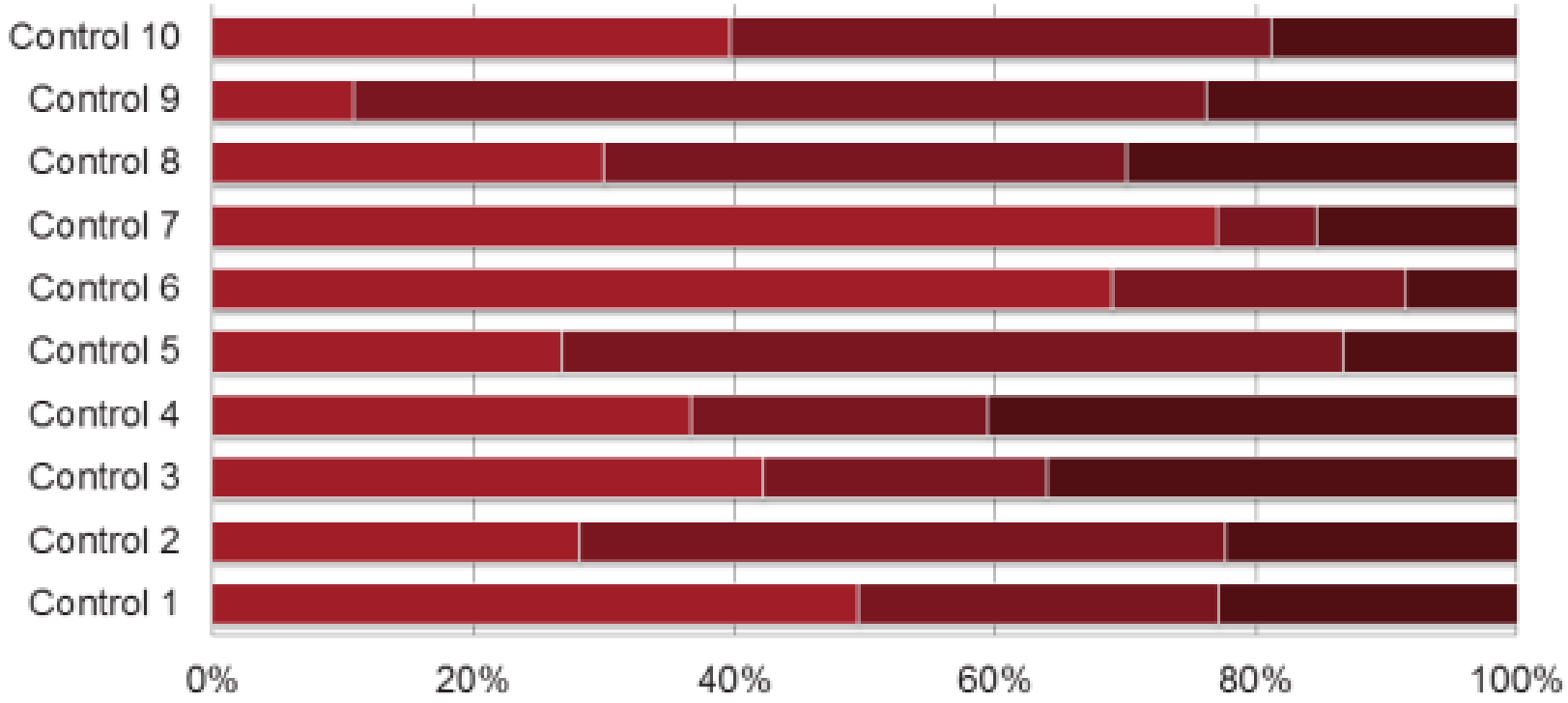
3.1.6 Report the Results

Examples of dashboards



I. Operational Dashboard

Example



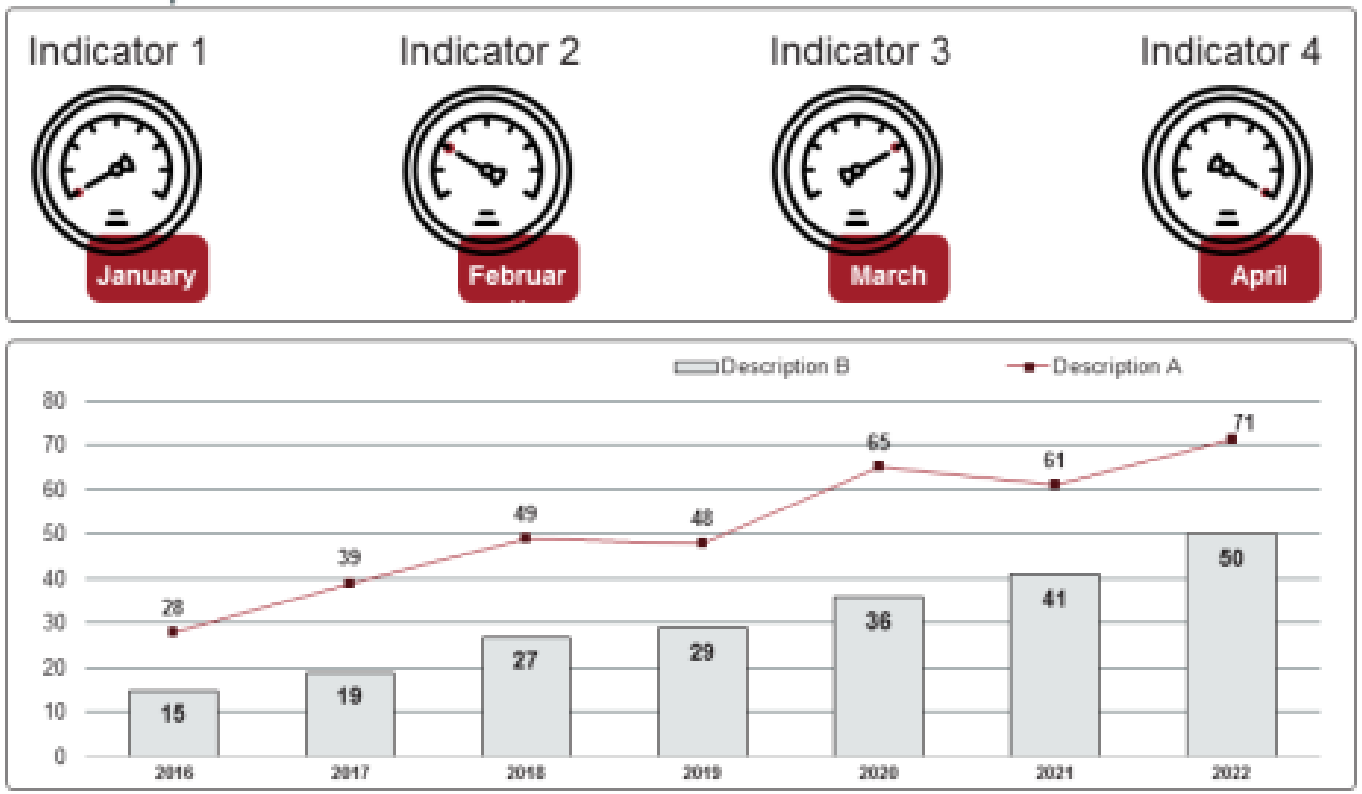
II. Tactical Dashboard

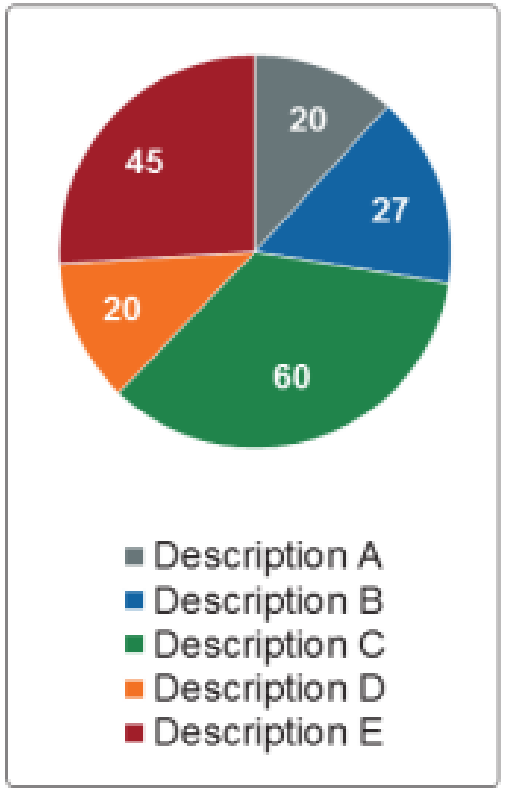
Example

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		

III. Strategic Dashboard

Example





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.

