DAY 1

Certified ISO/IEC 27001 Lead Implementer

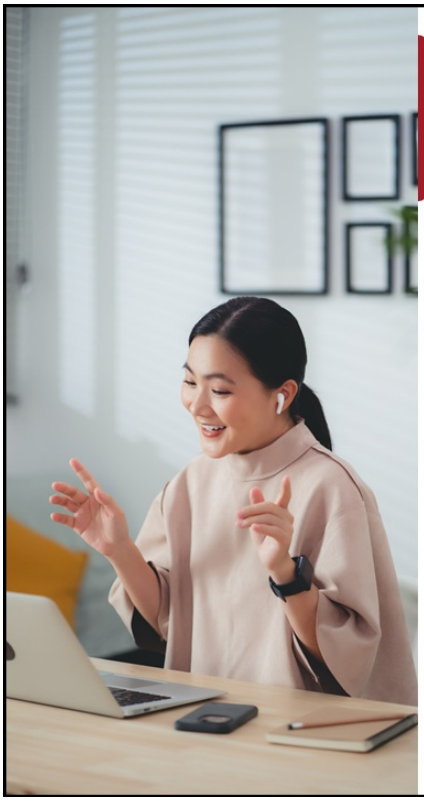
Version 10.0

Document number: ISMSLID1V10.0

Introduction

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

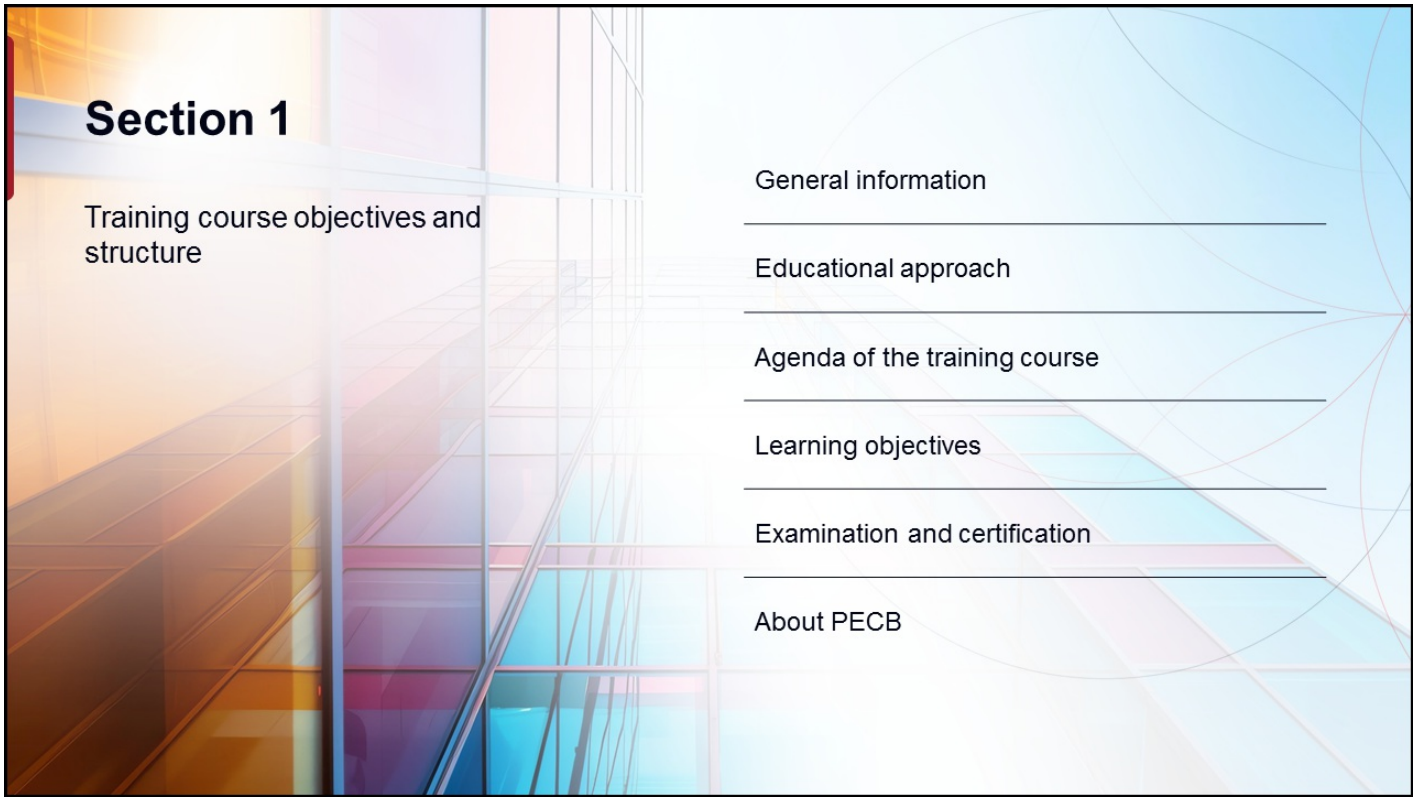
- Their name and current role
- Background in information security management
- Familiarity with ISO/IEC 27001 and related standards (e.g., ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27005, ISO/IEC 27701)
- Familiarity with other management system standards (e.g., ISO 9001, ISO 14001, ISO/IEC 27701, ISO 22301, etc.)
- Goals and expectations for this training course



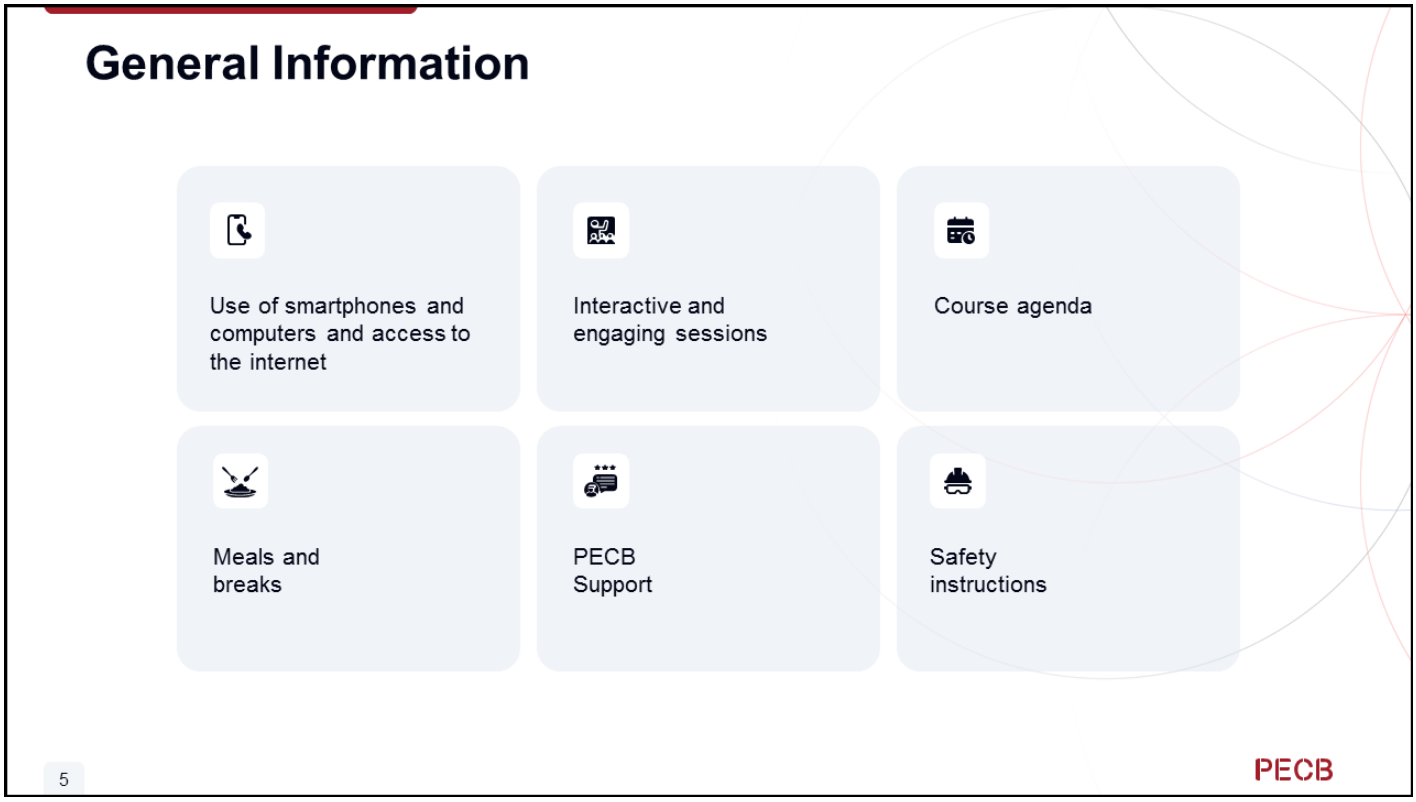
Day 1 Agenda

Section 1	Training course objectives and structure
Section 2	Standards and regulatory frameworks
Section 3	Information security management system based on ISO/IEC 27001
Section 4	Fundamental concepts and principles of information security
Section 5	Initiation of the ISMS implementation
Section 6	Understanding the organization and its context
Section 7	ISMS scope

PECB



This section presents the objectives of the training course and its structure, including the examination and certification process, as well as more information about PECB.



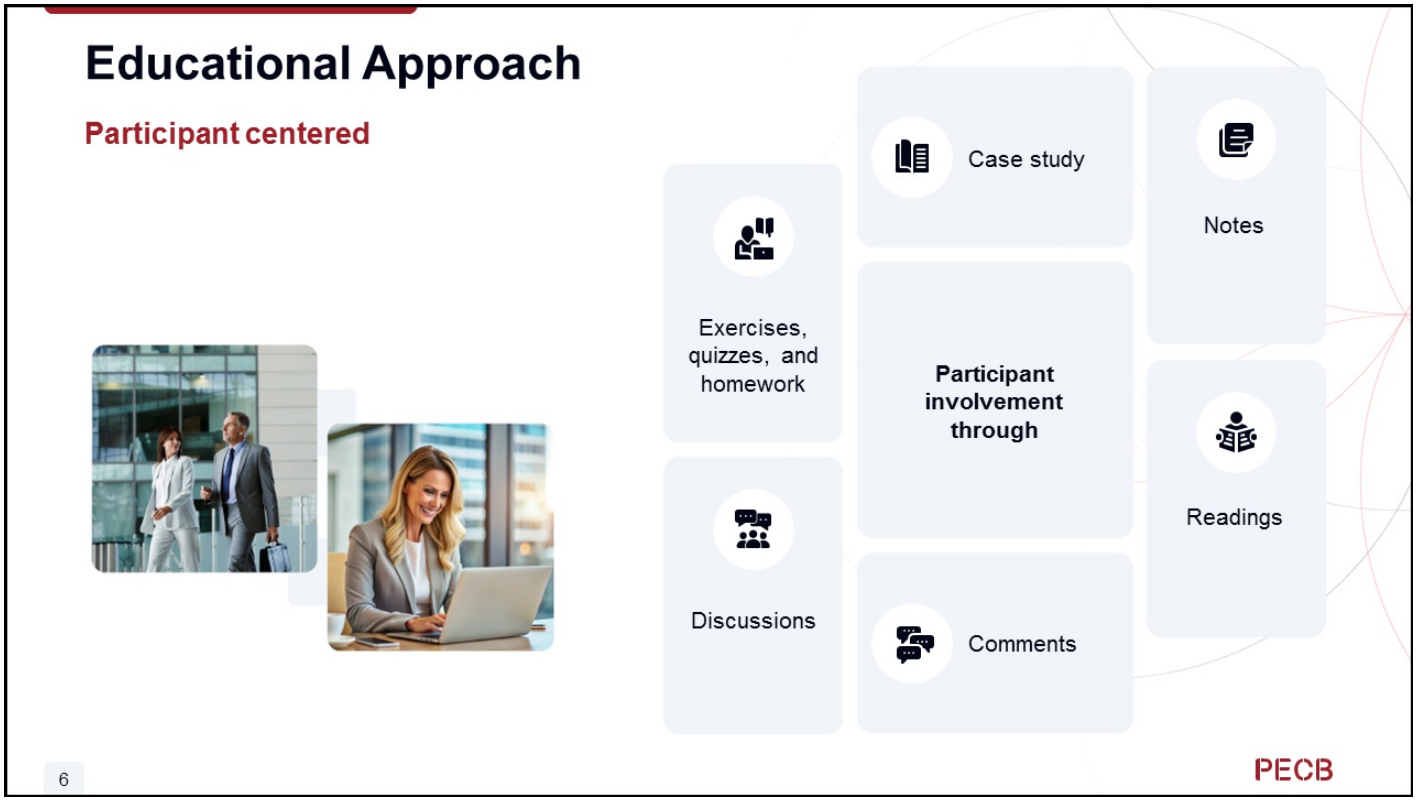
- All should be aware of the exit doors in the facility in case any emergency arises.
- All should agree on the training course schedule. All should arrive on time.
- All should set their smartphones on silent or vibrate mode (if you need to take a call, please do so outside the classroom).
- Recording 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.

PECB Support

To enhance customer satisfaction, PECB operates a dedicated ticket system to manage inquiries, complaints, and suggestions.

If you encounter any issues during your training session, we encourage you to address them with your trainer first. You may contact the PECB partner organizing the session or PECB directly if further assistance is needed. PECB can mediate any disputes between you and the partner organizing the training session.

For comments, questions, complaints, or feedback regarding your training experience—including trainer performance, facilities, exams, certification processes, or course materials—please submit a ticket through the PECB Help Center (https://help.pecb.com/.) or email us at support@pecb.com. Additionally, you can submit feedback on training course materials directly through the KATE application.



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.

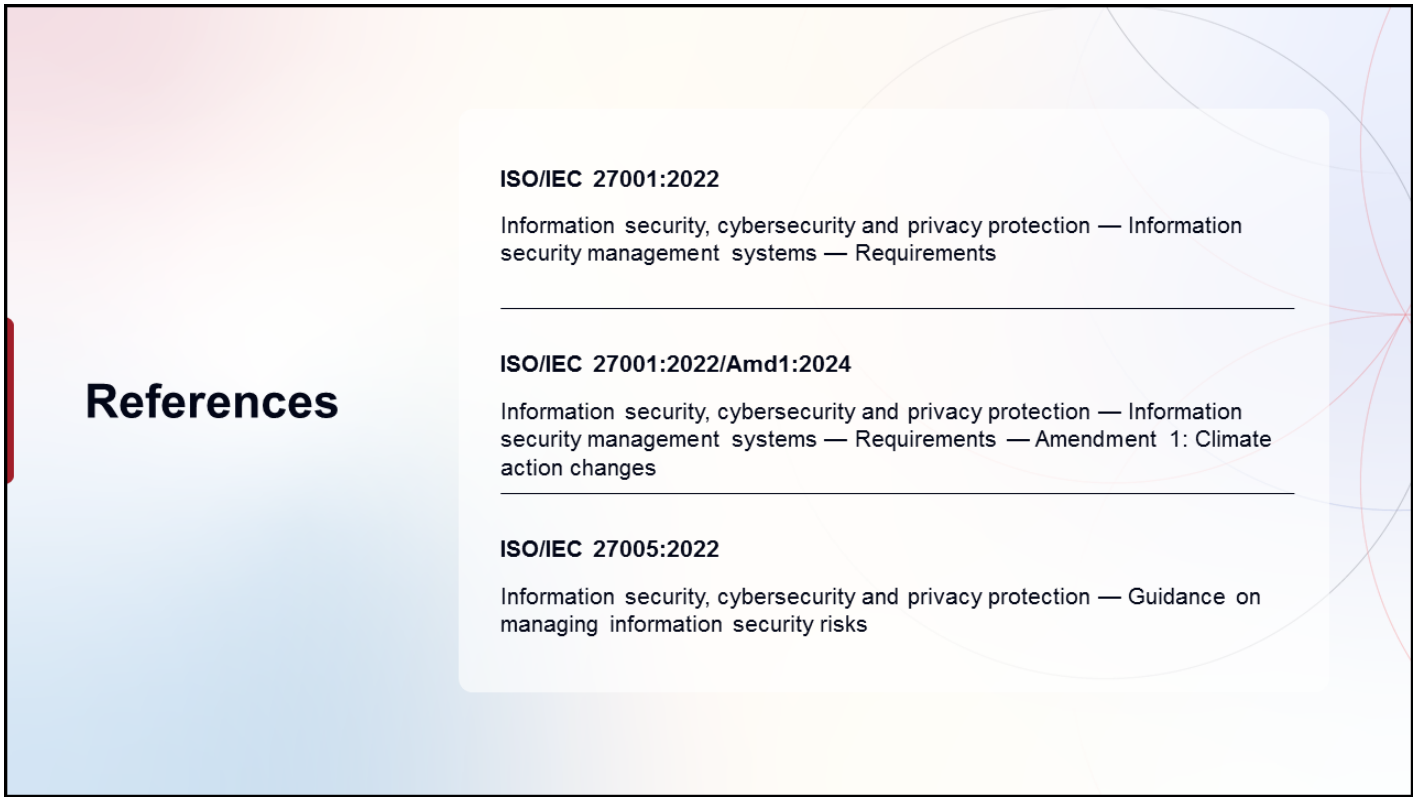
Quizzes, in particular, are important since they help participants prepare for the certification exam.

