ISO/IEC 27001:2022 Foundation

Accredited by ANAB

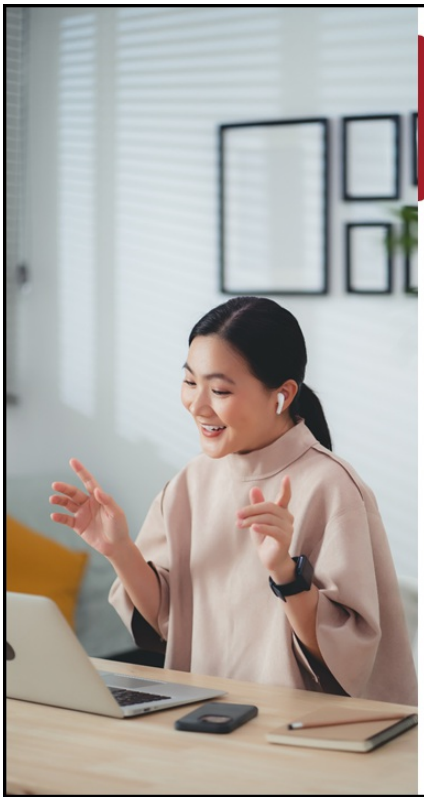
Version 7.0

Document number: ISMSFDD1V7.0

Introduction

The trainer and participants should begin by sharing a brief introduction, including:

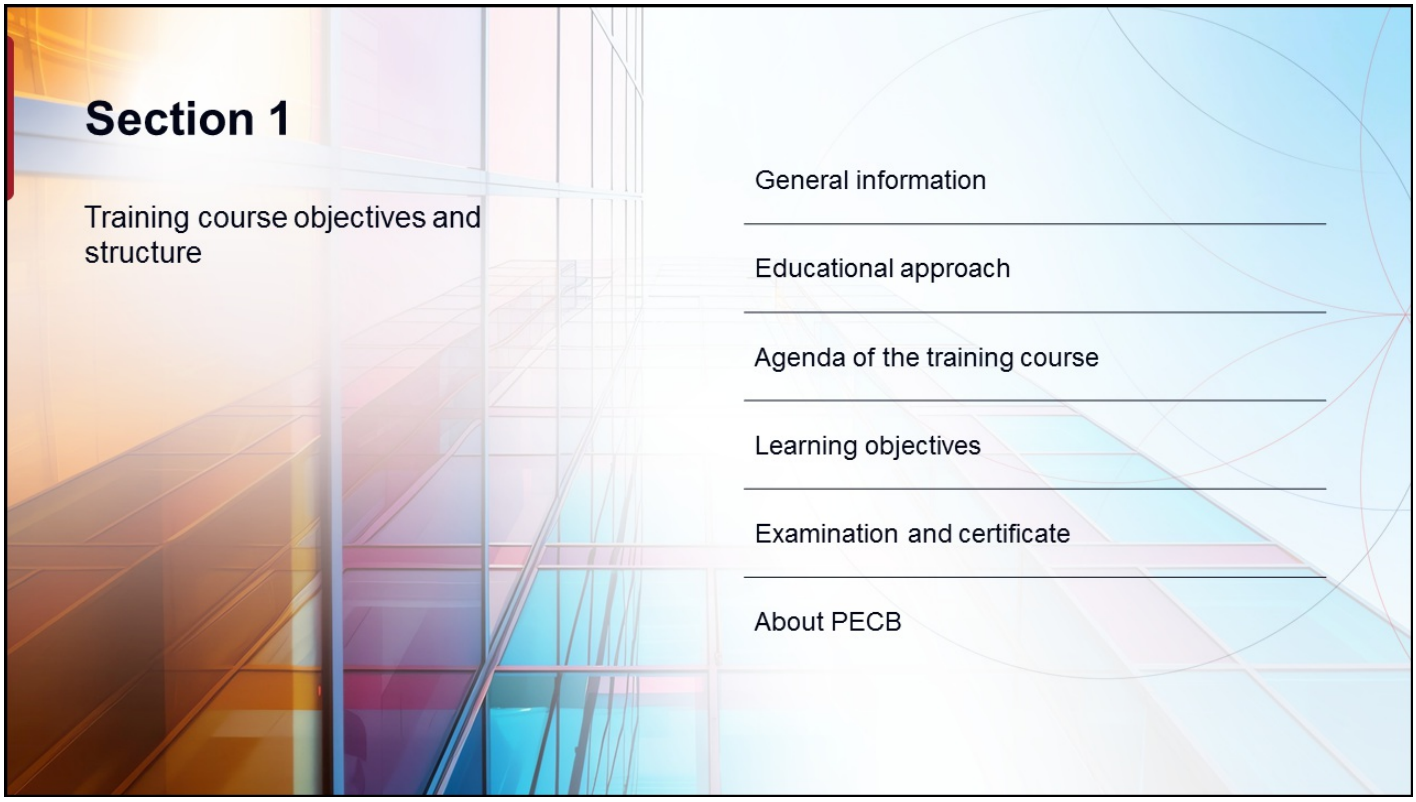
- Their name and current role
- Background in information security management
- Familiarity with ISO/IEC 27001 and related standards (e.g., ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27005, ISO/IEC 27701)
- Familiarity with auditing standards and best practices, as well as experience with auditing in the context of information security
- Goals and expectations for this training course



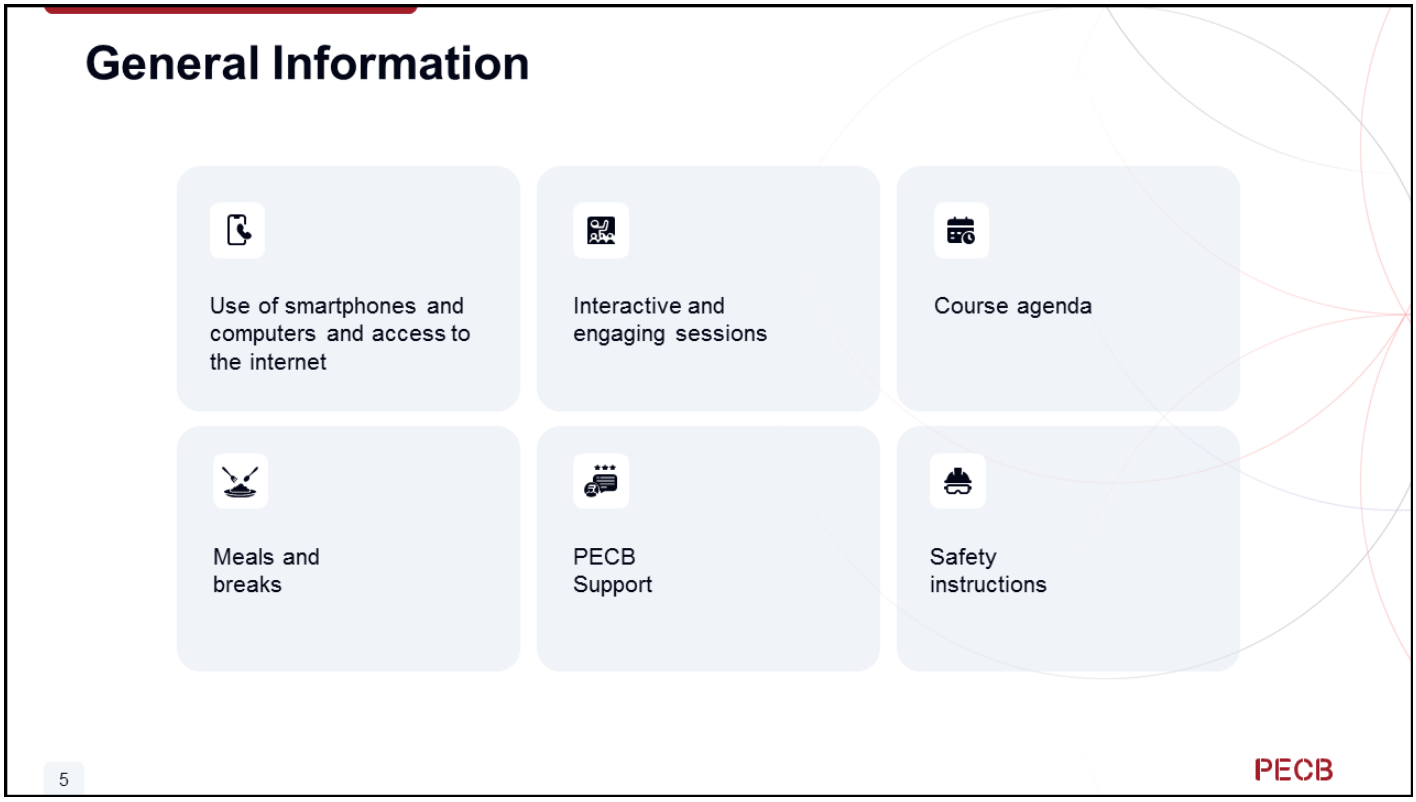
Day 1 Agenda

Section 1	Training course objectives and structure
Section 2	Standards and regulatory frameworks
Section 3	Information security management system (ISMS)
Section 4	Fundamental information security concepts and principles
Section 5	Understanding of the organization and its context
Section 6	Leadership

PECB



This section presents the training course and its approach. It briefly discusses the learning objectives that participants will be able to achieve upon the completion of the training course. In addition, the competency domains of the examination and the requirements for getting the certificate are explained. The section is wrapped up by a short preview of PECB and its services.



- All should be aware of the exit doors in the facility in case any emergency arises.
- All should agree on the training course schedule. All should arrive on time.
- All should set their smartphones on silent or vibrate mode (if you need to take a call, please do so outside the classroom).
- Recording devices are prohibited because they restrict free discussions.
- All sessions are designed to encourage participants to interact and take the most out of the training course.

Customer Service

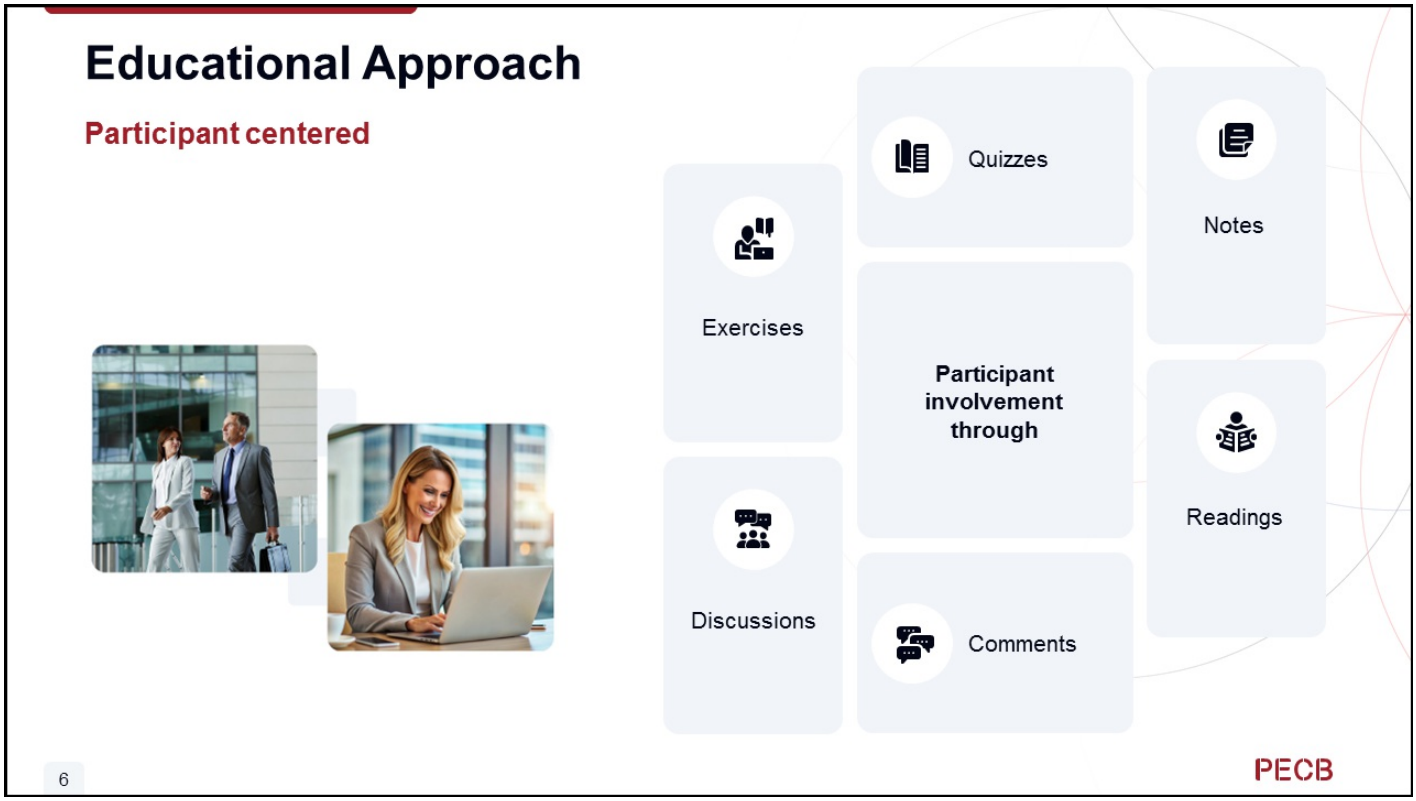
To ensure customer satisfaction and continual improvement, PECB Customer Service has established a support ticket system for handling complaints.

In case of inconvenience, we invite you to discuss the situation with the trainer first. If necessary, do not hesitate to contact the head of the training organization where you are registered. In all cases, we remain at your disposal to arbitrate any dispute that may arise between you and the training organization.

To send comments, questions, or complaints, please open a support ticket on the PECB website, at the PECB Help Center (https://pecb.com/help).

In case of dissatisfaction with the training (trainer, training room, equipment, etc.), the examination, or the certification processes, please open a ticket under **Make a complaint** category on the PECB Help Center.

If you have suggestions for improving PECB's training course materials, we are willing to read and evaluate your feedback. You can do so directly from our KATE application or you can open a ticket directed to the Training Development Department on the PECB Help Center.



To optimize the learning experience,PECB recommends scheduling two short breaks (15 minutes), and a lunch break (one hour) per training day. Time of the breaks can be adjusted accordingly.

Interaction by means of questions and suggestions is highly encouraged. Participants can best contribute to the training course by partaking in exercises, case studies, and discussions. Participants are also advised to take personal notes.

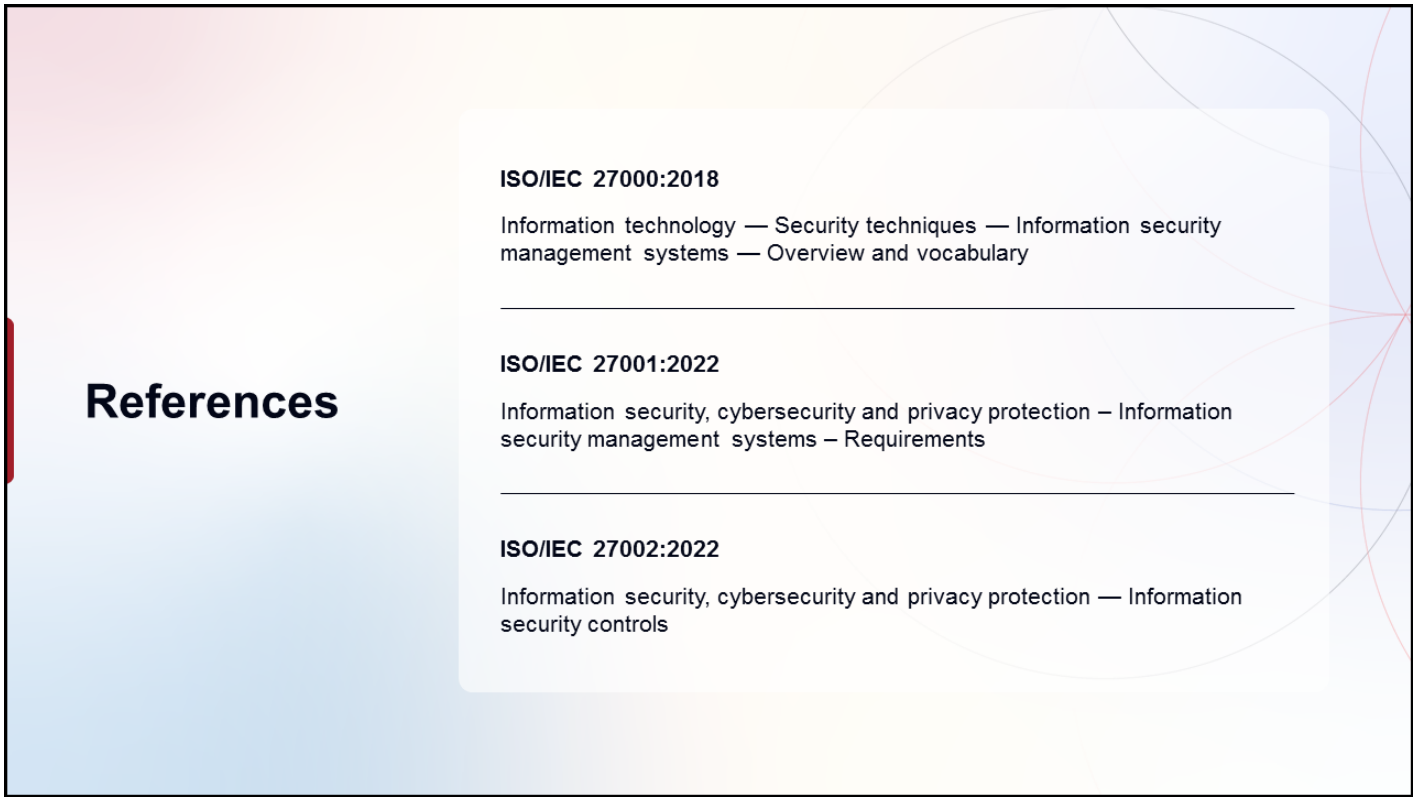
Quizzes, in particular, are important since they help participants prepare for the certification exam.

At the end of each day, there is a slide with a set of exercises given as homework. Completing the homework may help you better understand this training course, however, they are not mandatory.

Remember: This training course is yours; you are the main contributor to its success.

In addition to the training course materials, PECB also offers free content to help trainees get additional information and stay updated. Such free materials include:

- Articles
- Whitepapers
- InfoKits
- Magazine
- Webinars



Note: To see the complete list of references cited in this training course, please go to the Index file.

Day 1: Introduction to the information security management system (ISMS) and ISO/IEC 27001:2022

- Section 1: Training course objectives and structure
- Section 2: Standards and regulatory frameworks
- Section 3: Information security management system (ISMS)
- Section 4: Fundamental information security concepts and principles
- Section 5: Understanding of the organization and its context
- Section 6: Leadership

Day 2: Information security management system (ISMS) and certificate exam

- Section 7: Planning
- Section 8: Support
- Section 9: Operation
- Section 10: Performance evaluation
- Section 11: Improvement
- Section 12: Information security controls
- Section 13: Closing of the training course

Learning Objectives

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

1. Describe the main information security management concepts, principles, and definitions
2. Explain the main ISO/IEC 27001:2022 requirements for an information security management system (ISMS)
3. Identify approaches, methods, and techniques used for the implementation and management of an ISMS

9

PECB

This training course is designed to help the participants understand the fundamental concepts and principles of an information security management system (ISMS) based on ISO/IEC 27001:2022. From an educational perspective, competency consists of the following three elements:

1. Knowledge
2. Skill
3. Behavior (attitude)

If participants wish to obtain in-depth knowledge on how to implement an ISMS based on ISO/IEC 27001:2022 through a high-level approach and comprehensive methodology, we recommend them to take the PECB Certified ISO/IEC 27001 Lead Implementer training course. If they wish to acquire knowledge about an ISMS audit process, including the audit principles, techniques, and best practices, we recommend them to take the PECB Certified ISO/IEC 27001 Lead Auditor training course.

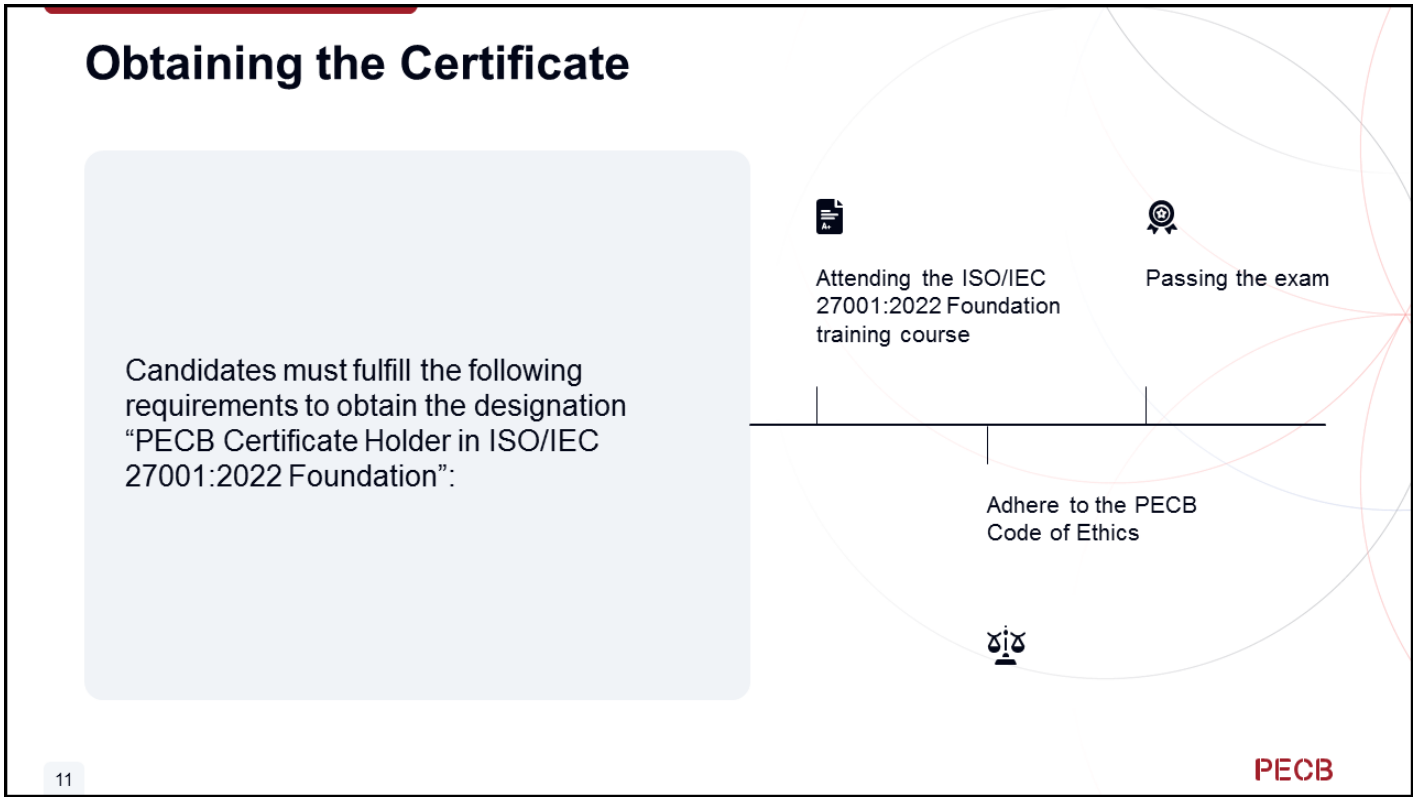
Examination

Competency domains

- Fundamental principles and concepts of an information security management system (ISMS)
- Information security management system (ISMS)

- The purpose of the exam is to evaluate whether candidates have understood the fundamental information security management concepts and are familiar with ISO/IEC 27001:2022 requirements so that they are able to be part of ISMS implementation projects.
- The PECB Examination Committee ensures that the exam questions are adequate and based on professional practice.
- The competency domains are covered in the exam.

PECB



Considering that the "ISO/IEC 27001:2022 Foundation" is an entry-level training course, candidates are not required to have professional experience in any ISMS project or audit.

The set of criteria and the process for obtaining the certificate will be explained in detail on the second day of this training course.

Important note: Fees are included in the exam price. Candidates will not have to pay any additional fees when applying for the certificate.

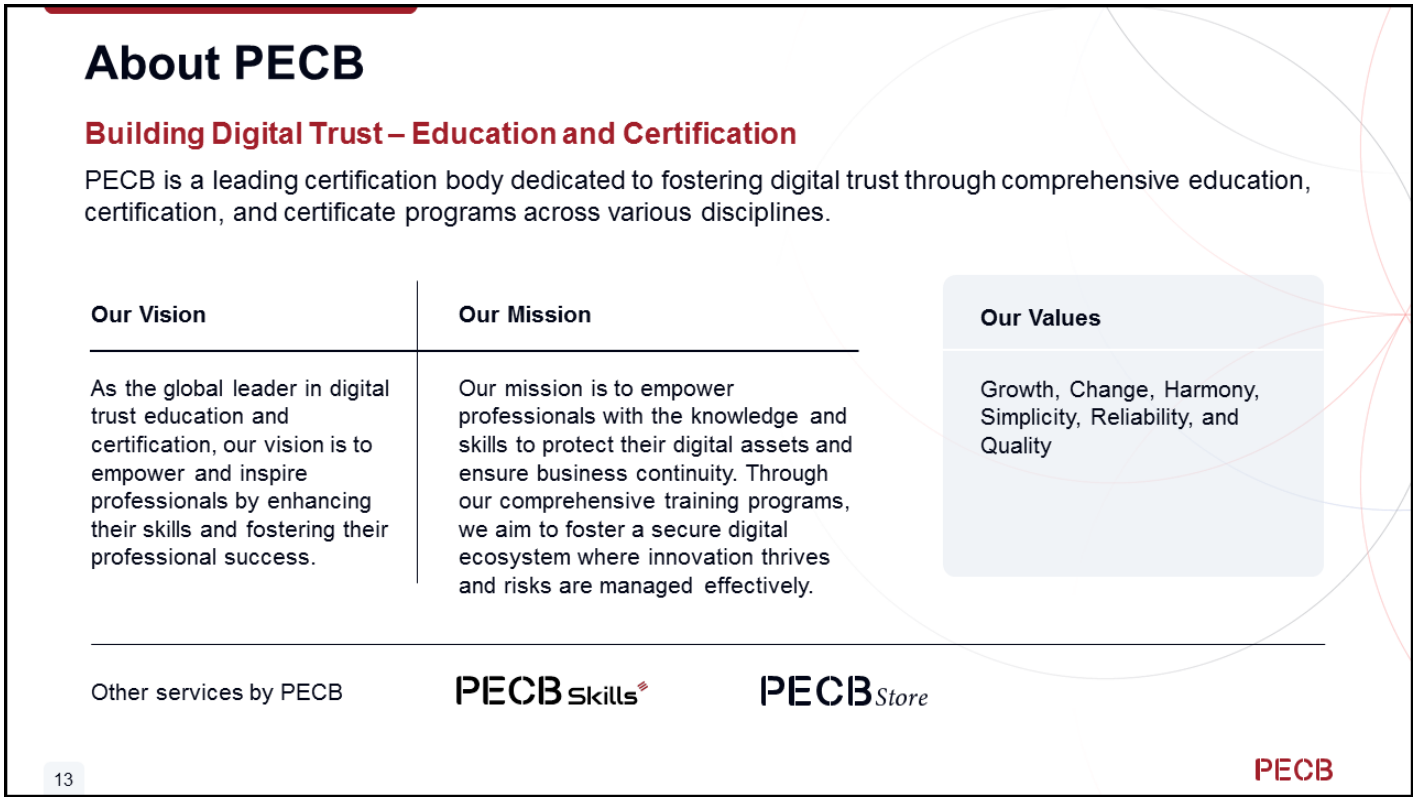
PECB Certificate

Candidates who meet all the prerequisites for the certificate program will receive a certificate.