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. A.To begin the ISMS implementation
B. B.To improve the ISMS implementation
C. C.To prohibit the ISMS implementation

Section 22

Internal audit

- What is an audit?
- Types of audits
- Create an internal audit program
- Designate a responsible person
- Establish independence, objectivity, and impartiality
- Plan audit activities
- Perform audit activities
- Follow up on nonconformities

3.2 Internal audit

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 9.2.1 and 9.2.2

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

a) conforms to

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

2) the requirements of this document;

b) is effectively implemented and maintained.

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

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

The organization shall:

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

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

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

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

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

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.

- **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.

Types of Audits

Second party audit
The organization is audited by its customer.

External

Second party audit
The organization audits its supplier.

Customer

Supplier

Third party audit
The organization is audited by an independent organization.

Differences Between Internal and External Audits

Main characteristics

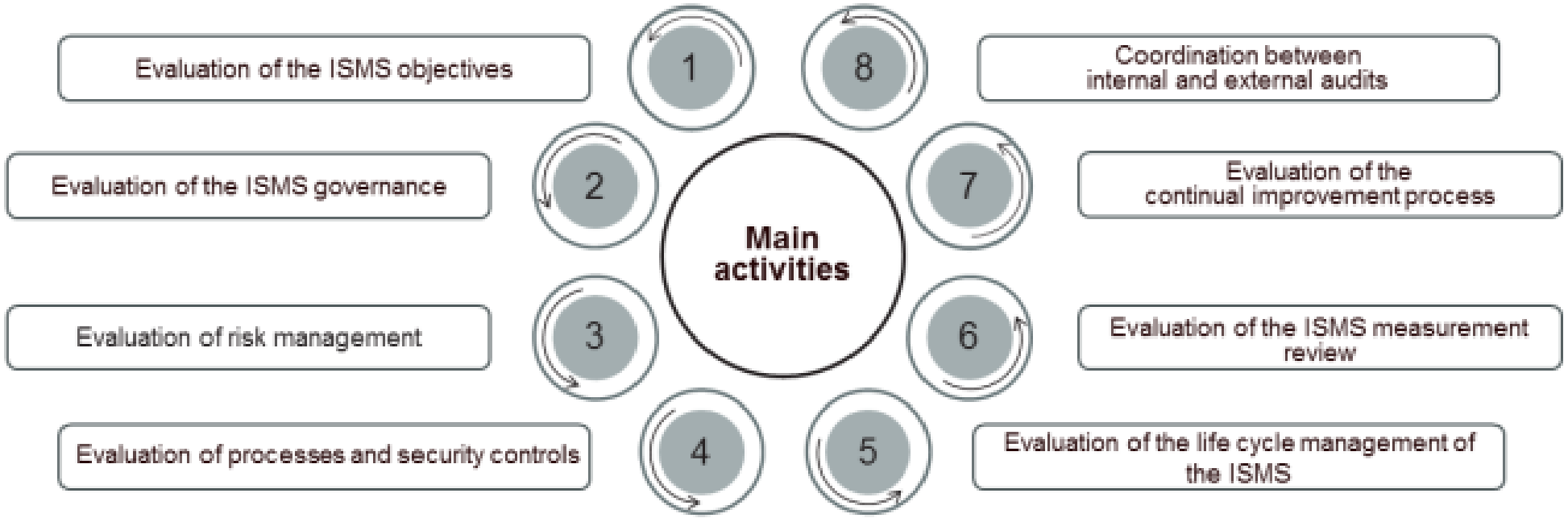
Internal audit

1. Independent of the activities audited (not of the organization)
2. Considers the effectiveness and efficiency of the ISMS
3. Advisory role within the organization for the improvement of the ISMS
4. May be conducted on an ongoing basis

External audit

1. Independent of the audited organization and its activities
2. Considers only the effectiveness of the ISMS
3. No advisory role within the organization (only general recommendations)
4. Always conducted in a planned and a timely manner

Main Services and Activities of the Internal Audit



ISO 19011

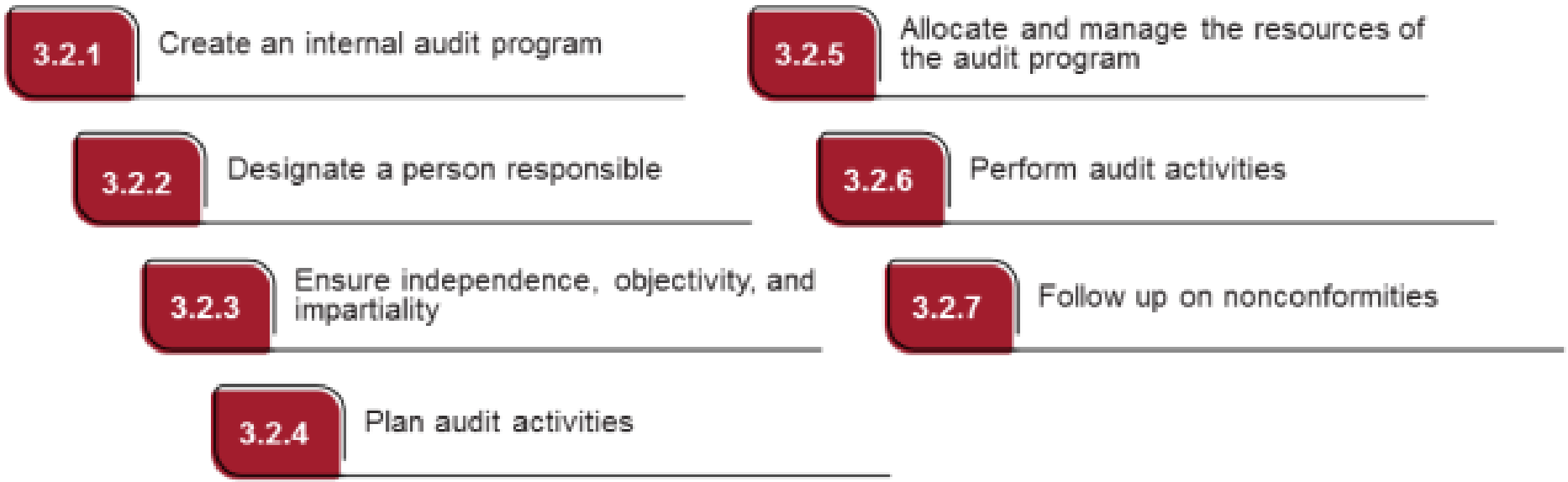
Guidelines for auditing management systems