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.

Agenda of the Training Course

Day 1

Introduction to ISO/IEC 27001 and initiation of an ISMS implementation

Day 2

Implementation plan of an ISMS

Day 3

Implementation of an ISMS

Day 4

ISMS monitoring, continual improvement, and preparation for the certification audit

Day 5

Certification exam

Note: To view the detailed agenda of the training course, including the contents of each section, please go to the **Index** file.

PECB

Learning Objectives

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

1. Explain the fundamental concepts and principles of an information security management system (ISMS) based on ISO/IEC 27001
2. Interpret the ISO/IEC 27001 requirements for an ISMS from the perspective of an implementer
3. Initiate and plan the implementation of an ISMS based on ISO/IEC 27001, by utilizing PECB's IMS2 Methodology and other best practices
4. Support an organization in operating, maintaining, and continually improving an ISMS based on ISO/IEC 27001
5. Prepare an organization to undergo a third-party certification audit

9

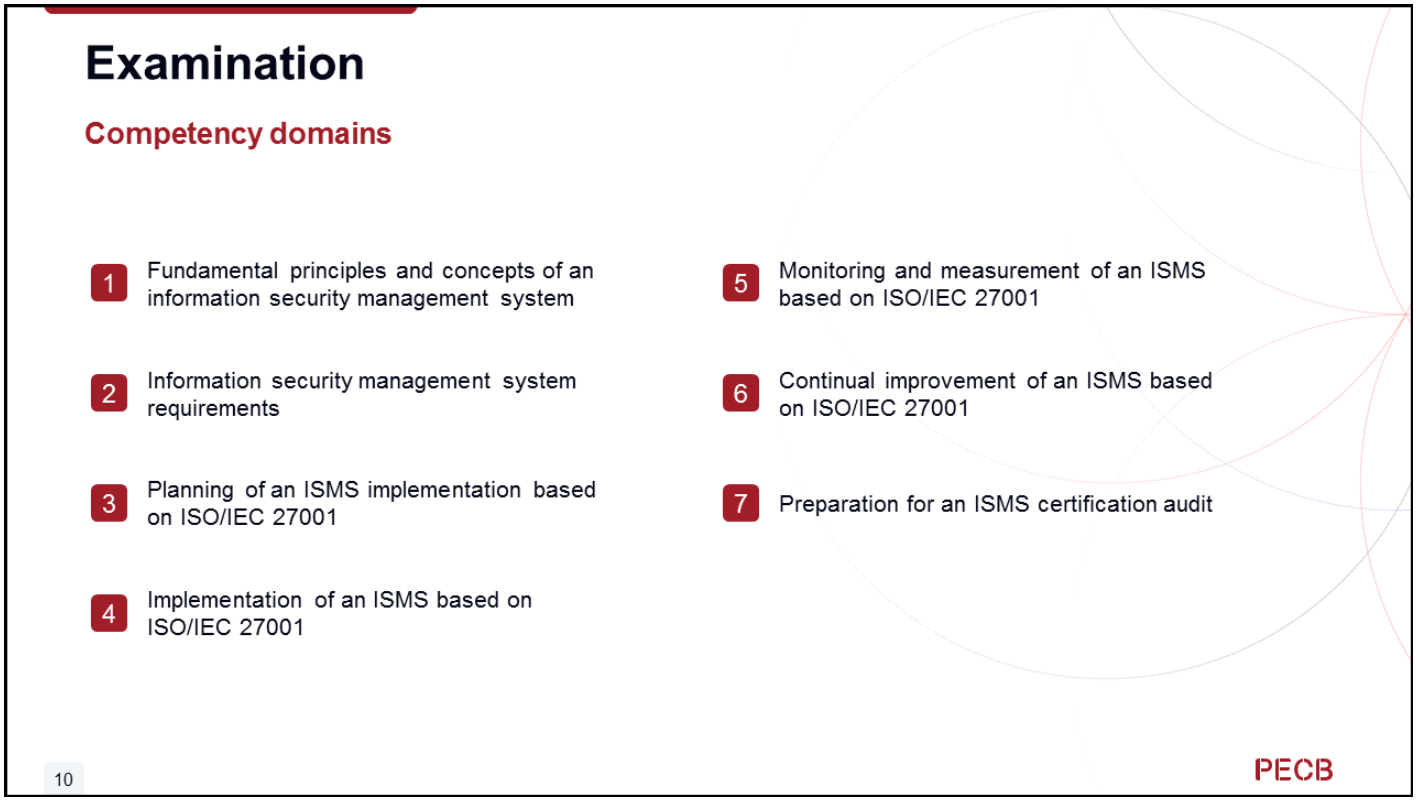
PECB

This training course is intended to help participants develop their competencies to participate in the implementation of an information security management system (ISMS). From an educational perspective, competence consists of the following three elements:

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

This training course provides a comprehensive methodology for the implementation of the ISMS based on the ISO/IEC 27001 requirements, not merely a list of the ISO/IEC 27001 requirements. Therefore, general knowledge of the information security concepts is required for the successful completion of the training course.

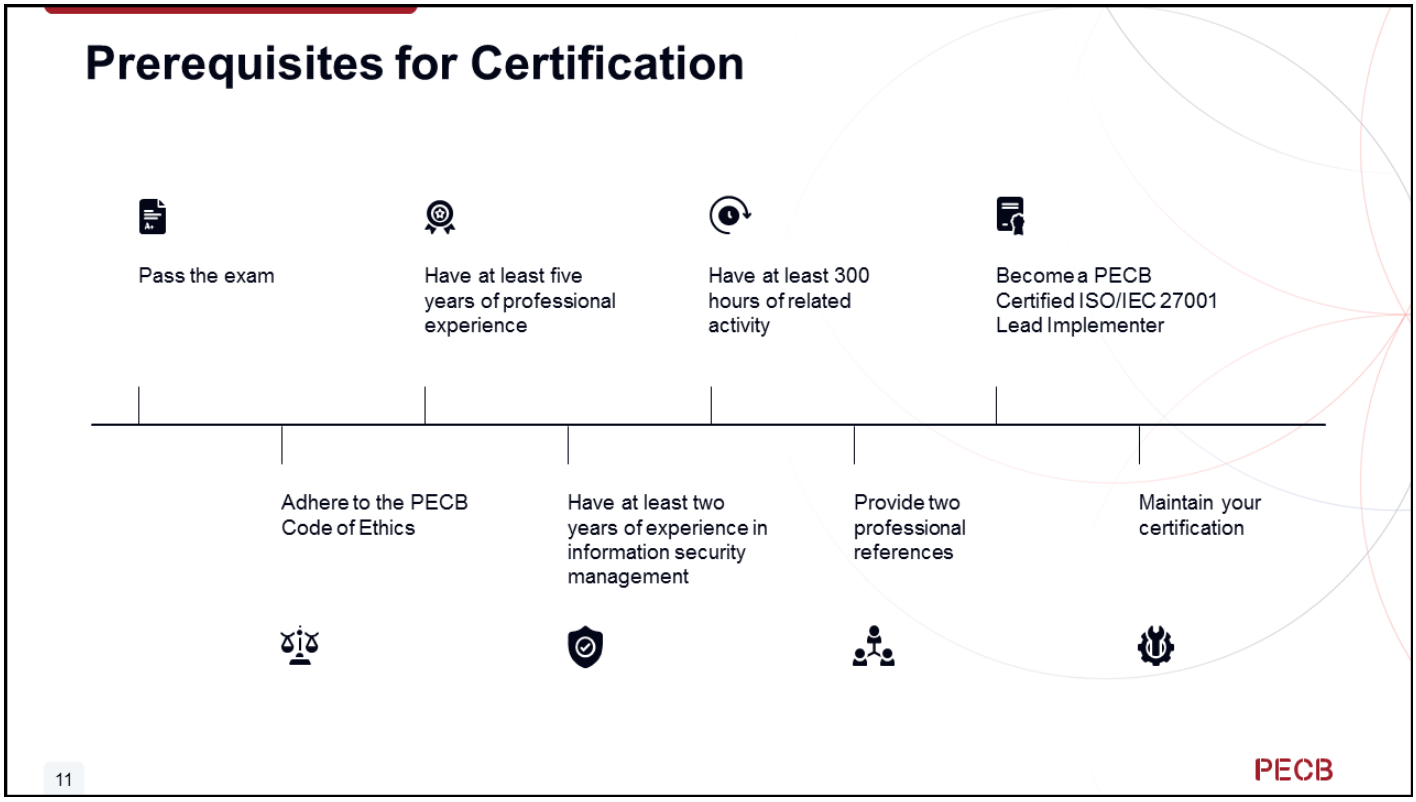
If participants wish to obtain more in-depth knowledge of an ISMS audit process, including the audit principles, techniques, and best practices, we recommend them to take the PECB Certified ISO/IEC 27001 Lead Auditor training course.



The purpose of the certification exam is to evaluate whether candidates have mastered the information security management concepts, methods, and techniques so that they are able to participate in information security project assignments.

The PECB Examination Committee ensures that the exam questions are adequate and based on professional practice.

All competency domains are covered in the exam. Please visit https://help.pecb.com/index.php/list-of-pecb-exams/ to find the ISO/IEC 27001 Lead Implementer candidate handbook and read a detailed description of each competency domain.



Individuals who do not meet all the prerequisites for certification cannot claim to be PECB ISO/IEC 27001 Lead Implementer-certified.

A less experienced candidate can apply for the “PECB Certified ISO/IEC 27001 Implementer” credential or “PECB Certified ISO/IEC 27001 Provisional Implementer” credential.

PECB certifications are valid for three years. In order to maintain and renew a certification, PECB certified professionals must comply with certain requirements.

The certification process, including its maintenance and renewal, will be explained in detail in the last day of this training course.

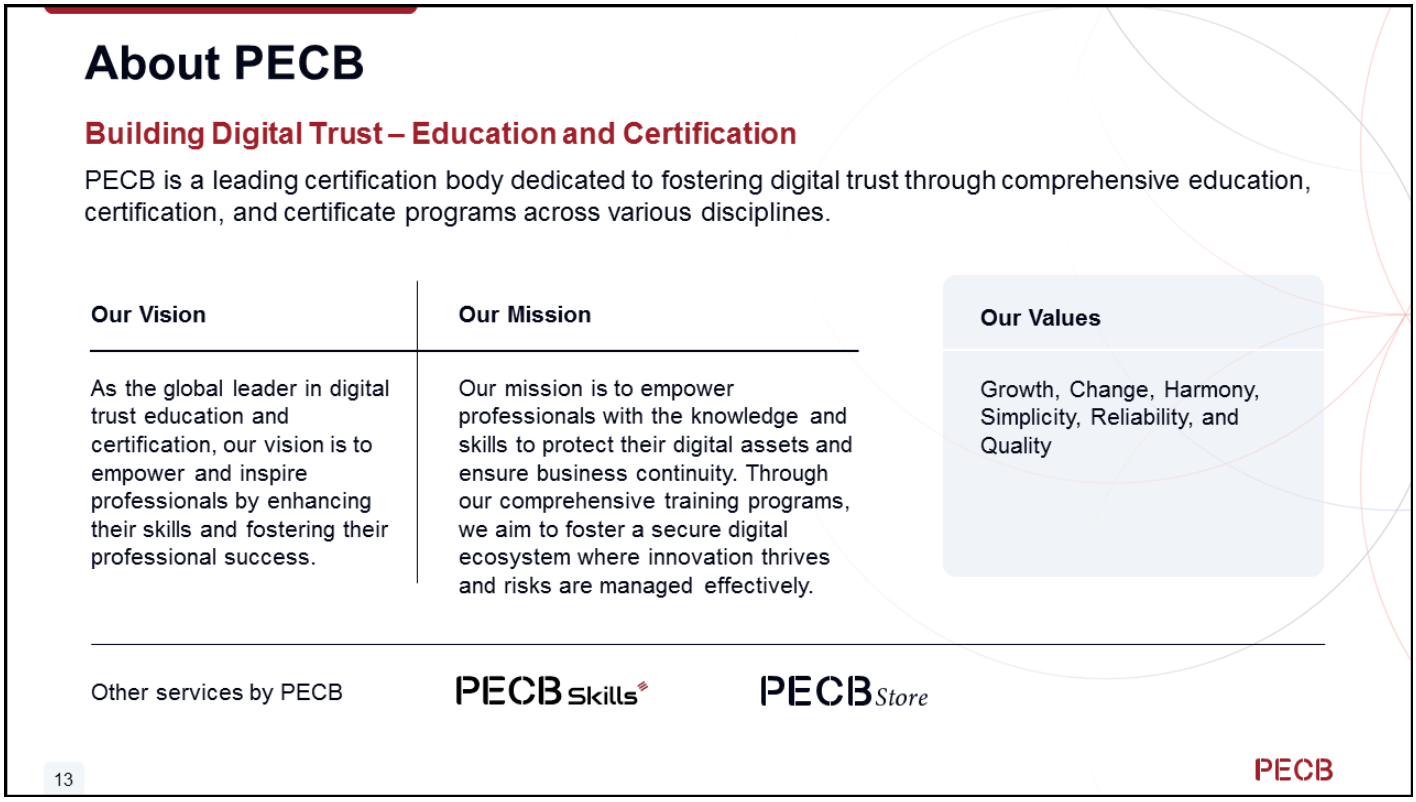
PECB Certificate

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

12

PECB

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



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.