12

PECB

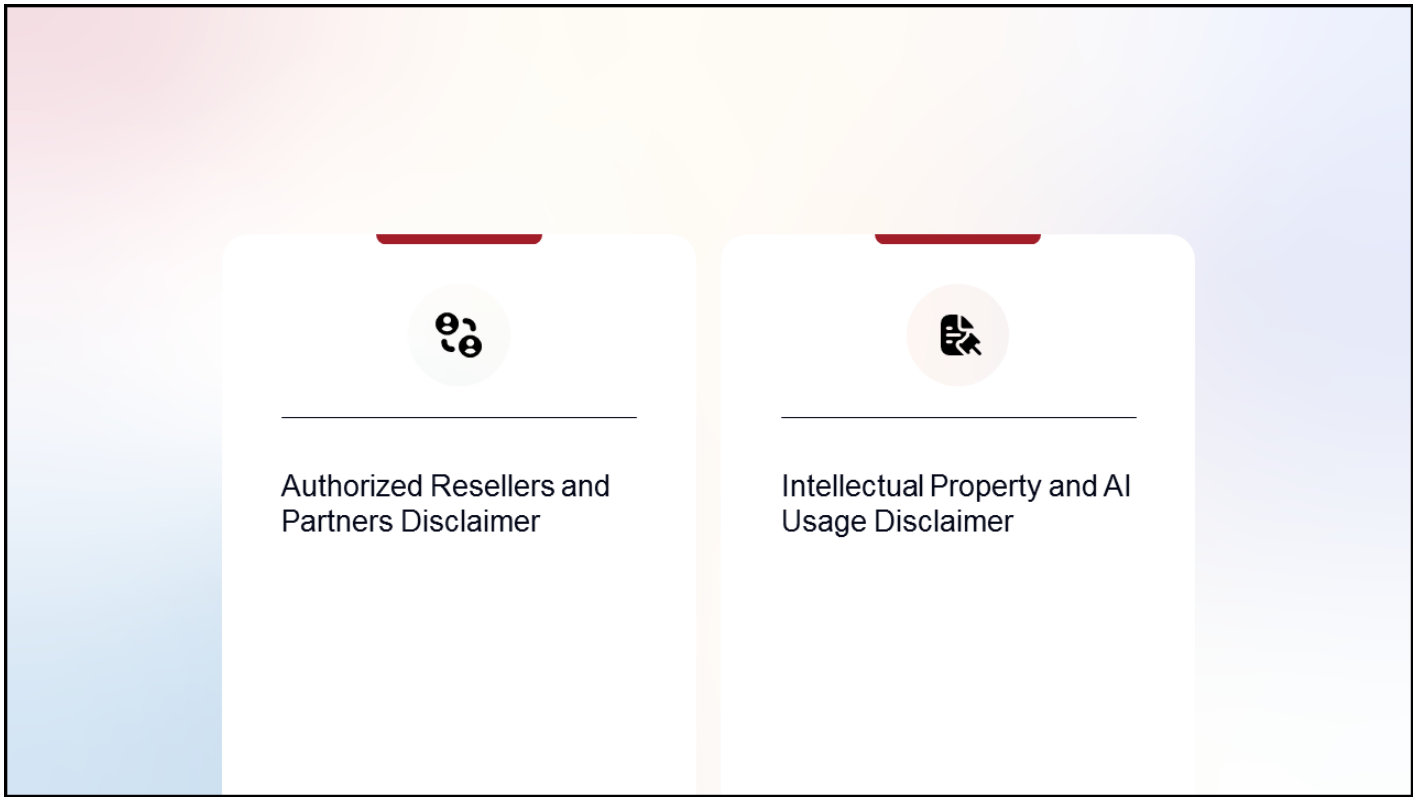
After passing the exam, candidates have a maximum period of one year to apply for the respective certificate.



Why Choose PECB?

At PECB, we are committed to your success. We work closely with you to understand your unique challenges and provide tailored training solutions that meet your specific needs. Our goal is to help you build a secure digital future, protect your business integrity, and ensure operational resilience.

- **Expertise and Accreditation –** At PECB, we blend deep expertise with globally recognized and accredited training portfolio. Our training courses are designed by industry leaders and adhere to the highest standards.
- **Flexible Learning Options –** We offer flexible learning options, allowing you to access our training programs online or in-person, so you can learn at your own pace.
- **Industry-Relevant Training –** Our training programs are continuously updated to reflect the latest industry trends and threats. This ensures that you receive the most current and relevant information to protect your organization effectively.
- **Global Reach –** Our extensive network of over 2,600 partners and 2,100 trainers globally, ensuring you receive top-tier training and support, no matter where you are located, providing you with consistent quality and accessibility.



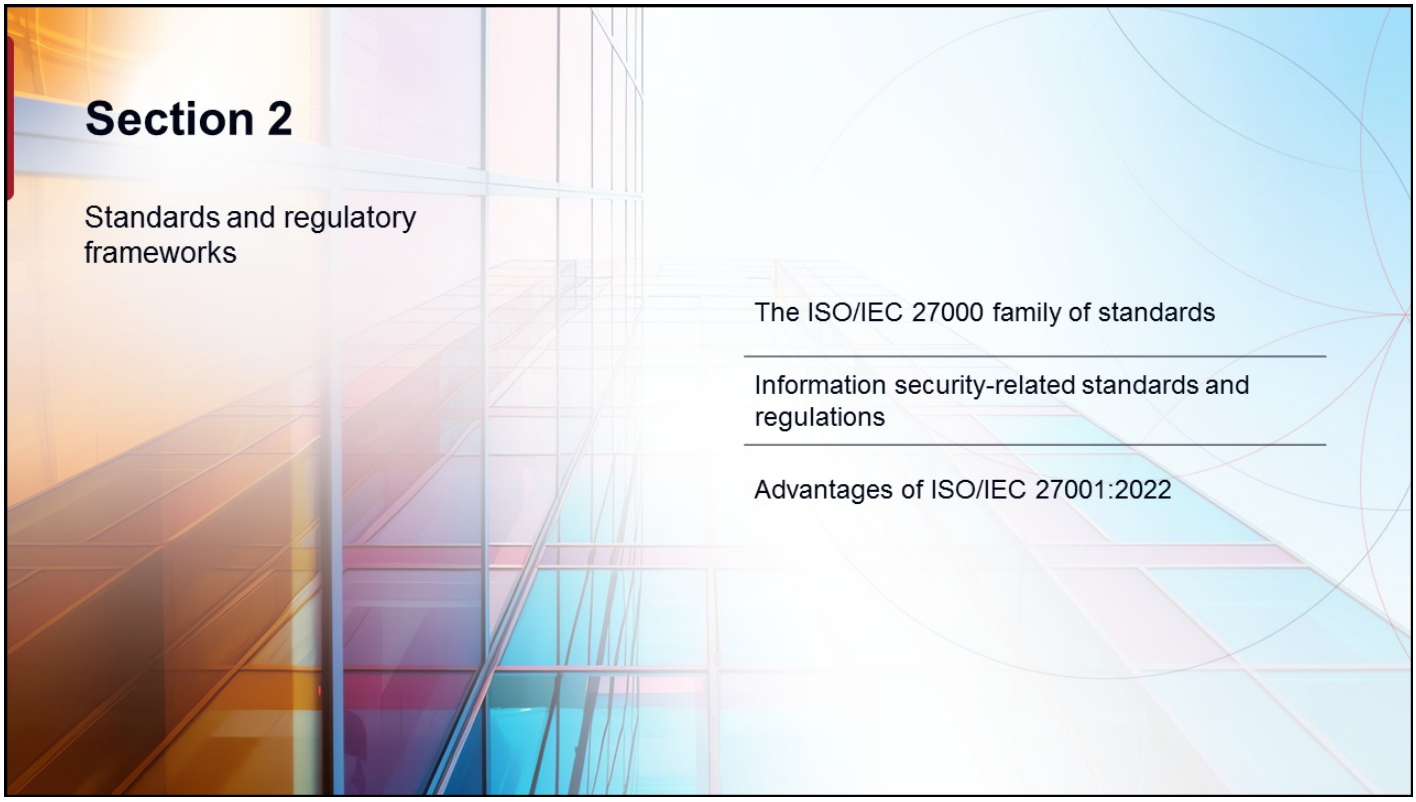
Authorized Resellers and Partners Disclaimer

PECB Group Inc. (“PECB”) provides its training courses exclusively through a vetted network of authorized resellers and partners. Customers and prospective clients are urged to verify the legitimacy of resellers prior to purchasing any PECB training courses or exam vouchers. PECB does not recognize transactions made through unauthorized providers and it disclaims any responsibility for courses, certifications, or vouchers obtained through illegitimate sources.

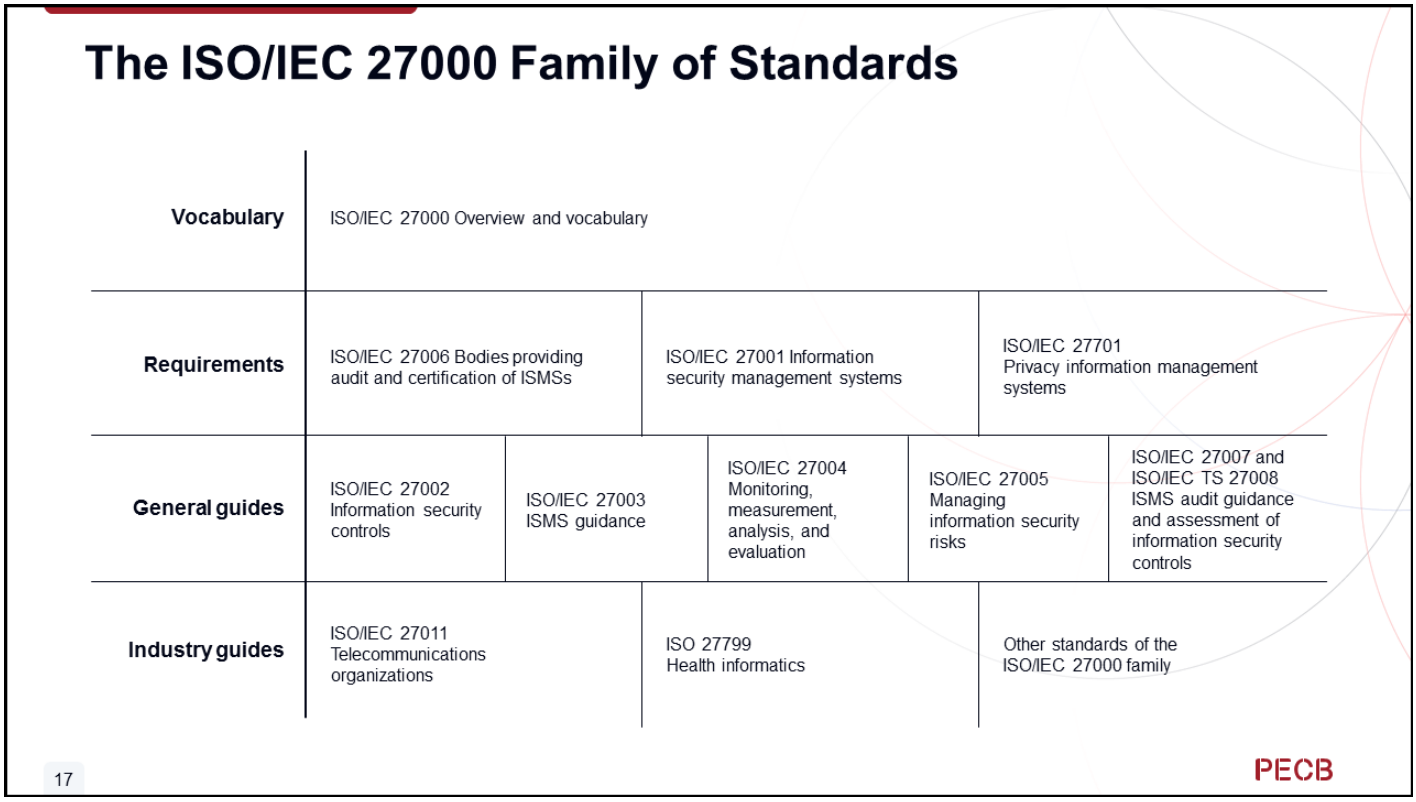
To ensure authenticity, please refer to PECB’s official website (www.pecb.com/resellers) or contact PECB’s customer service to confirm the status of a reseller. Any suspicious activity or counterfeit offers should be reported to PECB immediately to facilitate prompt investigation and appropriate legal action. PECB reserves the right to take legal action against unauthorized resellers, distributors, or individuals who misrepresent their affiliation with PECB.

By accessing or using PECB's training course materials, you acknowledge that you have read, understood, and agree to be bound by these terms and conditions. PECB Group Inc. reserves the right to modify or update these terms and conditions at any time without notice.

Intellectual Property and AI Usage DisclaimerPECB Group Inc. ("PECB") maintains stringent protections over its intellectual property, including but not limited to training course materials, documentation, and related proprietary content ("PECB IP"). Unauthorized inclusion, integration, or utilization of PECB IP within any artificial intelligence (AI) tools or platforms, including but not limited to generative language models such as ChatGPT, is strictly prohibited without prior express written consent from PECB. This prohibition extends to any derivative works, adaptations, or modifications of PECB content created utilizing artificial intelligence (AI) or machine learning algorithms. Any breach of this prohibition will result in immediate suspension of the infringer’s access to PECB training course materials, revocation of licenses, and may prompt rigorous legal action. PECB reserves the right to pursue all available legal remedies, including but not limited to seeking injunctive relief to prevent further unauthorized use, and claiming monetary damages for intellectual property infringement and associated losses.



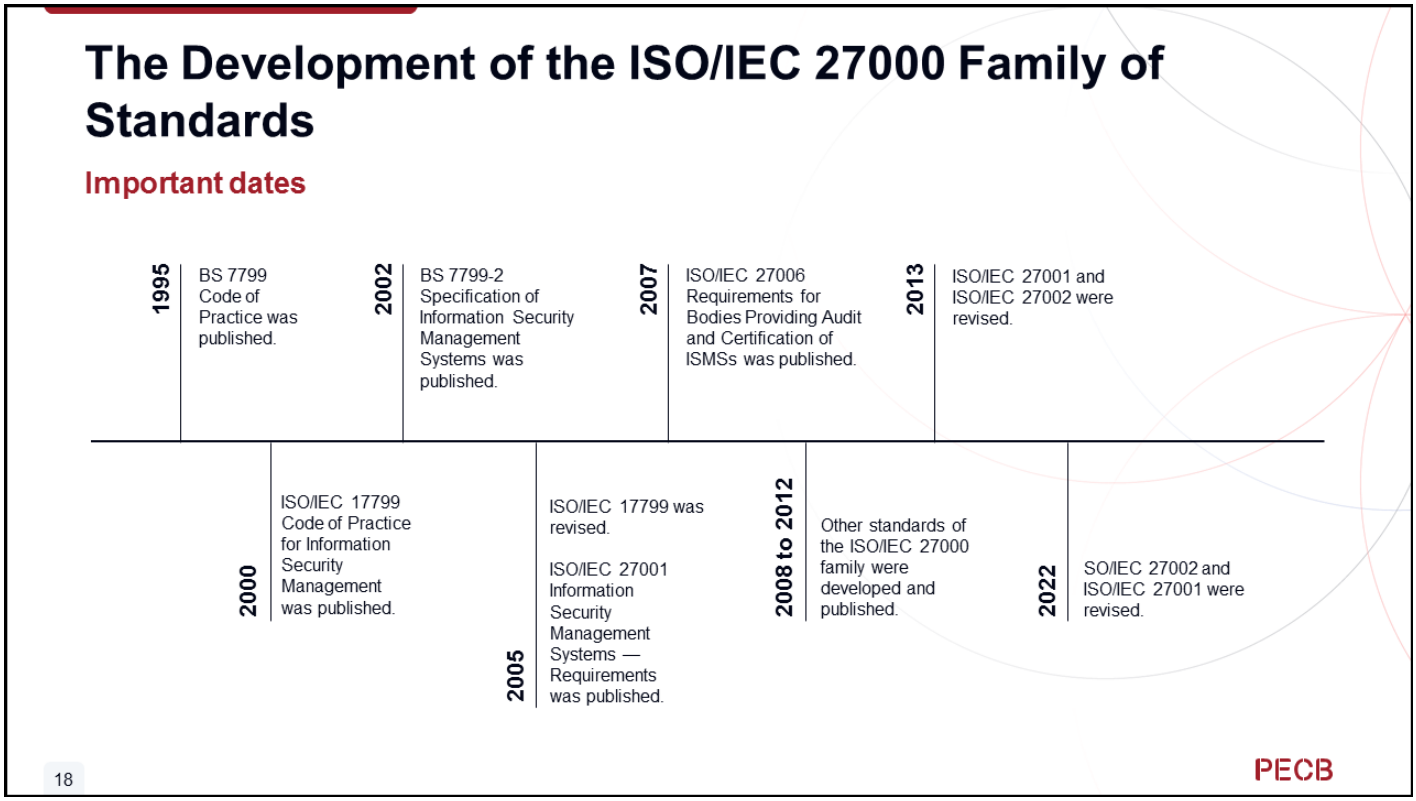
This section provides information that will help the participant gain knowledge on ISO/IEC 27001:2022 and the advantages it brings, and other standards and regulations related to information security.



The ISO/IEC 27000 family of standards is a series of information security standards. These standards are:

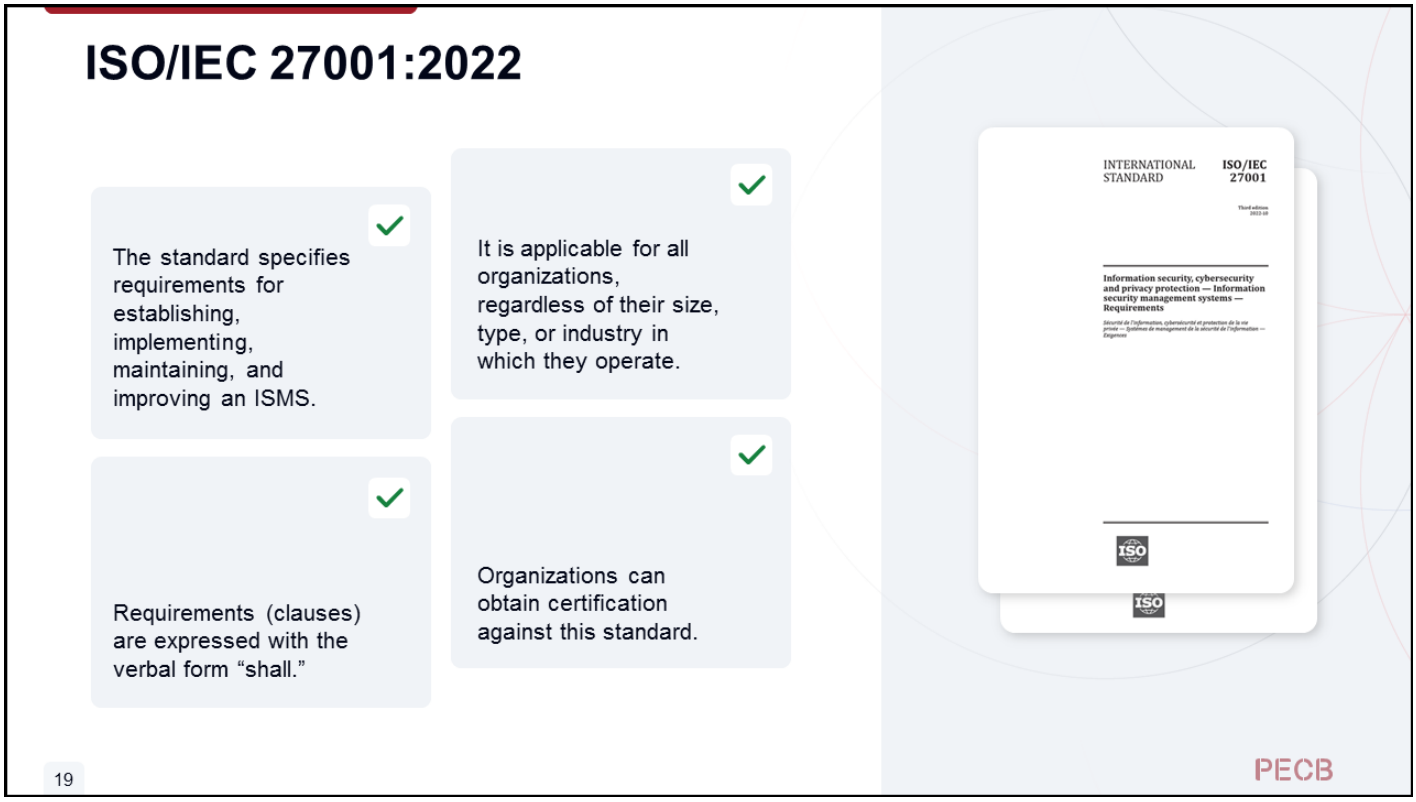
- **ISO/IEC 27000:** Overview and vocabulary commonly used in information security
- **ISO/IEC 27001:2022:** Requirements for establishing, implementing, maintaining, and continually improving an ISMS
- **ISO/IEC 27002:** Provides generic information security controls and their implementation guidance
- **ISO/IEC 27003:** Guidance on implementing an ISMS
- **ISO/IEC 27004:** Guidance on monitoring, measurement, analysis, and evaluation of an ISMS
- **ISO/IEC 27005:** Guidance on managing information security risks
- **ISO/IEC 27006:** Requirements for organizations providing audit and certification of ISMS
- **ISO/IEC 27007:** Guidance for information security management systems auditing
- **ISO/IEC TS 27008:** Guidance for the assessment of information security controls
- **ISO/IEC 27011:** Guidance on the implementation of information security controls in the telecommunications industry
- **ISO/IEC 27031:** Guidance on information and communication technology readiness for business continuity
- **ISO/IEC 27701:** Specifies the requirements and provides guidance for establishing, maintaining, and continually improving a privacy information management system (PIMS) as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management (as a result of the processing of PII)
- **ISO 27799:** Guidance on the use of ISO/IEC 27002 in health informatics

Source: https://www.iso.org/home.html



The history behind the development of the standards pertaining to the ISO/IEC 27000 family:

- BS 7799, which consisted of a set of controls, was published by the British Standards Institution (BSI) in 1995. Many of these controls are recognizable in today's ISO/IEC 27002. It was developed by the UK government's Department of Trade and Industry (DTI). The document provided practices for information security management and it was intended to help organizations establish and implement an ISMS and ensure the availability, confidentiality, and integrity of their information.
- The Specification for Information Security Management Systems – BS 7799-2 was published in 2002. The previously published BS 7799 became BS 7799-1.
- These documents were eventually adopted as ISO standards, BS 7799-2 becoming ISO/IEC 27001, and BS 7799-1 becoming ISO/IEC 27002; this logically puts the requirements first and the code of practice (guidance) second.
- They were later supplemented by ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, and various sector-specific interpretive guidance standards.
- ISO/IEC 27002 was revised in 2022. The release of the new version of ISO/IEC 27002 was followed by the publication of the updated version of ISO/IEC 27001.



ISO/IEC 27001:2022 is:

- A set of normative requirements for the establishment, implementation, operation, monitoring, and review of an information security management system (ISMS)
- A set of requirements for selecting security controls tailored to the needs of each organization based on industry best practices
- An internationally recognized process, defined and structured to manage information security
- An international standard that fits all types of organizations, regardless of their size or sector in which they operate (e.g., commercial enterprises, government agencies, nonprofit organizations)

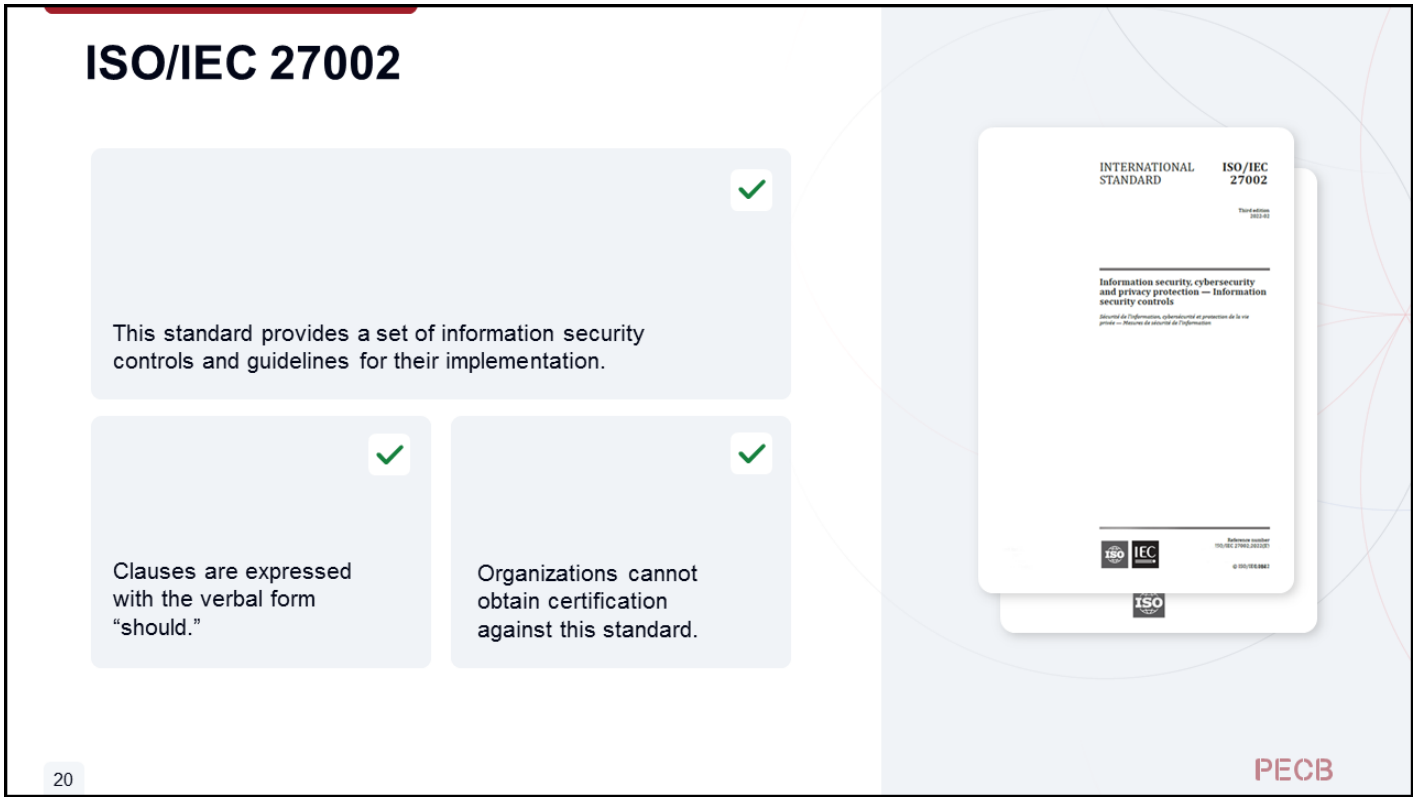
ISO/IEC 27001, clause 0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization’s information security management system is influenced by the organization’s needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization’s processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization’s ability to meet the organization’s own information security requirements.