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

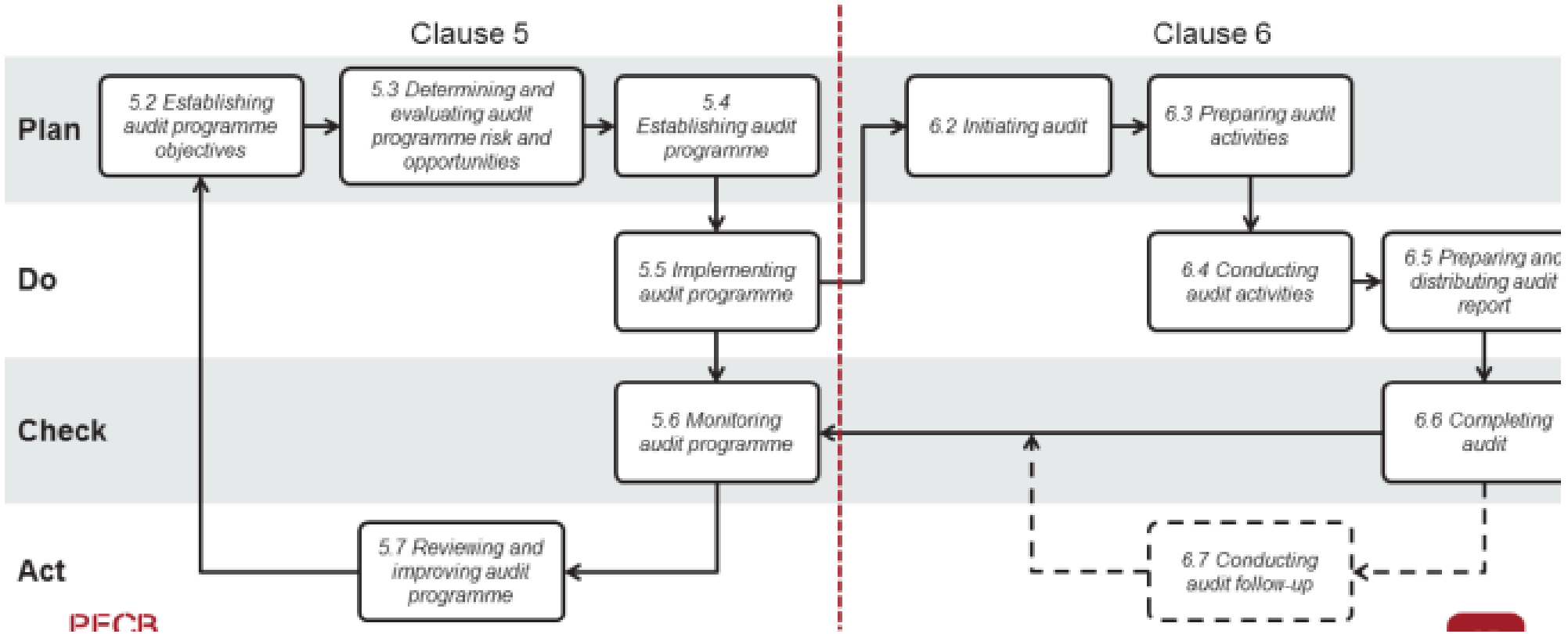
3.2 Internal Audit

List of activities



3.2.1 Create an Internal Audit Program

ISO 19011, Figure 1

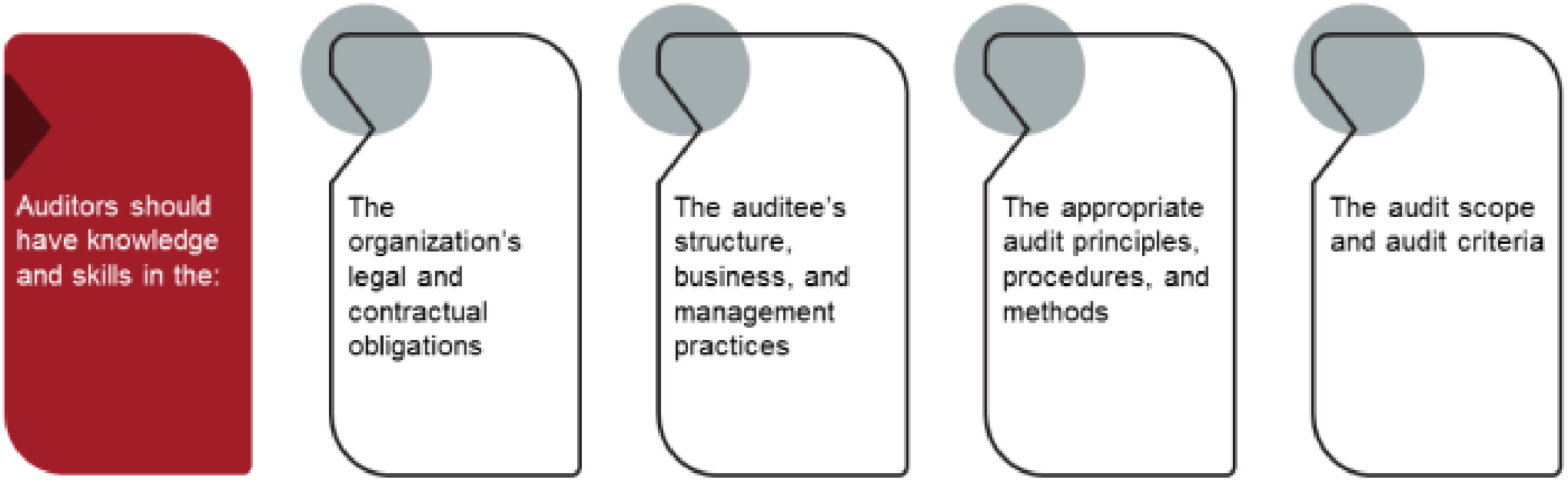


3.2.2 Designate a Person Responsible

Internal auditor's roles and responsibilities

- Develop an internal audit program (roles and responsibilities, procedures, work papers, auditor training, etc.)
- Ensure that the best audit practices and procedures are followed during the audit
- Plan audit activities
- Manage resources
- Develop performance criteria and ensure that the audit meets these criteria
- Write audit reports
- Implement a continual improvement evaluation program by an external auditor
- Follow up on nonconformities and recommendations from previous audits

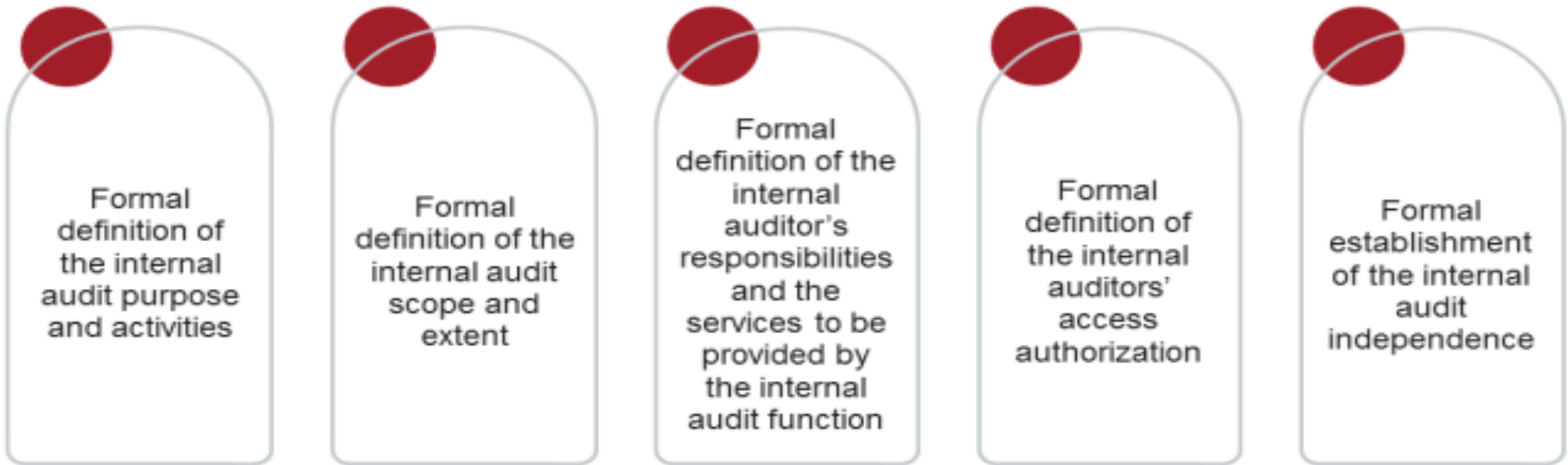
Generic Knowledge and Competences



3.2.3 Ensure Independence, Objectivity, and Impartiality

Audit charter

Structure of the audit charter



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.

Access and Independence

Principles

1

Access to resources and collaboration

- Internal auditors should have unrestricted access to executives, employees, offices, information, explanations, and documented information necessary for the proper conduct of the audit.
- This need for access must be documented (usually in the audit charter).

2

Independence

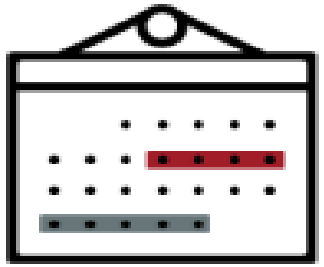
- Internal auditors must be independent of the processes being audited; this is ensured if auditors report directly to the organization's audit board rather than to top management.
- This need for independence should be reflected in the organizational chart.

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.

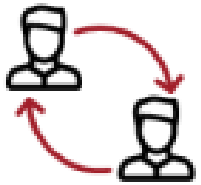


A more detailed annual planning

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.