PECB Digital Badges

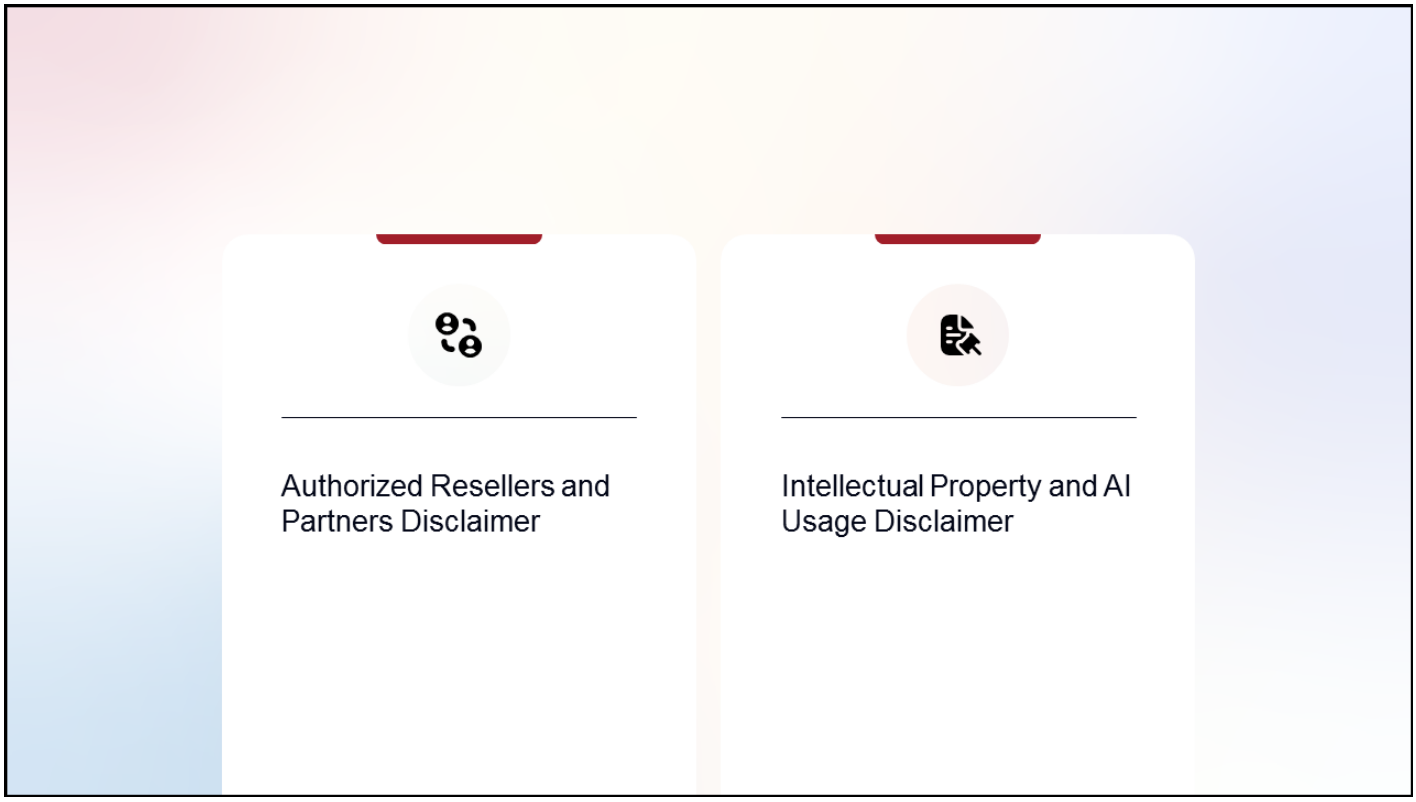
- Besides the certificate, PECB-certified professionals can also claim their digital badge on Credly through their PECB account.
- Digital badges contain shareable information about who has issued the badge, who has earned it, the criteria for earning the badge, issue and expiration date, and achievement evidence.
- Digital badges are a powerful online representation that allows professionals to demonstrate their knowledge and skills.
- PECB-certified individuals can easily and safely share their digital badges on social media platforms or add it to their resume and business cards.
- It is important to note that PECB-certified individuals can claim digital badges for all PECB certificates. All they need to do is to head to their PECB accounts. To learn more about this, please visit https://pecb.com/en/pecb-digital-badges.

14

PECB

Digital badges have many benefits; they enable individuals to:

- Demonstrate competence and commitment to the profession
- Show willingness to learn and develop in a profession
- Prove that they are up to date with the latest industry developments
- Obtain and utilize more career opportunities



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.

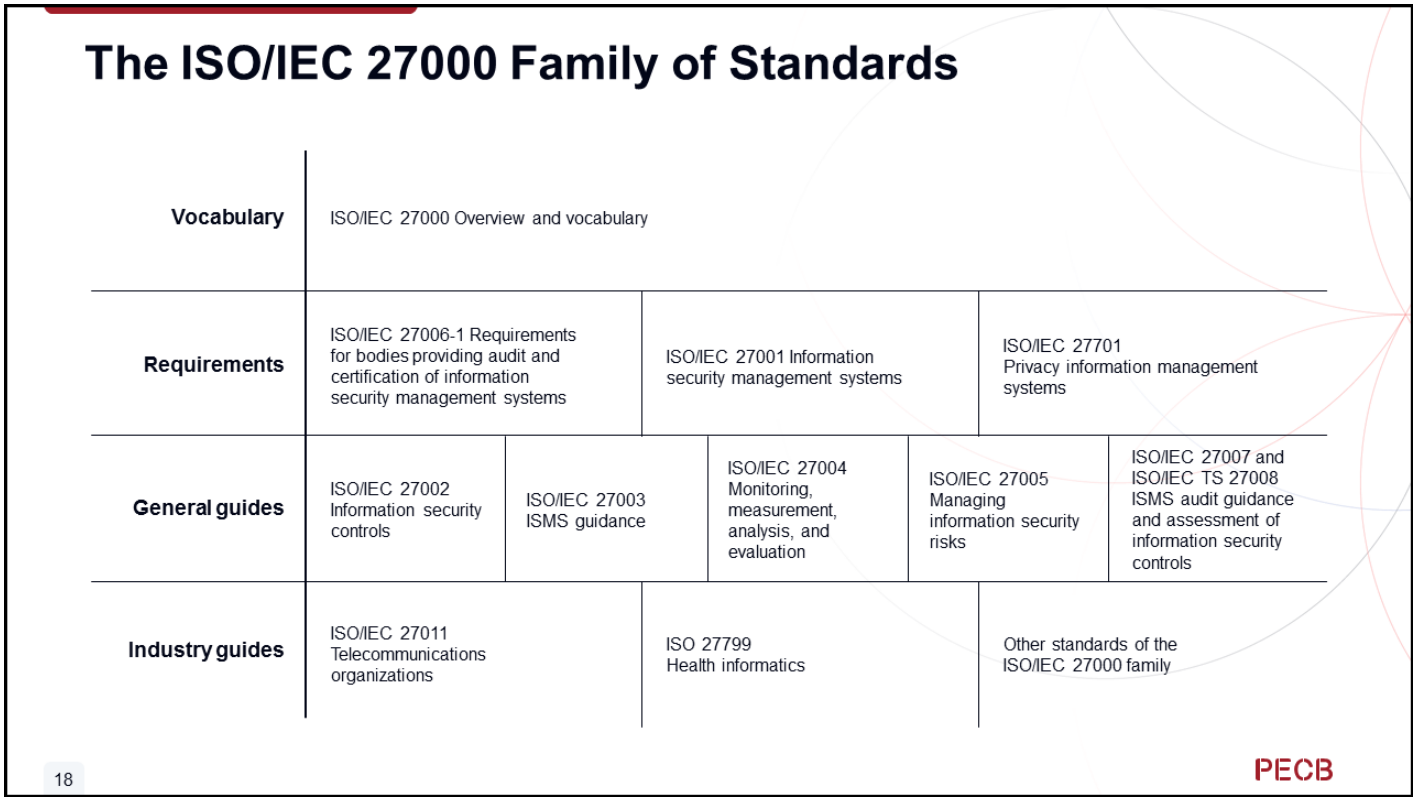
To ensure authenticity, please refer to PECB’s official website (https://pecb.com/en/partner/active_partners) or contact PECB’s customer service to confirm the status of a reseller. Any suspicious activity or counterfeit offers should be reported to PECB immediately to facilitate prompt investigation 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 Disclaimer:

PECB 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.

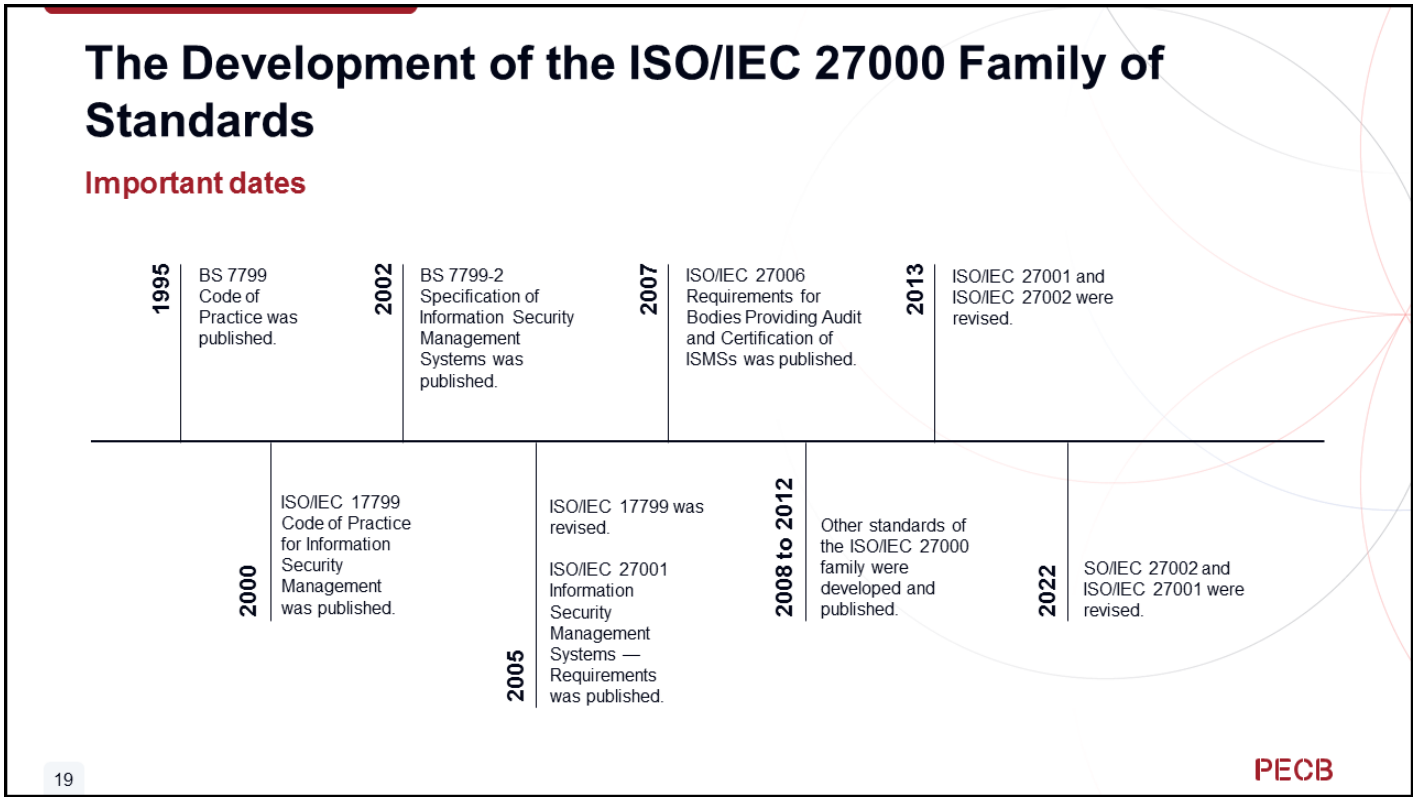
This section introduces the International Organization for Standardization (ISO) and ISO/IEC 27001. The advantages of having an ISMS in place are also discussed.



The ISO 27000 family includes the following standards:

- **ISO/IEC 27000** provides the overview of ISMS. It also provides terms and definitions commonly used in the ISMS family of standards. A free copy of this standard can be downloaded on the ISO website.
- **ISO/IEC 27001** specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS.
- **ISO/IEC 27701** specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a privacy information management system (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management.
- **ISO/IEC 27006-1** specifies general requirements for bodies providing ISMS audit and certification services.
- **ISO/IEC 27002** provides a reference set of generic information security controls including implementation guidance.
- **ISO/IEC 27003** provides explanation and guidance on ISO/IEC 27001.
- **ISO/IEC 27004** provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an ISMS in order to fulfill the requirements of ISO/IEC 27001, clause 9.1.
- **ISO/IEC 27005** provides guidelines for information security risk management.
- **ISO/IEC 27007** provides guidance on managing an ISMS audit program, conducting audits, and the competence of ISMS auditors.
- **ISO/IEC TS 27008** provides guidance on reviewing and assessing the implementation and operation of information security controls.
- **ISO/IEC 27011** provides guidelines supporting the implementation of information security controls in telecommunications organizations.
- **ISO 27799** provides guidelines for organizations in the health informatics industry in implementing the controls provided in ISO/IEC 27002.

Source: https://www.iso.org

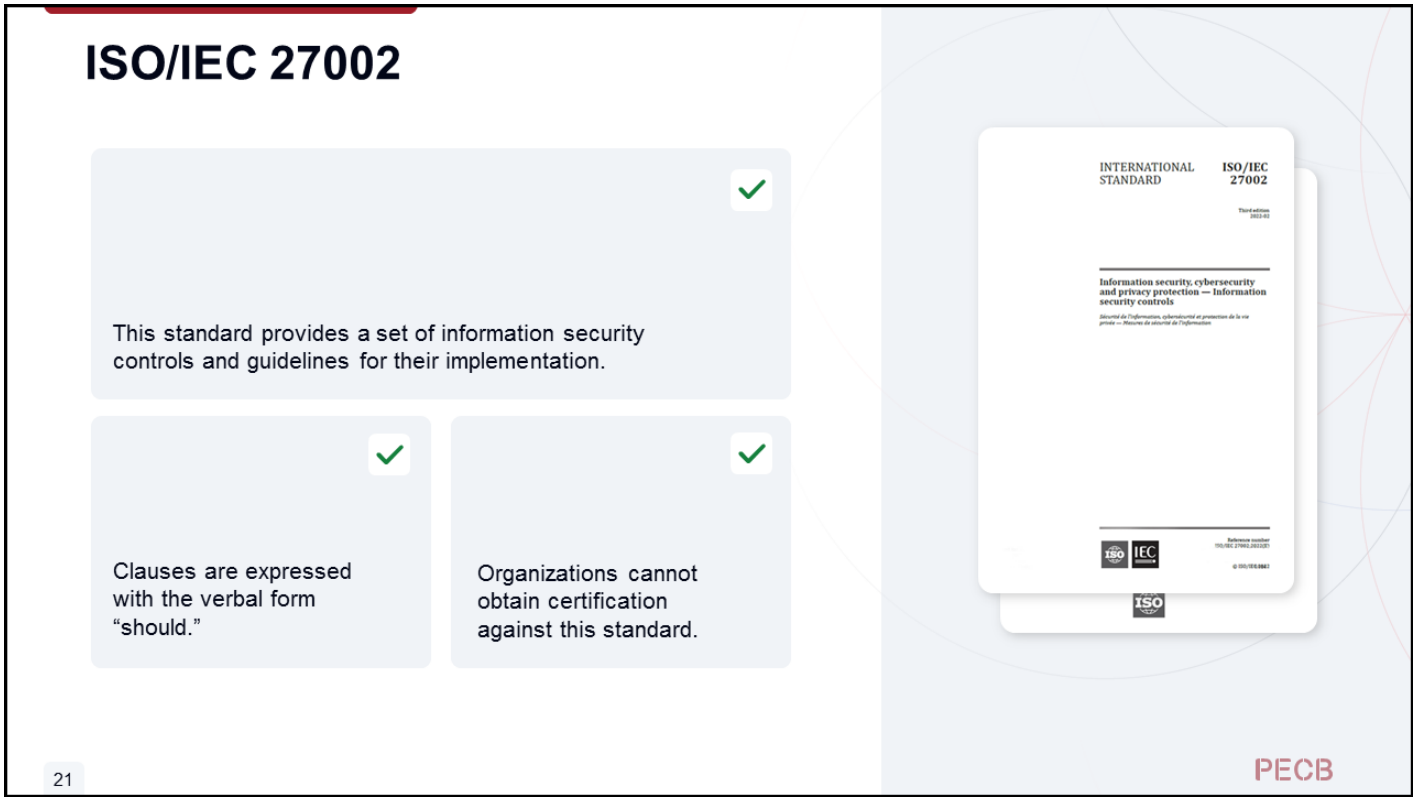


The history behind the development of the standards pertaining to the ISO/IEC 27000 family:

- 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, clause 0.1 General

This document 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.