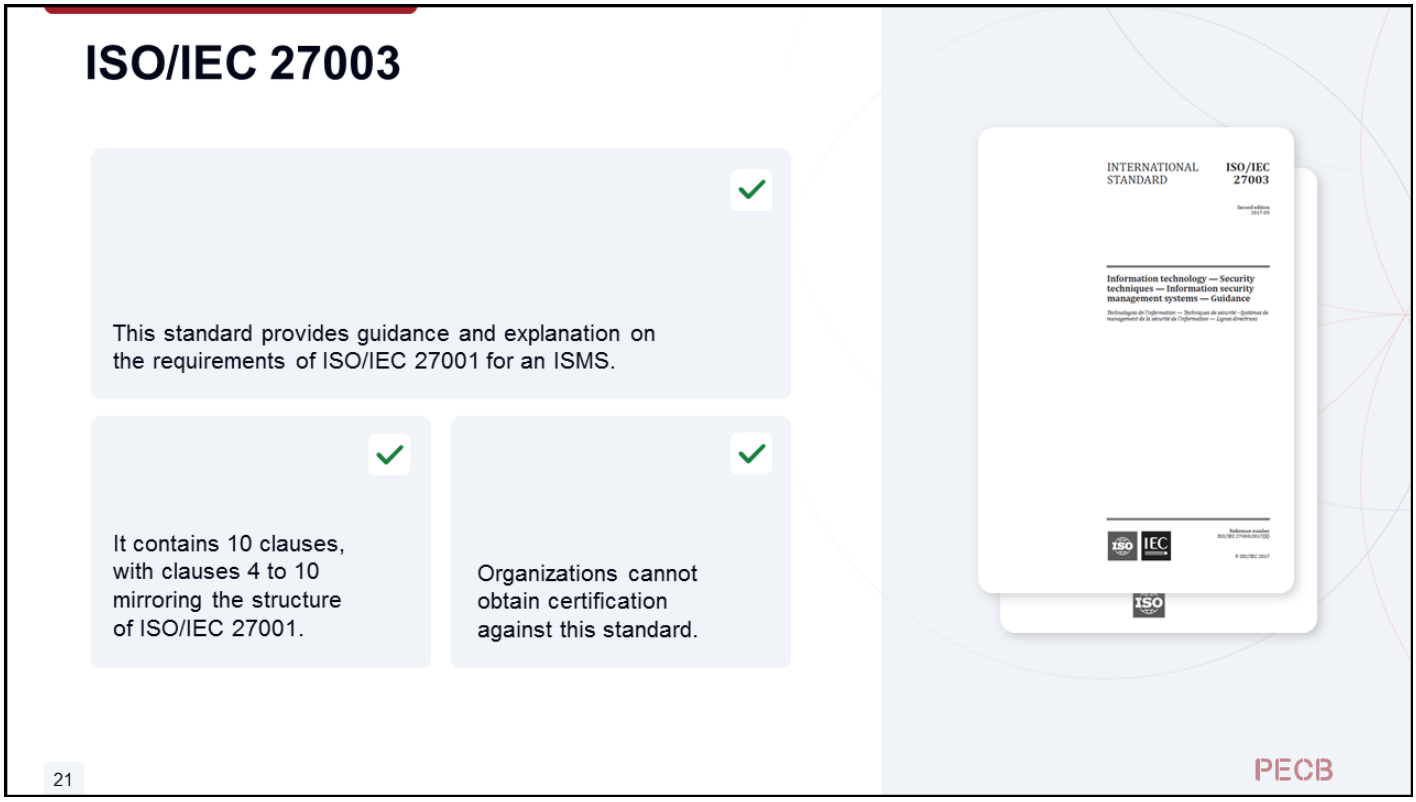
ISO/IEC 27002:

- ISO/IEC 27002 provides guidelines for the implementation of information security controls necessary to treat the information security risks of an ISMS based on ISO/IEC 27001:2022.
- It provides a list of information security controls generally practiced in the information security industry, their purpose, and implementation guidance.
- Clauses 5 to 8, in particular, provide detailed guidance to support the controls specified in Annex A of ISO/IEC 27001:2022.

ISO/IEC 27002, clause 1 Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a. *within the context of an information security management system (ISMS) based on ISO/IEC 27001;*
b. *for implementing information security controls based on internationally recognized best practices;*
c. *for developing organization-specific information security management guidelines.*



ISO/IEC 27003, Introduction

This document provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them. It is not the intention of this document to provide general guidance on all aspects of information security.

This document does not add any new requirements for an ISMS and its related terms and definitions. Organizations should refer to ISO/IEC 27001 and ISO/IEC 27000 for requirements and definitions. Organizations implementing an ISMS are under no obligation to observe the guidance in this document.

The Payment Card Industry Data Security Standard (PCI DSS)

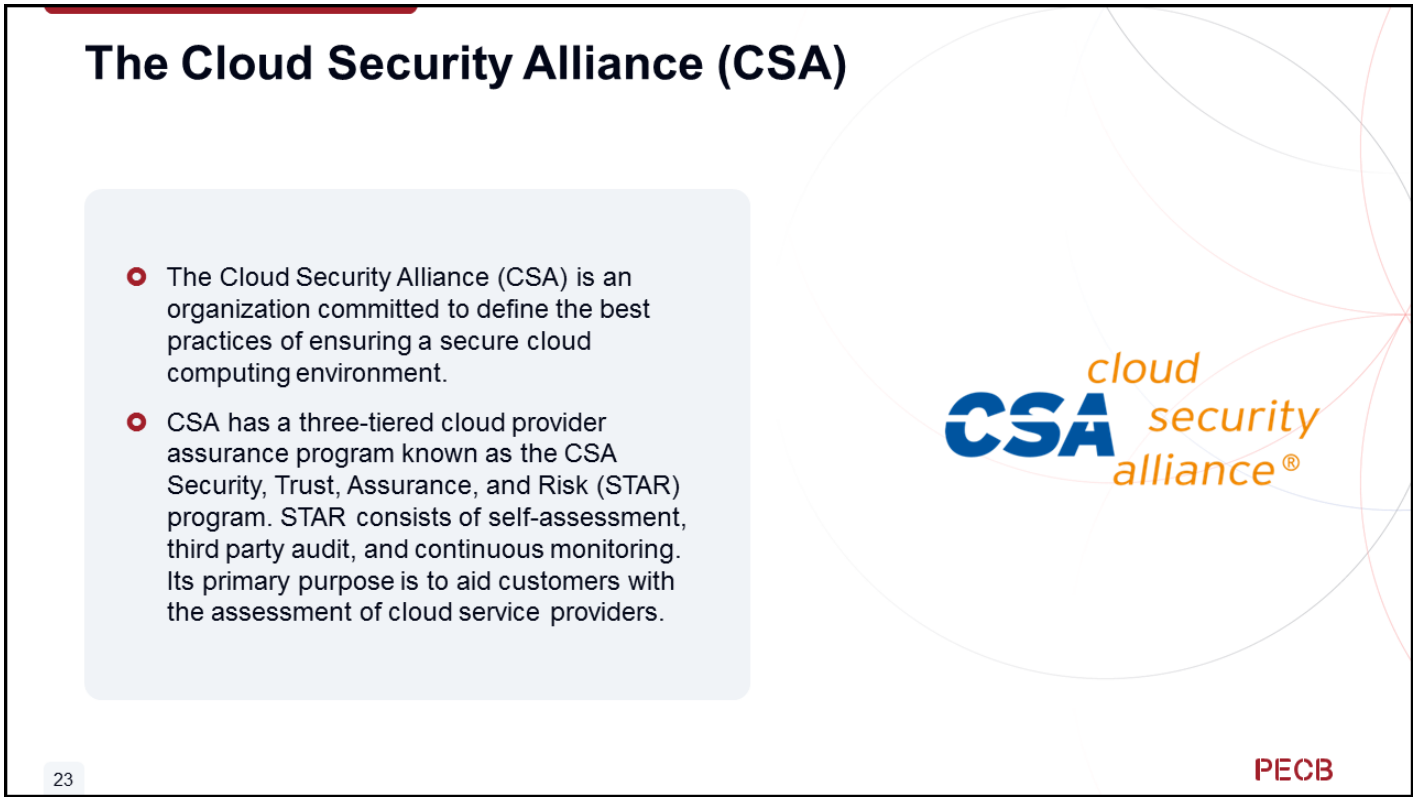
- The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards which unify the information security programs and policies with regard to credit card information.
- PCI DSS applies to any organization that accepts, transmits, or stores any cardholder data.
- PCI Security Standards Council was founded in 2006 by American Express, Discover, JCB International, MasterCard, and Visa Inc.

22

PECB

PCI DSS consists of 6 goals and 12 requirements. These goals are to:

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong control access measures
- Regularly monitor and test networks
- Maintain an information security policy



The CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider. Basically, any organization that undergoes ISO/IEC 27001 certification can simultaneously undergo to CSA Star assessment and obtain the CSA Star Certification. CSA STAR guidelines are relevant for cloud service providers (CSPs) that fall mainly in the below-listed industries:

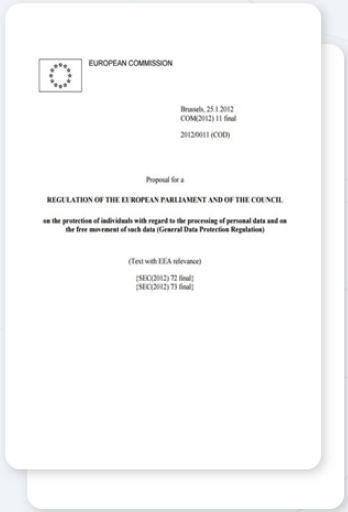
- Cloud Service Providers
- Data Center Hosting
- Web Hosting
- Intellectual Property Protection
- Finance and health care services

The General Data Protection Regulation (GDPR)

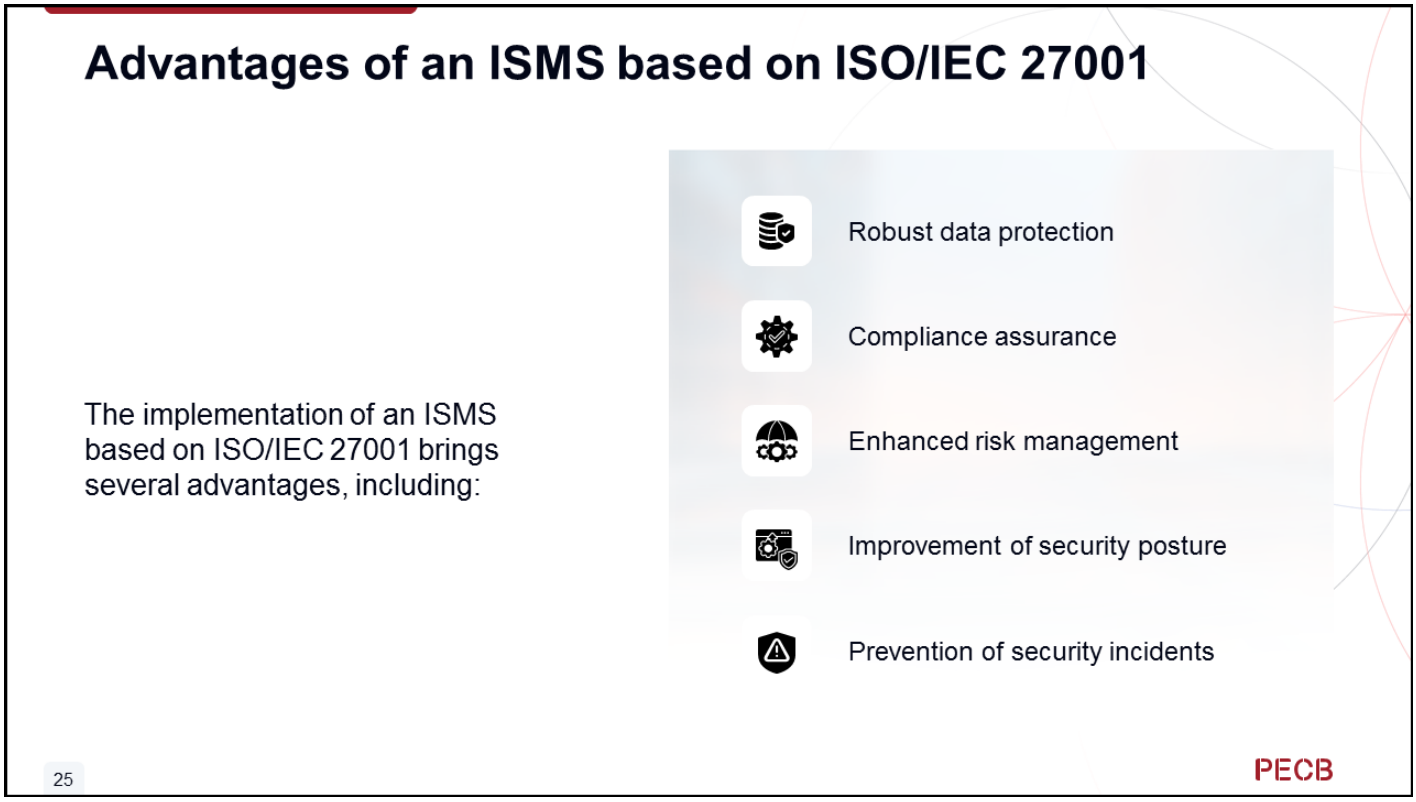
GDPR specifies the requirements for the protection of natural persons with regard to the processing and free movement of personal data.

The GDPR is available at: http://eur-lex.europa.eu/

ISO/IEC 27001:2022 is the leading international standard for information security. Thus, the ISO/IEC 27001:2022 framework can be used to support compliance with the GDPR. Furthermore, ISO/IEC 27001:2022 and the GDPR overlap in many areas, such as data confidentiality, availability, and integrity, as well as risk assessment, etc.



PECB



1. **Robust data protection**
   - Enhanced security measures that protect sensitive data from unauthorized access, breaches, and leaks
   - Ensured data confidentiality, integrity, and availability
2. **Compliance assurance**
   - Security practices aligned with legal and regulatory requirements
   - Adherence to data protection laws
3. **Enhanced risk management**
   - Identification and evaluation of security risks enable organizations to prioritize and proactively address potential threats.
   - Implementation of security controls and incident response plans minimizes the impact of security incidents.
4. **Improvement of security posture**
   - Better management of information security threats
   - Implementation of internationally recognized information security controls
5. **Prevention of security incidents**
   - Prevention of security incidents reduces financial losses associated with data breaches and recovery effects.
   - Efficient resources allocation and risk mitigation measures lead to cost savings.

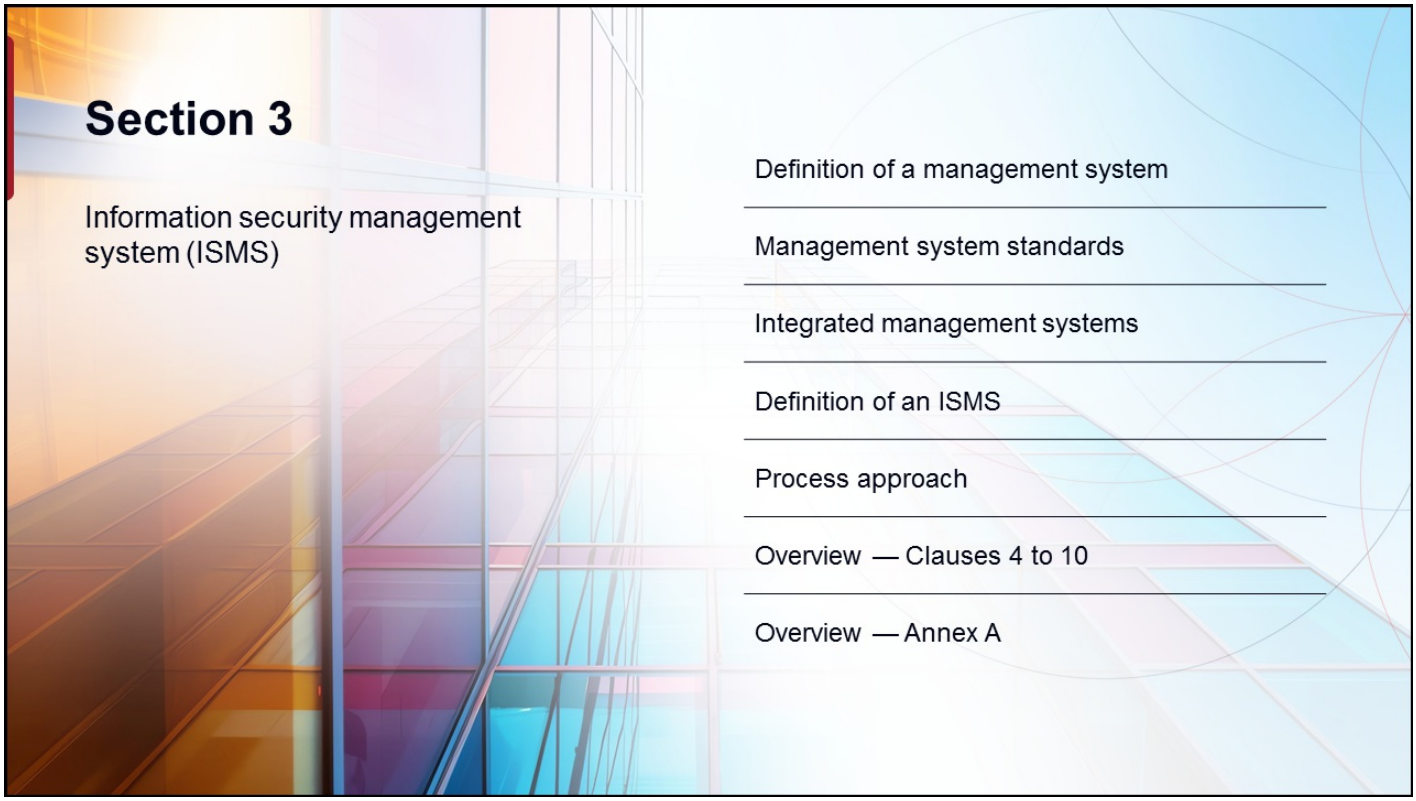
Section 2 Summary

- The ISO/IEC 27000 family of standards includes information security standards.
- ISO/IEC 27001:2022 is the main standard of the family that specifies the requirements for an ISMS.
- ISO/IEC 27701 specifies the PIMS requirements and provides guidance to PII controllers and processors to hold responsibility and accountability for PII processing.
- ISO/IEC 27002 provides guidance for the implementation of information security controls.
- In a normative standard, requirements (clauses) are written using the imperative verb "shall." On the other hand, in a guideline standard, clauses are written using the verb, "should."
- The advantages of having an ISMS in place include: improved information security, good governance, international recognition, competitive advantage, incremental revenue, etc.

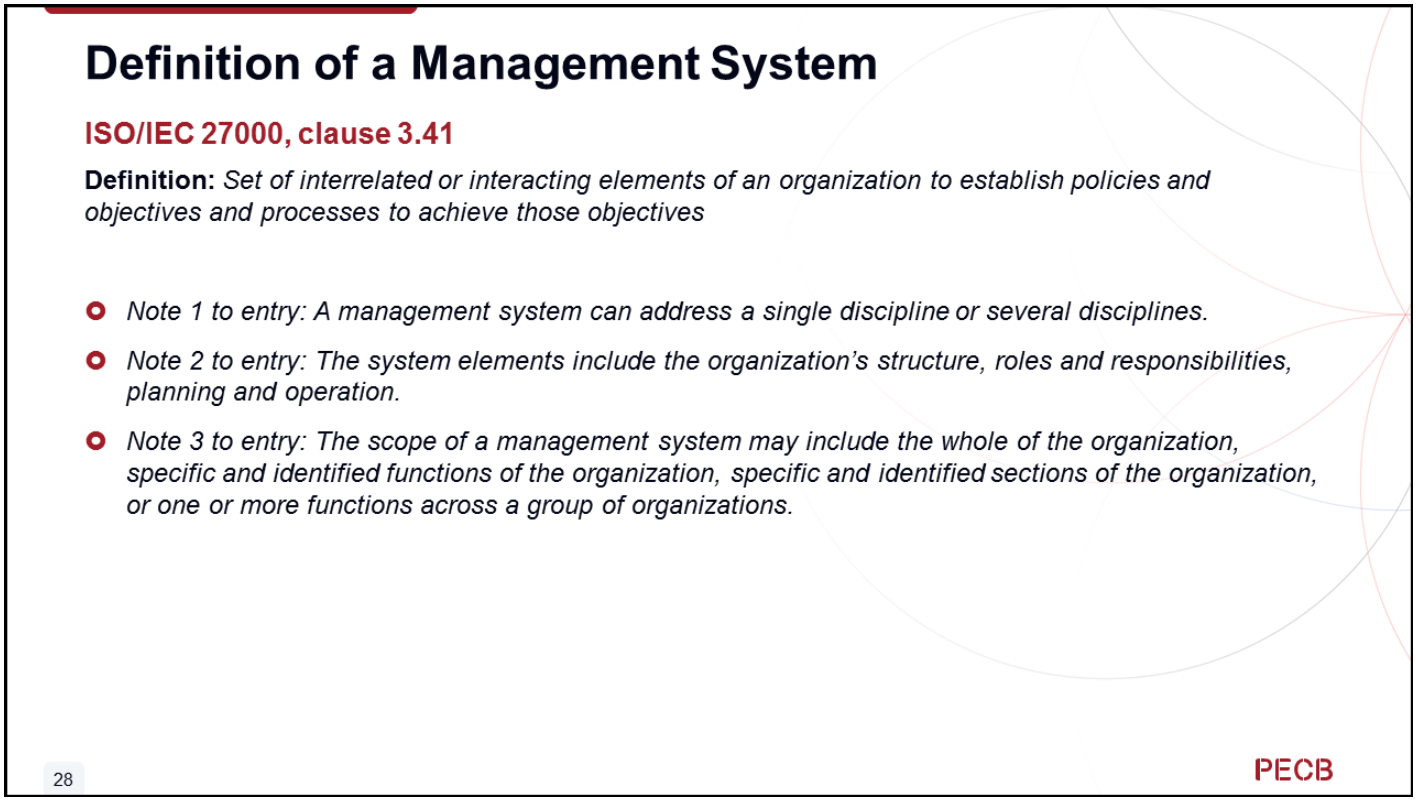
Questions?

Exercise 1

Note: To complete Exercise 1, please go to the Exercises Worksheet.



This section provides information that will help the participant gain knowledge on the definition of a management system and an ISMS, process approach, and the structure of ISO/IEC 27001:2022, including an overview of clauses 4 to 10 and Annex A.



A management system is a system that allows organizations to establish policies and objectives and to subsequently implement them. The management system of an organization may include management systems in different fields, including quality, information security, environment, etc.

Organizations use management systems to develop their policies and put them into effect through objectives using:

- An organizational structure
- Systematic processes and associated resources
- An effective assessment methodology
- A review process to ensure that the problems are adequately solved and that opportunities for improvement are recognized and implemented when justified

Note: What is implemented must be controlled and measured; what is controlled and measured must be managed.

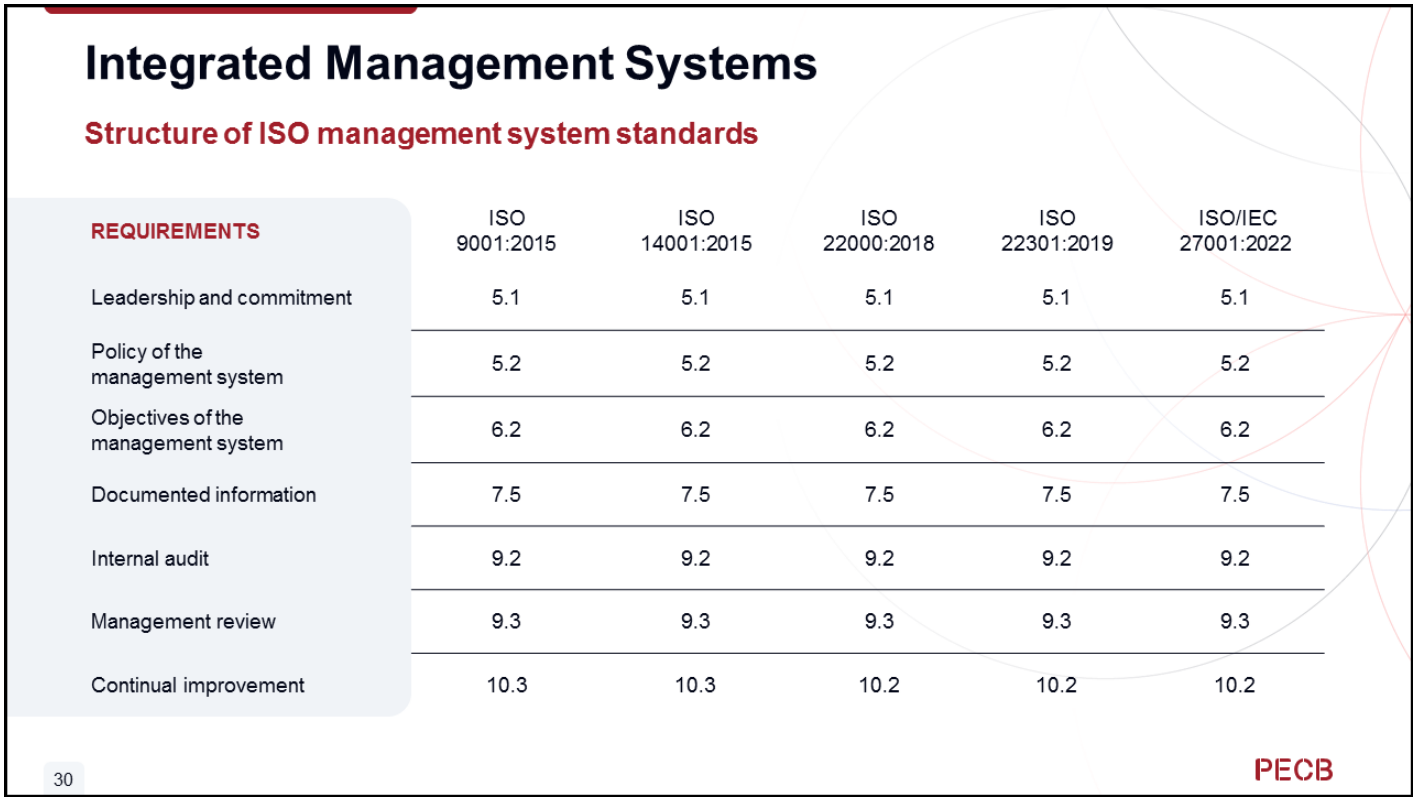
ISO/IEC 27001:2022 indicates that the organization must evaluate the information security performance and the effectiveness of the information security management system (clause 9.1). This clause is an essential component of a management system, since it is impossible to validate whether the organization has achieved its objectives without evaluating the effectiveness of processes and controls.

ISO publications range from traditional activities, such as agriculture and construction, to the most recent developments in information technologies, such as the digital coding of audiovisual signals for multimedia applications.

ISO 9000 and ISO 14000 families of standards are among the best known. ISO 9001 has become an international reference with regard to quality. ISO 14001, on the other hand, helps organizations enhance their environmental performance. Both standards are generic and applicable to any organization, regardless of size or complexity of processes.

For detailed information on each standard, please visit https://pecb.com or https://www.iso.org.