3.2.5 Allocate and Manage the Resources of the Audit Program

Financial resources



Competent personnel

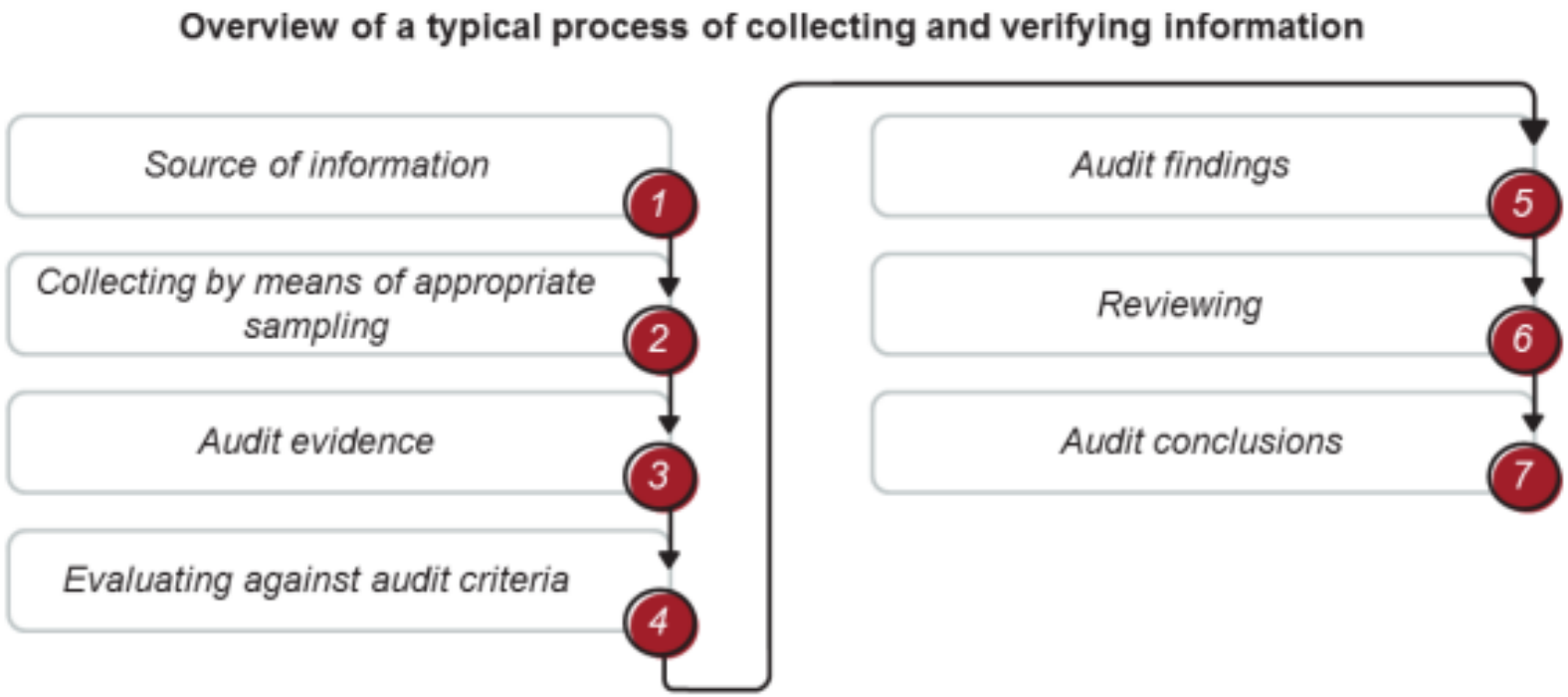
Tools

Audit policies and procedures

Logistics

3.2.6 Perform Audit Activities

ISO 19011, Figure 2



Perform Audit Activities

Audit procedures should include information on how to:

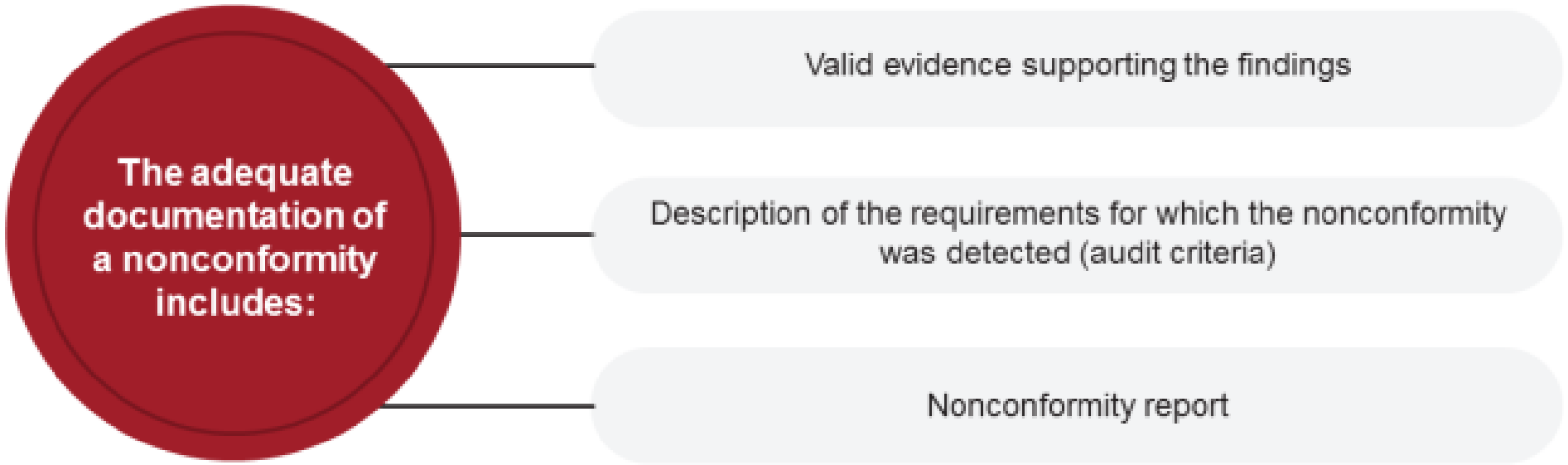
1. Plan and schedule audits
2. Manage the audit risks
3. Ensure the competence of audit team members
4. Assign the roles and responsibilities of audit team members
5. Select and use suitable sampling methods
6. Conduct follow-up audit, if applicable
7. Report the audit conclusions to the auditee
8. Maintain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

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

Document the Nonconformities



Nonconformity Report

Example

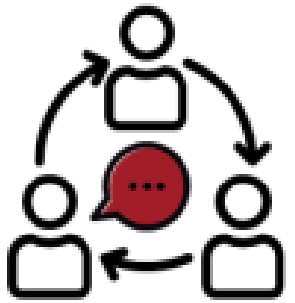
NONCONFORMITY REPORT		
Nonconformity N°: 3	**Client:** Thalia Technologies	**File N°:** 34527
Process: Assets Management	**Clause number:** Control 5.9	**Site:** Montreal
Audit criteria: An inventory of information and other assets, including owners, shall be developed and maintained.		
Description of 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* (circled) Minor*

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.



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 23

Management review

- Preparing a management review
- Conducting a management review
- Management review outputs
- Management review follow-up activities

3.3 Management Review

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 9.3.1 and 9.3.2

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) *changes in needs and expectations of interested parties that are relevant to the information security management system;*
d) *feedback on the information security performance, including trends in:*
    1) *nonconformities and corrective actions;*
    2) *monitoring and measurement results;*
    3) *audit results;*
    4) *fulfilment of information security objectives;*
e) *feedback from interested parties;*
f) *results of risk assessment and status of risk treatment plan;*
g) *opportunities for continual improvement.*

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.

Suitable	Adequate	Effective
Results are achieved in the best possible way	Outputs fulfill established criteria	The system fulfills the organization's needs

3.3 Management Review

List of activities

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.

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

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

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.

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 regular management reviews at scheduled intervals 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 24

Treatment of nonconformities

- Root-cause analysis process
- Root-cause analysis tools
- Corrective action procedure
- Preventive action procedure

4.1 Treatment of Nonconformities

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 10.2

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
   1) take action to control and correct it;
   2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1) reviewing the nonconformity;
   2) determining the causes of the nonconformity; and
   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

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

Documented information shall be available as evidence of:

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

g) the results of any corrective action.