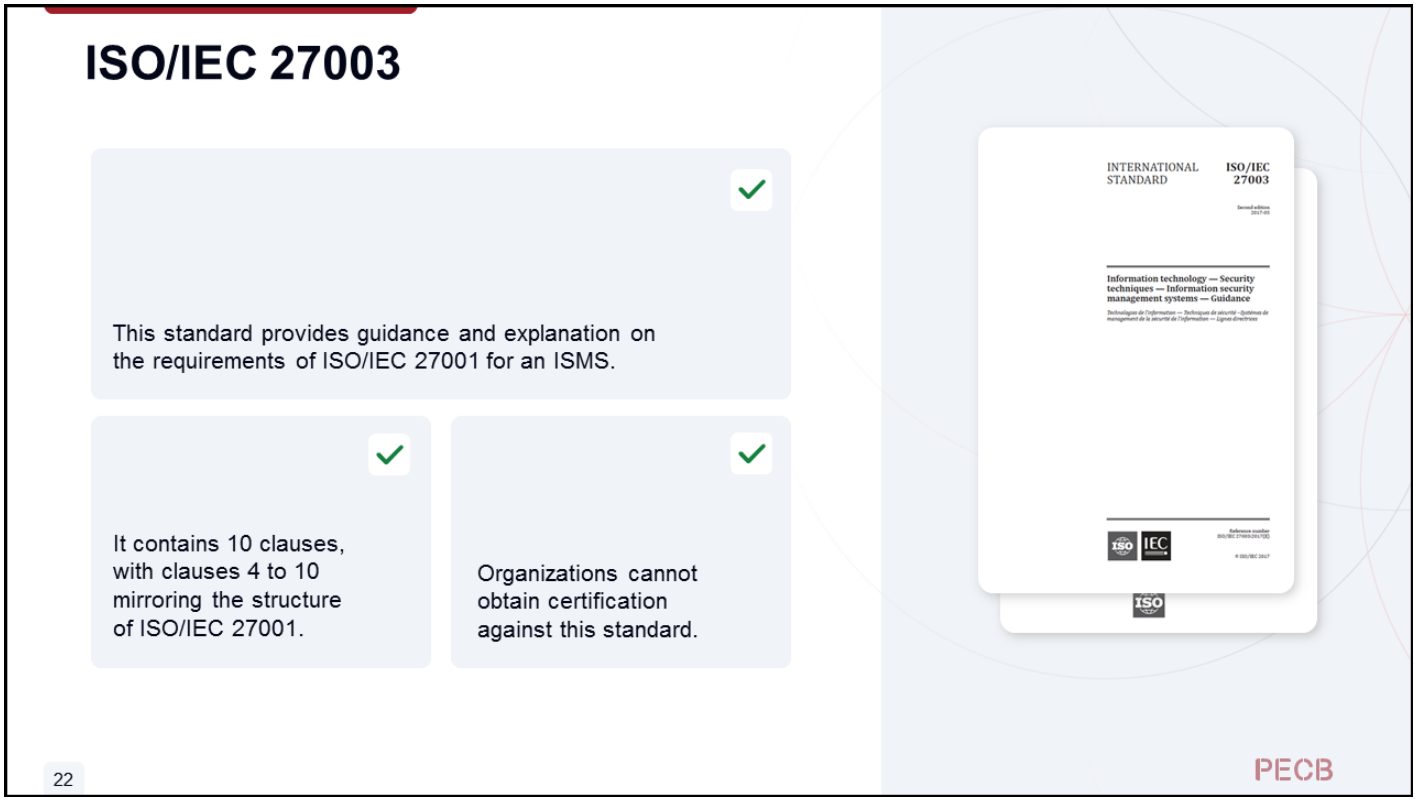


Important note: Information security controls provided in Annex A of ISO/IEC 27001 are aligned with ISO/IEC 27002 controls.

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:

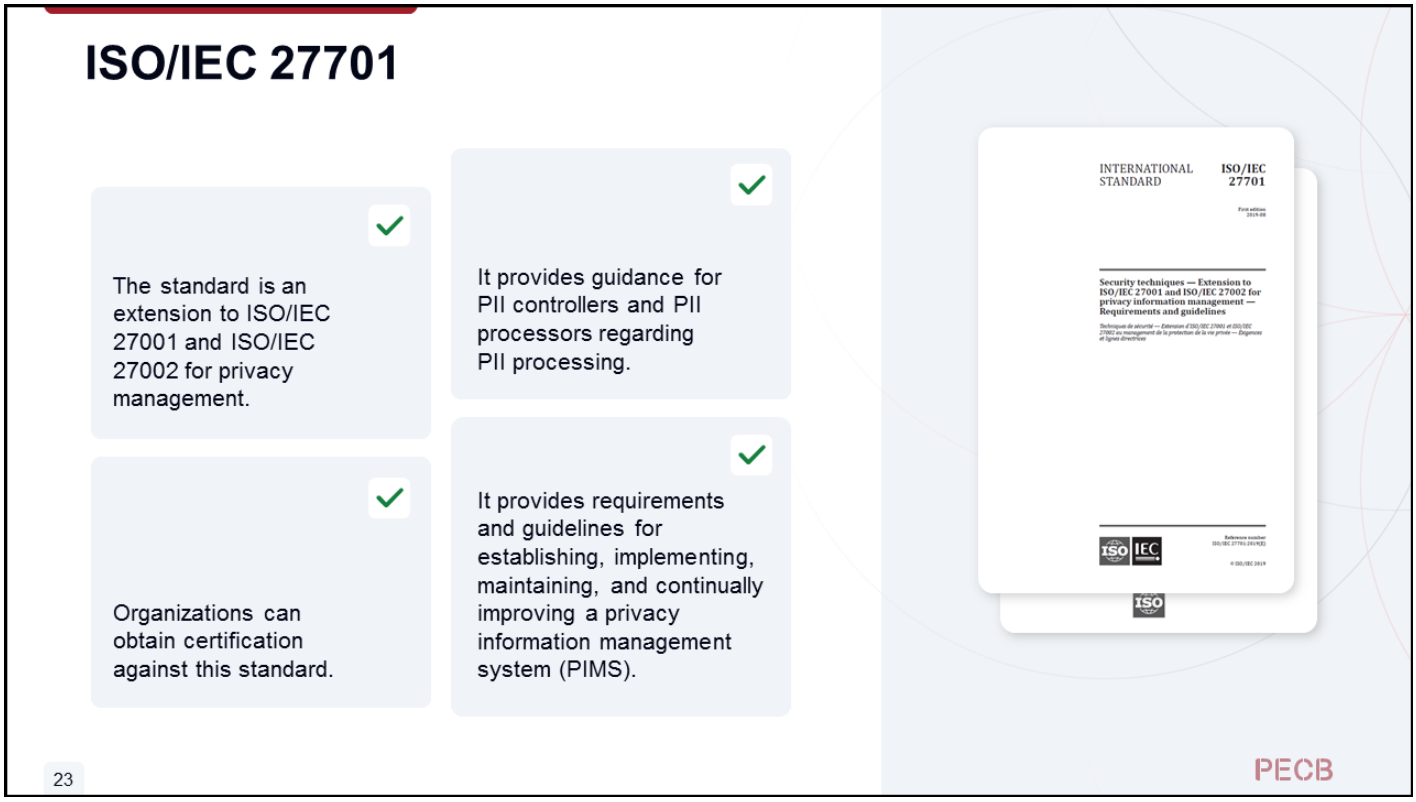
a. *within the context of an information security management system (ISMS) based on ISO/IEC 27001;*
b. *for implementing information security controls based on internationally recognized best practices;*
c. *for developing organization-specific information security management guidelines.*



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.

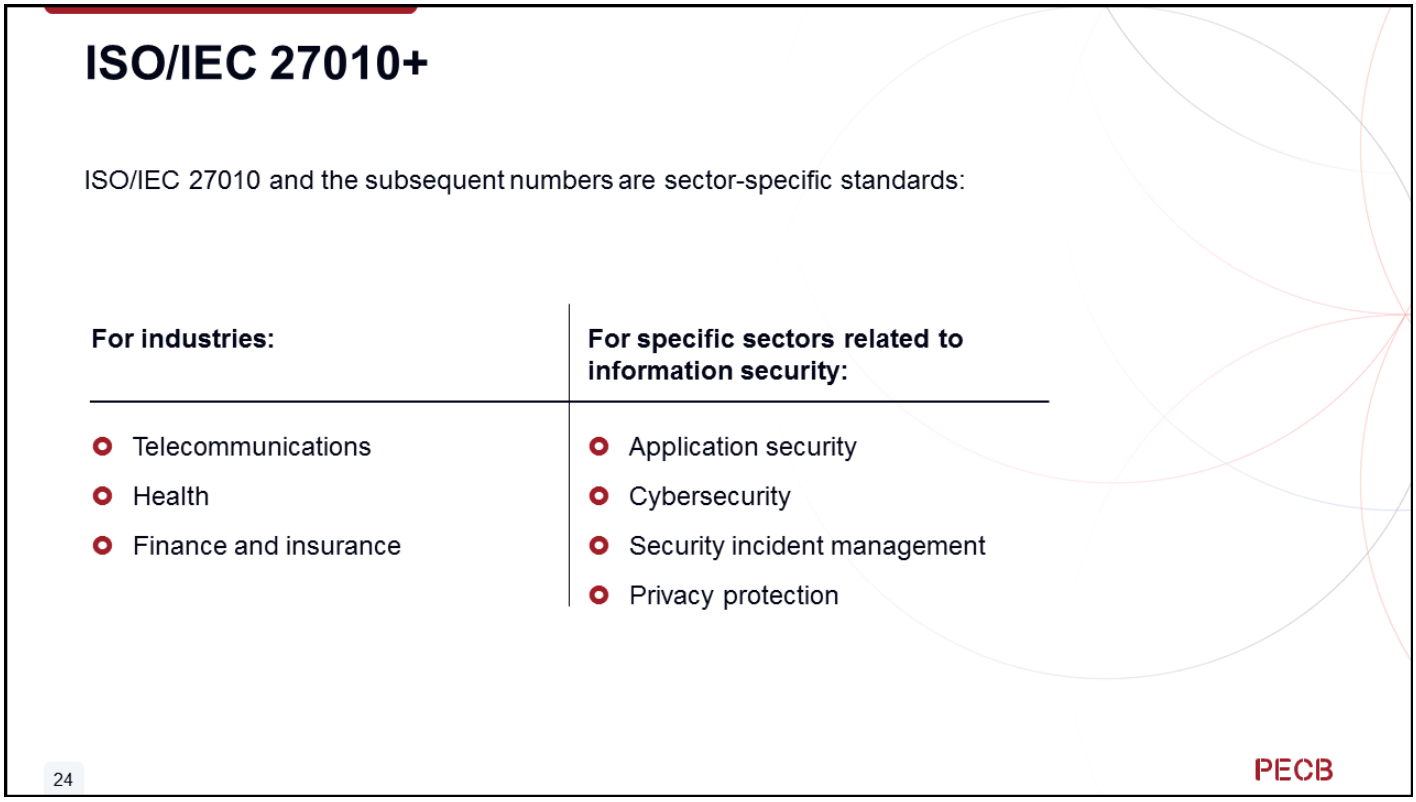


ISO/IEC 27701, clause 1 Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

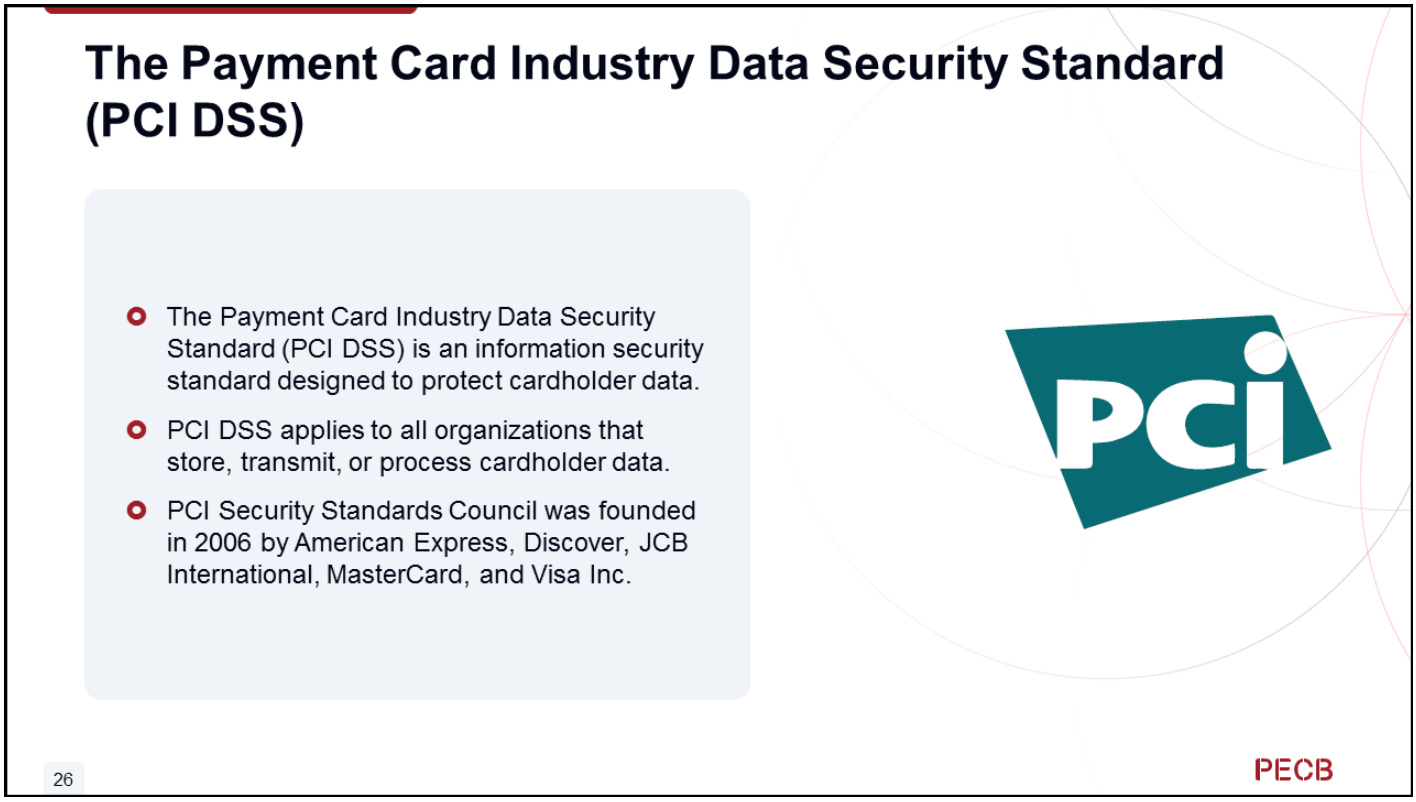


Some of these standards include:

- ISO/IEC 27010:2015, Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011:2016, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
- ISO/IEC 27013:2021, Information security, cybersecurity and privacy protection – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014:2020, Information security, cybersecurity and privacy protection – Governance of information security
- ISO/IEC TR 27015:2012, Information technology – Security techniques – Information security management guidelines for the financial services
- ISO/IEC TR 27016:2014, Information technology – Security techniques – Information security management – Organizational economics
- ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27031:2011, Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032:2023, Cybersecurity – Guidelines for internet security
- ISO/IEC 27033-1:2015, Information technology – Security techniques – Network security – Part 1: Overview and concepts
- ISO/IEC 27034-1:2011, Information technology – Security techniques – Application security – Part 1: Overview and concepts
- ISO/IEC 27035-1:2023, Information technology – Information security incident management – Part 1: Principles and process
- ISO/IEC 27036-1:2021, Cybersecurity – Supplier relationships – Part 1: Overview and concepts
- ISO/IEC 27037:2012, Information technology – Security techniques – Guidelines for identification, collection, or acquisition and preservation of digital evidence

Slide Notes Extension

- ISO/IEC 27038:2014, Information technology – Security techniques – Specification for digital redaction
- ISO/IEC 27039:2015, Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)
- ISO/IEC 27040:2015, Information technology – Security techniques – Storage security
- ISO/IEC 27041:2015, Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method
- ISO/IEC 27042:2015, Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043:2015, Information technology – Security techniques – Incident investigation principles and processes
- ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework



PCI DSS seeks to establish and maintain secure network and systems, ensure the security of cardholder data, establish a vulnerability management program, implement access controls, control and assess networks at planned intervals, and establish an information security policy.

PCI DSS consists of the following 12 requirements:

1. Implement and sustain network security measures
2. Avoid default configurations for system components
3. Safeguard stored account data
4. Implement encryption to secure cardholder data during transmission
5. Defend systems and network from malicious software
6. Establish and sustain secure systems and software
7. Limit access to system components and cardholder data based on business necessity
8. Employ user identification and authentication measures for system component access
9. Implement measures to control physical access to cardholder data
10. Monitor access to network components and cardholder data
11. Regularly assess and test the security of systems and networks
12. Establish an information security policy and make it available to the personnel

STAR consists of two main levels of assessment. Level 1 assessments are self-assessments of security and privacy which organizations can conduct themselves. Level 2 assessments are independent third party audits.