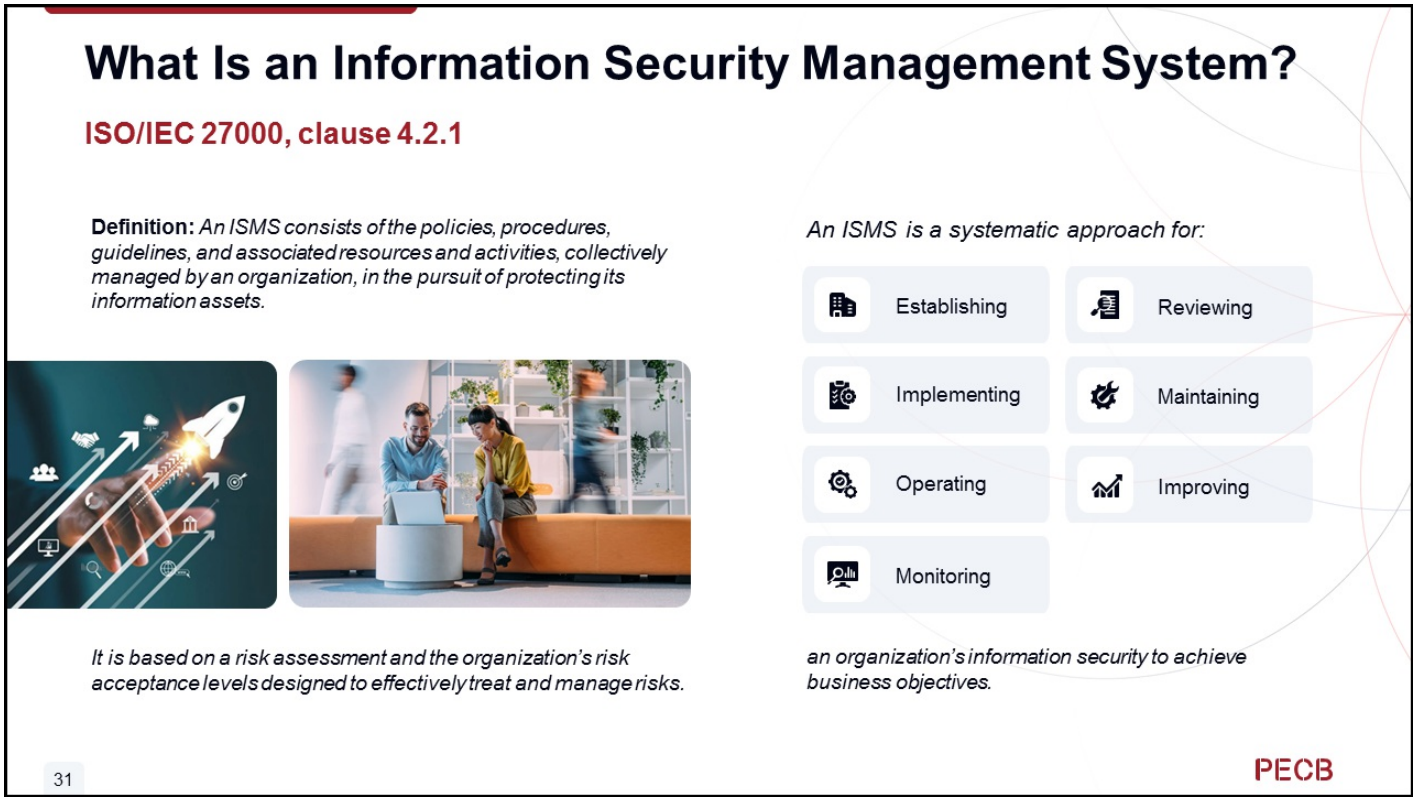
If you would like to purchase any of the standards, PECB offers discounted prices to all trainees that purchase them via https://store.pecb.com.



As organizations manage several compliance frameworks simultaneously, it is recommended to implement an integrated management system (IMS). An IMS is a management system which integrates all the components of a business into a coherent system so as to enable the achievement of its purpose and mission. The table on the slide presents the requirements that are common to all management systems which allow for integration.

There are several good reasons for integration, including to:

- Harmonize and optimize practices
- Formalize informal systems
- Reduce duplication and therefore costs
- Reduce risks and increase profitability
- Shift focus toward achieving business goals
- Create and maintain consistency
- Improve communication



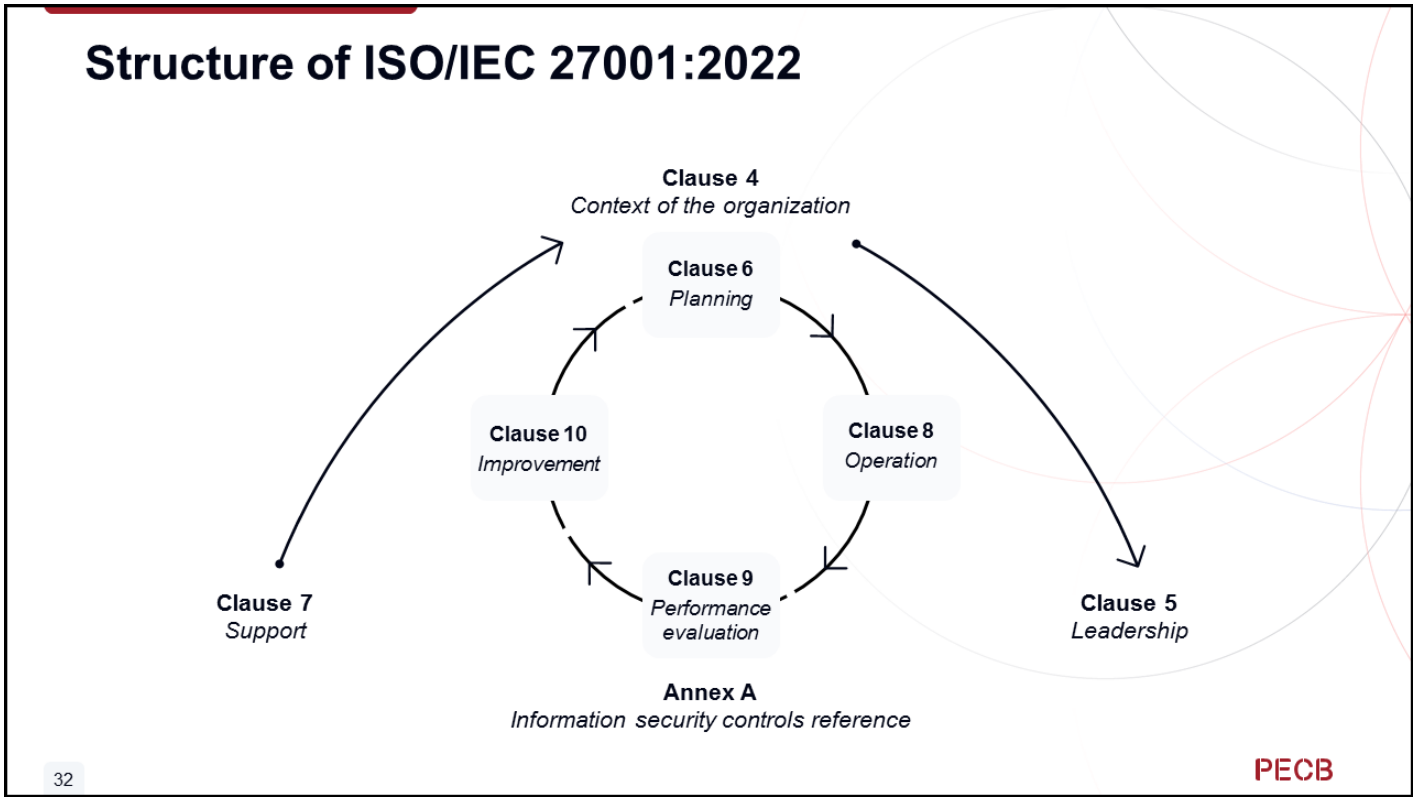
The ISMS consists of measures and controls that ensure the minimization of information security risks and the enhancement of information security. An organization with an effective ISMS in place takes into consideration information security in all its procedures, policies, and activities.

ISO/IEC 27000, clause 3.28 Information security

Preservation of confidentiality, integrity and availability of information

Having an effective ISMS in place helps an organization in:

- Reducing information security risks and minimizing exposure to information security breaches
- Protecting assets and sensitive information
- Creating competitive advantage
- Improving reputation and increasing customer confidence
- Protecting the confidentiality, availability, and integrity of information



An organization seeking certification against ISO/IEC 27001:2022 must comply with requirements set out in the standard's clauses 4 to 10.

Context of the Organization – Overview

ISO/IEC 27001:2022, clause 4

- Clause 4.1 *Understanding the organization and its context* – The organization shall establish the external and internal factors related to the ISMS that can affect the achievement of the ISMS intended outcome(s).
- Clause 4.2 *Understanding the needs and expectations of interested parties* – The organization shall determine the interested parties and the information security requirements relevant to these interested parties.
- Clause 4.3 *Determining the scope of the information security management system* – The organization shall establish the ISMS scope by setting its boundaries and applicability. The scope shall be available as documented information.
- Clause 4.4 *Information security management system* – The organization shall comply with the standard's requirements to establish, implement, maintain, and continually improve an information security management system.

PECB

Leadership – Overview

ISO/IEC 27001:2022, clause 5

- Clause 5.1 *Leadership and commitment* – Top management shall ensure that the ISMS is compatible with the organization's strategic orientation. Top management shall integrate the ISMS requirements into the organization's business processes, determine the necessary resources for the ISMS, and communicate the importance of an effective information security management.
- Clause 5.2 *Policy* – Top management shall create an information security policy that shall be appropriately available and communicated to all interested parties. The policy shall be aligned with the purpose of the organization and shall include the information security objectives, a commitment to fulfill the information security requirements and a commitment for continual improvement.
- Clause 5.3 *Organizational roles, responsibilities and authorities* – Top management shall assign the appropriate information security roles and responsibilities in order to ensure that the information security management system conforms to the requirements of ISO/IEC 27001:2022.

PECB

Planning – Overview

ISO/IEC 27001:2022, clause 6

- Clause 6.1 *Actions to address risks and opportunities* – The organization shall determine the risks and opportunities to achieve the intended outcome(s); prevent or reduce undesired effects; and achieve continual improvement. The organization shall also plan actions to address risks and opportunities, implement those actions, and evaluate their effectiveness.
- Clause 6.2 *Information security objectives and planning to achieve them* – The organization's objectives shall be measurable and consistent with the information security policy. They shall also be aligned with the requirements and the results of risk assessment and treatment. The objectives shall be monitored, appropriately communicated, updated, and available as documented information.
- Clause 6.3 *Planning of changes* – The organization shall determine the need for changes to the ISMS and implement those changes in a planned manner.

PECB

Support – Overview

ISO/IEC 27001:2022, clause 7

- Clause 7.1 *Resources* – The organization shall determine and provide the necessary resources for the appropriate implementation of the ISMS.
- Clause 7.2 *Competence* – The organization shall ensure that it has the competent personnel to perform the tasks related to the ISMS.
- Clause 7.3 *Awareness* – The organization shall ensure that its employees are aware of the information security policy, their roles in the ISMS, and the implications of failing to conform to the ISMS requirements.
- Clause 7.4 *Communication* – The organization shall establish, implement, and maintain arrangements for communication with relevant external and internal interested parties.
- Clause 7.5 *Documented information* – The organization's ISMS shall include documented information required by ISO/IEC 27001:2022 and records to demonstrate the effectiveness of the ISMS.

PECB

Operation – Overview

ISO/IEC 27001:2022, clause 8

- Clause 8.1 *Operational planning and control* – The organization shall plan, implement, and control the necessary processes to comply with the standard requirements. The organization shall also implement the plans, keep documented information as evidence of the implementation of planned processes, control and review the planned changes, and determine and control the outsourced processes.
- Clause 8.2 *Information security risk assessment* – The organization shall conduct information security risk assessments at planned intervals and shall keep documented information of the risk assessment results.
- Clause 8.3 *Information security risk treatment* – The organization shall implement the information security risk treatment plan and shall keep documented information on risk treatment results.

PECB

Performance Evaluation – Overview

ISO/IEC 27001:2022, clause 9

- Clause 9.1 *Monitoring, measurement, analysis and evaluation* – The organization shall evaluate the performance and effectiveness of the information security management system and keep documented information as evidence of the monitoring and measurement outputs.
- Clause 9.2 *Internal audit* – The organization shall perform internal audits at planned intervals in order to validate whether the information security management system is effectively implemented, maintained, and complies with the organization's own requirements as well as the standard's requirements.
- Clause 9.3 *Management review* – The top management shall perform reviews of the ISMS at planned intervals in order to ensure its suitability, adequacy and effectiveness. The organization shall keep documented information as evidence of the management review outputs.

PECB

Improvement – Overview

ISO/IEC 27001:2022, clause 10

- Clause 10.1 *Continual improvement* – The organization shall ensure the continual improvement of the suitability, adequacy, and effectiveness of the information security management system.
- Clause 10.2 *Nonconformity and corrective action* – The organization shall take the appropriate actions when a nonconformity occurs. It shall evaluate and implement those actions, review their effectiveness and, if necessary, make changes. The organization shall also keep documented information as evidence of the results of corrective actions.

PECB

Annex A

- Annex A is part of ISO/IEC 27001 and it contains 93 controls that should be considered when intending to comply with the standard.

- The list of information security controls of Annex A is not exhaustive. The organization may add additional controls from other sources, when needed.

- If a certain control is not applicable, the organization should provide an acceptable justification for its exclusion.

PECB

Note: Since ISO/IEC 27002 is a guideline standard, there is no requirement to follow its recommendations in order to obtain an ISO/IEC 27001 certification.

114 controls in Annex A, 2013 version (dark)

A.5 *Information security policies*

A.6 *Organization of information security*

A.7 *Human resource security*

A.8 *Asset management*

A.9 *Access control*

A.10 *Cryptography*

A.11 *Physical and environmental security*

A.12 *Operations security*

A.13 *Communications security*

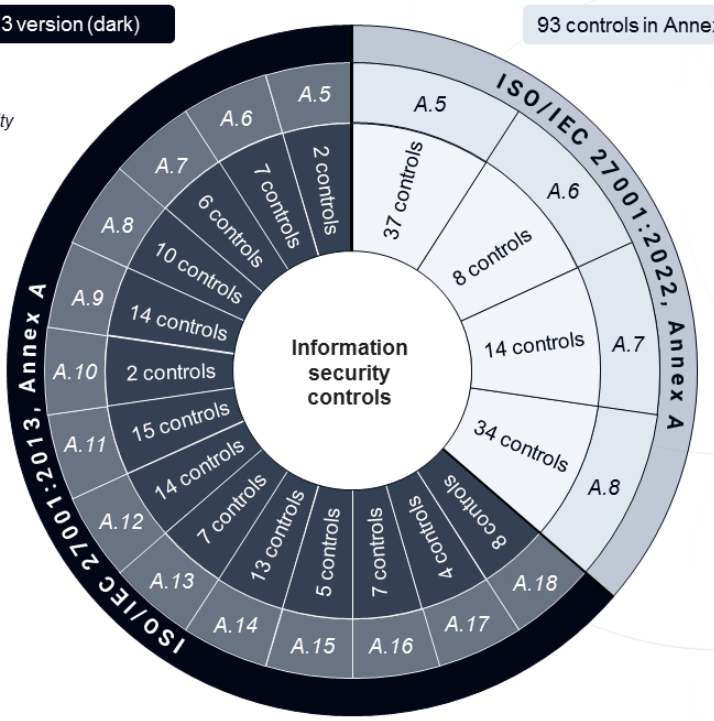
A.14 *System acquisition, development and maintenance*

A.15 *Supplier relationships*

A.16 *Information security incident management*

A.17 *Information security aspects of business continuity management*

A.18 *Compliance*



93 controls in Annex A, 2022 version (light)

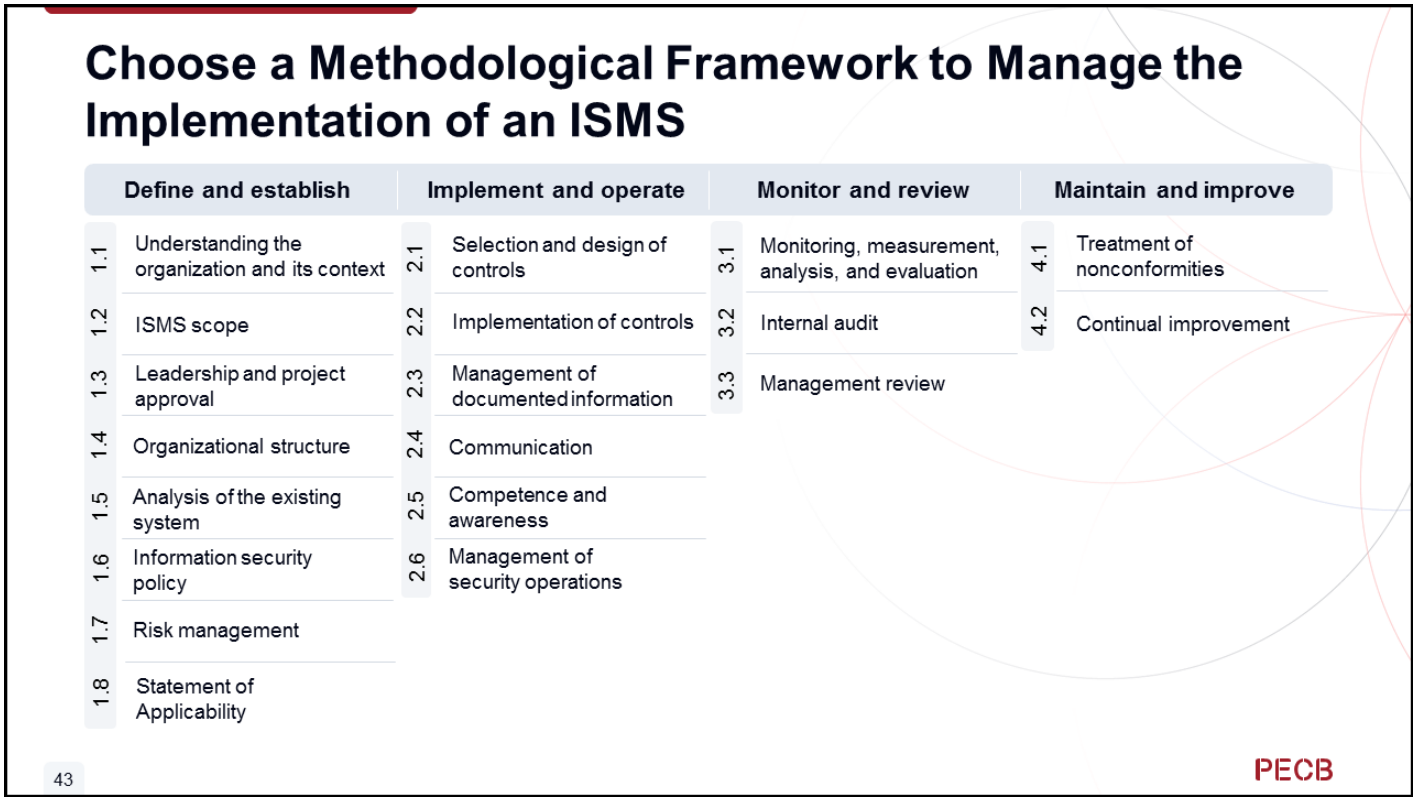
A.5 *Organizational controls*

A.6 *People controls*

A.7 *Physical controls*

A.8 *Technological controls*

PECB



By following a structured and effective methodology, an organization can cover the minimum requirements for the implementation of a management system.

Important notes:

1. The methodology in the slide is not intended to be used strictly; each organization must adapt it to its business context (requirements, size, scope, objectives, etc.).
2. The sequence of steps can be changed (inversion, merging, etc.). For example, establishing a documentation management procedure can be completed before the understanding of the organization.
3. Many processes are iterative because of the need for continual development throughout the implementation project (e.g., communication and awareness).

Discussion questions

1. How can a management system help an organization?
2. What is an information security management system (ISMS) and what benefits does it bring?
3. What is Annex A in ISO/IEC 27001:2022 and what does it consist of?

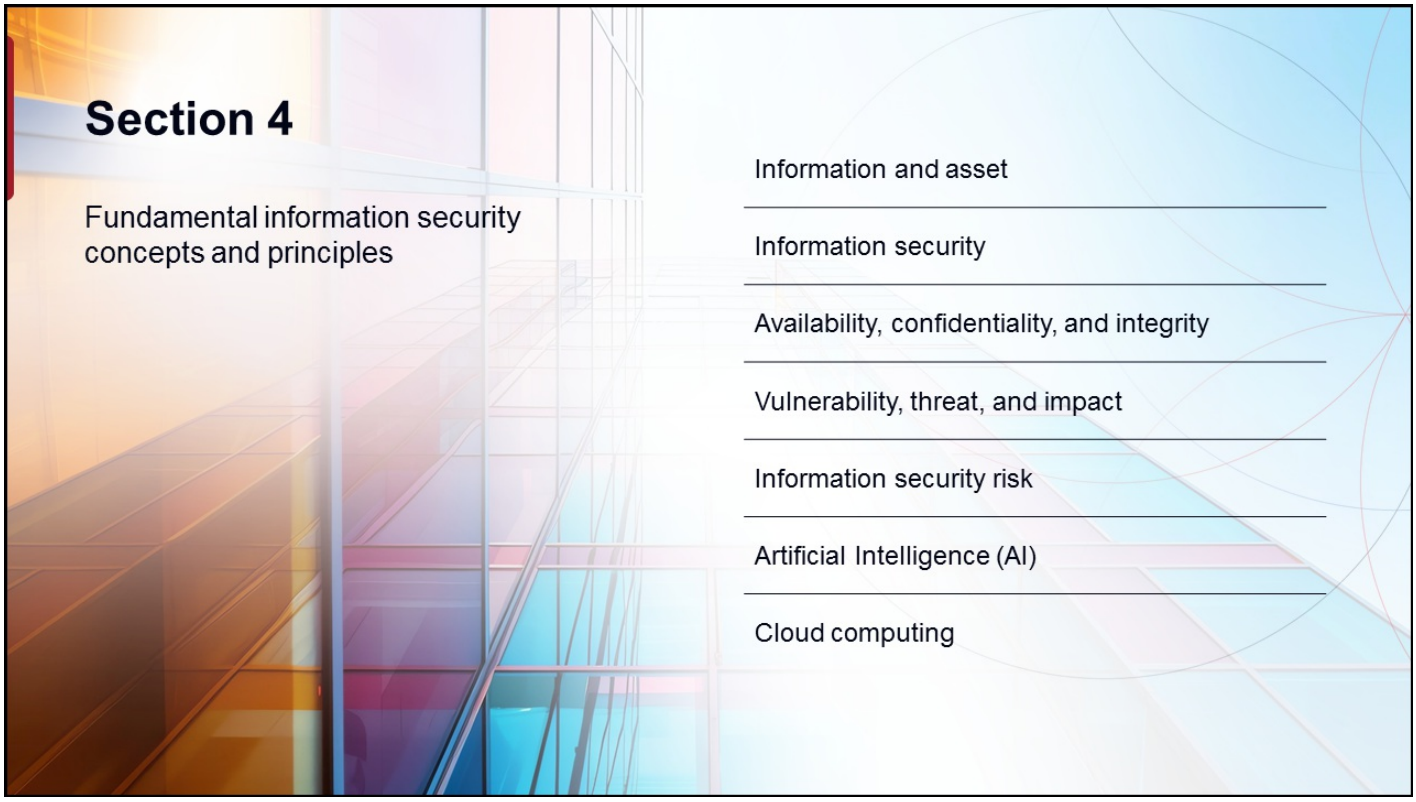
Section 3 Summary

- A management system is a set of interrelated elements of an organization to establish policies and processes to achieve specific objectives.
- An ISMS presents the policies, procedures, guidelines, activities, and controls to be implemented by an organization that intends to reduce information security risks and increase information security awareness within the organization.
- An organization must comply with requirements set out in clauses 4 to 10 of ISO/IEC 27001:2022 if seeking certification against this standard.
- Annex A is part of ISO/IEC 27001:2022 and contains 93 controls that should be considered when intending to comply with the standard.
- The list of information security controls of Annex A is not exhaustive.
- The application of the process approach changes between organizations, depending on their size, complexity, and activities.

Questions?

Quiz 1

Note: To complete Quiz 1, please go to the Quizzes Worksheet.



This section provides information that will help the participant gain knowledge on the fundamental principles and concepts of information security, such as confidentiality, integrity, availability, vulnerability, threat, impact, information security risk, artificial intelligence (AI), and cloud computing.

Information and Asset

ISO 9000, clause 3.8.2 and ISO 55000, clause 3.2.1

Definitions

- ***Information:*** *meaningful data*
- ***Asset:*** *item, thing or entity that has potential or actual value to an organization*

Personal or individual assets include:

- Virtual assets, such as bank accounts, medical data, email accounts, and digital customer identities
- Physical assets, such as personal devices and PC

Organizational assets include:

- Virtual assets, such as online branding, reputation, business plans, and intellectual property
- Physical assets, such as servers, connected cables, and workstations

47

PECB

ISO/IEC 27000, clause 3.35 Information system

Set of applications, services, information technology assets, or other information-handling components

ISO/IEC 27001, Annex A controls 5.9 to 5.11 specify the information security controls linked to asset management.

ISO/IEC 27001, Annex A 5.9 Inventory of information and other associated assets

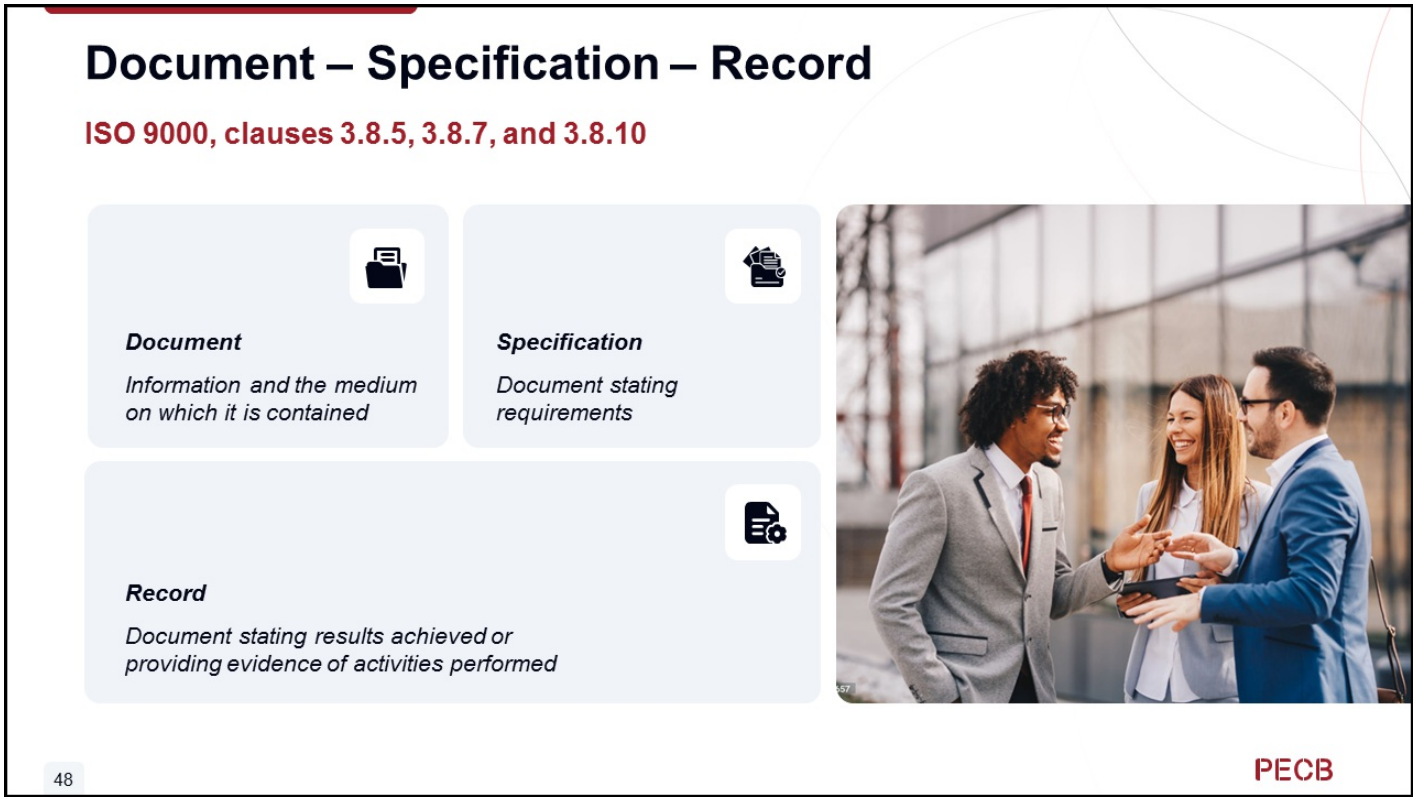
An inventory of information and other associated assets, including owners, shall be developed and maintained.