Definitions

ISO 9000, clauses 3.3.2, 3.12.3, 3.12.2, and 3.12.1

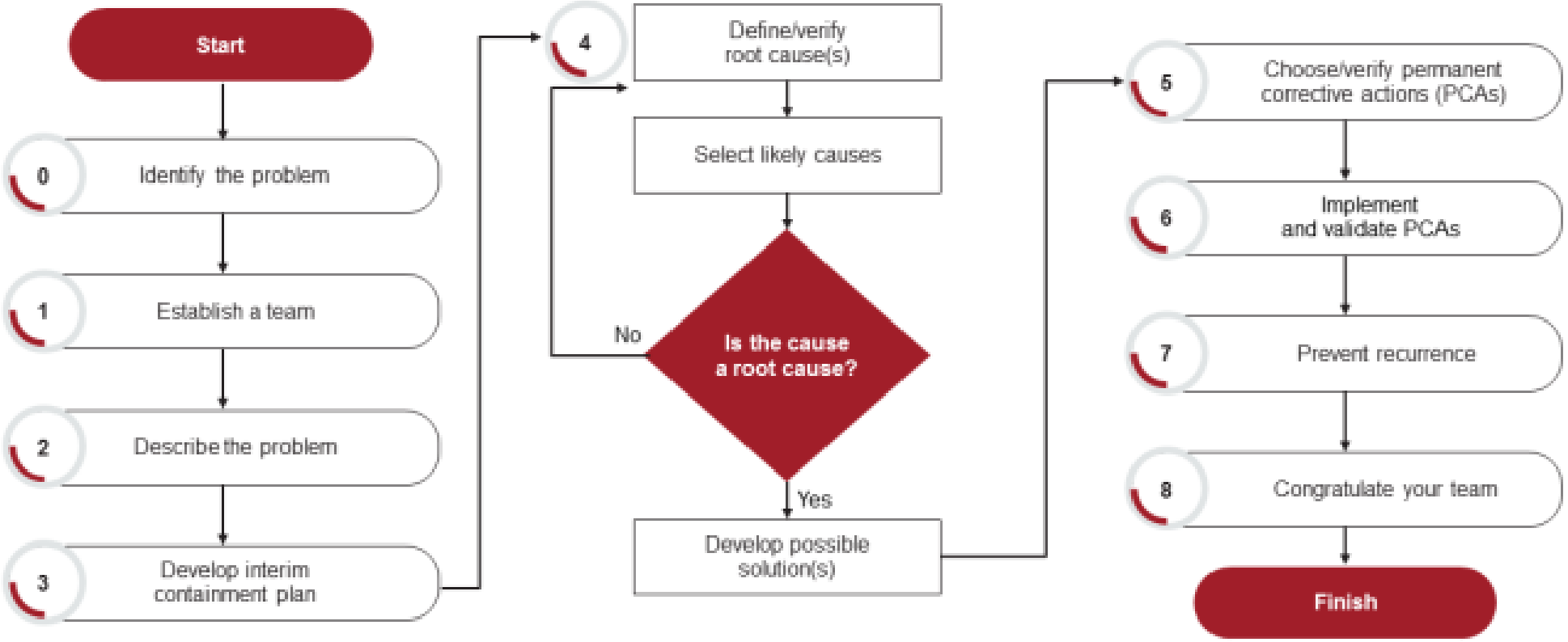
Continual improvement	***Correction***	***Corrective action***	***Preventive action***
Recurring activity to enhance the performance	*Action to eliminate a detected nonconformity*	*Action to eliminate the cause of a nonconformity and to prevent recurrence*	*Action to eliminate the cause of a potential nonconformity or other potential undesirable situation*

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**:

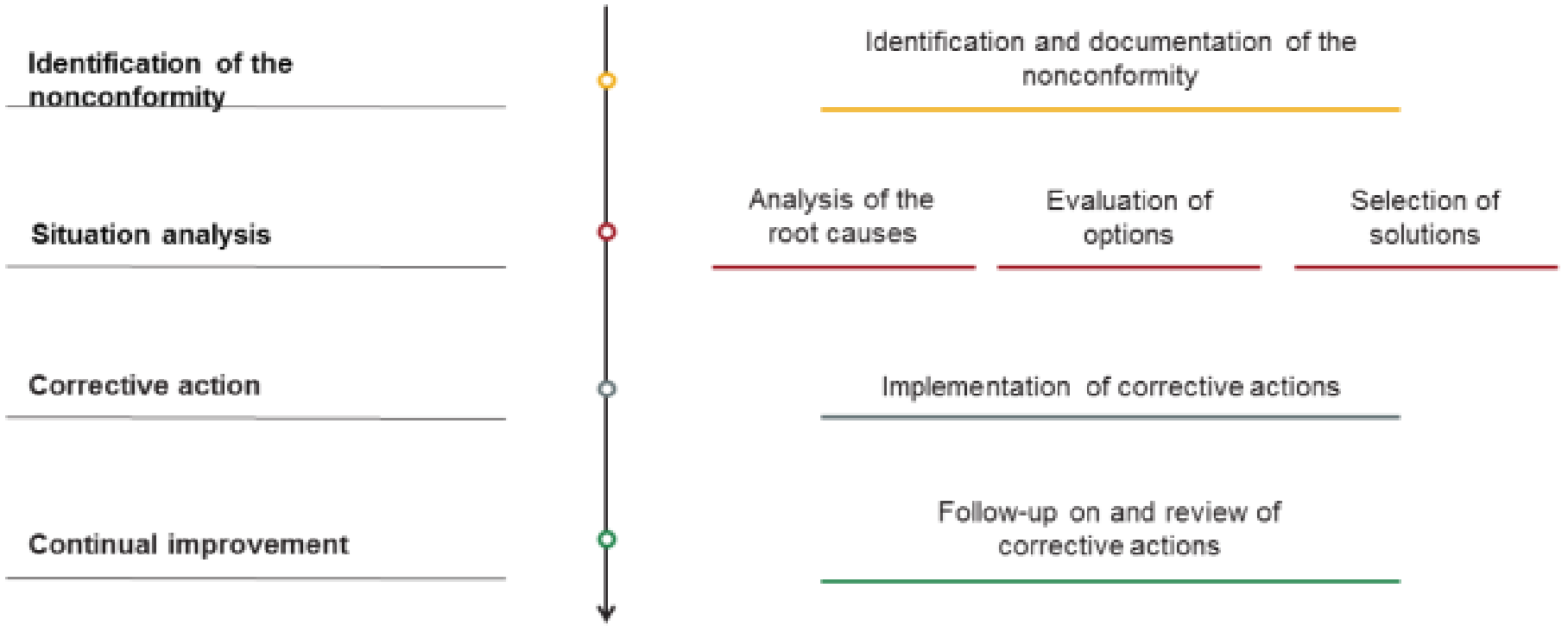


Asking the Right Questions

The questions needed for the analysis of any problem

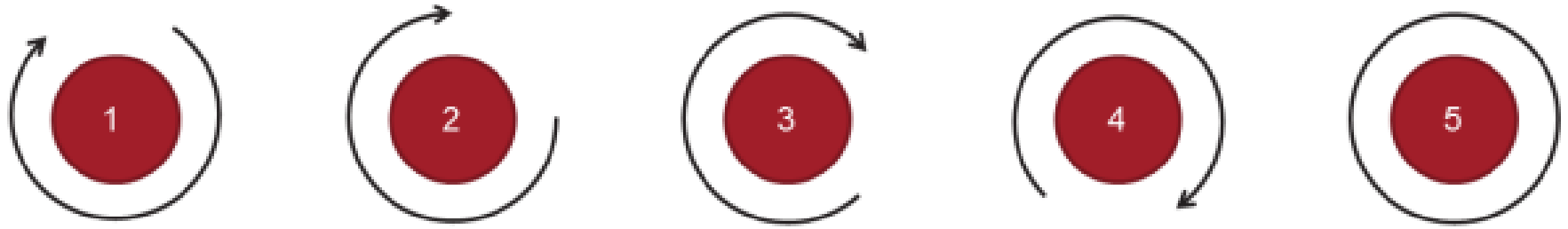
Current situation	Questioning	Solution tracking	Remaining option(s)
What has been done?	Why is this necessary?	What else could we do?	What will be done?
How is it done?	Why is it done this way?	How to do it differently?	How will this be done?
Who did it?	Why this person?	Who else could do it?	Who will 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?

4.1.2 Determine the Corrective Actions



4.1.4 Draft an Action Plan

An action plan:



1. Can be written in a summarized fashion
2. Must allow to correct the nonconformity
3. Should be based on a preventive and corrective approach
4. Must include an execution period
5. Must allow the obtainment of verifiable results

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.

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.