The STAR program enables cloud service customers to learn more about the level of security and privacy of cloud service providers. Cloud service providers, on the other hand, can use the program to improve and communicate their security posture and build customer trust.

The CSA STAR Certification is an independent third party assessment of the security of a cloud service provider. Organizations that undergo ISO/IEC 27001 certification can simultaneously undergo CSA STAR assessment and obtain the CSA STAR certification. CSA STAR guidelines are relevant, among others, for the following:

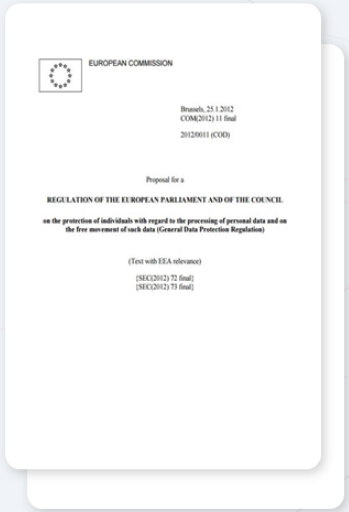
- Cloud service providers
- Data center hosting companies
- Web hosting companies
- Finance and health care service providers

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/

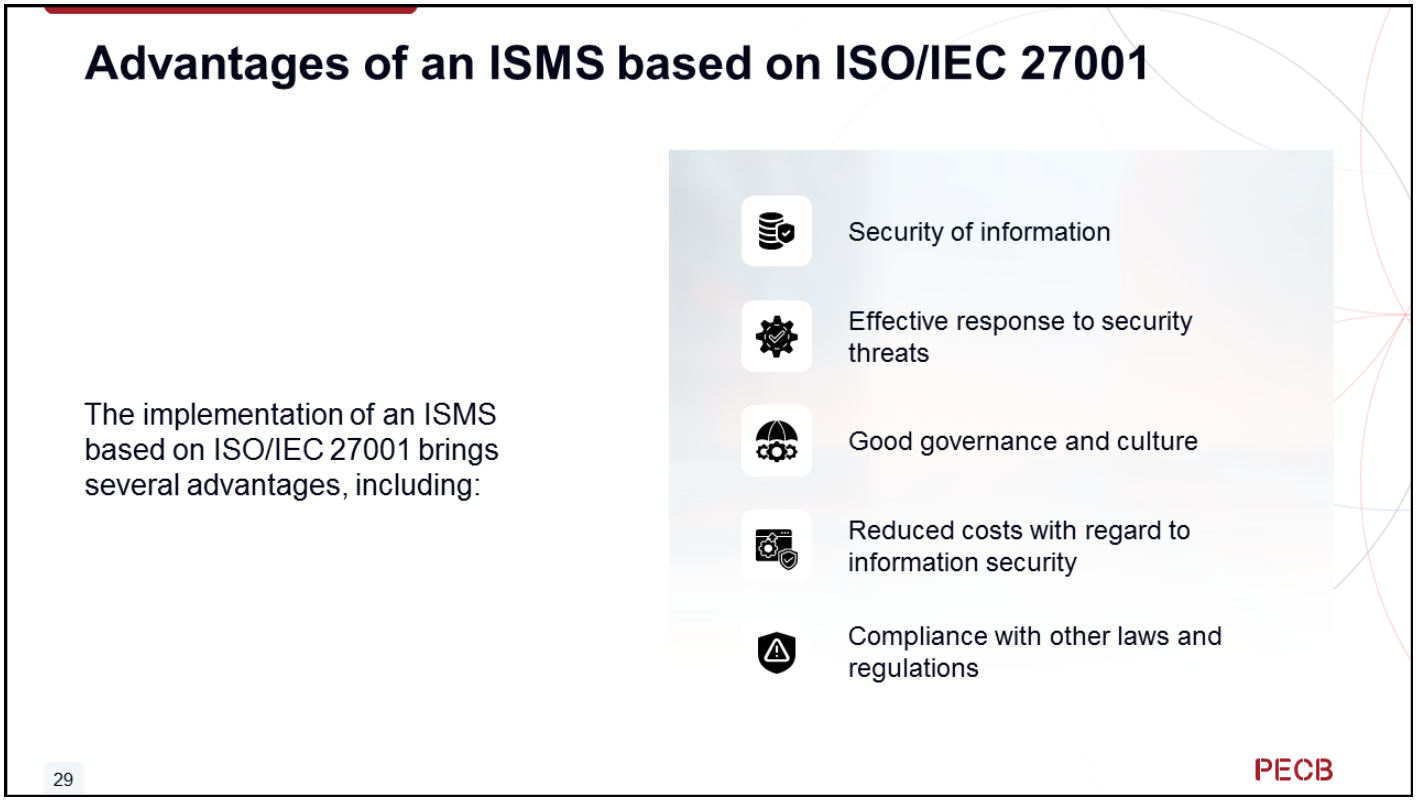
ISO/IEC 27001:2022 is the leading international standard for information security. Thus, the ISO/IEC 27001:2022 framework can be used to support compliance with the GDPR. Furthermore, ISO/IEC 27001:2022 and the GDPR overlap in many areas, such as data confidentiality, availability, and integrity, as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



28

PECB

The regulation has been in effect since May 25, 2018. It enforces severe fines for noncompliance with its privacy and security standards, with potential penalties amounting to tens of millions of euros.



1. **Security of information:** ISO/IEC 27001 provides requirements that address the security of all information, regardless of the format (digital or hard copy) or the place where the information is stored.
2. **Effective response to security threats:** ISO/IEC 27001 lists several controls that aim to prevent, address, and respond to the existing and any arising risks that may threaten the security of information.
3. **Good governance and culture:** ISO/IEC 27001 provides specific requirements for the top management of organizations and holds them accountable for information security. In addition, the standard requires to provide awareness sessions and empower the personnel with regard to information security. This enables the organization to establish a culture where everyone within the organization understands security risks and embraces their information security responsibilities.
4. **Reduced costs with regard to information security:** ISO/IEC 27001 requires organizations to conduct risk assessments at planned intervals. As such, organizations identify, evaluate, and treat information security risks in a timely manner. This prevents information security incidents which can be very costly to organizations.
5. **Compliance with other laws and regulations:** ISO/IEC 27001 overlaps with several laws and regulations. As such, organizations that meet the requirements of ISO/IEC 27001 ensure partial compliance with several other regulations (e.g., GDPR, PCI DSS).

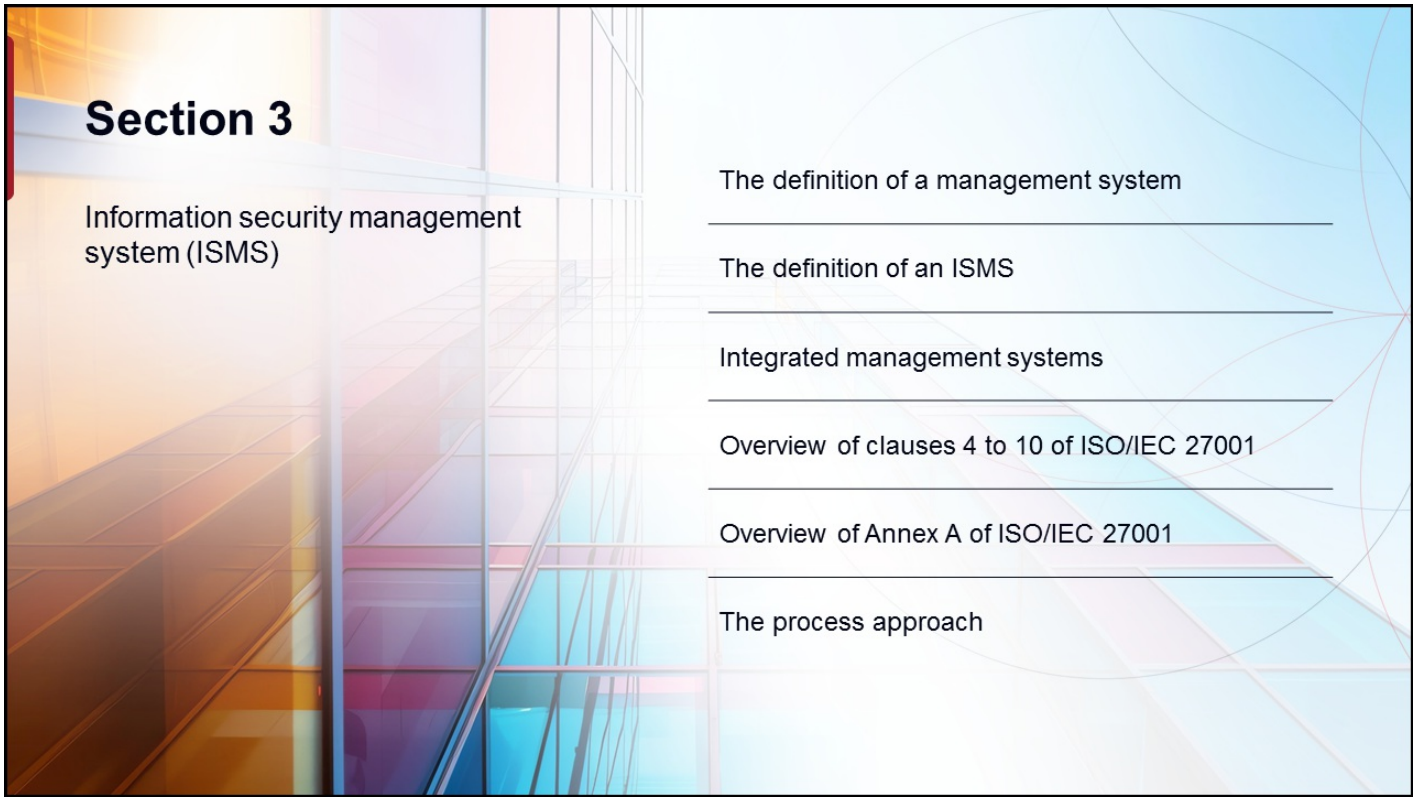
Section 2 Summary

- The ISO/IEC 27000 family of standards addresses information security.
- ISO/IEC 27001 specifies requirements for establishing, implementing, maintaining, and improving an ISMS.
- ISO/IEC 27002 provides a set of information security controls and guidelines for their implementation.
- ISO/IEC 27003 provides guidance and explanation on the requirements of ISO/IEC 27001 for an ISMS.
- ISO/IEC 27701 provides requirements and guidelines for establishing, implementing, maintaining, and continually improving a PIMS.
- The effective implementation of ISO/IEC 27001 requirements ensures the security of all information, effective response to information security threats, good governance and culture, reduced costs with regard to information security, compliance with other laws and regulations, etc.

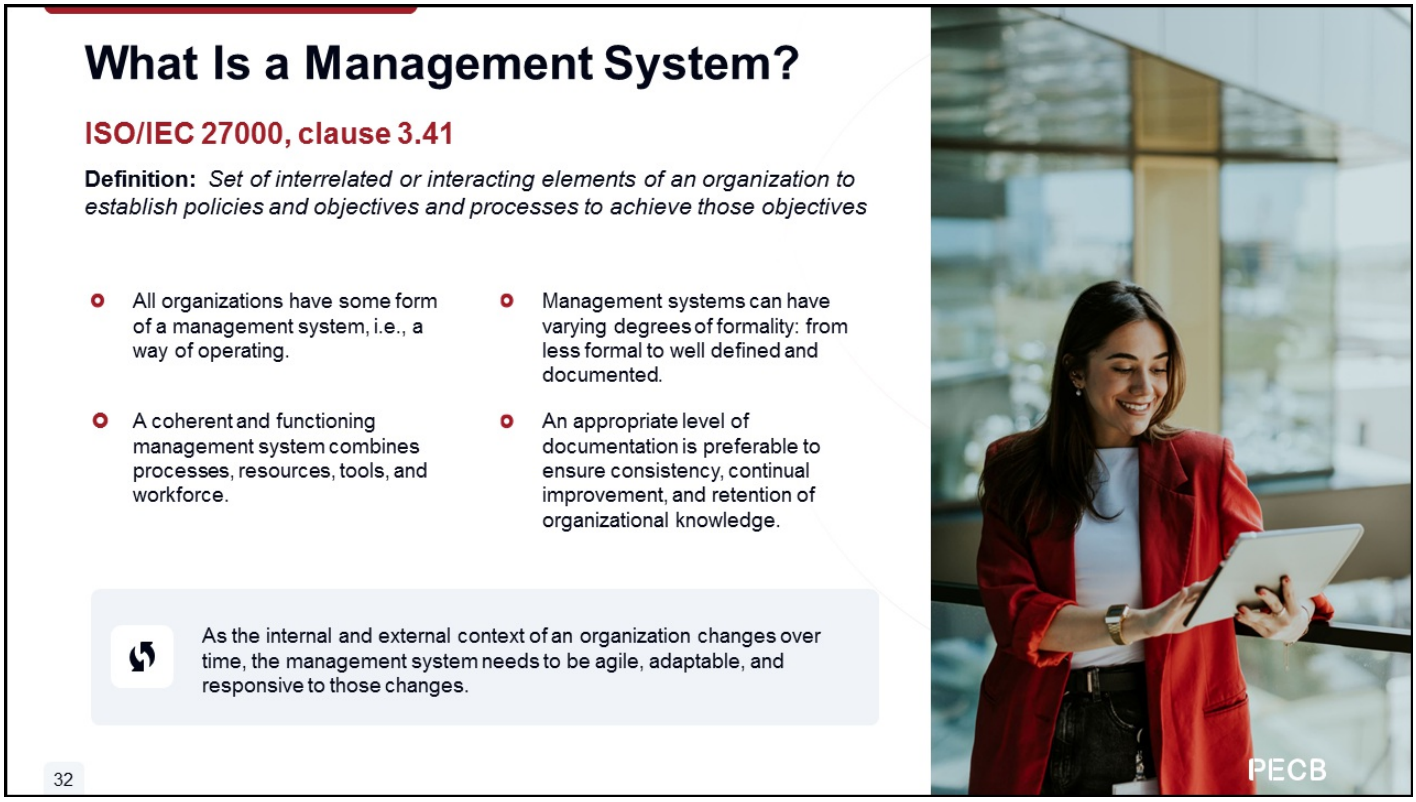
Questions?

Quiz 1

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



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



ISO/IEC 27000, clause 3.41 Management system (cont'd)

- *Note 1 to entry: A management system can address a single discipline or several disciplines.*
- *Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.*
- *Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.*

Organizations implement management systems to improve their operations and enhance their business performance, while also increasing customer satisfaction. An organization may have several management systems in place, such as a quality management system, information security management system, business continuity management system, etc.

Note: What is implemented must be controlled and measured, and what is controlled and measured must be managed. The "Performance evaluation" clause is an essential component of any management system because without the evaluation of the effectiveness of processes and controls in place, it is impossible to check if the organization has reached its objectives.

What Is an Information Security Management System?

ISO/IEC 27000, clause 4.2.1

Definition: *An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.*

It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

An ISMS is a systematic approach for:

- Establishing
- Reviewing
- Implementing
- Maintaining
- Operating
- Improving
- Monitoring

an organization's information security to achieve business objectives.