ISO/IEC 27001, Annex A 5.10 Acceptable use of information and other associated assets

Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.

ISO/IEC 27001, Annex A 5.11 Return of assets

Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.



ISO 9000, clause 3.8.5 Document (cont'd)

EXAMPLE: Record, specification, procedure document, drawing, report, standard.

- *Note 1 to entry: The medium can be paper, magnetic, electronic or optical computer disc, photograph or master sample, or combination thereof.*
- *Note 2 to entry: A set of documents, for example specifications and records, is frequently called "documentation".*

It is important to be able to differentiate between documents and records. In dictionaries, a record is a type of document, but in ISO terminology, these are distinct concepts. A record is the output of a process or control. As an example:

1. An audit procedure is a document. The implementation of this procedure (i.e., the performance of an audit) generates an audit report and these audit reports become records.
2. A documented process for management reviews is a document. This process generates records, such as management review minutes.
3. A documented procedure for continual improvement is a document. A filled corrective action form is a record.

Information Security

- ISO/IEC 27000, clause 3.28 defines information security as the *"preservation of confidentiality, integrity and availability of information."*
- Information security determines what information needs to be protected, why it should be protected, how to protect it, and what to protect it from.
- Information security covers information of all kinds, such as printed or handwritten, transmitted by email or website, mentioned during conversations, etc.
- Organizations can ensure information security by implementing appropriate policies and controls that are aligned with their objectives and reduce vulnerabilities and mitigate threats.

49

PECB

ISO/IEC 27002, clause 0.2 Information security requirements

It is essential that an organization determines its information security requirements. There are three main sources of information security requirements:

a. *the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;*
b. *the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their sociocultural environment;*
c. *the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.*

ISO/IEC 27000, clause 3.27 Information processing facilities

Any information processing system, service or infrastructure, or the physical location housing it

ISO/IEC 27000, clause 3.30 Information security event

Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant

ISO/IEC 27000, clause 3.31 Information security incident

Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

ISO/IEC 27000, clause 3.32 Information security incident management

Set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents

ISO/IEC 27000, clause 3.35 Information system

Set of applications, services, information technology assets, or other information-handling components

Slide Notes Extension

ISO/IEC 27000, clause 3.48 Non-repudiation

Ability to prove the occurrence of a claimed event or action and its originating entities

ISO/IEC 27000, clause 3.55 Reliability

Property of consistent intended behavior and results

Annex A of ISO/IEC 27001:2022 includes controls related to the classification of information:

ISO/IEC 27001:2022, Annex A 5.12 Classification of information

Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

ISO/IEC 27001:2022, Annex A 5.13 Labelling of information

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Confidentiality, Integrity, and Availability

ISO/IEC 27000, clauses 3.7, 3.10, and 3.36

Definitions

3.10 ***Confidentiality***

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.36 ***Integrity***

Property of accuracy and completeness

3.7 ***Availability***

Property of being accessible and usable on demand by an authorized entity

PECB

Confidentiality

Confidentiality requires that only authorized users have access to protected and sensitive data.

Some of the practices employed to address confidentiality are:

- An authentication process that requires a user identification and password when addressing confidential data
- Security methods to ensure viewer authorization
- Access controls that provide restrictions on the network access based on the employee's roles and responsibilities

52

PECB

Confidentiality: Ensuring that the information is only accessible to authorized individuals.

Example: The personal data of employees must only be accessible to the authorized human resources department personnel.

Several types of access controls can ensure the confidentiality of information. Authentication is a method to provide access control. An information security management system's access controls can be:

- Physical (example: locks on doors, filing cabinets that lock, safes)
- Digital (example: internal networks access controls, remote access controls, web access controls)

Integrity

Integrity ensures that:

- Information is not modified when in storage or in transit
- Only authorized modifications are made
- Data is accurate, authentic, and safe from unauthorized access in order for users to be able to rely on the correctness of information when processing it

Integrity controls must be included in the procedures. These contribute to the reduction in the risk of error, theft, and fraud. Data validation controls, user trainings, and certain controls at the operational level are good examples.

53

PECB

Integrity: Data must be complete and intact.

Example: Accounting data must be authentic (complete and exact). The accuracy of information is ensured by avoiding unjustified alterations of such information.

Many devices manipulating data, including disk drives and other media (as well as telecommunications systems), contain devices for automatic data integrity verification. Data integrity controls are essential in operating systems, software, and applications. They allow the avoidance of intentional or involuntary corruption of programs and data.

Integrity must be protected by:

- Preventing someone, with the authority to modify, from making an error and incorrectly changing the data
- Preventing someone, without the authority to modify, from making any changes
- Preventing any program or application that interacts directly with the target information from making any unauthorized changes

Data that is previously stored must remain unchanged during data transportation.

Data can experience changes due to:

- Storage erosion
- Natural or intentional errors
- System damages

Availability

Information availability is crucial for modern information security. Ensuring information availability means that information is accessible:

- As required
- When required
- Where required
- To the person(s) requiring

Information security managers usually face three challenges:

- Denial of service (DoS) as a result of intentional attacks (e.g., a programmer is not aware of a defect that could harm the software due to a specific and unexpected input)
- Losing protection capacities of information systems due to natural disasters or human activities
- Equipment failures

54

PECB

Availability: Information must be easily accessible by persons who need it.

Example: Data related to customers must be accessible in the marketing department.

In practice, the availability of information requires a control system such as the backup of data, capacity planning, procedures and criteria for approval of the systems, the incident management procedures, the management of removable media, the information processing procedures, the maintenance and testing of equipment, continuity concept procedures, and the procedures to control the usage of systems.

Vulnerability

ISO/IEC 27000, clause 3.77

Definition

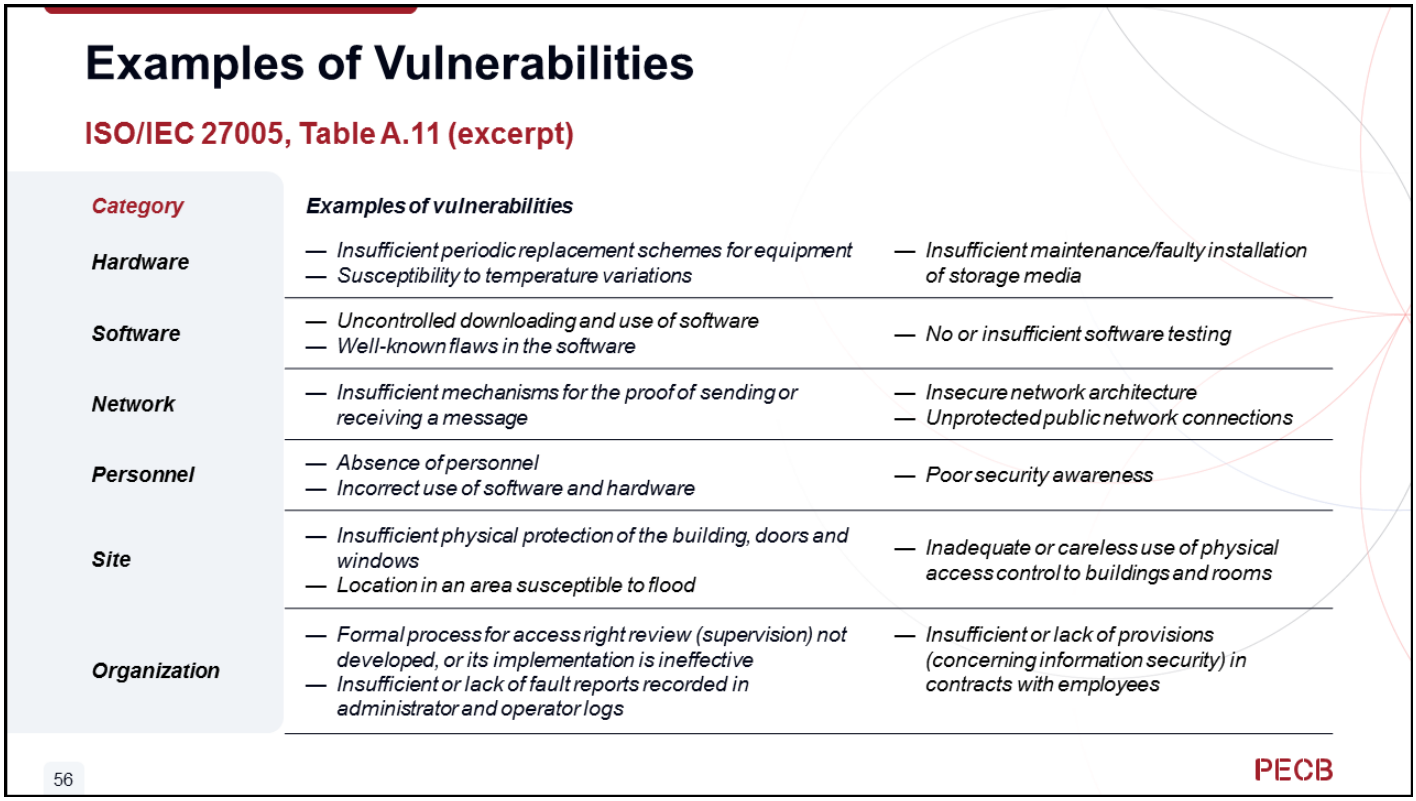
Weakness of an asset or control that can be exploited by one or more threats

- Vulnerabilities that do not have corresponding threats may not require controls, but should be recognized and monitored for changes.
- Controls that are implemented incorrectly or malfunction could become vulnerabilities.

55

Organizations may accept certain vulnerabilities because of some other benefits, e.g., purchasing laptop computers in contrast to desktop computers, which improve the mobility of workers, but increase the chances of theft.

Vulnerabilities can be divided into two groups: extrinsic and intrinsic. Intrinsic vulnerabilities are related to the characteristics of the asset. Extrinsic vulnerabilities, on the other hand, are the external factors that might impact the asset. For example, a server located in an area that is prone to seasonal flooding is considered an extrinsic vulnerability. The inability of a server to process data is considered an intrinsic vulnerability.



Annex A of ISO/IEC 27005 provides a typology for the classification of vulnerabilities that can be used in principle. However, the list of vulnerabilities should be used with caution, because the list is not exhaustive. New vulnerabilities occur regularly due to, among others, evolution and changes in technology.

Annex A should be used as a guide or reminder to help organize and structure the collection of relevant data on vulnerabilities rather than as a checklist to follow blindly.

ISO/IEC 27005, Annex A.2.5.2 Examples of vulnerabilities

Table A.11 gives examples for vulnerabilities in various security areas, including examples of threats that can exploit these vulnerabilities. The lists can provide help during the assessment of threats and vulnerabilities, to determine relevant risk scenarios. In some cases, other threats can exploit these vulnerabilities as well.

Threats

ISO/IEC 27005, clauses 3.1.9 and 7.2.1

Definition:

Potential cause of an information security incident that can result in damage to a system or harm to an organization

A threat exploits a vulnerability of an asset to compromise the confidentially, integrity and/or availability of corresponding information.

57

By definition, a threat has the potential to harm assets such as information, processes, and systems and, therefore, harm the organization. Threats are associated with the negative aspect of risk and, as such, refer to undesirable occurrences.

Examples of Threats

ISO/IEC 27005, Table A.10 (excerpt)

Category	Threat description	
Physical threats	— Fire (A, D, E) — Water (A, D, E)	— Dust, corrosion, freezing (A, D, E)
Natural threats	— Climatic phenomenon (E)	— Seismic phenomenon (E)
Infrastructure failures	— Loss of power supply (A, D, E)	— Failure of a telecommunications network (A, D, E)
Technical failures	— Failure of device or system (A)	— Violation of information system maintainability (A, D)
Human actions	— Terror, attack, sabotage (D) — Social Engineering (D)	— Unauthorized processing of personal data (A, D)
Compromise of functions or services	— Error in use (A) — Abuse of rights or permissions (A, D)	— Forging of rights or permission (D)
Organizational threats	— Lack of staff (A, E) — Lack of resources (A, E)	— Violation of laws and regulations (A, D)

Type of risk source: *D = deliberate; A = accidental; E = environmental.*

PECB

Annex A of ISO/IEC 27005 provides a typology for the classification of threats. Same as with the list of vulnerabilities, the list of threats is not exhaustive. New threats occur regularly due to trends in technology and capabilities of threat agents evolving.

Annex A should be used as a guide or checklist to help organize and structure the collection and collation of relevant data on threats, rather than as a checklist to follow blindly.

Relationship between Vulnerability and Threat

Examples

Vulnerabilities	Threats
Warehouse unprotected and without surveillance	Theft
Complicated data processing procedures	Data input error by personnel
No segregation of duties	Fraud, unauthorized use of a system
Unencrypted data	Information theft
Use of pirated software	Lawsuit, virus
No review of access rights	Unauthorized access by former employees
Lack of data backup procedures	Accidental power interruption

59

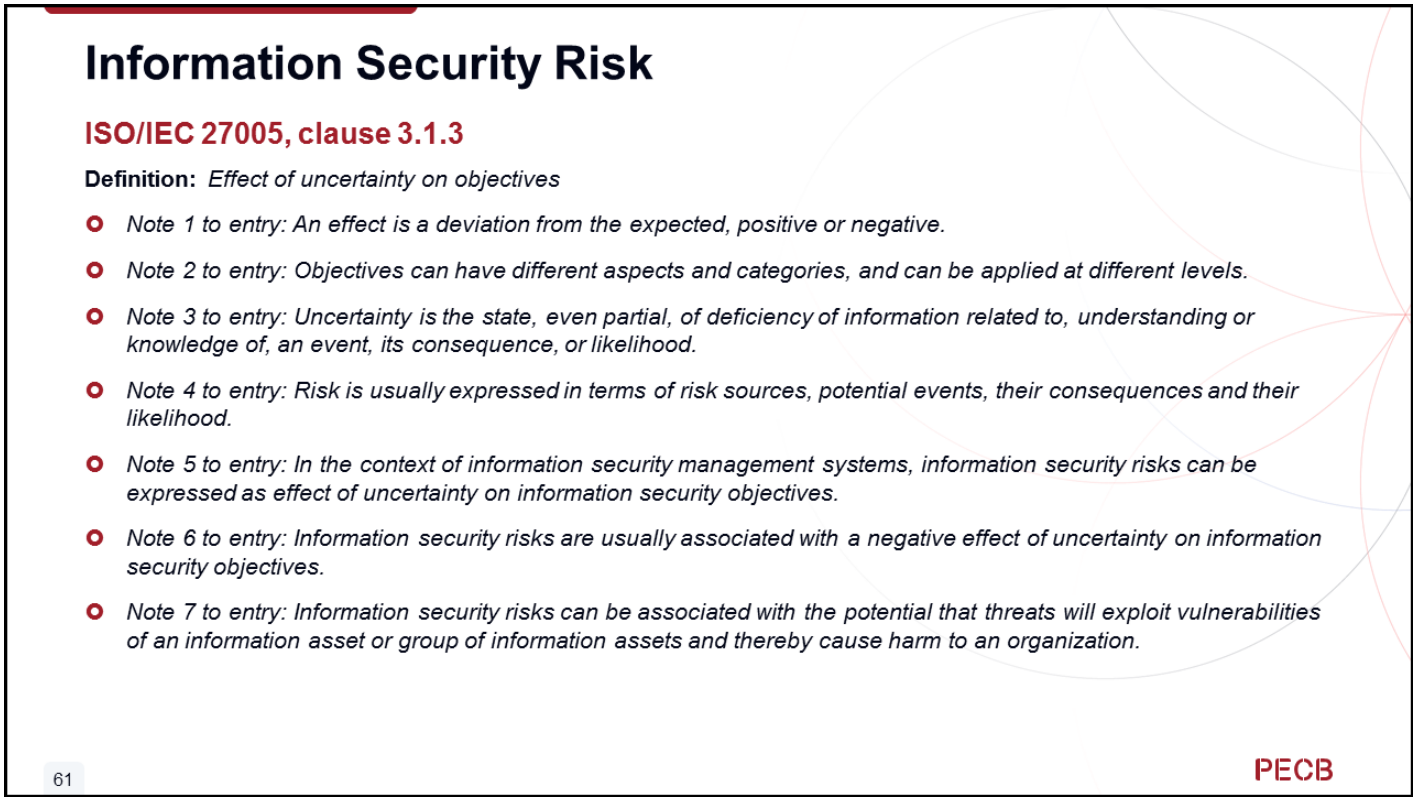
PECB

The presence of a vulnerability itself does not produce damage; a threat must exist to exploit it. A vulnerability that does not correspond to a threat may not require the set-up of a control, but it must be identified and monitored in case of changes.

The incorrect implementation, use, or malfunction of a control could, in itself, represent a threat. A control can be effective or ineffective, based on the environment in which it operates. On the other hand, a threat that is not vulnerable cannot represent a risk.

The following is a list of potential impacts that can affect availability, integrity, or confidentiality, or a combination of them:

1. Financial losses
2. Loss of assets or their value
3. Loss of customers and suppliers
4. Lawsuits and penalties
5. Loss of competitive advantage
6. Loss of technological advantage
7. Loss of efficiency or effectiveness
8. Violation of the privacy of users or customers
9. Service interruption
10. Inability to provide service
11. Loss of branding or reputation
12. Disruption of operations
13. Disruption of third party operations (suppliers, customers)
14. Inability to fulfill legal obligations
15. Inability to fulfill contractual obligations
16. Endangering safety of staff and users



ISO/IEC 27000 clause 3.57 Residual risk

Risk remaining after risk treatment

- *Note 1 to entry: Residual risk can contain unidentified risk.*
- *Note 2 to entry: Residual risk can also be referred to as "retained risk".*

ISO/IEC 27000, clause 3.62 Risk acceptance

Informed decision to take a particular risk

- *Note 1 to entry: Risk acceptance can occur without risk treatment or during the process of risk treatment.*
- *Note 2 to entry: Accepted risks are subject to monitoring and review.*

ISO/IEC 27000, clause 3.63 Risk analysis

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

- *Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.*
- *Note 2 to entry: Risk analysis includes risk estimation.*

ISO/IEC 27000, clause 3.64 Risk assessment

Overall process of risk identification, risk analysis and risk evaluation

ISO/IEC 27000, clause 3.66 Risk Criteria

Terms of reference against which the significance of risk is evaluated

- *Note 1 to entry: Risk criteria are based on organizational objectives, and external context and internal context.*
- *Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.*

ISO/IEC 27000, clause 3.67 Risk evaluation

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

magnitude is acceptable or tolerable

- *Note 1 to entry: Risk evaluationassists in the decision about risk treatment.*

Slide Notes Extension

ISO/IEC 27000, clause 3.68 Risk identification

Process of finding, recognizing and describing risks

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

ISO/IEC 27000, clause 3.69 Risk management

Coordinated activities to direct and control an organization with regard to risk

ISO/IEC 27000, clause 3.70 Risk management process

Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing risk

- *Note 1 to entry: ISO/IEC27005 uses the term "process" to describe risk management overall. The elements within the risk management process are referred to as "activities".*

ISO/IEC 27000, clause 3.71 Risk owner

Person or entity with the accountability and authority to manage a risk

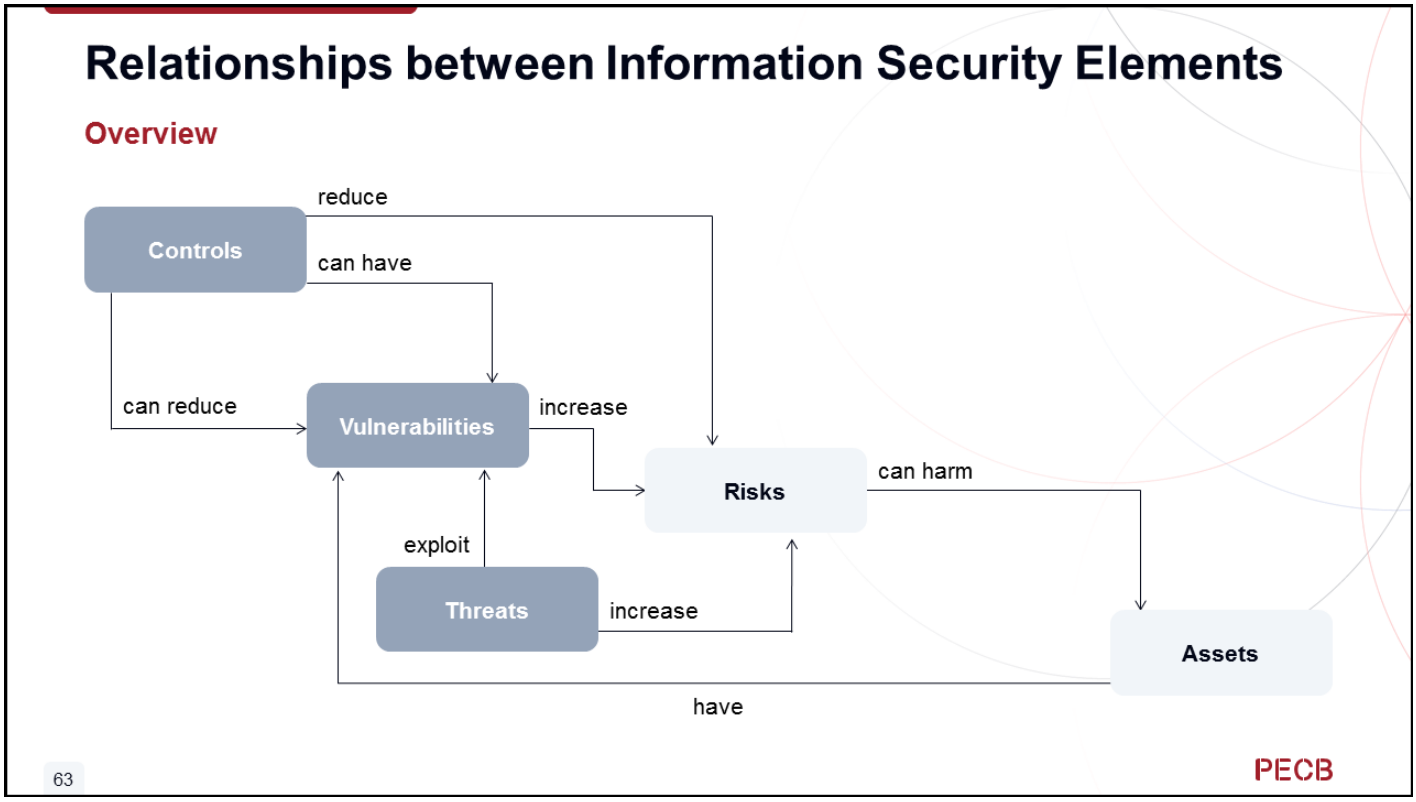
ISO/IEC 27000, clause 3.72 Risk treatment

Process to modify risk

Note 1 to entry: Risk treatment can involve:

- *avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*
- *taking or increasing risk in order to pursue an opportunity;*
- *removing the risk source;*
- *changing the likelihood;*

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

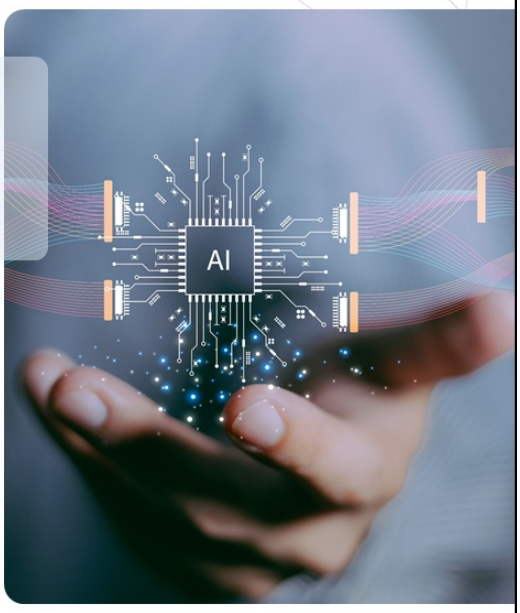


1. Assets and controls can present vulnerabilities that can be exploited by threats.
2. The combination of threats and vulnerabilities can increase the potential effect of the risk.
3. Controls allow the reduction of vulnerabilities. An organization has limited alternatives to act against threats. For example, controls can be implemented to provide protection against system intrusions, but it is impossible for an organization to take action to reduce the number of hackers on the internet.

Note: The relation descriptors are valid for the two components which they interconnect to — they are not intended to be read as a "story" from end to end or through a sequence of components and relationships.

Artificial Intelligence (AI)

The Oxford English Dictionary defines Artificial Intelligence (AI) as "*the theory and development of computer systems able to perform tasks usually requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.*"



The interconnectivity and fast data transfers that are made possible through the usage of 5G is expected to allow AI applications to become integral parts of our lives.

Common application areas of AI are:

Banking	Banking	Healthcare	Autonomous vehicles

64

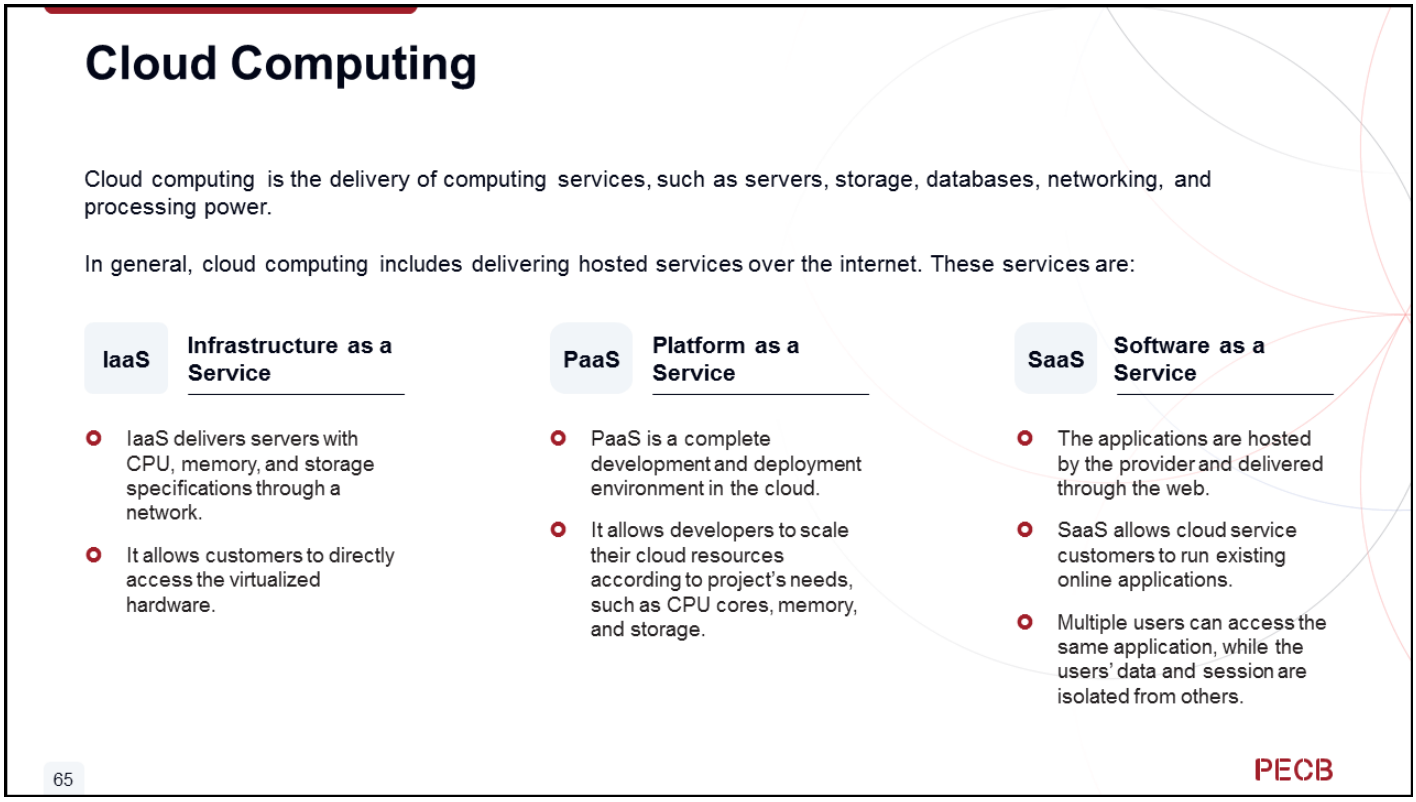
PECB

Weak AI

- Weak AI is also known as narrow AI.
- Weak AI is focused on a specific task and outperforms humans when conducting technical and automated tasks. However, when weak AI has to conduct a task that it does not recognize, it will not be able to complete it unless it is specifically programmed to do so.
- The benefit of weak AI is the automation of tasks.
- Examples of weak AI include Apple's Siri, Alexa, AlphaGo, etc.