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. **All nonconformities should be included in a single inclusive action plan.**
    A. True
    B. False
5. **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

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

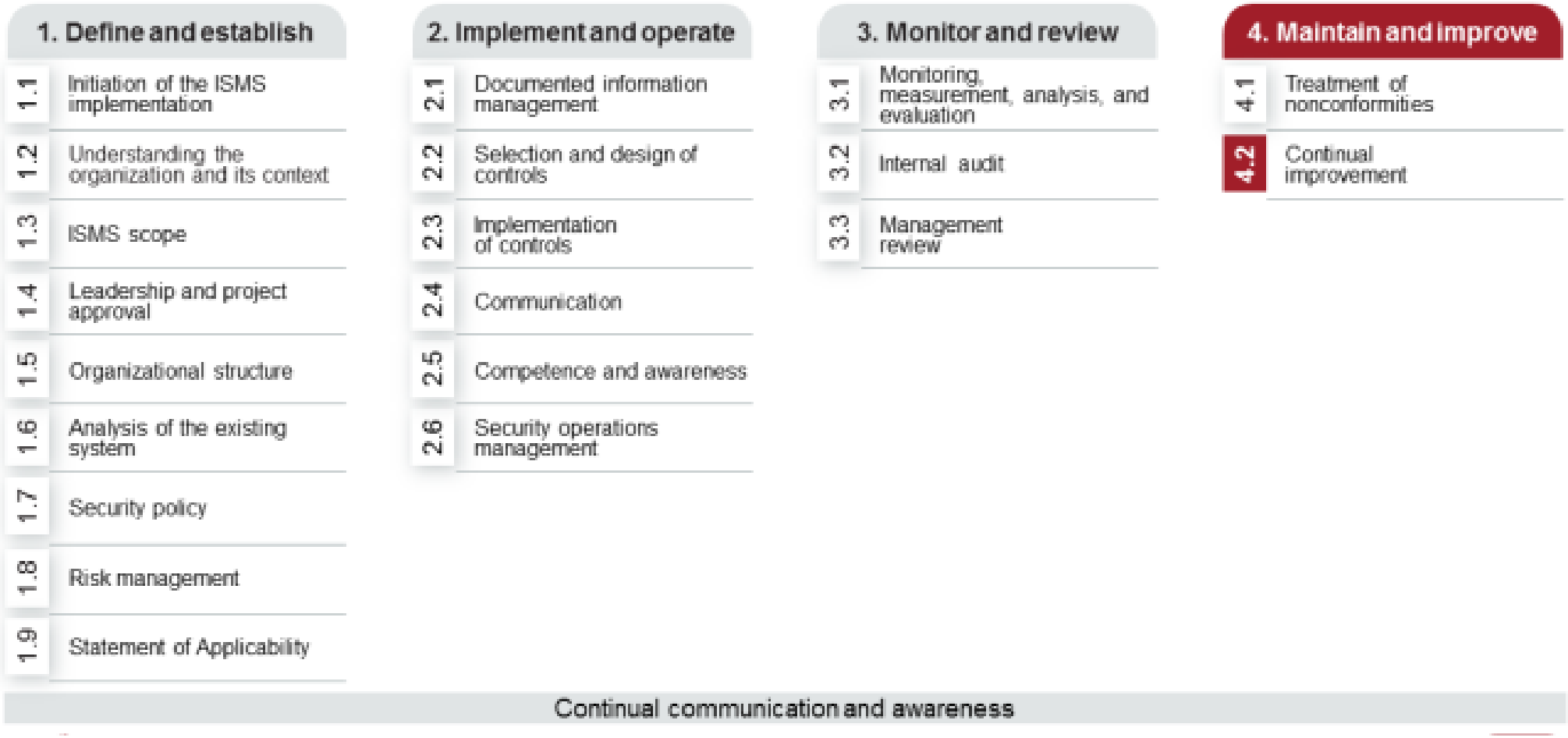
A. Identification and documentation of the nonconformities
B. Follow-up on and review of corrective actions
C. Evaluation of options and selection of solutions

Section 25

Continual improvement

- Continual monitoring process
- Maintenance and improvement of the ISMS
- Continual update of the documented information
- Documentation of the improvements

4.2 Continual Improvement



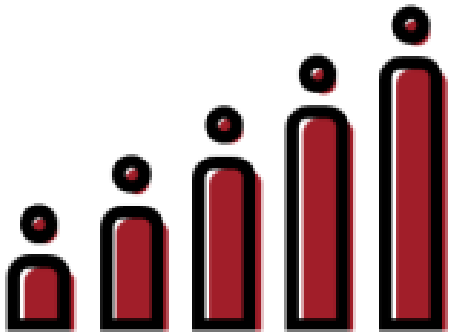
ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 10.1

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

Continual Improvement

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



With small but certain steps

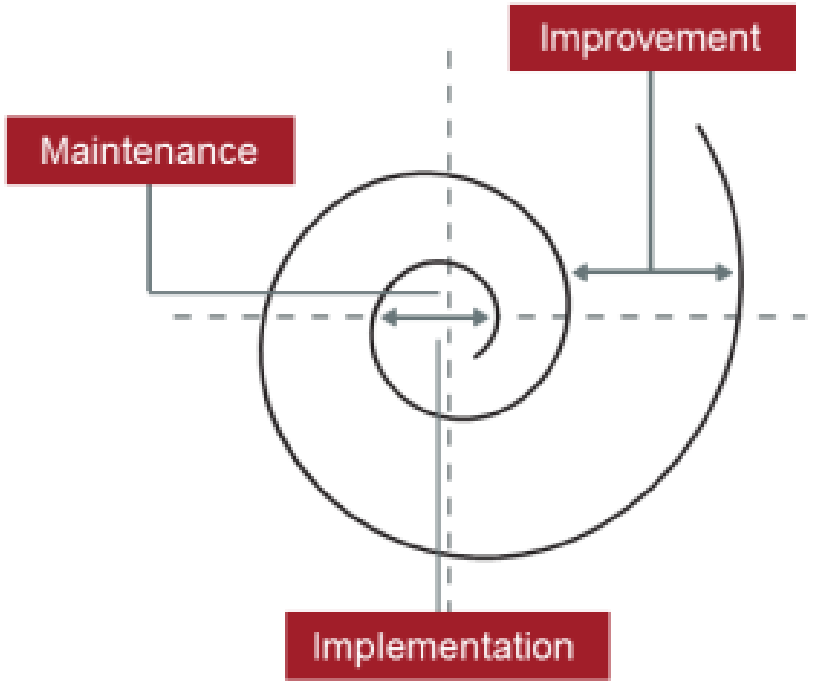
4.2 Continual Improvement

List of activities

4.2.1 Establish the Change Factors to Be Monitored

ISMS change factors to monitor:			
Organizational changes	**Changes in technologies**	**External changes**	**Changes from the ISMS**
• Mission • Business objectives • Budget and resources • New products and services • Change in personnel	• Hardware • Software • IT procedures • IT processes	• Laws and regulations • Clients, suppliers, concerns, and requirements • Vendors • Changes in the environment (e.g., new competitors)	• ISMS policy • New risk scenarios • Changes of procedures • Test and exercise results • Audit results

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.

4.2.3 Ensure the Continual Update of Documented Information

Continual change

ISMS documentation

- Information security policy
- Objectives, targets, and action plans
- Risk analysis
- Strategy
- Awareness programs
- Education programs
- Incident management plans
- Business continuity and resumption plans
- Documented information control

Factors of change

- Organizational evolution
- New rules
- Changes in business scope
- Incidents
- Faulty operation
- Failures
- Risk management reports
- Test results
- Internal audits
- External audits

Review and update

The Benefits of Continual Improvement

Continual change

Increased efficiency

Continual improvement allows for increased productivity, since the changes may lead to long-term positive outputs.

Collaborative teams

Working continuously together toward a common goal will help in building and reinforcing the existing relations of the team.

Increased customer satisfaction

While organizations actively seek for ways to improve their management system, they indirectly increase the value and quality of the products and services they offer.

Error reduction

While organizations actively seek for ways to improve their management system, they indirectly reduce the number of errors.