33

PECB

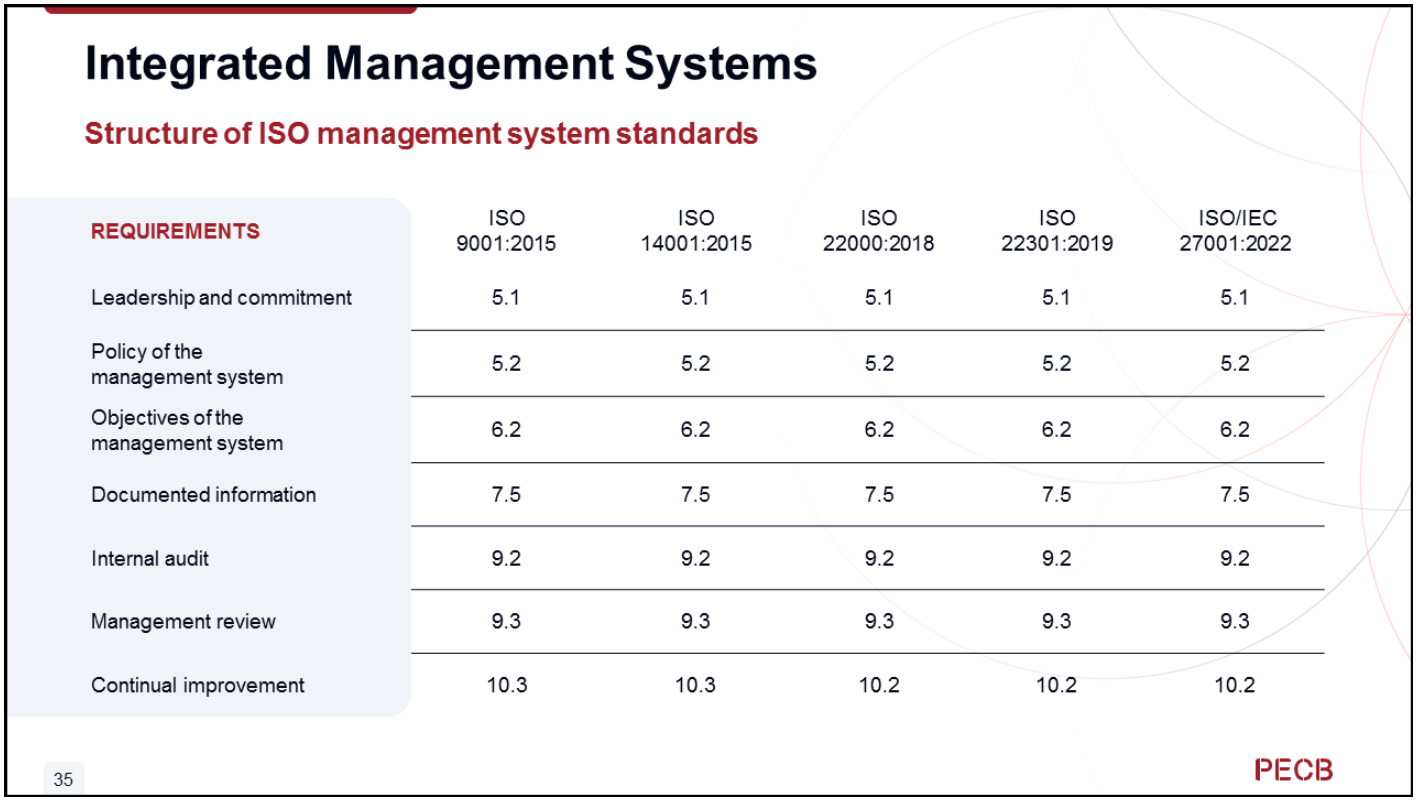
The ISMS consists of measures and controls that ensure the minimization of information security risks and the enhancement of information security. An organization with an effective ISMS in place takes into consideration information security in all its procedures, policies, and activities.

ISO 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.

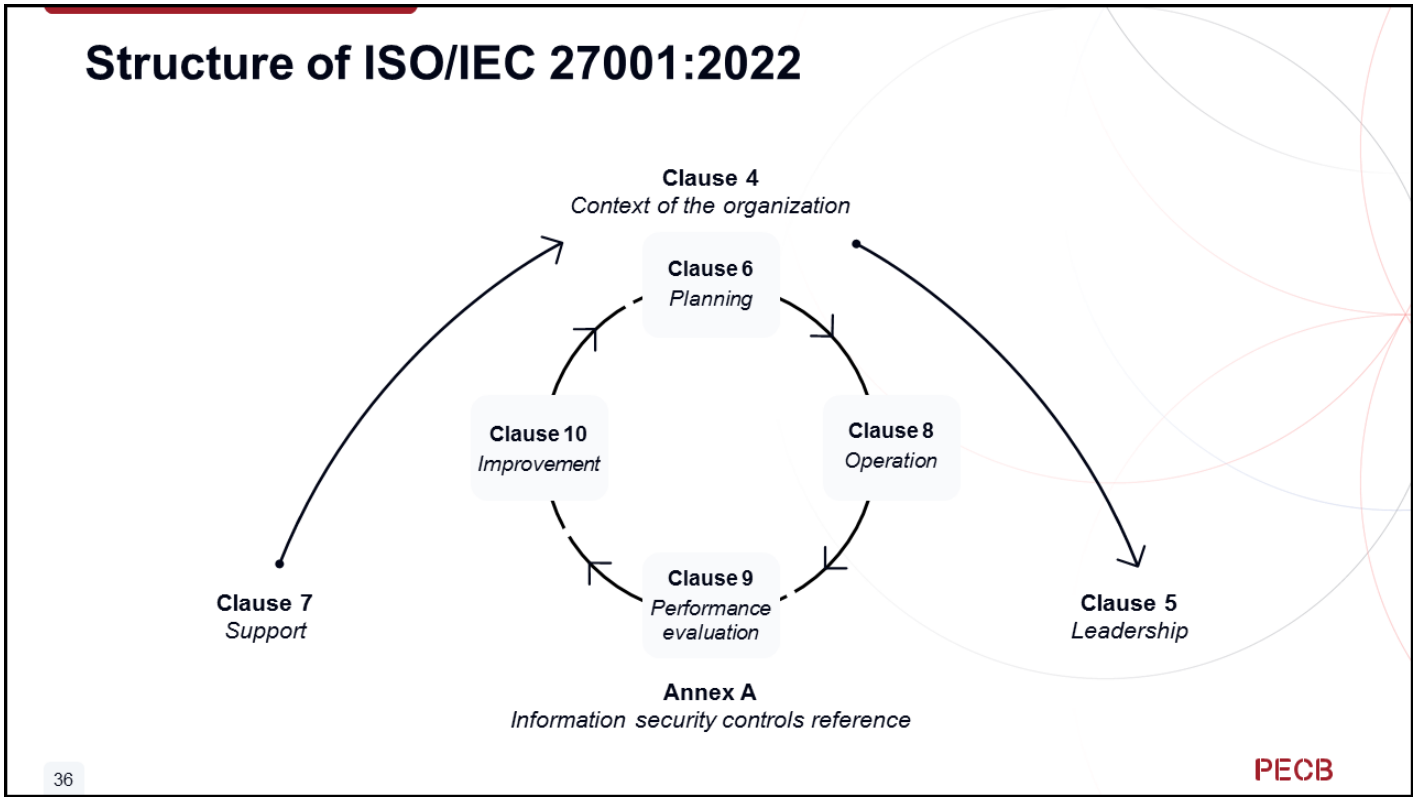
If you would like to purchase any of the standards, PECB offers discounted prices to all trainees that purchase them via https://store.pecb.com.



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



ISO/IEC 27001, clause 1 Scope

Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

Context of the Organization – Overview

ISO/IEC 27001, clause 4

- Clause 4.1 *Understanding the organization and its context* – The organization must identify the internal and external factors that are relevant to its purpose and can affect the achievement of the ISMS objectives, including determining whether climate change is a relevant issue.
- Clause 4.2 *Understanding the needs and expectations of interested parties* – The organization must determine the interested parties relevant to the ISMS and their information security requirements. This clause also requires organizations to take into consideration the other relevant requirements of interested parties that need to be addressed by the ISMS, including requirements related to climate change.
- Clause 4.3 *Determining the scope of the information security management system* – The organization must establish the ISMS scope by determining its boundaries and applicability. The scope must be available as documented information.
- Clause 4.4 *Information security management system* – The organization must establish, implement, maintain, and continually improve an ISMS based on the requirements of the standard.

PECB

Leadership – Overview

ISO/IEC 27001, clause 5

- Clause 5.1 *Leadership and commitment* – The top management must ensure that the ISMS is compatible with the organization's strategic orientation. The top management must ensure the integration of the ISMS requirements into the organization's business processes, determine the necessary resources for the ISMS, ensure that the ISMS achieves the objectives, promote continual improvement, and support the employees who hold information security responsibilities.
- Clause 5.2 *Policy* – The top management must establish an information security policy that is appropriately available and communicated to all interested parties. The policy must be aligned with the purpose of the organization and must 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* – The top management must appropriately assign and communicate information security roles and responsibilities. The assigned individuals must ensure that the ISMS conforms to the requirements of ISO/IEC 27001 and must report on the ISMS performance to the top management.

PECB

Planning – Overview

ISO/IEC 27001, clause 6

- Clause 6.1 *Actions to address risks and opportunities* – The organization must determine the risks and opportunities to ensure that the ISMS achieves its objectives, prevent or minimize undesired effects, and ensure continual improvement. The organization must plan actions to address risks and opportunities, implement those actions, and evaluate their effectiveness. The organization must also apply an information security risk assessment and risk treatment process.
- Clause 6.2 *Information security objectives and planning to achieve them* – The organization must establish information security objectives that are measurable and consistent with the information security policy. They must also be aligned with the applicable information security requirements, and the results of the risk assessment and risk treatment processes. The objectives must be appropriately communicated, and updated.
- Clause 6.3 *Planning of changes* – The organization must determine the need for changes to the ISMS and implement those changes in a planned manner.

PECB

Support – Overview

ISO/IEC 27001, clause 7

- Clause 7.1 *Resources* – The organization must determine and provide the necessary resources to establish, implement, maintain, and continually improve the ISMS.
- Clause 7.2 *Competence* – The organization must determine and ensure the competence of persons who affect the information security performance.
- Clause 7.3 *Awareness* – The organization must 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 must establish, implement, and maintain arrangements for communication with relevant external and internal interested parties.
- Clause 7.5 *Documented information* – The organization's ISMS must include documented information required by ISO/IEC 27001 and other documented information that demonstrate the effectiveness of the ISMS. The organization must create, update, and control such documented information.

PECB

Operation – Overview

ISO/IEC 27001, clause 8

- Clause 8.1 *Operational planning and control* – The organization must plan, implement, and control the necessary processes to comply with the standard's requirements. The organization must 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 must conduct information security risk assessments at planned intervals and must keep documented information of the risk assessment results.
- Clause 8.3 *Information security risk treatment* – The organization must implement the information security risk treatment plan and must keep documented information on risk treatment results.

PECB

Performance Evaluation – Overview

ISO/IEC 27001, clause 9

- Clause 9.1 *Monitoring, measurement, analysis and evaluation* – The organization must evaluate the performance and effectiveness of the ISMS and keep documented information as evidence of the monitoring and measurement outputs.
- Clause 9.2 *Internal audit* – The organization must conduct internal audits at planned intervals in order to validate whether the ISMS is effective and continues to fulfill the organization's own requirements as well as the standard requirements.
- Clause 9.3 *Management review* – The top management must review the ISMS at planned intervals in order to ensure its suitability, adequacy and effectiveness. The organization must keep documented information as evidence of the management review outputs.

PECB

Improvement – Overview

ISO/IEC 27001, clause 10

- Clause 10.1 *Continual improvement* – The organization must 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 must take the appropriate actions when a nonconformity occurs. It must evaluate and implement those actions, review their effectiveness and, if necessary, make changes. The organization must also keep documented information as evidence of the results of corrective actions.

PECB

Annex A

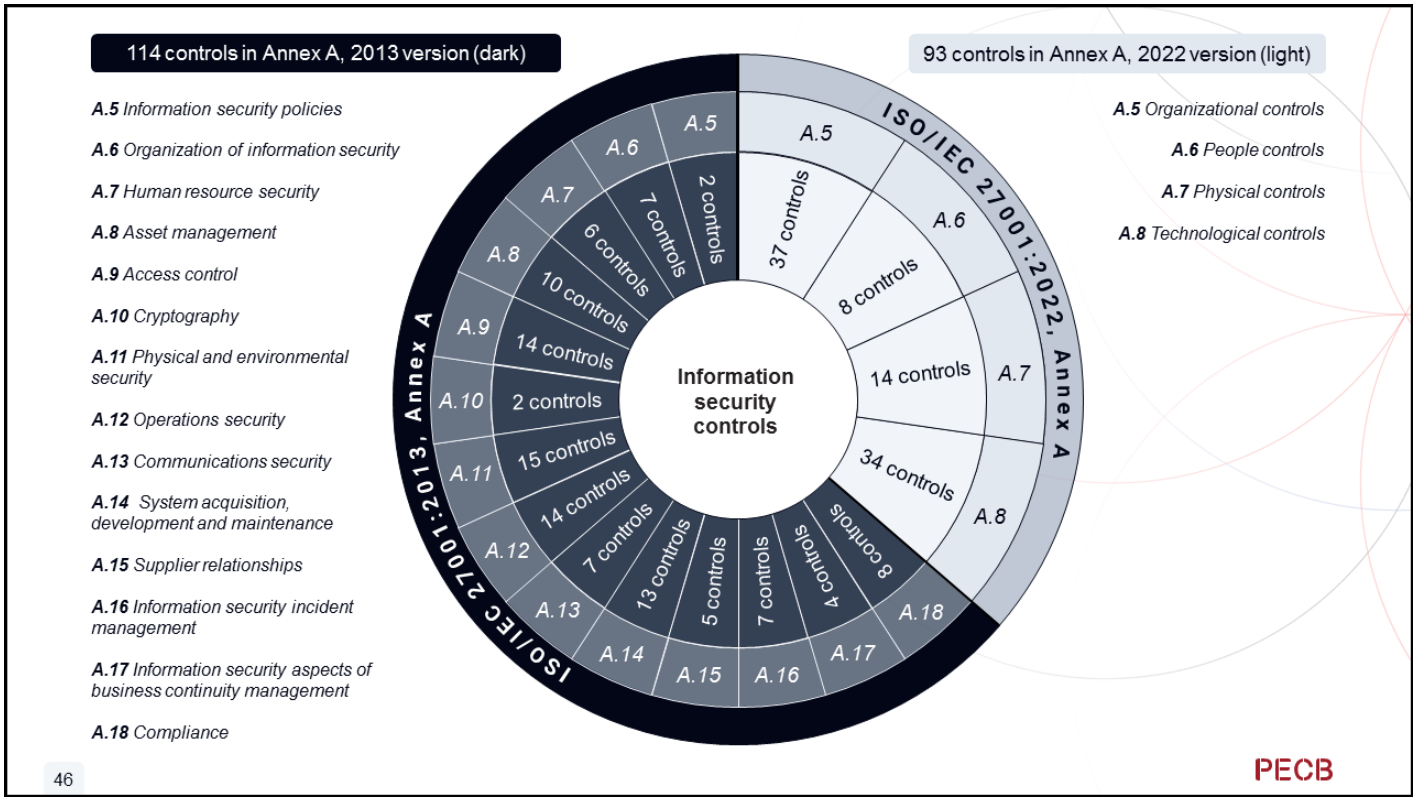
- Annex A is part of ISO/IEC 27001 and it contains 93 controls that should be considered when intending to comply with the standard.