Strong AI

- Strong AI is also known as artificial general intelligence (AGI).
- AGI has the capacity to understand newly presented problems and derive solutions based on prior knowledge.
- The benefit of strong AI is problem-solving.
- Examples of strong AI include AI that can communicate in natural language, use critical thinking, etc.



NIST SP 500-291, Chapter 3

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing services work differently depending on the provider, but they all serve the same purpose. Many providers offer a friendly browser-based dashboard for all IT professionals to manage their accounts easily.

The benefits of cloud computing include:

- **Cost reduction:** Cloud computing reduces the cost needed to manage and maintain the network system.
- **Flexibility:** The cloud system gives employees more flexibility by giving them the opportunity to access data from wherever they are.
- **Security:** Cloud computing promotes the security of information because data can be accessed no matter what happens to the machine.
- **Productivity:** Cloud computing removes the need for many tasks such as software patching, "racking and stacking," hardware set-up, etc., allowing IT teams to spend time on accomplishing more important business goals.
- **Reliability:** In case of any incident, if the business continuity plan of the organization includes cloud security services, the data most likely will not be lost. Instead, it will be secured in a safe location.

Note: Application Programming Interface (API) allows different applications to communicate with each other.

Section 4 Summary

- Information security determines what information needs to be protected, how should it be protected and by whom.
- Confidentiality ensures that only authorized users have access to protected and sensitive data.
- Integrity ensures that the information is not modified or changed when in storage of transit.
- Availability ensures that information is easily accessible and usable on demand by an authorized entity
- Vulnerability is a weakness of an asset or control that can be exploited by threats.
- Threat is a potential cause resulting in an unwanted incident that can cause harm to the organization.
- Information security risk is presented as the combination of the consequences of an event and the associated likelihood of occurrence.
- Information security controls are classified by function and type.
- Cloud computing services include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Questions?

Quiz 2

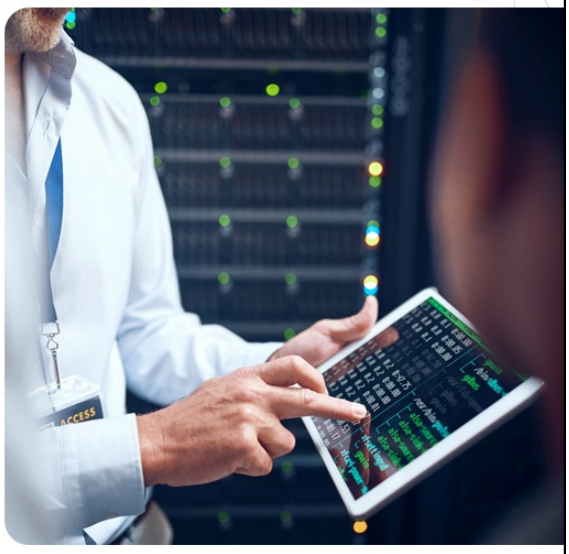
Note: To complete Quiz 2, please go to the Quizzes Worksheet.

This section elaborates on the importance of understanding the context of an organization, including the ISMS objectives and preliminary scope definition, internal and external environment, its interested parties, and business requirements.

ISO/IEC 27001:2022 Requirements

ISO/IEC 27001:2022, clause 4.1

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.



68

PECB

An organization wishing to comply with ISO/IEC 27001:2022 should, at least, be able to:

- Demonstrate that their ISMS is aligned with its mission, objectives, and business strategies
- Identify and document the organization's activities, functions, services, products, partnerships, supply chains, and relationships with interested parties
- Define the external and internal factors that can influence the ISMS
- Recognize and take into account issues related to information security within their industrial sector, such as risk, legal and regulatory obligations, and customer requirements
- Establish and document objectives for the ISMS

Definitions related to the concept of organization

ISO 9000, clause 3.2.1 Organization

Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

ISO 9000, clause 3.5.2 Infrastructure

System of facilities, equipment and services needed for the operation of an organization

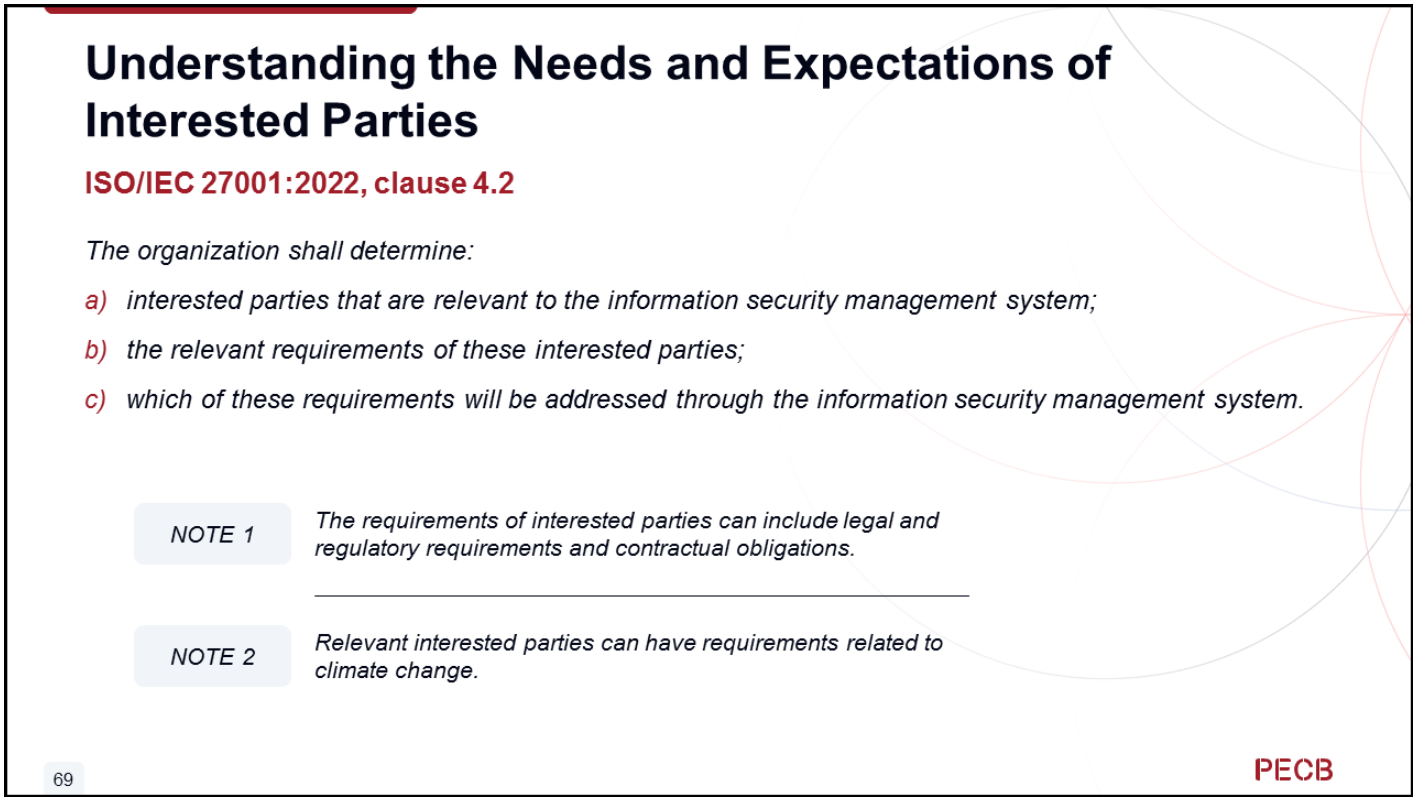
ISO 9000, clause 3.6.4 Requirement

Need or expectation that is stated, generally implied or obligatory

Notes on terminology:

- An organization is a structured entity and is usually registered with a government body. This may be, for example, a company, institution, charity, association, or a combination thereof. An organization can be public or private.
- The use of "organization" in ISO/IEC 27001:2022 can refer to a component of a registered or otherwise formally established entity, i.e., a separate department, business function, specific geographic location (such as an organization's data center but excluding their separate administrator offices).
- Do not confuse the use of the term "requirement" in the context of the specifications laid down in a standard and "requirements of the organization." The organization's requirements may come from different

interested parties. They can be explicit (defined by contracts, agreements, regulations) or implicit (not documented).



ISO/IEC 27003, clause 4.2 Understanding the needs and expectations of interested parties

External interested parties can include: a) regulators and legislators; b) shareholders including owners and investors; c) suppliers including subcontractors, consultants, and outsourcing partners; d) industry associations; e) competitors; f) customers and consumers; and g) activist groups.

Internal interested parties can include: h) decision makers including top management; i) process owners, system owners, and information owners; j) support functions such as IT or Human Resources; k) employees and users; and l) information security professionals.

Note: As for other management systems standards, ISO has published an amendment for ISO/IEC 27001:2022 to address climate action changes that may impact ISMS implementation. Changes introduced from this amendment include two new requirements: determining whether climate change is a relevant issue and the requirements of interested parties related to climate change, provided in clauses 4.1 and 4.2 of the standard, respectively.

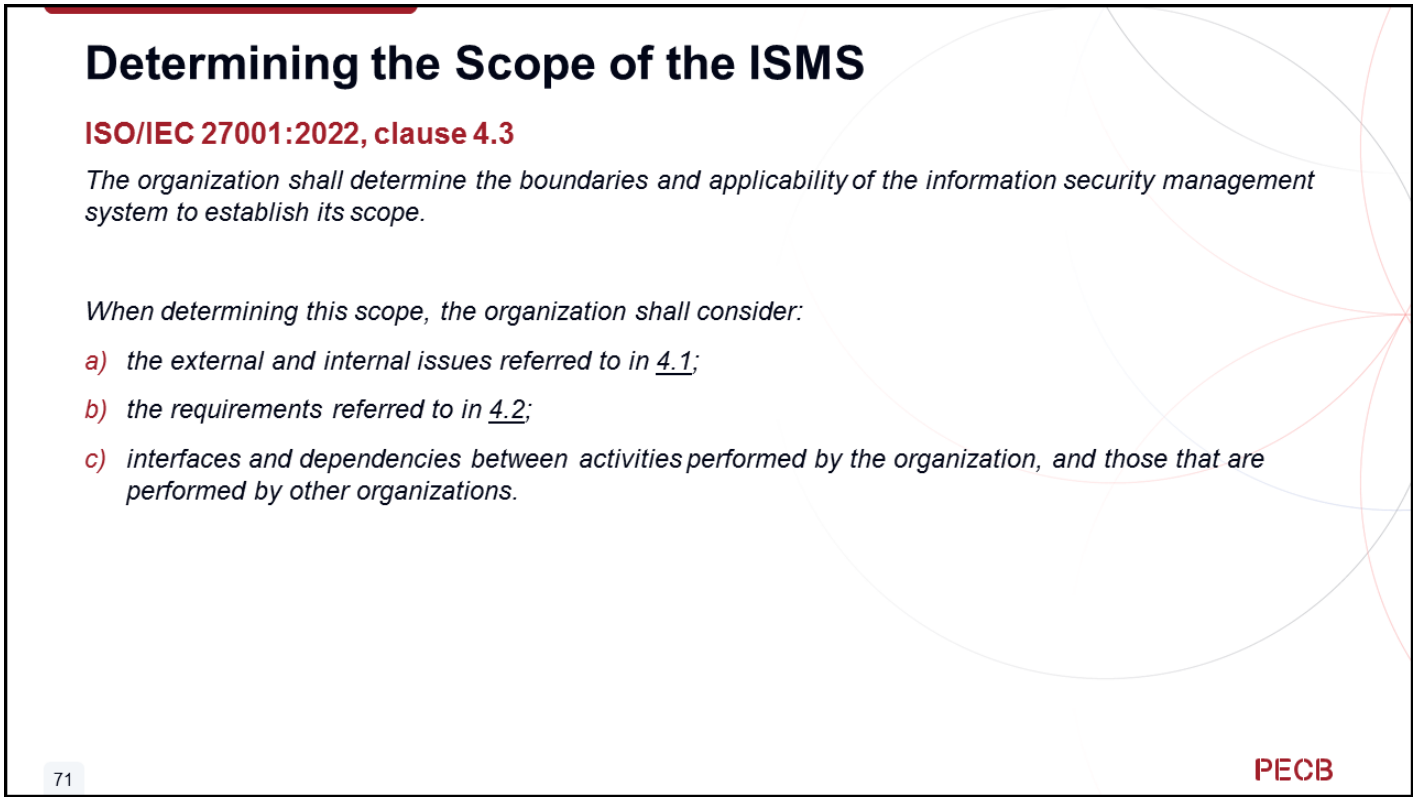
Understand the Mission, Objectives, Values, and Strategies

70

PECB

It is necessary to obtain an overview of the organization in order to understand the information security challenges that the organization faces and the risk inherent in that market segment. General information about the respective organization should be collected in order to better appreciate its mission, strategies, main purpose, values, etc. This helps ensure consistency and alignment between the information security strategic objectives and the organization's mission.

- **Mission:** The mission is what justifies and defines the organization's existence. It serves as a reference point to keep everyone clear on where the organization is headed.
  - Implications for information security management: The information security management aims to support the organization in fulfilling its mission, that is the protection of its information assets. The ISMS must, therefore, be aligned with the organization's mission.
- **Values:** Values are the fundamental and enduring beliefs that are shared by all the members of an organization which influence the behavior of individuals.
  - Implications for information security management: The values of the organization influence the choices made by professionals in information security management. For example, values can influence the priorities and policies in terms of evaluating information security risks.
- **Objectives:** An objective is the result that the organization intends to achieve. Objectives are generally predetermined, quantified, and time-bound (e.g., increase the market share by 5% in the upcoming 24 months).
  - Implications for information security management: As for strategy, information security management system must be aligned with the organization's objectives so as to achieve the ultimate objective and ensure that information security is achieved.
- **Strategies:** The strategy consists of a defined sequence of actions aimed at achieving one or more goals.
  - Implications for information security management: The choice and results of actions will also depend on the information security strategy defined by the organization.



Any exclusion made in the scope must be justified.

ISO/IEC 27003, clause 4.3 Determining the scope of the information security management system

The scope defines where and for what exactly the ISMS is applicable and where and for what it is not. Establishing the scope is therefore a key activity that determines the necessary foundation for all other activities in the implementation of the ISMS. For instance, risk assessment and risk treatment, including the determination of controls, will not produce valid results without having a precise understanding of where exactly the ISMS is applicable. Precise knowledge of the boundaries and applicability of the ISMS and the interfaces and dependencies between the organization and other organizations is critical as well. Any later modifications of the scope can result in considerable additional effort and costs.

The following factors can affect the determination of the scope:

a. *the external and internal issues described in 4.1;*
b. *the interested parties and their requirements that are determined according to ISO/IEC 27001, 4.2;*
c. *the readiness of the business activities to be included as part of ISMS coverage;*
d. *all support functions, i.e. functions that are necessary to support these business activities (e.g. human resources management; IT services and software applications; facility management of buildings, physical zones, essential services and utilities); and*
e. *all functions that are outsourced either to other parts within the organization or to independent suppliers.*

Determine the Preliminary Scope

To establish the scope of an ISMS, a multi-step approach can be followed:

1. **Determine the preliminary scope:** This activity should be conducted by a small, but representative group of management.
2. **Determine the refined scope:** The functional units within and outside the preliminary scope should be reviewed, possibly followed by inclusion or exclusion of some of these functional units to reduce the number of interfaces along the boundaries. When refining the preliminary scope, all functions necessary to support the business activities in the scope should be considered.
3. **Determine the final scope:** The refined scope should be evaluated by all the management within the refined scope. If necessary, it should be adjusted and then precisely described.
4. **Approve the scope:** The documented information describing the scope should be formally approved by the top management.

72

PECB

Some topics which should be considered when making the initial decisions regarding the ISMS scope include:

- What are the mandates for information security management established by organizational management and what are the obligations imposed externally on the organization?
- Is the responsibility for the proposed in-scope systems held by more than one management team (e.g., people in different subsidiaries or different departments)?
- How will the ISMS-related documents be communicated throughout the organization (e.g., on paper or through the intranet)?
- Can the current management systems support the organization's needs? Is it fully operational, well maintained, and functional as intended to be?

The organization should also consider activities that have an impact on the ISMS or activities that are outsourced, either to other parts within the organization or to independent suppliers. For such activities, interfaces (physical, technical, and organizational) and their influence on the scope should be identified.

Documenting the Scope

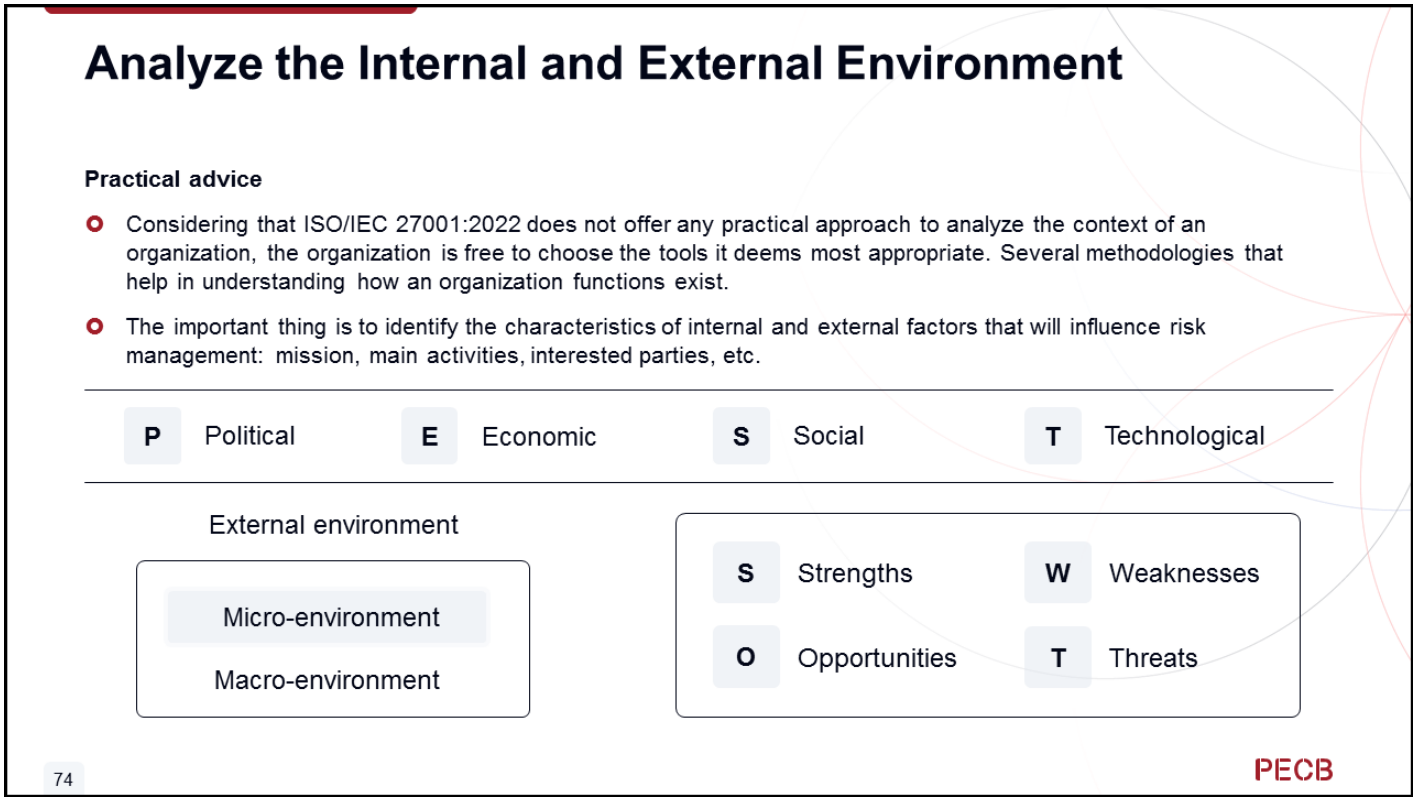
ISO/IEC 27001:2022, clause 4.3

The scope shall be available as documented information.

Documented information describing the scope should include:

- The organizational scope, boundaries, and interfaces
- The information and communication technology scope, boundaries, and interfaces
- The physical scope, boundaries, and interfaces

PECB



There are several models that have been developed to analyze and understand the strategic context of an organization. Note that this step does not become a project in itself. In most organizations, studies have been conducted internally or by consulting other firms on their strategic positioning. It should be enough to simply collect these studies, analyze them, and interview some key interested parties to ensure an adequate understanding of the organization.

The following are some of the frequently used models:

SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis: The SWOT analysis is used to conduct a thorough analysis of an organization's strengths, weaknesses, opportunities, and threats. The analysis is done for the purpose of formulating policies and determining where the organization should invest its resources (take advantage of opportunities, reduce weaknesses, face threats). Strengths and weaknesses seek to assess the internal issues, while opportunities and threats are used to assess the external issues of an organization.

PEST (Political, Economic, Social, and Technological) analysis: The PEST analysis allows the organization to analyze the market forces and opportunities in the four following areas: political, economic, social, and technological. Some authors have added two additional categories: environmental and legal.

Porter's Five Forces analysis: The Porter's Five Forces analysis examines the competitiveness level of an organization by employing the five factors that influence the business environment within an industry. These five forces consist of the intensity of rivalry among competitors, the bargaining power of customers, the threat of potential entrants in the market, the bargaining power of suppliers, and the threats of alternative products.

Analyze the Internal and External Environment

Organizational structure and key players

Understanding the structure and main actors of the organization related to the scope at the following levels:

- Strategic (Who sets the strategic directions?)
- Steering (Who coordinates and manages the operations?)
- Operational (Who is involved in operations and other support activities?)

When analyzing the internal environment, it is necessary to identify the structures comprising the various bodies and relations between them (hierarchical and functional). These include separation of duties, responsibilities, authority, and communication within the organization that should be studied. The functions outsourced to the subcontractors should also be identified.

75

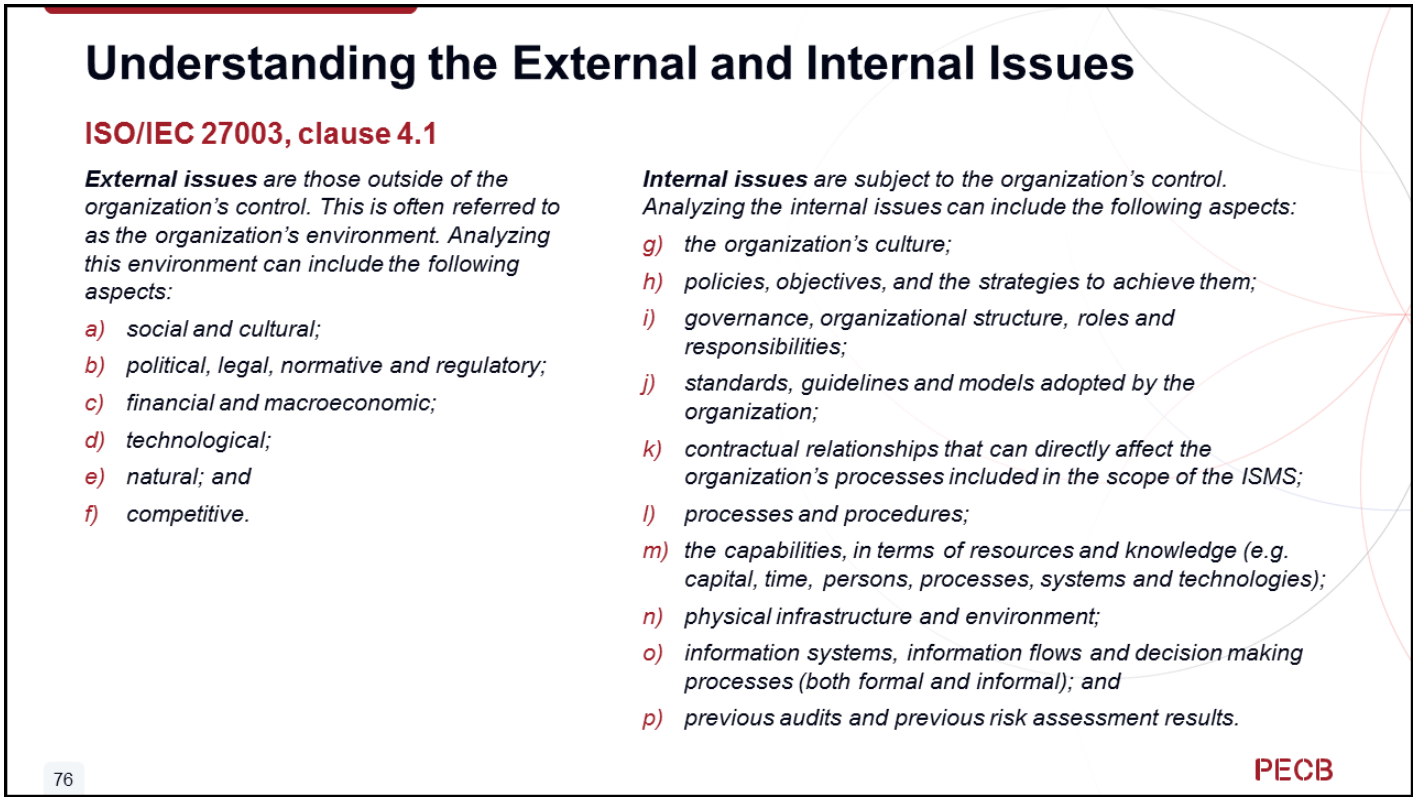
PECB

The structure of the organization may be of different types:

1. The divisional structure: each division is under the authority of a division director responsible for strategic, administrative, and operational decisions within this unit.
2. The functional structure: functional authority exercised over proceedings, the nature of work, and, sometimes, the decisions or planning (e.g., production, information technology, human resources, marketing). Notes:

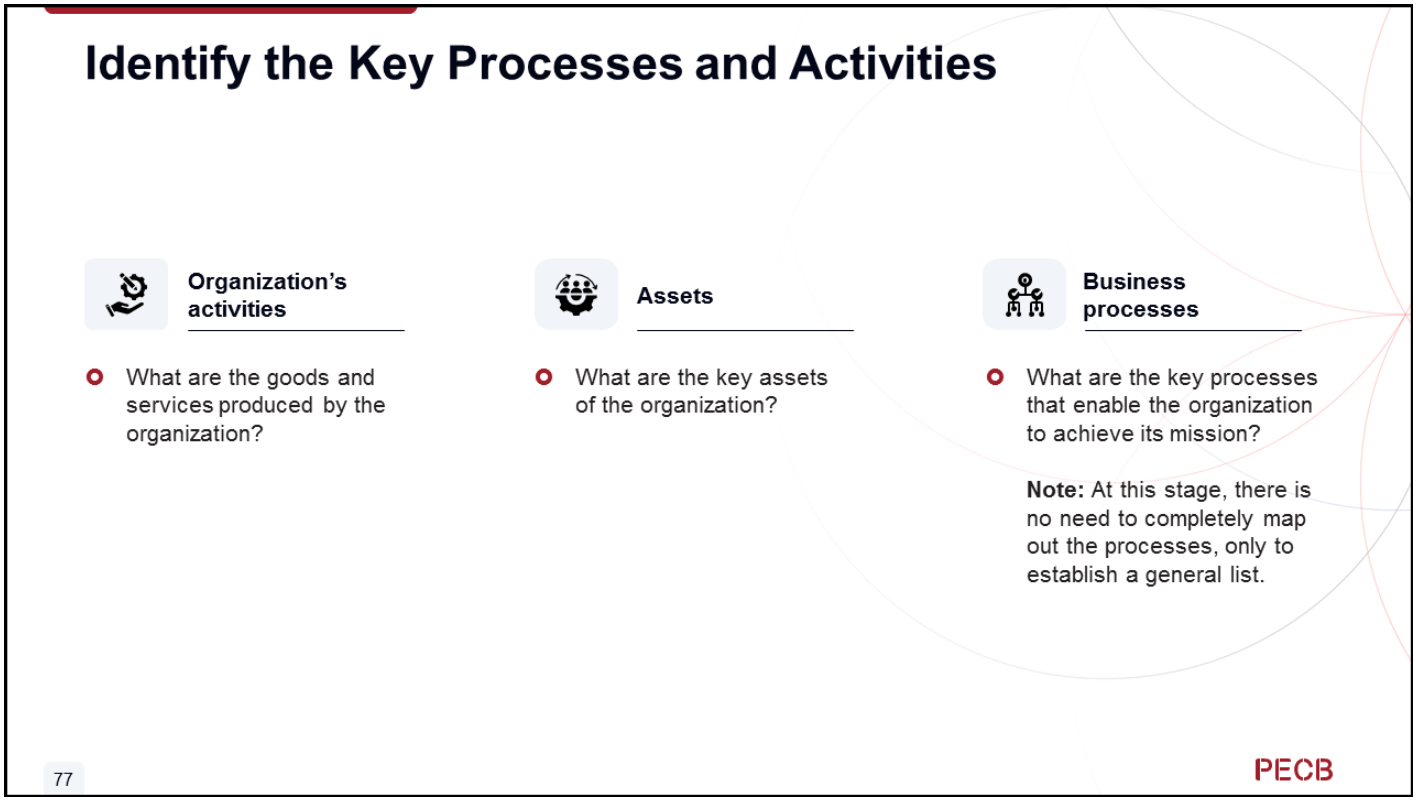
- A division within the organization or a divisional structure can be organized into functions and vice versa.
- We say that an organization has a matrix structure where the entire organization is based on the two structure types.
- Whatever the structure, the following levels are distinguished:
    1. The decision level (responsible for policy making and the strategies)
    2. The steering level (responsible for the coordination and management of activities)
    3. The operational level (responsible for production and support activities)

The organizational chart is an excellent tool to get to understand the internal environment. It shows, using a scheme, the structure of the organization. This representation shows the links of subordination and delegation of authority, but also dependencies. Even if the chart illustrates that no formal authority exists, based upon the links, the information flows can be deduced.