4.2.4 Document the Improvements

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

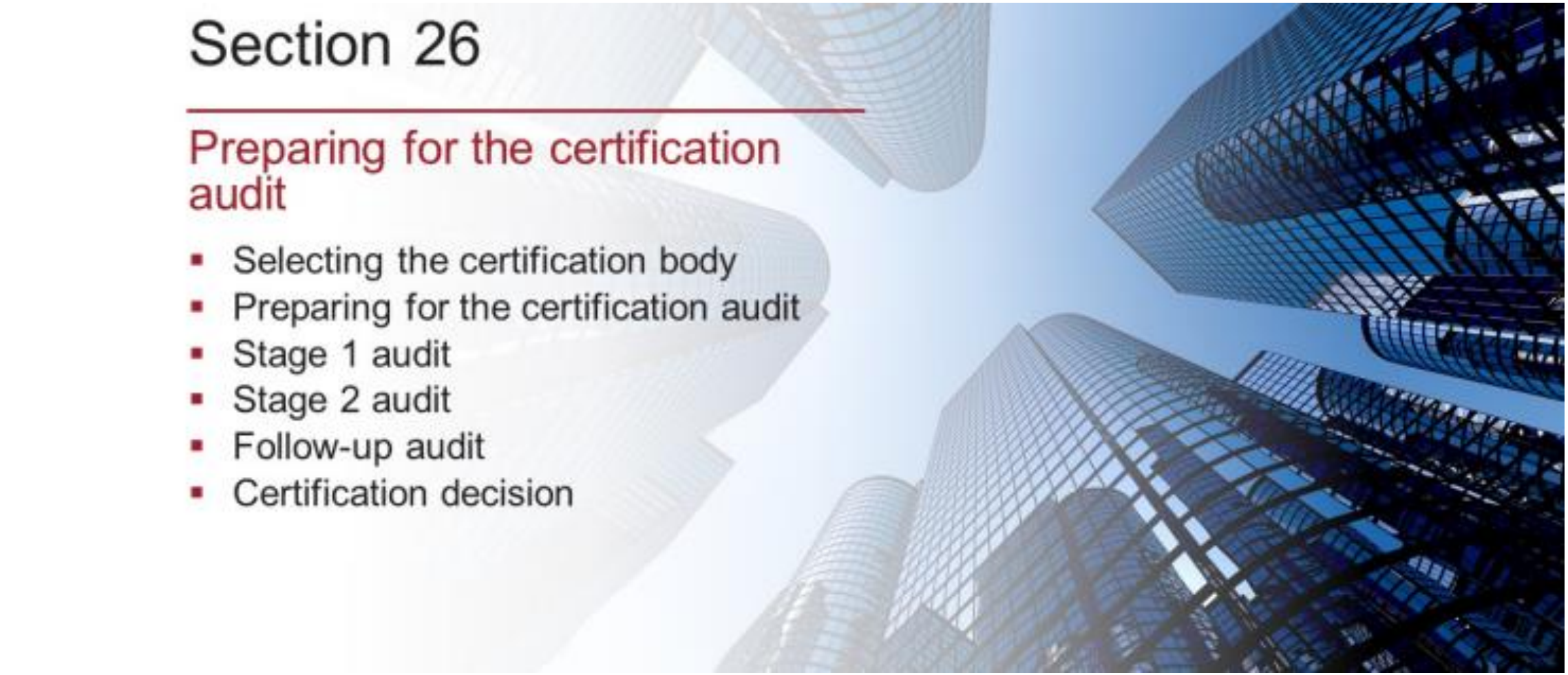
The ISMS coordinator should record plan modifications using a record of changes, which lists the page number, change comment, and date of change. The record of changes, depicted in the slide, should be integrated into the different documents included in the ISMS.

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 26

Preparing for the certification audit

- Selecting the certification body
- Preparing for the certification audit
- Stage 1 audit
- Stage 2 audit
- Follow-up audit
- Certification decision



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 1

The requirements set out in this document 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 document.

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 for at least three months

Accreditation Bodies

- An accreditation body is an authoritative, independent organization that verifies whether a conformity assessment body meets established criteria and is competent to carry out conformity assessment tasks.
- Activities covered by accreditation include but are not limited to: testing, calibration, inspection, certification of management systems, persons, products, processes and services, and validation and verification.
- Accreditation bodies usually have their authority from government.

IAS INTERNATIONAL ACCREDITATION SERVICE

This image cannot currently be displayed.

UKAS

cofrac

DAkkS Deutsche Akkreditierungsstelle

Certification Bodies

Certification bodies certify management systems (ISO/IEC 17021-1), persons (ISO/IEC 17024), and products, processes, and services (ISO/IEC 17065).

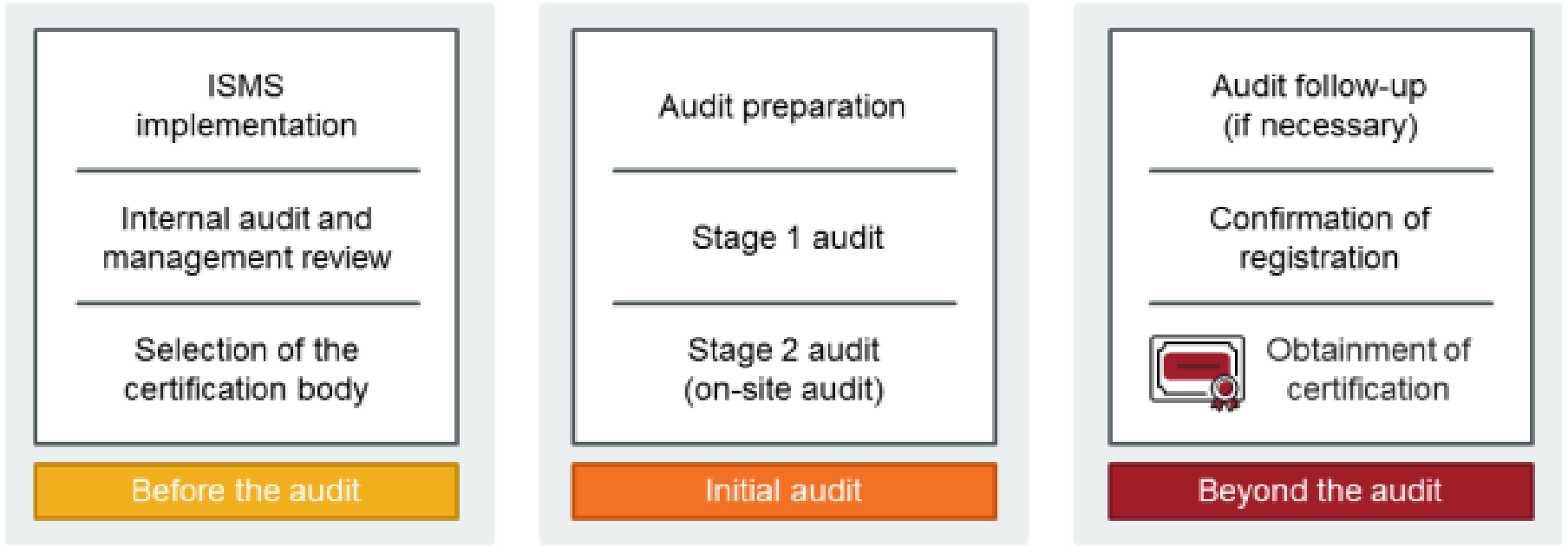
Certification bodies are always third-party, impartial conformity assessment bodies.

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

Management System Certification Bodies

- Management system certification bodies should conduct their activities in a competent, consistent, and impartial manner.
- For this purpose, ISO/IEC 17021-1 sets out the requirements that these bodies must adhere. Requirements include:
  - General requirements
  - Structural requirements
  - Resource requirements
  - Information requirements
  - Process requirements
  - Management system requirements
- Adherence to ISO/IEC 17021-1 not only facilitates the recognition of a certification body, it also ensures the acceptance of their certifications on a national and international basis.

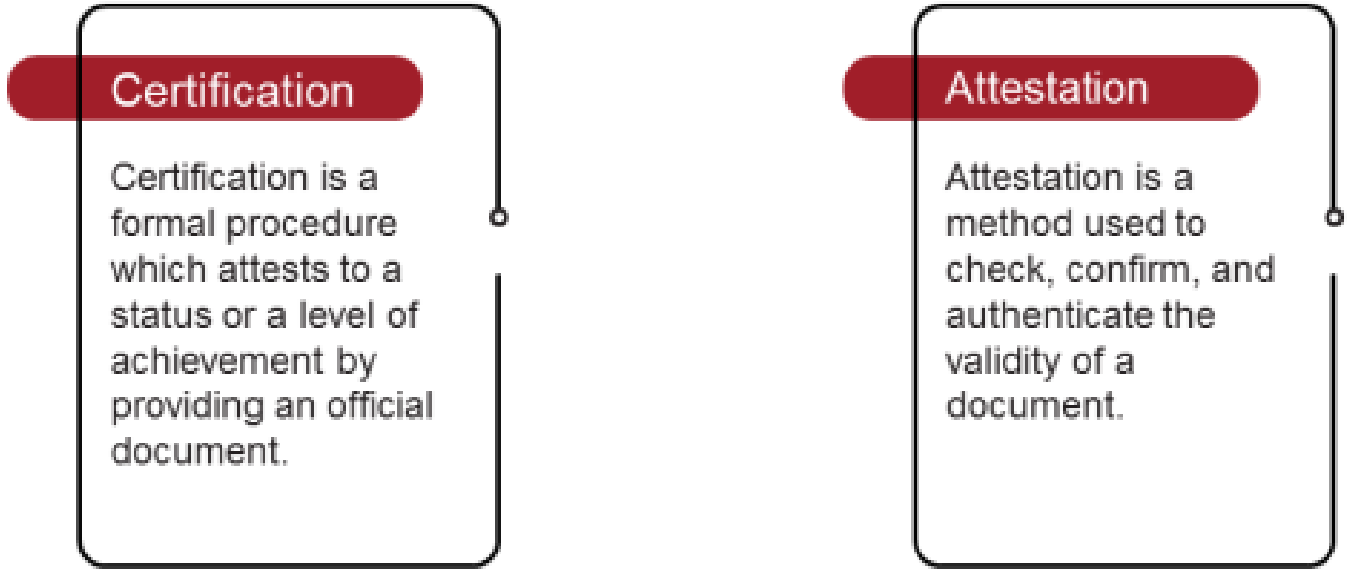
Certification Process



Note:
After obtaining the certification, a surveillance audit will be conducted to ensure continual improvement.