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

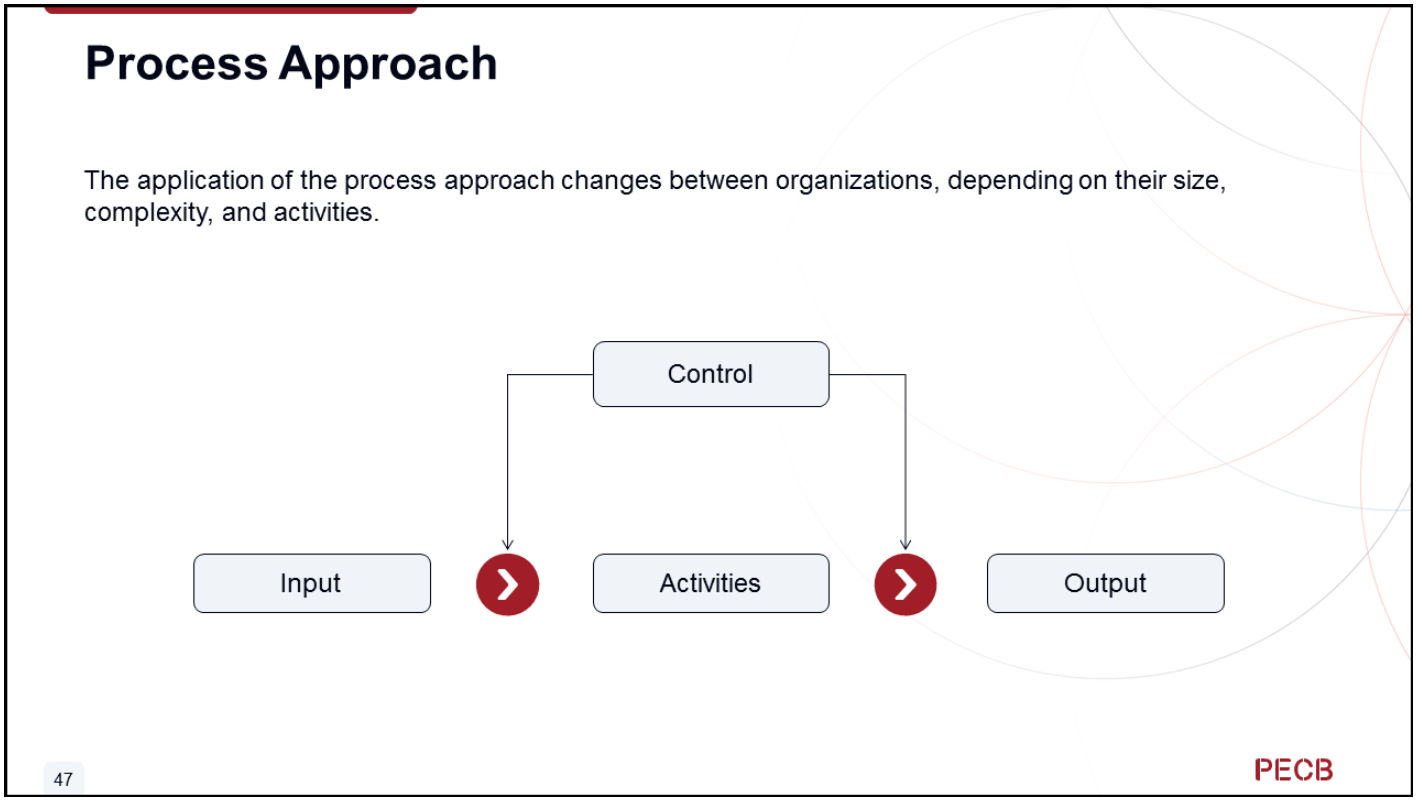
- If a certain control is not applicable, the organization should provide an acceptable justification for its exclusion.

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.



PECB



A process can be defined as a logical group of interrelated tasks performed to reach a defined objective. It is a sequence of structured and measured activities designed to create a product or service for a specific purpose, typically for a market sector or a particular client.

For an organization to function effectively, it must implement and manage numerous interrelated and interactive processes. Often, the output element of a process directly forms the input element to the next process. The identification and orderly management of processes within an organization, especially the interactions of these processes, is called “process approach.”

Controls are used to ensure that the conduct of the business processes is performed in a secure manner in terms of information processing. These security processes and controls are dependent on the business processes because they are part of them.

For example, security measures relating to human resources should be integrated into an organization’s existing processes for human resources management. This will allow the human resources management processes to be more secure, ensuring that:

- The organization has clearly defined everyone’s responsibilities in terms of information security.
- Background checks of applicants are performed according to the criticality of the information they will have to process.
- The organization has a formal disciplinary process in case of information security breaches.
- The organization has a formal process for removing the access rights from employees who leave the organization.

Note: To complete Exercise 1 and Quiz 2, please go to the Exercises Worksheet and Quizzes Worksheet respectively.

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, information security controls, cybersecurity, and information privacy.

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

50

PECB

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

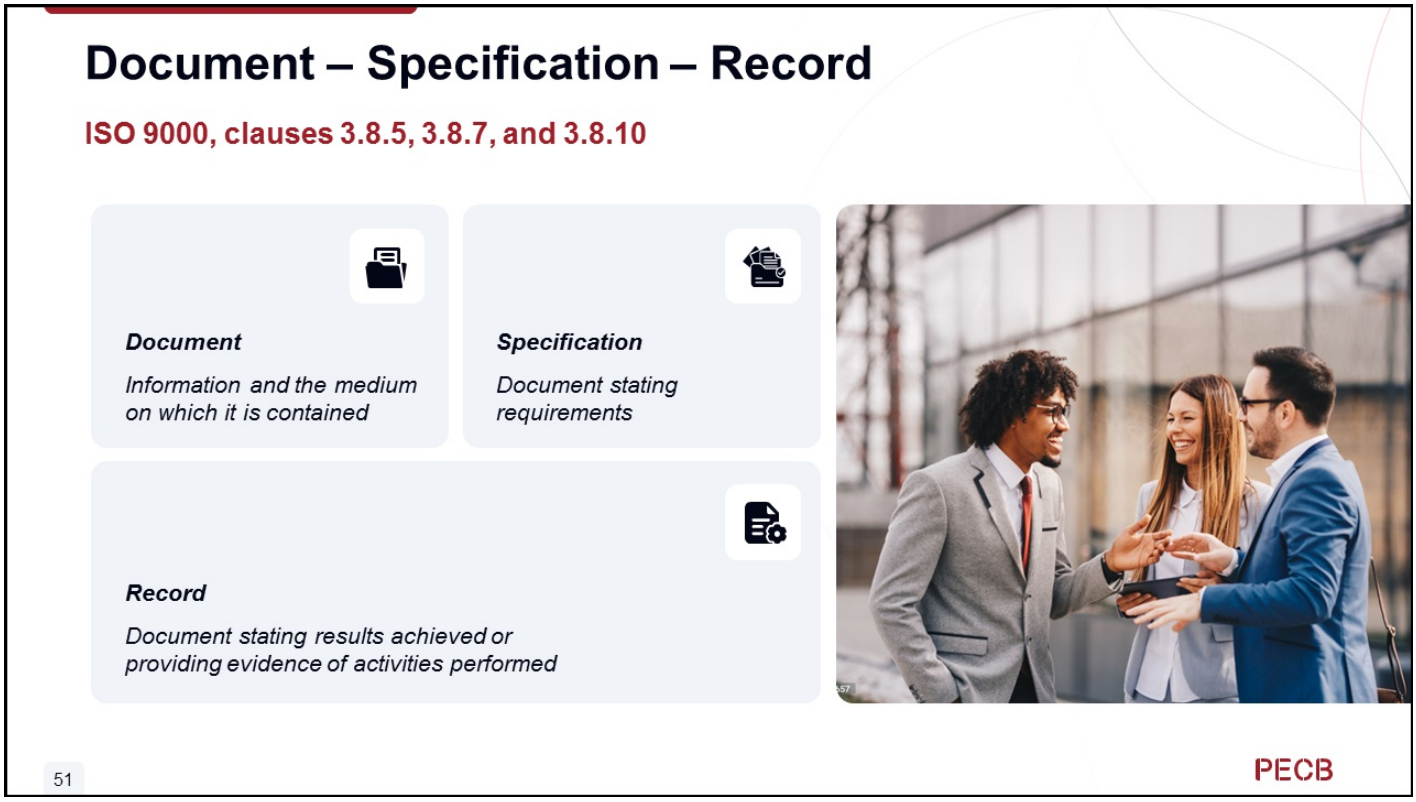
An inventory of information and other associated assets, including owners, shall be developed and maintained.

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".*

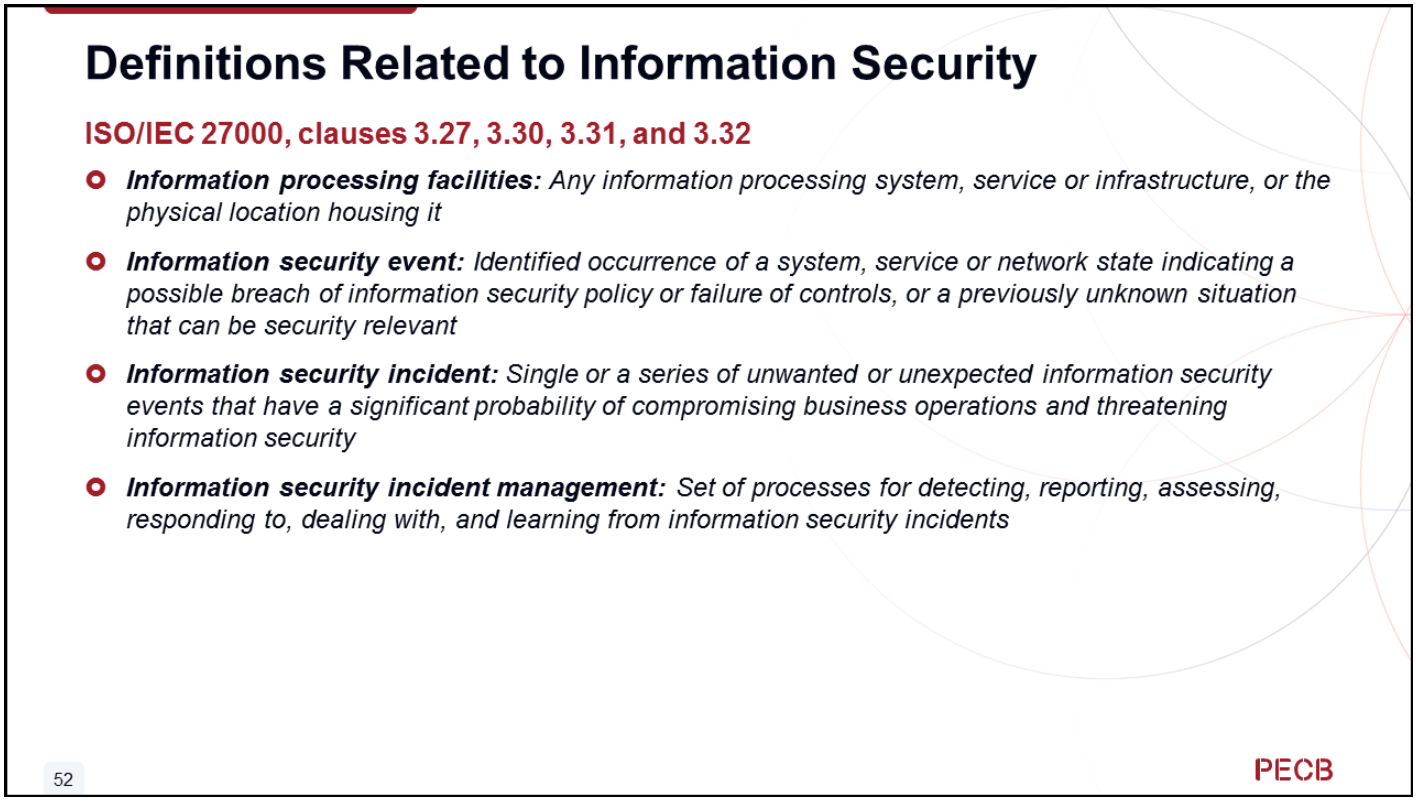
ISO 27000, clause 3.19 Documented information

Information required to be controlled and maintained by an organization and the medium on which it is contained

- *Note 1 to entry: Documented information can be in any format and media and from any source.*
- *Note 2 to entry: Documented information can refer to*
  - *the management system, including related processes;*
  - *information created in order for the organization to operate (documentation);*
  - *evidence of results achieved (records).*

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.



ISO/IEC 27000, clause 3.35 Information system

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

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 includes controls related to the classification of information:

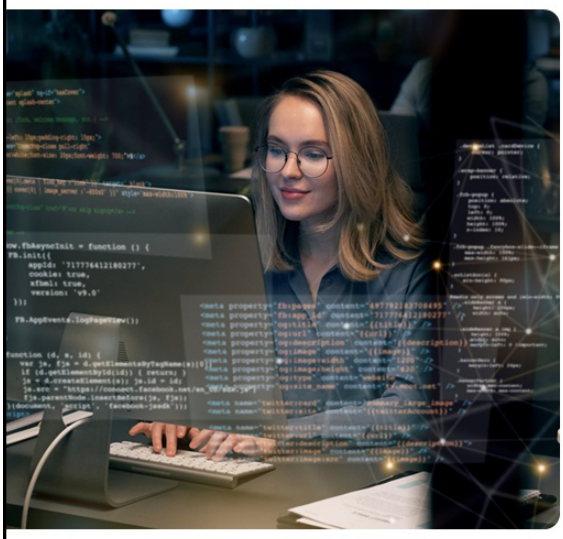
ISO/IEC 27001, Annex A 5.12 Classification of information

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, 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.

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.

53

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.*

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

Ensuring confidentiality of information means that only authorized users have access to sensitive data.

Organizations can achieve this by:

- Employing authentication methods, e.g., multi-factor authentication, which require user identification and password when trying to access confidential data
- Establishing a data access policy
- Implementing access controls that provide access to users only to the information that they need to perform their jobs
- Encrypting information to conceal its meaning

55

PECB

For example, the personal data of employees must be accessible only by the authorized Human Resources Department personnel.

Access controls can be physical, e.g., locks on doors, filing cabinets that can be locked, and safes, and logical, e.g., access controls to information.

Integrity

Ensuring the integrity of information entails that:

- Information is not modified when in storage or transit
- Only authorized modifications are made
- Data is accurate, consistent, reliable, and safe from unauthorized access

Some controls that can be used to ensure the integrity of information include converting the data to a secret code that is available only to authorized individuals, implementing access and version controls, and establishing backup procedures.

56

PECB

For example, the data processed and stored in the Finance Department should remain accurate and authentic, avoiding unauthorized access and modification of such information.

There can be cases when data is changed unintentionally. Some examples include data changes due to:

- Storage erosion
- Natural or intentional errors
- System damages

Data integrity controls are essential in operating systems, software, and applications to prevent the intentional or accidental corruption of data.

Integrity controls must be included in the organizational procedures, so that personnel are aware of them. These procedures are useful in reducing the risk of data error, theft, or fraud. Data validation controls, user trainings, and certain controls at the operational level are good examples.

Availability

Ensuring information availability means that information is accessible:

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

To achieve this, organizations should maintain and improve their physical infrastructure, such as servers and disks, and establish record retention policies, data backup and recovery procedures, incident management procedures, information processing procedures, and procedures to control the usage of systems.

57

PECB

For example, customer data must be accessible to the Marketing Department personnel.