ISO/IEC 27003, clause 4.1 Understanding the organization and its context

As both the external and the internal issues will change over time, the issues and their influence on the scope, constraints and requirements of the ISMS should be reviewed regularly.



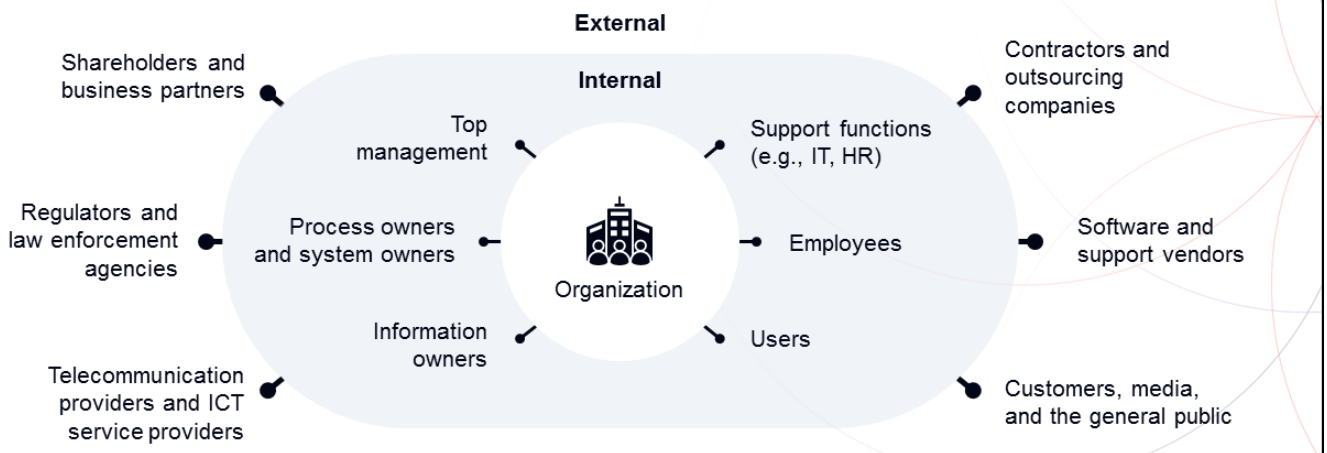
It is essential for the ISMS project manager to know the **organization's activities** that affect information security. The type of products and services offered by the organization will have a major impact on its business model. In addition, these products and services may expose the organization to special risks, such as information security risks, liabilities, fines, etc.

The ISMS project manager should also understand the organization's **business processes** because these processes expose the organization to numerous information security risks. The risk manager should analyze and understand the nature of these processes and determine the direct and indirect risks to which the organization is exposed during operations.

The identification of the organization's assets is crucial when developing an ISMS. The increasingly complex technical management environments tend to enhance the rate of difficulty of protecting assets since such assets are subject to constant advancement. Thus, the ISMS project manager has to pay particular attention to:

- Clearly identify the owners of the assets
- Have the owners understand, consistently and unambiguously, the value of the assets for which they are responsible
- Define a complete set of related information security requirements for each asset
- Describe, unequivocally, where assets are stored, moved, and used (whether in a physical or logical way)
- Determine the value that the organization attaches to the evaluated assets which can be absolute (e.g., a purchase price or replacement) or relative (direct cost or indirect loss caused by this asset)

Examples of Relevant Internal and External Interested Parties



78

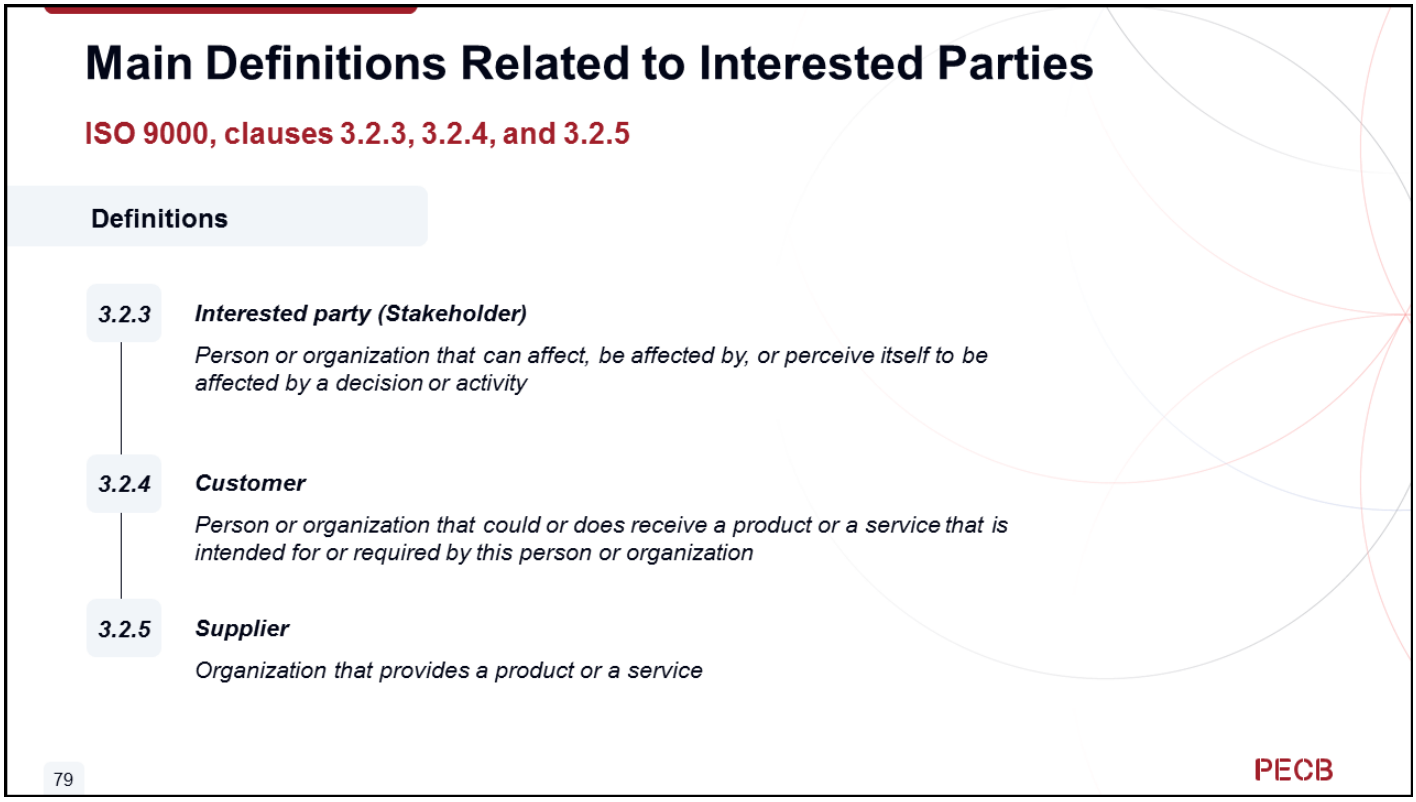
PECB

ISO/IEC 27001:2022 often raises the topic of the interested parties, which, in this context, denotes both the internal and external interested parties of the organization with interests in the process of information security management. ISO/IEC 27001:2022 also stipulates that the ISMS is intended to ensure the selection of appropriate and proportional security controls to protect the assets and give confidence to interested parties.

It is rather challenging to identify, analyze, and manage interested parties since a number of issues may arise. Some are conceptual, such as how to deal with cultural differences. Others are procedural, such as:

- How to approach and proceed with the management of interested parties
- The need to effectively balance the conflicting interested parties' interests
- How to map interested parties when the boundaries between groups are unclear, when multiple group memberships exist, or when strong coalitions between groups are apparent

Note on terminology: Some experts define stakeholders as a sub-category of the interested parties. Stakeholders are those who take direct action in relation with the ISMS (such as employees, customers, or suppliers). The media or legislators would only be interested parties because they do not generally work directly in relation to the ISMS.



ISO 9000, clause 3.2.3 Interested party (cont'd)

Stakeholder

EXAMPLE Customers, owners, people in an organization, providers, bankers, regulators, unions, partners or society that can include competitors or opposing pressure groups.

- *Note 1 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified by adding the Example.*

ISO 9000, clause 3.2.4 Customer (cont'd)

EXAMPLE Consumer, client, end-user, retailer, receiver of product or service from an internal process, beneficiary and purchaser.

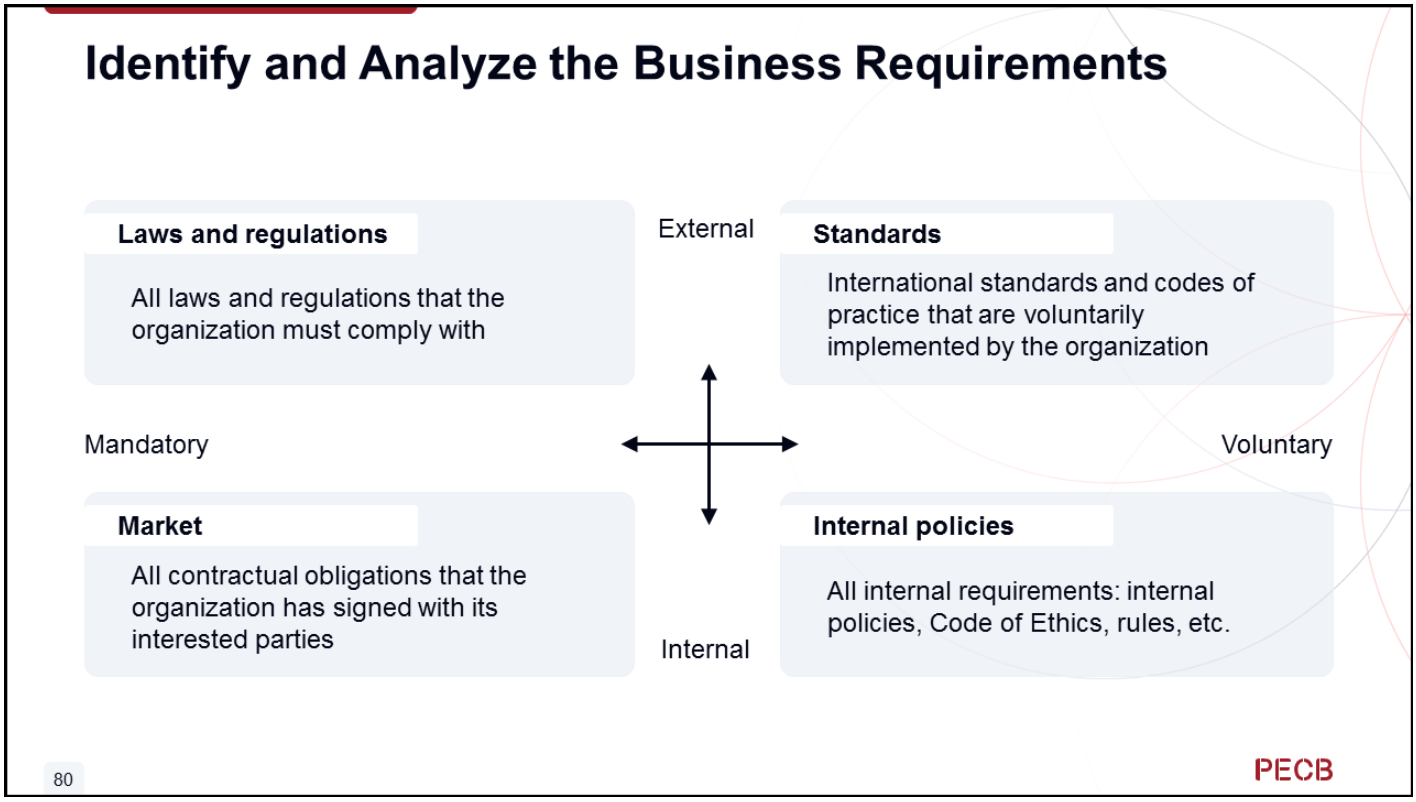
- *Note 1 to entry: Acustomer can be internal or external to the organization.*

ISO 9000, clause 3.2.5 Provider (cont'd)

Supplier

EXAMPLE Producer, distributor, retailer or vendor of a product or a service.

- *Note 1 to entry: A provider can be internal or external to the organization.*
- *Note 2 to entry: In a contractual situation, a provider is sometimes called "contractor".*



The organization must take into account the business, legal, or regulatory requirements and contractual obligations that were agreed upon with various interested parties. To do so, it is important to identify and take into account all the requirements of the organization that could influence the course of the ISMS implementation. Finally, they must be included in the risk assessment process whereby the risk of noncompliance is analyzed.

It should be noted that for the identification and analysis of legal and contractual requirements, it is necessary to involve legal advisors or lawyers qualified in the field. An expert in information security is usually not suited, for example, to analyze the legal implications and as a result may fail to identify the legal and contractual requirements.

The ISMS requirements for all organizations are mainly derived from four sources:

1. **Laws and regulations:** See the following slide.
2. **Standards:** Organizations must comply with a set of international standards and codes of practice related to their industry sector. Although the implementation of regulatory frameworks is a voluntary choice, from the information security management point of view, they become obligations to comply with (the risk of losing its certification in case of serious failure).
3. **Market:** Market requirements include all contractual obligations that the organization has signed with its interested parties. A breach of contractual obligations may result in penalties (when stated in the contracts) or civil suits for damages. Market requirements are all implicit rules that an organization should fulfill in order to conduct business. For example, although the organization has no contractual obligation to deliver its products as planned, it goes without saying that this is a commercial policy basis to meet the scheduled delivery times and failing to do so will lead to a loss of market share, customer trust, profits, etc.
4. **Internal policies:** Internal policies are formulated principles, rules, and guidelines that include all the requirements defined inside the organization: internal policies (human resources, food safety management, supply chain, etc.), ethical codes, work rules, etc. In case of failure, we can consider that these are violations of internal policies without necessarily involving any legal considerations.

Legal and Regulatory Conformity

Key areas to monitor

- Data protection
- Privacy
- Cybercrimes
- Digital signature
- Intellectual property
- Electronic payments
- Records management

81

PECB

1. **Data protection:** Many countries have established data protection laws and regulations that aim at safeguarding data and data subjects. As such, organizations have to establish procedures and implement measures for protecting the data that they store and process in order to comply with these regulatory requirements.
2. **Privacy:** In order to comply with certain laws, many organizations are obliged to establish a policy for ensuring information privacy, through which they increase awareness of statutory, regulatory, and business requirements regarding the treatment and protection of personal information.
3. **Cybercrimes:** They encompass any illegal activity that is performed through a computer and network and that is intended to cause harm to organizations' systems and gain unauthorized access to data. Targeted organizations might experience, among others, financial and reputational damages. In order to prevent and respond to these activities, organizations should establish adequate procedures and measures. Protective measures are not considered as crimes (e.g., responding to spam by countermeasures, such as a buffer overflow attack).
4. **Digital signature:** It is an electronic signature that enables organizations to verify the authenticity of a message or document by verifying who the author of a document is and if the content has been modified. As a result, an electronic document that is digitally signed has the same legal validity as a hard copy document signed in handwriting, as long as there are regulations that give full legal value to it. In some countries, electronic records must ensure the preservation of "traces" as evidence of integrity and safety procedures developed on the basis of recognized standards for electronic records, e.g., the NF Z42-013 standard, or ISO 14721, which provides the reference model for an open archival information system (OAIS).
5. **Intellectual property:** The aim of intellectual property laws is to enable organizations or individuals to protect certain intangible assets. Patent rights, especially, help in protecting the ideas and inventions of individuals or enterprises.
6. **Electronic payments:** Electronic payment laws have been created in some countries aiming at facilitating funds transfers and protecting the rights of clients.
7. **Records management:** Some national laws require from organizations to establish procedures for identifying, classifying, modifying, storing, or destroying records. ISO 15489-1 defines concepts and principles which are helpful in records management.

Information Security Management System (ISMS)

ISO/IEC 27001:2022, clause 4.4

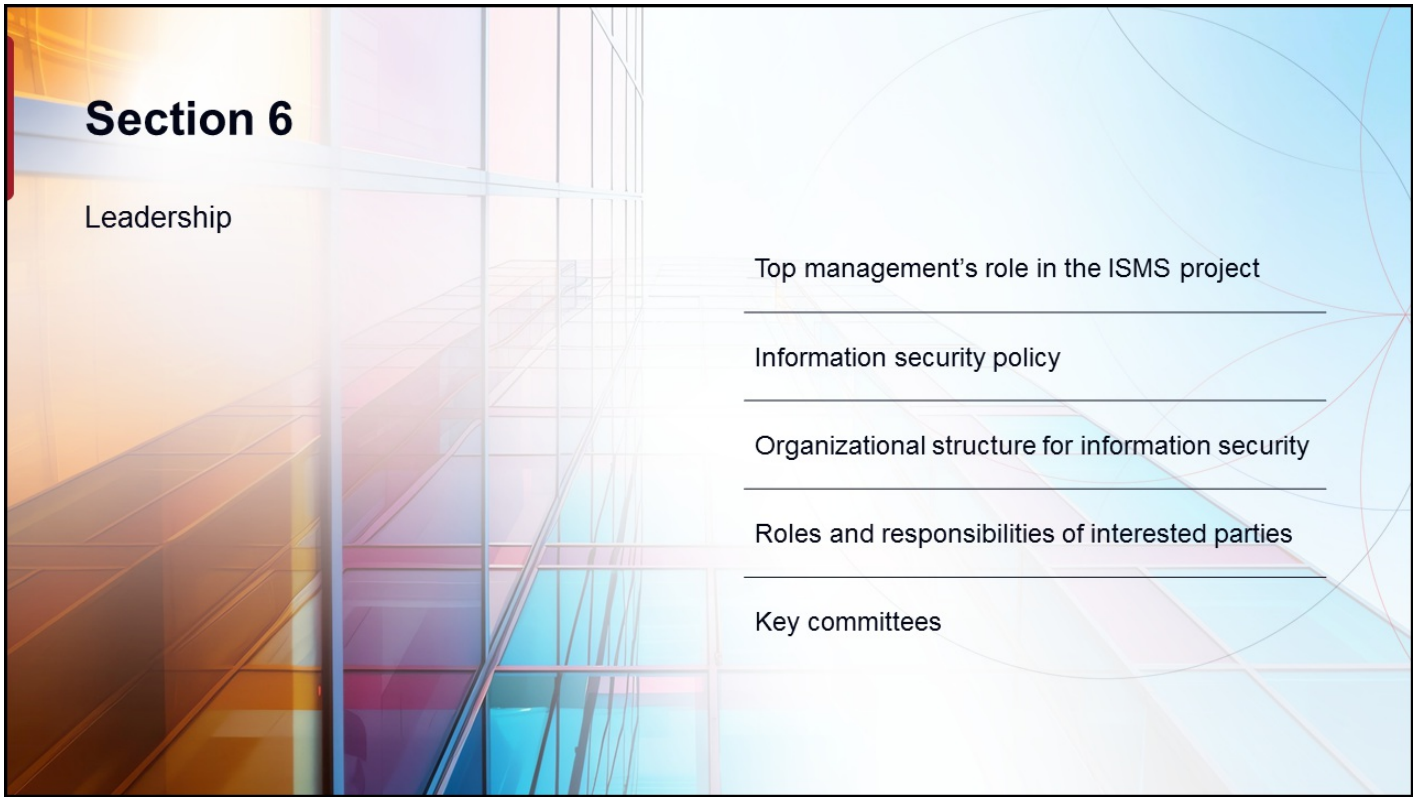
The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

PECB

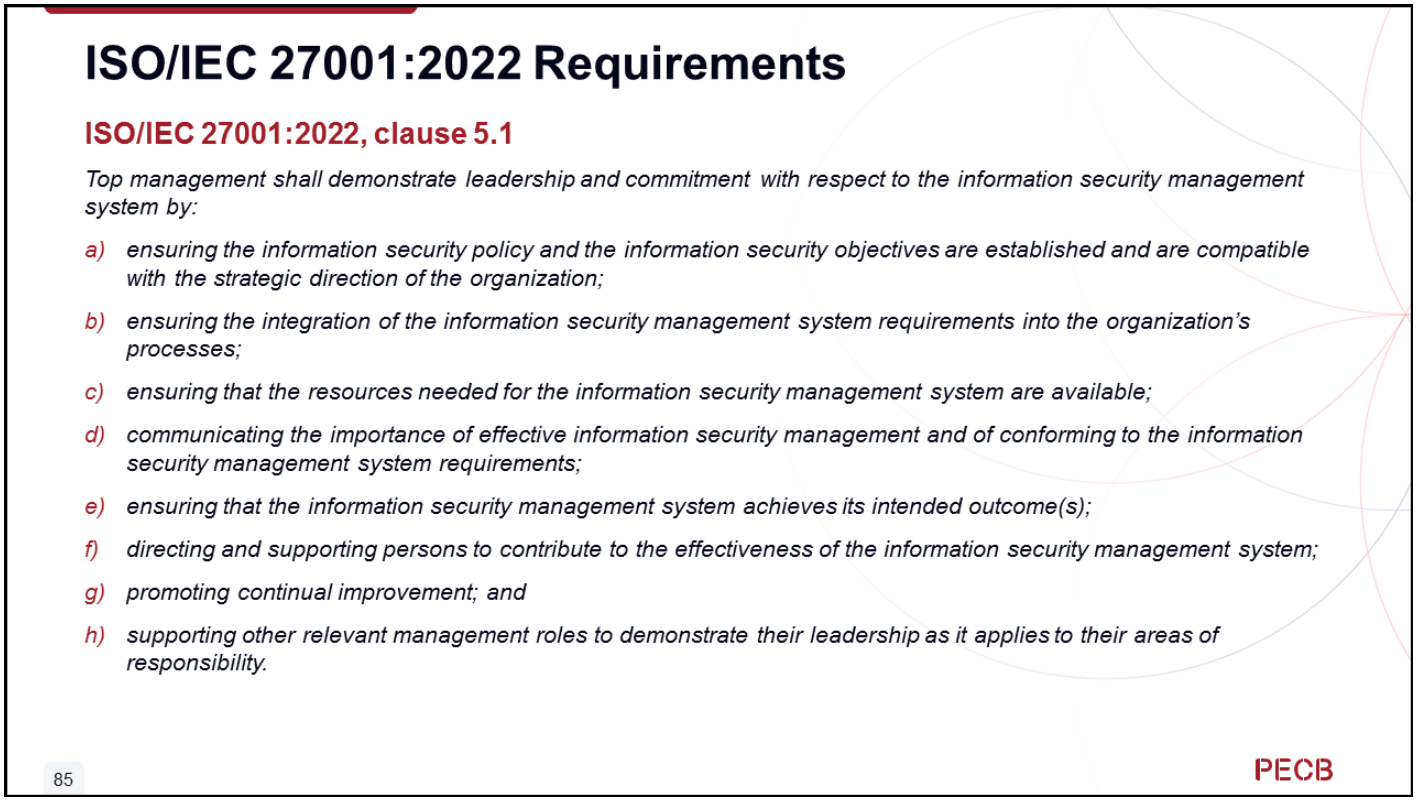
Section 5 Summary

- The ISMS should be well aligned with the organization's mission, objectives, and business strategies.
- ISMS objectives are essential when determining the scope.
- It is important to identify the internal and external factors that can influence the information security management system: mission, main activities, interested parties, etc.

Questions?



This section provides information on the information security policy, roles and responsibilities of interested parties and key committees, and organizational structure for information security.