Certification and Attestation

Differences



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 be conducted.

1. Selecting the Certification Body

Main criteria

1. Reputation and credibility
2. Geographical location
3. References in your sector
4. Possibility of a combined audit
5. Skills and experience of the audit team
6. Prices

Rejection of an Auditor

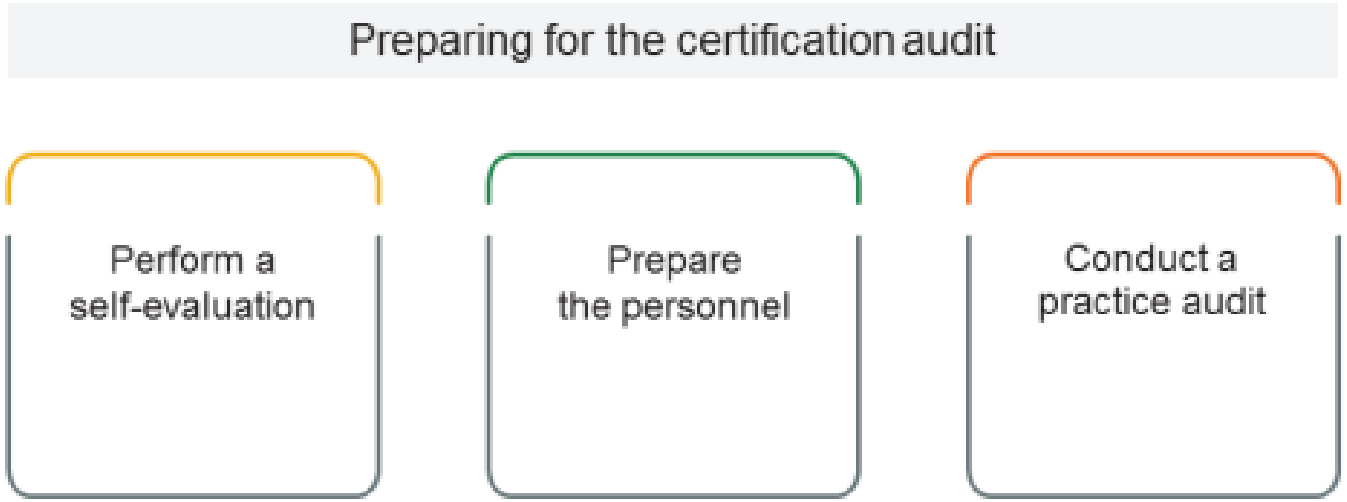
- The auditee can request the replacement of audit team members for valid reasons.
- The audit team could withdraw if it deems that the reasons cited are not valid.

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.

2. Preparing for the Certification Audit

Recommendations



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

3. Stage 1 Audit

1

Conduct on-site activities

- Evaluate the auditee's location and site-specific conditions of the audit
- Make contact with key personnel of the auditee
- Observe, in general, the technologies used and the operations of the ISMS

2

Prepare for stage 2 audit

- Validate the ISMS scope as well as the applicable legal, regulatory, and contractual constraints
- Validate that internal audits and management reviews have been performed
- Prepare for the stage 2 audit

3

Documented information review

- Understand how the management system operates
- Evaluate the design of the management system as well as its related processes or controls
- Verify that internal audits and management reviews have been performed

Note: The documented information review is the main activity of stage 1 audit.

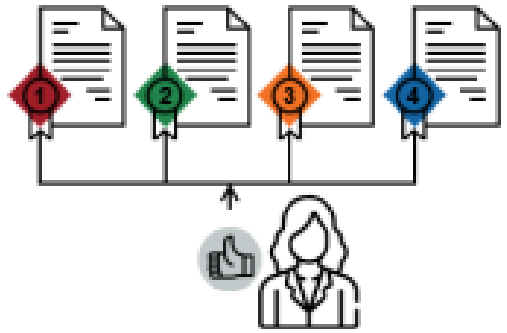
4. Stage 2 Audit

Evaluate if the management system:

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



5. Audit Follow-up

- Based on the audit conclusions, the auditor may have to conduct an audit follow-up before the organization is recommended for certification.
- During an audit follow-up, the auditor evaluates the effectiveness of all the corrections and corrective actions taken.

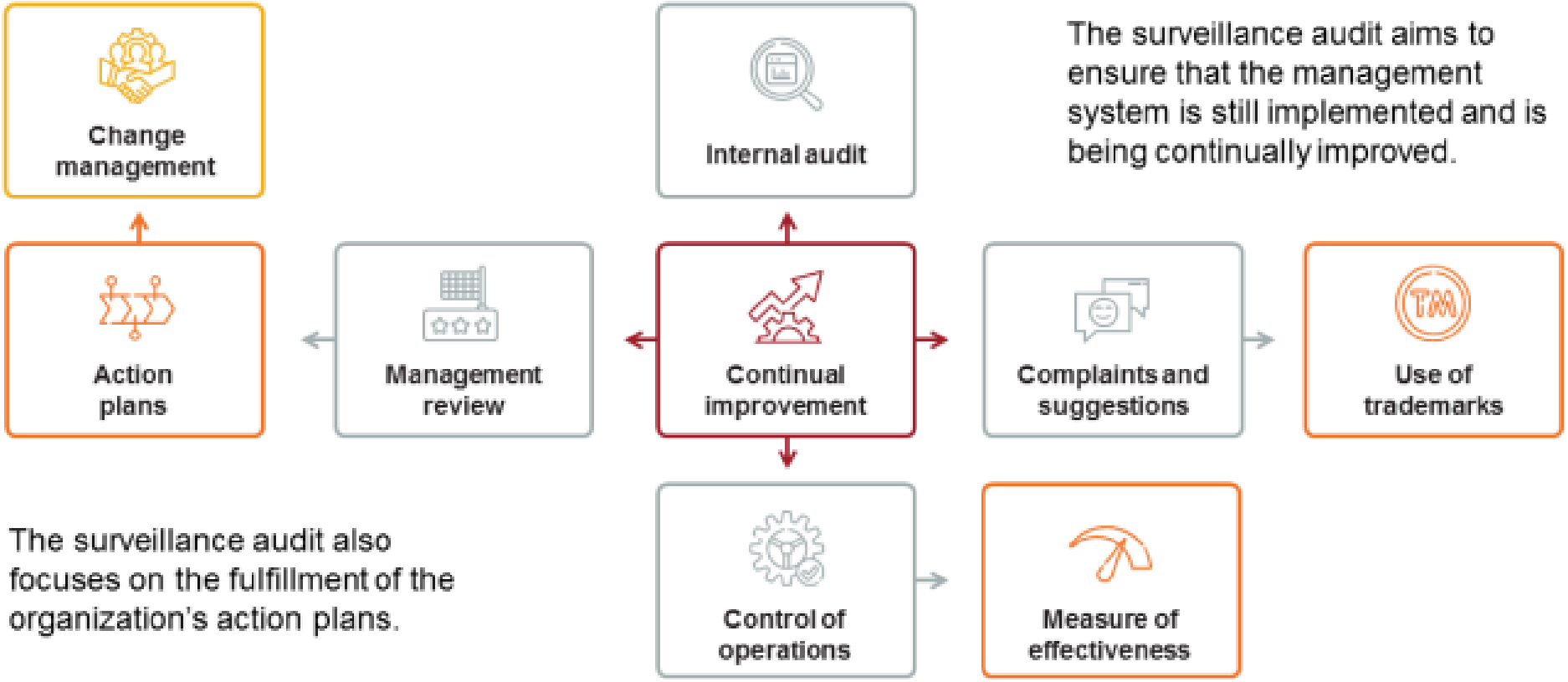
A major nonconformity often involves a follow-up audit.

6. Certification Decision

Important note:

The auditors that take part in the audit never take part in the certification decision.

Elements to Consider During a Surveillance Audit



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.*

Use of ISO Trademarks

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

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