ISO/IEC 27001:2022, clause 5.1 Leadership and commitment (cont'd)

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

An organization wishing to comply with ISO/IEC 27001:2022 shall at least:

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

Leadership and Project Approval

ISO/IEC 27021, clause 5.2

ISO/IEC 27001:2022 clause/subclause (if applicable)	5 Leadership
Intended outcome	*Directing, motivating and encouraging staff across the organization to deliver information security*
Knowledge required	— *Theories of leadership* — *Negotiation techniques*
Skills required	— *Set and give direction for information security across the organization* — *Provide guidance, set objectives and drive progress within the information security function, team and the business* — *Deliver commitments* — *Deploy responsibilities and authorities at the different levels of the organization*

86

PECB

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

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

Top Management's Commitment

The top management's commitment to the ISMS project can bring several benefits:

- Increased knowledge of applicable laws, regulations, contractual obligations, and standards related to information security
- Adequate allocation of resources dedicated to information security
- Identification and protection of critical assets
- Monitoring and review of information security processes
- Access to reliable information on the organization's level of risk exposure so as to take appropriate decisions

87

PECB

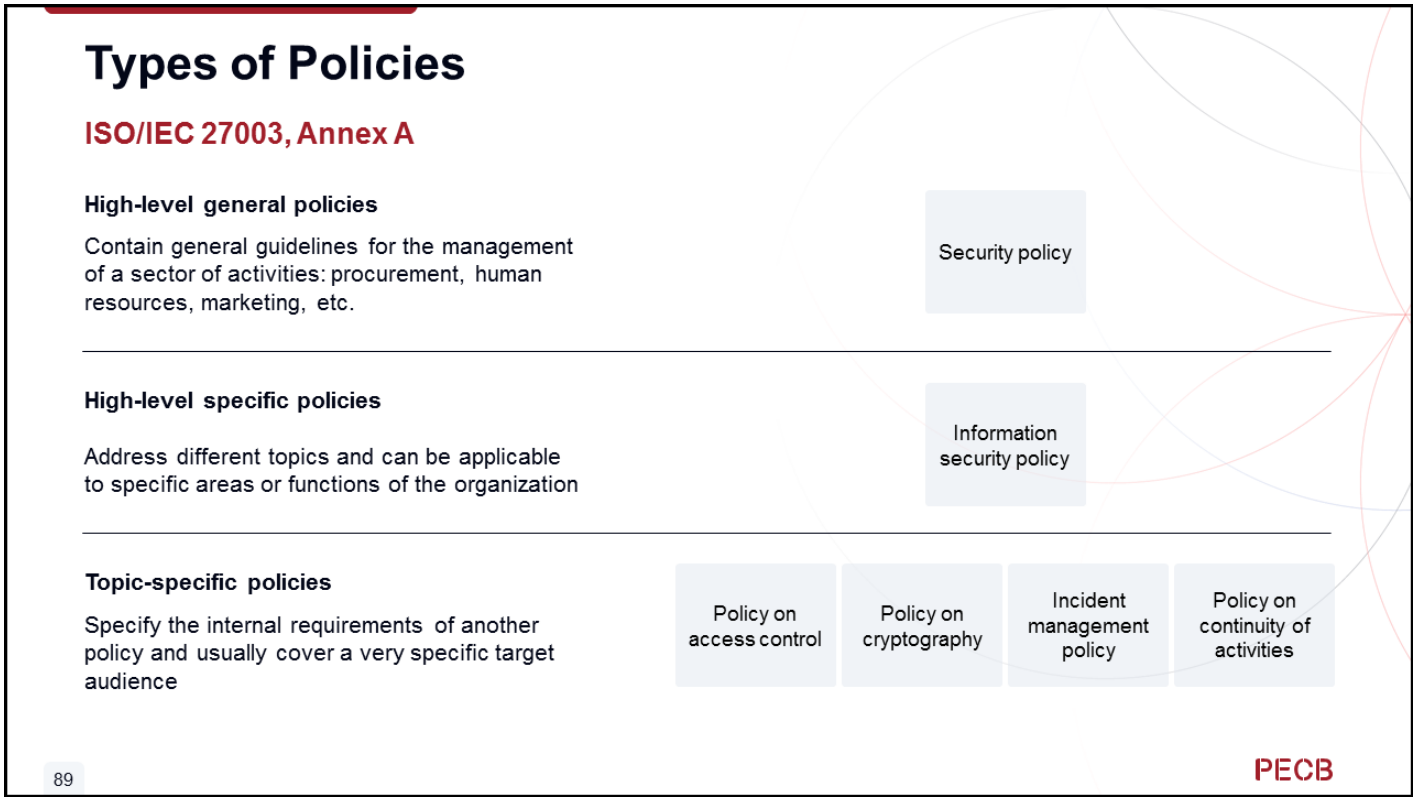
The declarations of support and authorization of the top management must be formally documented.

Role of the Top Management in the ISMS Project

Objective	Align the ISMS with the business objectives and strategy
Missions	1. Set the objectives and strategy for the ISMS 2. Validate the roles and responsibilities of key interested parties in the project 3. Validate the security policies of the ISMS 4. Approve the criteria for the acceptance of risk 5. Approve the risk treatment plan and allow the implementation of the ISMS 6. Provide adequate resources for the implementation and maintenance of the ISMS
Members	Top management (CEO, CIO, CFO, etc.)
Meeting frequency	Several meetings when marking the project milestones: risk analysis report, risk treatment planning, Statement of Applicability, management review, etc.

PECB

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



There are generally three levels of policies within an organization:

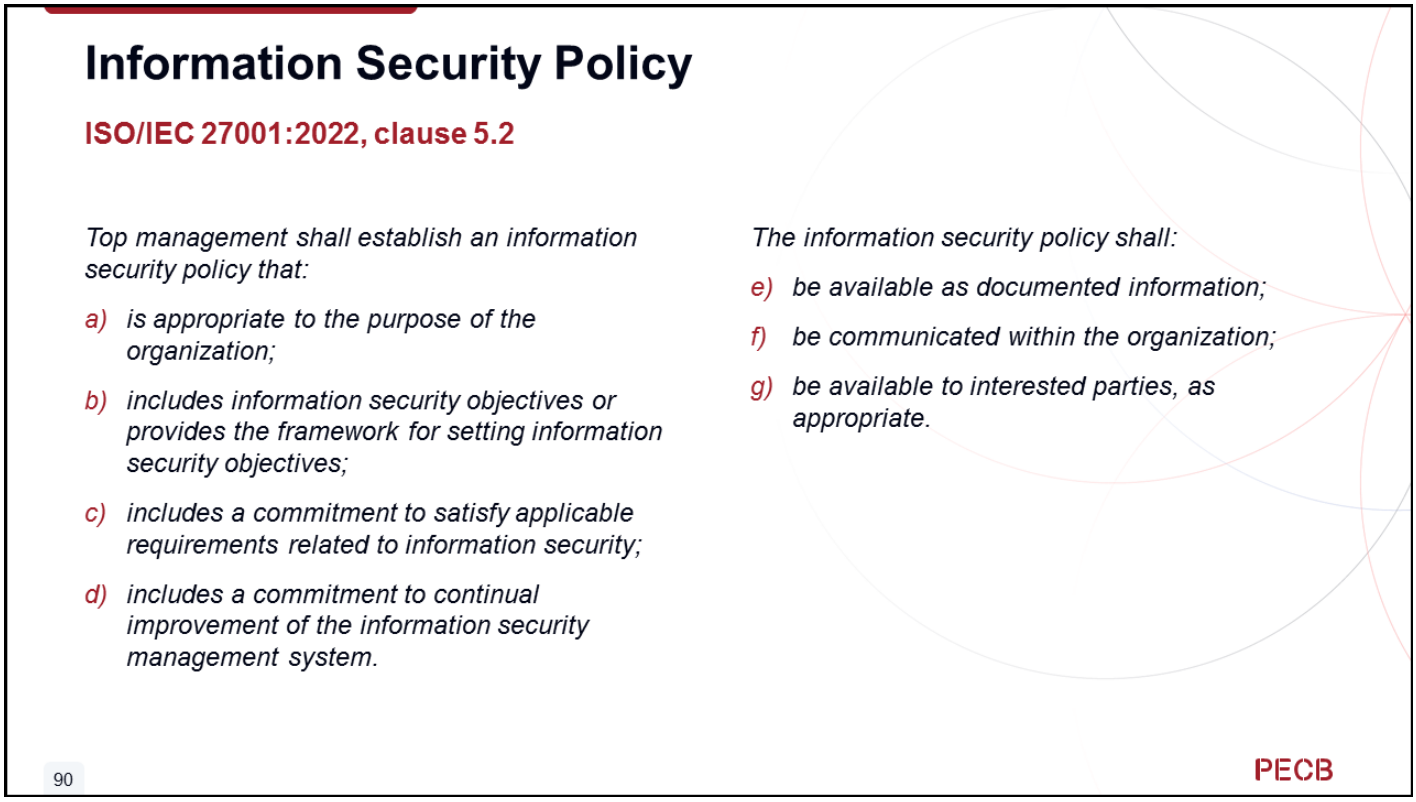
1.High-level general policies define a general framework within which the information security will be provided and the general objectives to ensure business continuity and to limit or prevent the potential damage of assets to an acceptable level and consequently limit the potential consequences of security incidents.

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

Note: Both types of policies are usually subject to a review process because of their sensitive nature with regard to the functional strategy of the organization they are supposed to support.

3.Topic-specific policies are policies that support the information security policy (i.e., high-level specific policy). These policies determine how to proceed in order to ensure information security in specific application areas. Examples include the following policies: security policy for access rights to information and technology infrastructure, policy on internet use, policy on archiving and destruction of documents, etc.

Note: Some of these topic-specific policies are independent, while others are attached to and dependent on another policy. For example, an organization may have a (general) security policy which is complemented by a (topic-specific) policy on physical security and another on information security. In turn, the information security policy may be a reference for the publication of specific policies as the policy on access control.

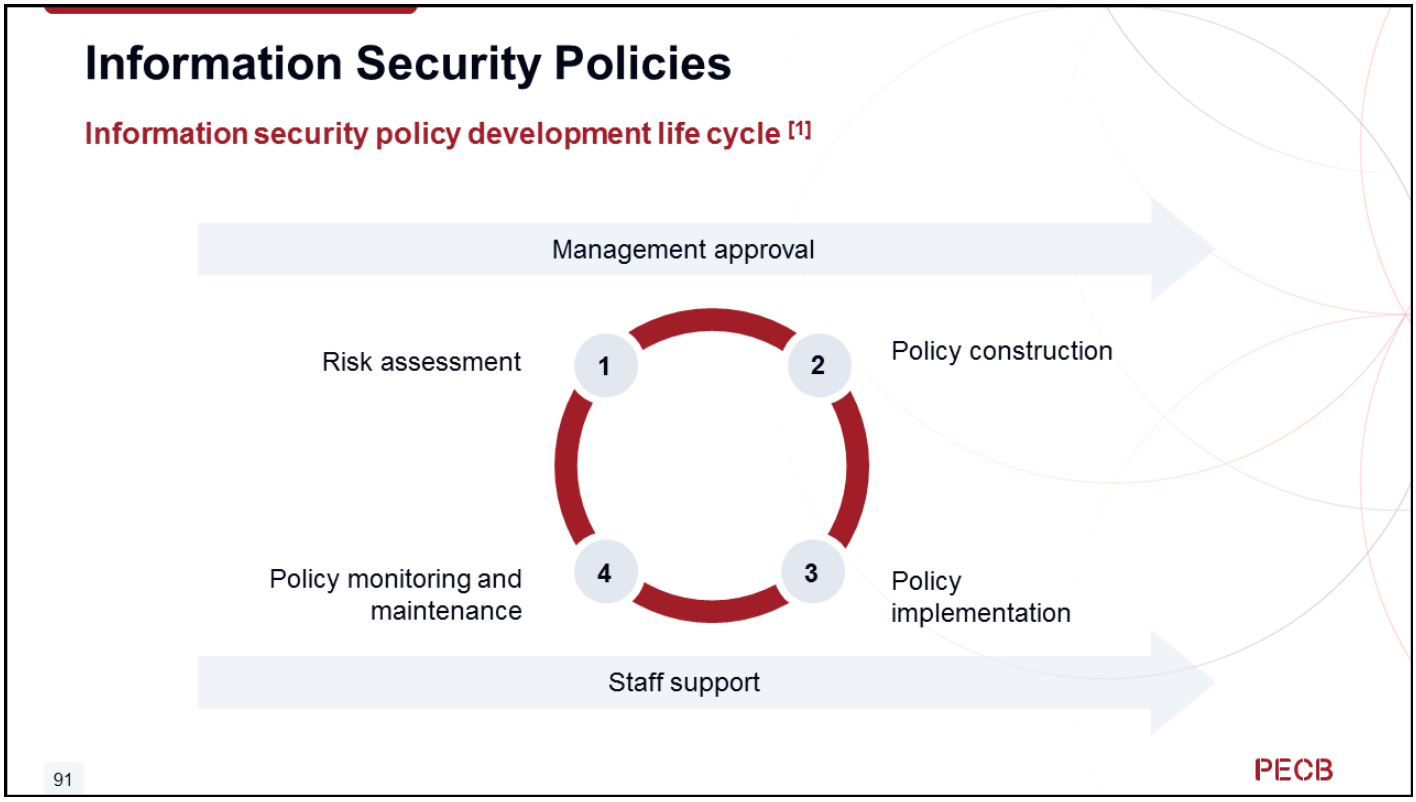


ISO/IEC 27003, clause 5.2 Policy

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

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

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



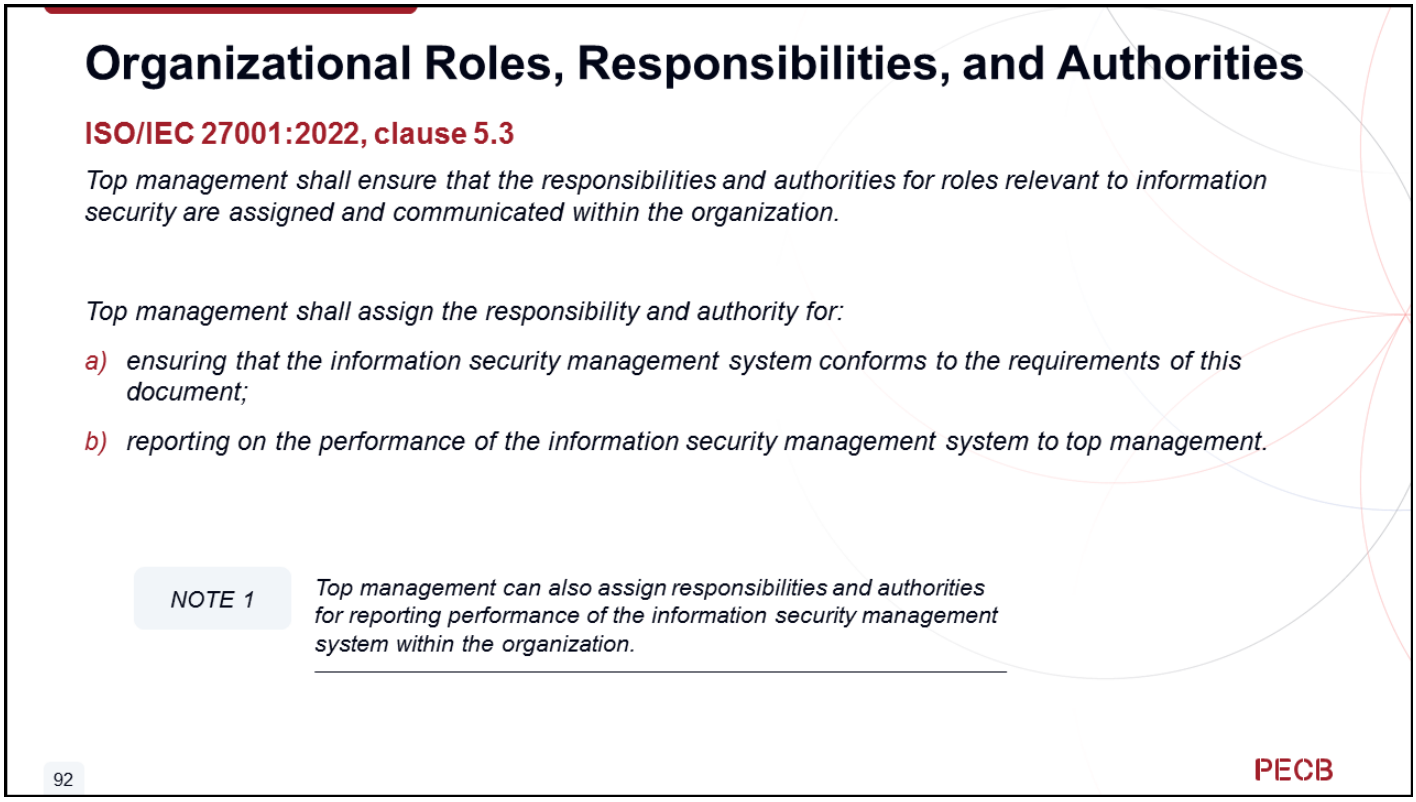
The policy development life cycle is an iterative process. The information security policy development life cycle usually comprises four phases: risk assessment, policy construction, policy implementation, and policy monitoring and maintenance. The management's approval and staff support are needed throughout the entire life cycle. It is the responsibility of the top management to approve the policies and communicate them to the relevant interested parties.

Phase 1: Risk assessment – In this phase, the assets that should be protected and the potential threats and vulnerabilities to these assets are identified. The results will enable the top management to evaluate the costs and benefits of implementing controls to reduce risks to an acceptance level. If the expenses are within the budget, the organization initiates the policy construction; otherwise, risk mitigation strategies need to be reviewed or the budget should be increased.

Phase 2: Policy construction – In this phase, the information security policy is developed based on the findings and recommendations of the risk assessment phase, business strategies of the organization, and the applicable legal requirements. Drafting the information security policy involves selecting control objectives to be achieved in the organization. The policy should then be reviewed and approved by the top management. A communication plan is needed during the policy construction phase in order to inform and receive feedback from relevant employees.

Phase 3: Policy implementation – This phase requires a detailed implementation plan on how to define security and control requirements, how to assign security responsibilities, how to perform tests, and how to conduct training and awareness sessions. The top management should ensure that the information security policy is available and accessible by all employees.

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

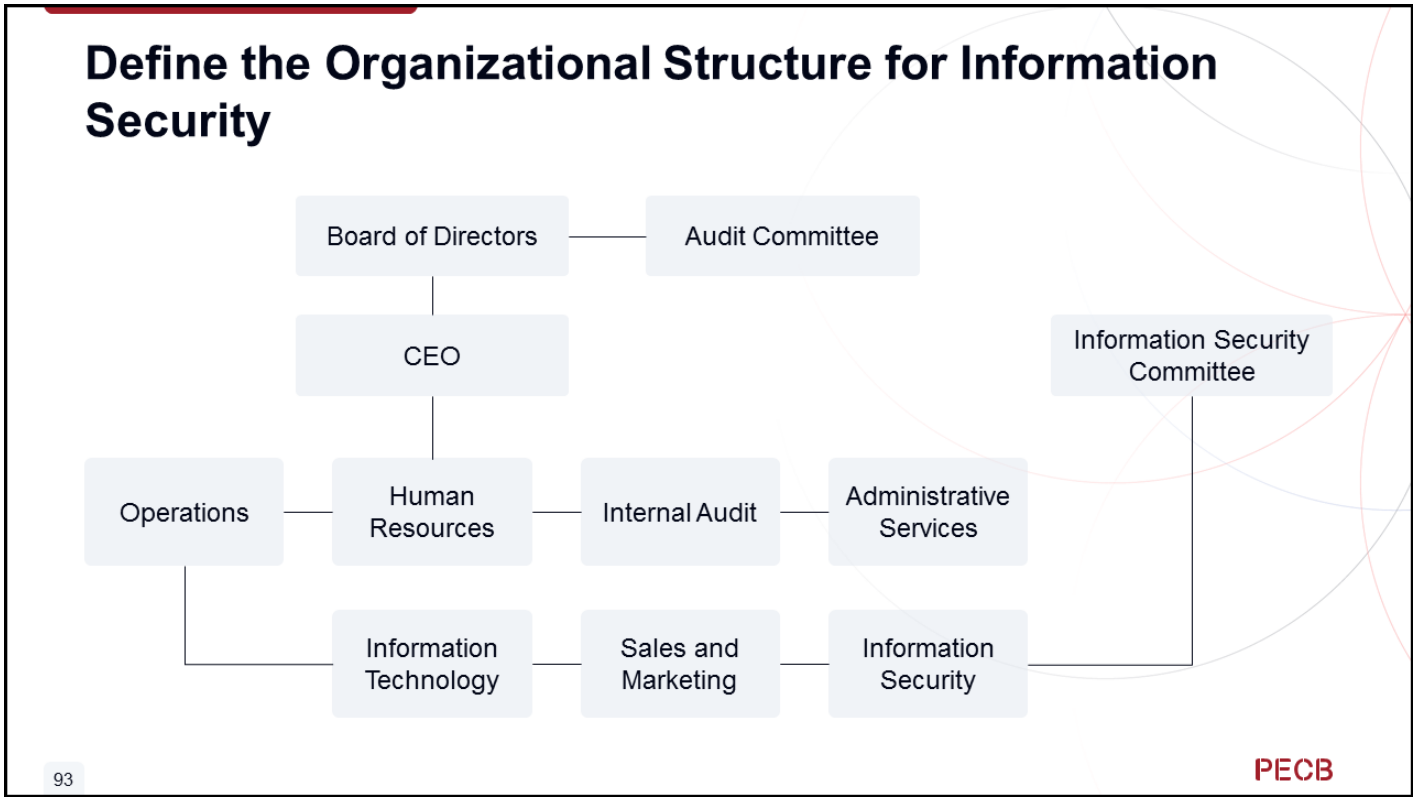


To comply with the requirements of ISO/IEC 27001:2022, an organization shall at least define the roles and responsibilities of the key interested parties related to the ISMS.

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

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

a. *information owners;*
b. *process owners;*
c. *asset owners (e.g. application or infrastructure owners);*
d. *risk owners;*
e. *information security coordinating functions or persons (this particular role is normally a supporting role in the ISMS);*
f. *project managers;*
g. *line managers; and*
h. *information users.*



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

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

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

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

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

Assign the Roles and Responsibilities of Interested Parties

Role	Main responsibilities
Head of information security	Coordinate activities related to information security management
Legal counsel	Identify compliance requirements (legal, regulatory, and contractual)
Head of Human Resources	Manage training and awareness programs on information security, consider the security controls in HR processes (recruitment, termination of employment, disciplinary process)
Facilities manager	Implement and manage physical security controls (access control to buildings, protection against fire, electricity maintenance, etc.)
Head of IT	Implement and manage solutions and technical measures in daily operations
Head of service center	Implement and manage services to users and the related controls (access control, incident management, etc.)
Public relations officer	Validate the impact on the organization's reputation, communications with external interested parties
Internal auditor	Validate the ISMS compliance and security controls
Documentation manager	Ensure that the documented information have the qualities of good management of knowledge and information heritage, preservation of evidence, and law enforcement

94

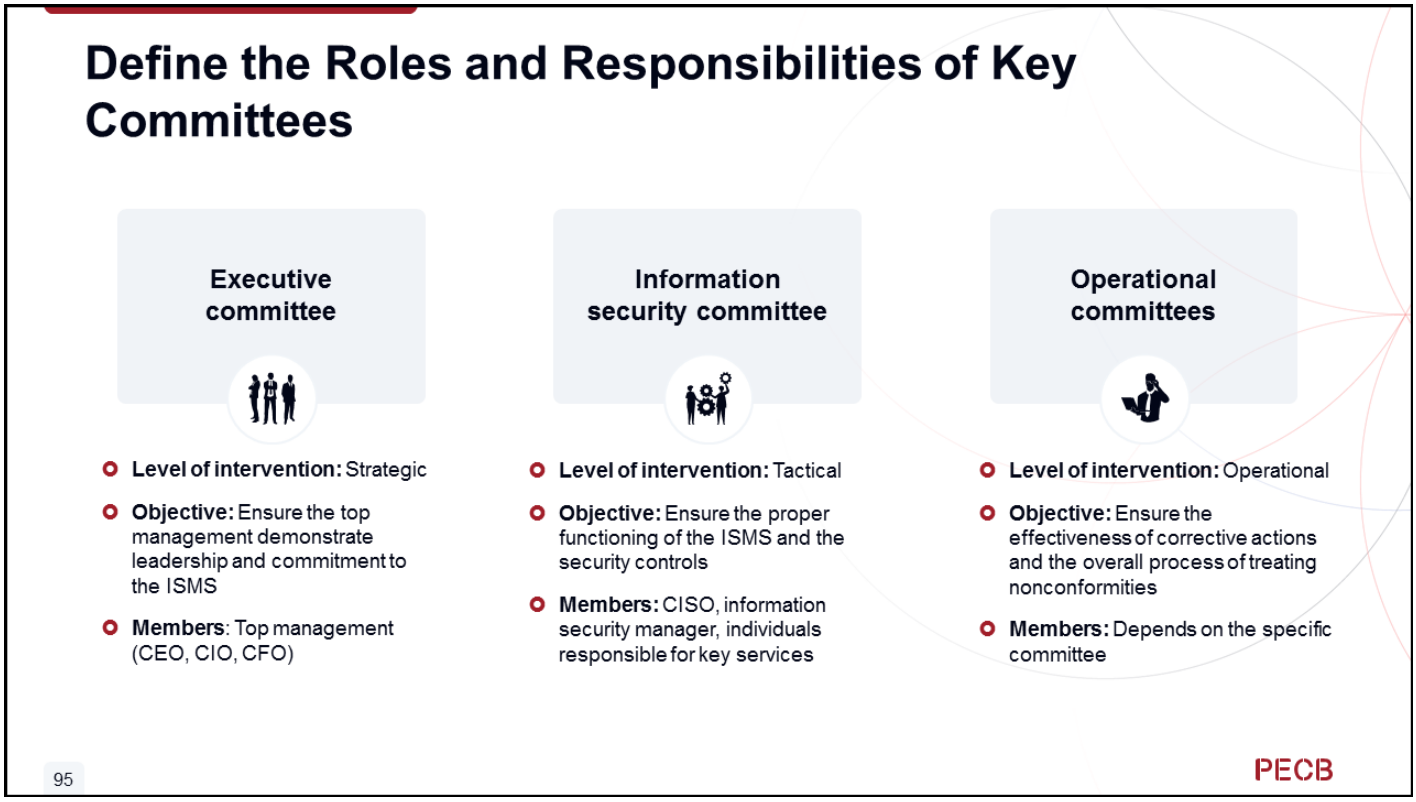
PECB

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

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

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

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



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

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

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

Discussion questions?

1. How can an organization's top management demonstrate leadership and commitment to the ISMS?
2. What does a high-level specific policy define?
3. Which phases comprise the information security policy development life cycle?
4. What is the role of the head of information security?

Section 6 Summary

- The information security policy development lifecycle contains four phases: risk assessment, policy construction, policy implementation, and policy monitoring and maintenance.
- The information security policy is a high-level specific policy that address different topics regarding information security within an organization.
- The chief information security officer (CISO) is important for information security management and should be placed in the organization's hierarchy.
- All roles and duties of responsibilities should be documented in the information security manual, employment contract, terms of security policy, and functions form.
- Organizations can create committees for managing information security, such as executive, information security, and operational committees.

Questions?

Quiz 3

Note: To complete Quiz 3, please go to the Quizzes Worksheet.

Day 1 Summary

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

- Definition of the ISMS and the benefits it brings to organizations
- Overview of the ISO/IEC 27001:2022 main clauses and Annex A
- Fundamental concepts and principles of information security
- Vulnerability, threat, and impact and their relationship
- Information security risks
- Artificial intelligence and cloud computing
- Mission, objectives, values, and strategies of the organization
- Management approval for the ISMS project
- Roles and responsibilities of interested parties and committees
- Information security policy