Information security managers usually face three types of challenges that impact the availability of information:

- Denial of service (DoS), as a result of intentional attacks, e.g., when 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

Vulnerability

ISO/IEC 27000, clause 3.77

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

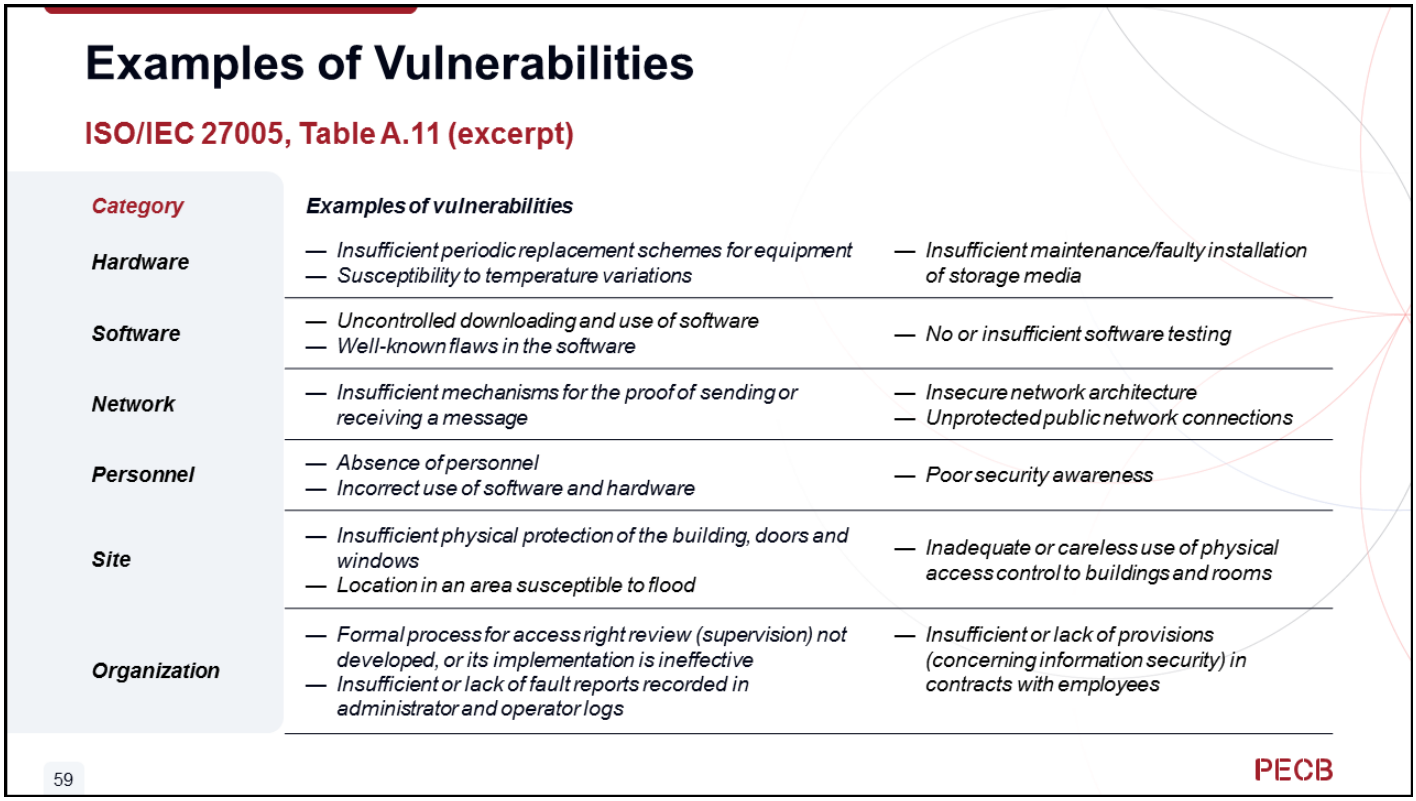
- Vulnerabilities that do not have corresponding threats may not require controls, but should be recognized and monitored for changes.
- Controls that are implemented incorrectly or malfunction could become vulnerabilities.

58

Organizations may accept specific vulnerabilities to utilize other benefits, e.g., buying laptops instead of desktop computers for the employees can increase the chances of theft but significantly improves employee mobility.

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.

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.

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

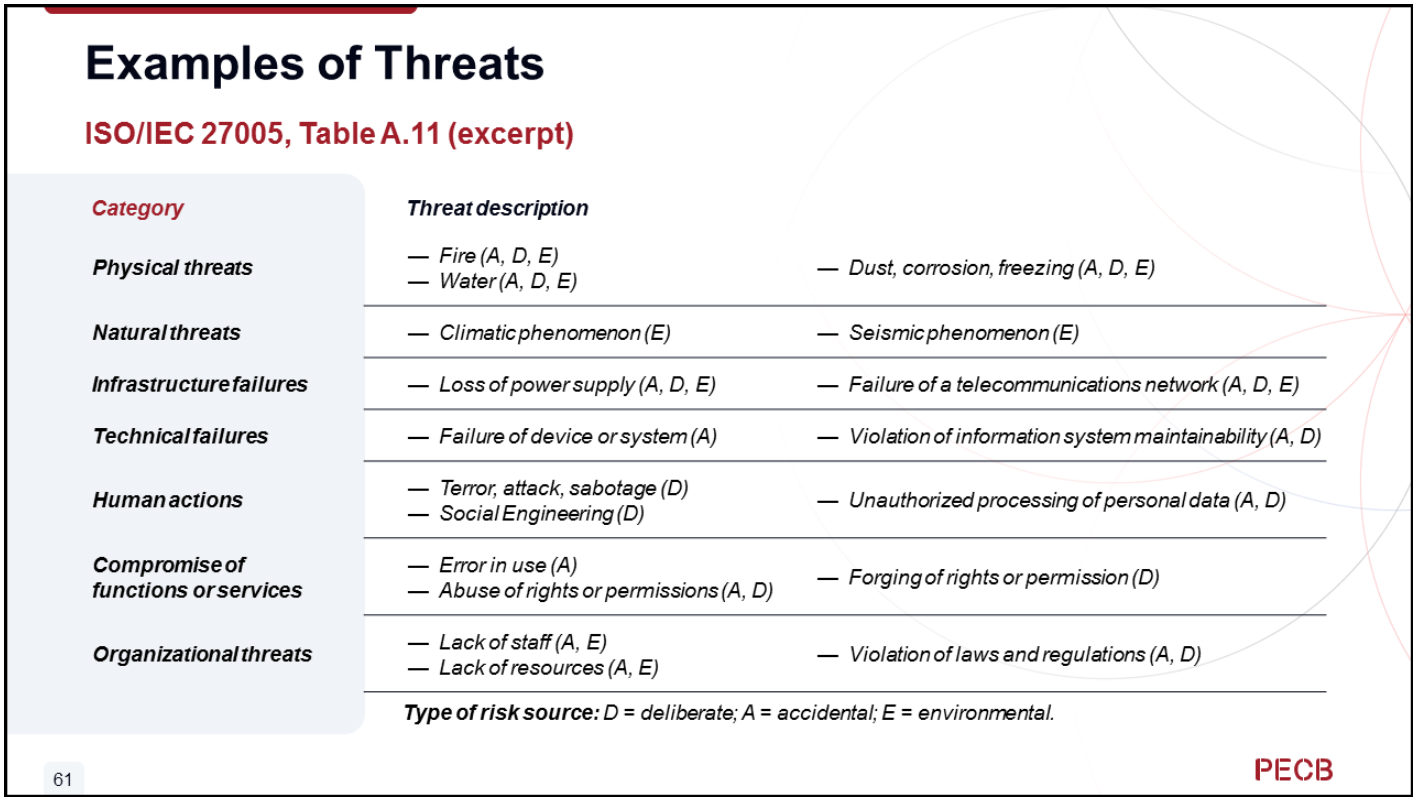
Definition:

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.

60

Threats are associated with the negative aspect of risk and, as such, refer to undesirable occurrences.



ISO/IEC 27005, Annex A.2.5.1 Examples of threats

Table A.10 gives examples of typical threats. The list can be used during the threat assessment process. Threats considered as risk sources can be deliberate, accidental or environmental (natural) and can result, for example, in damage or loss of essential services. The list indicates for each threat type where D (deliberate), A (accidental), E (environmental) is relevant. D is used for all deliberate actions aimed at information and assets related to information, A is used for all human actions that can accidentally damage information and assets related to information, and E is used for all incidents that are not based on human actions. The groups of threats are not in priority order.

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.

Relationship between Vulnerability and Threat

Examples

Vulnerabilities	Threats
Warehouse unprotected and without surveillance	Theft
Complicated data processing procedures	Data input error by personnel
Lack of password protection	Hacking
Unencrypted data	Information theft
Use of pirated software	Virus
No review of access rights	Unauthorized access by former employees
Lack of data backup procedures	Power interruption

62

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.

Consequences

Examples

Consequences on availability

- Service interruption
- Unavailability of service
- Disruption of operations

Consequences on confidentiality

- Invasion of the privacy of users or customers
- Invasion of the privacy of employees
- Leak of confidential information

Consequences on integrity

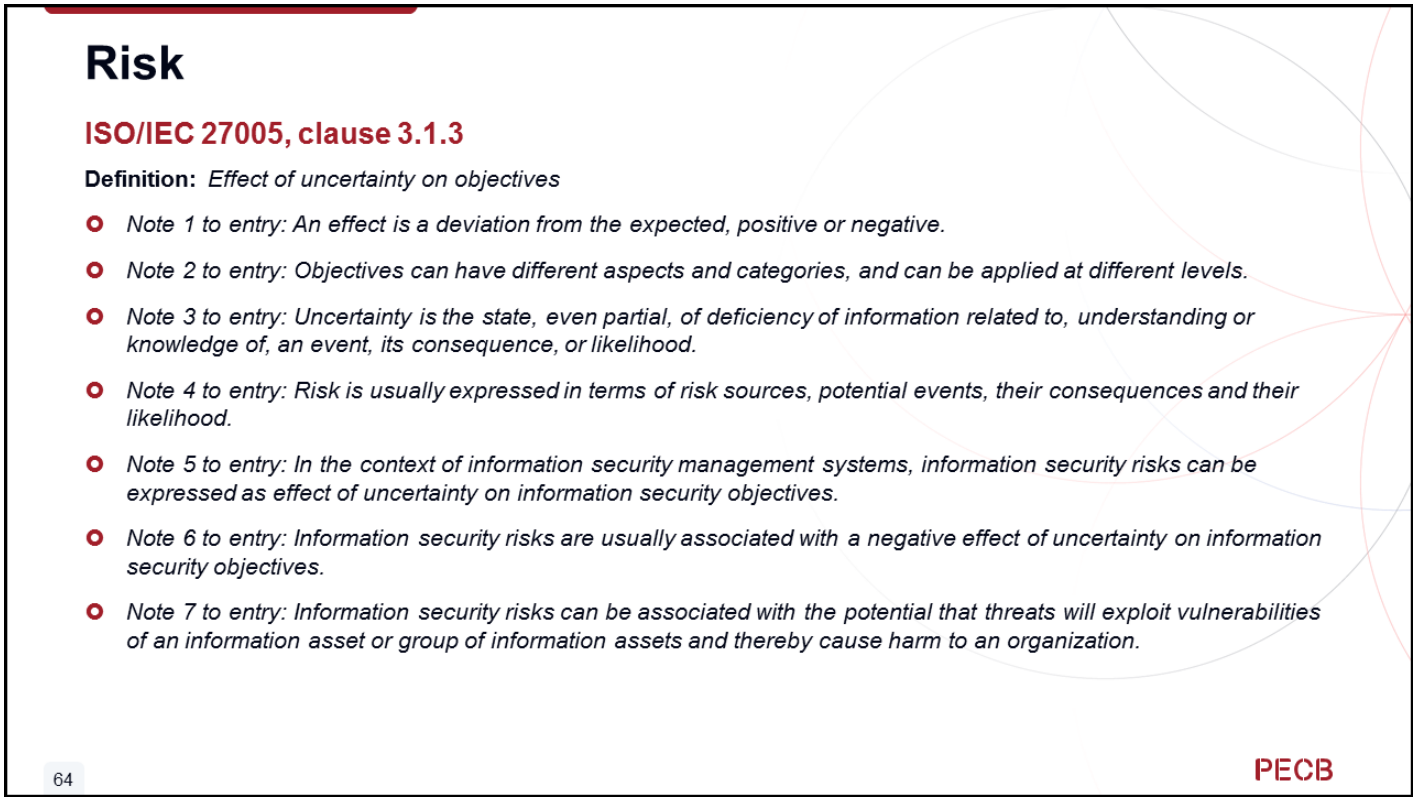
- Accidental change
- Deliberate change
- Incorrect results
- Incomplete results
- Loss of data

63

PECB

Below is a list of several potential consequences that may affect availability, integrity, or confidentiality (or a combination of the three):

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. Reputational damage
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. Endangerment of the safety of staff and users



ISO/IEC 27005, clause 3.1.5 Risk owner

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

ISO/IEC 27005, clause 3.1.7 Risk criteria

Terms of reference against which the significance of a 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 27005, clause 3.1.17 Residual risk

Risk remaining after risk treatment

- *Note 1 to entry: Residual risk can contain unidentified risk.*
- *Note 2 to entry: Residual risks can also contain retained risk.*

ISO/IEC 27005, clause 3.2.1 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

ISO/IEC 27005, clause 3.2.3 Risk assessment

Overall process of risk identification, risk analysis and risk evaluation.

ISO/IEC 27005, clause 3.2.4 Risk identification

Process of finding, recognizing and describing risks

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

Slide Notes Extension

ISO/IEC 27005, clause 3.2.5 Risk analysis

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

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

ISO/IEC 27005, clause 3.2.6 Risk evaluation

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

•Note 1 to entry: Risk evaluation assists in the decision about risk treatment.

ISO/IEC 27005, clause 3.2.7 Risk treatment

Process to modify risk

Note 1 to entry: Risk treatment can involve:

—avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
—taking or increasing risk in order to pursue an opportunity;
—removing the risk source;
—changing the likelihood;
—changing the consequences;
—sharing the risk with another party or parties (including contracts and risk financing); and
—retaining the risk by informed decision.

ISO/IEC 27005, clause 3.2.8 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.

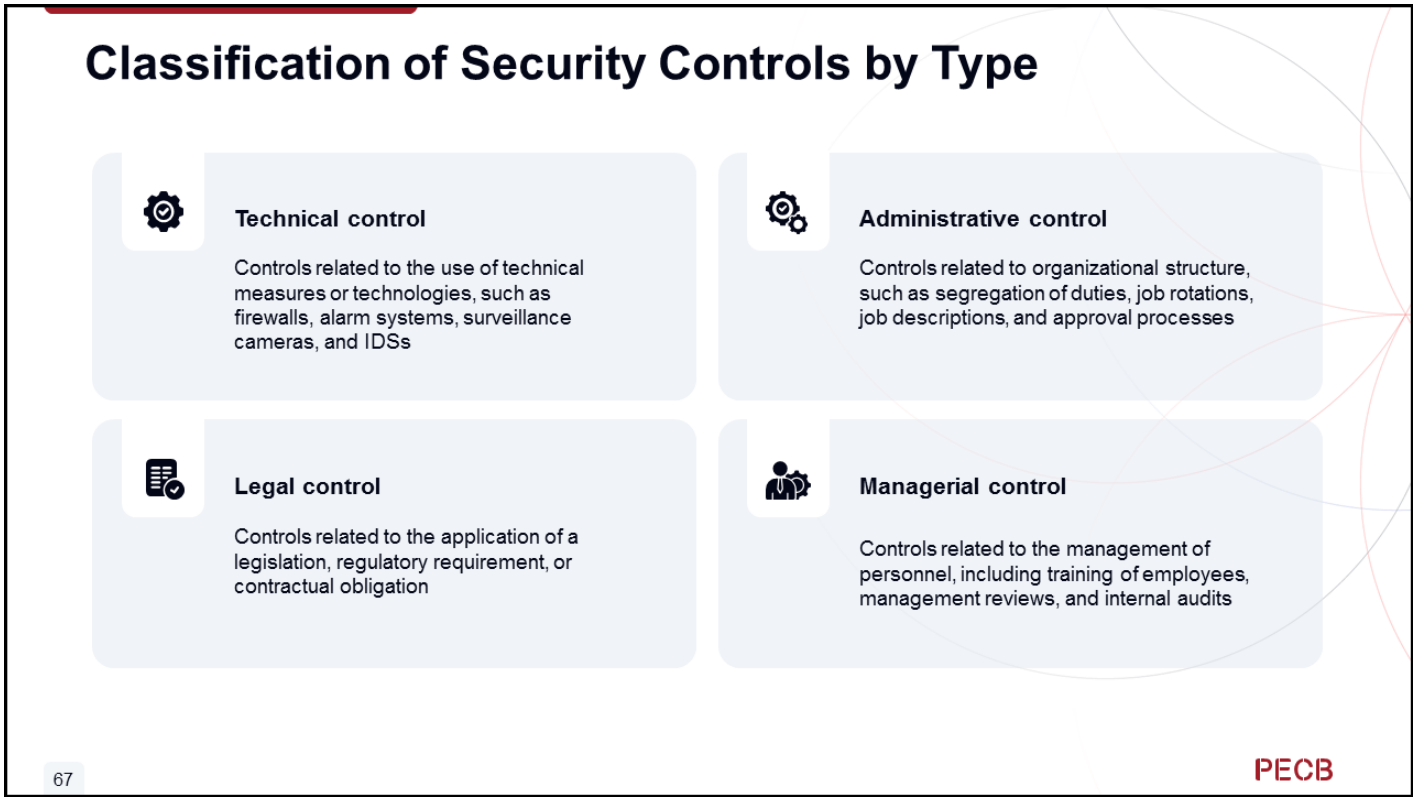
Information Security Risk

Based on NIST SP 800-30, information security risk is defined as *"the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems."*

Information security risk management is the process of identifying, analyzing, and mitigating information security risks and minimizing their impact.

Risk management is crucial for identifying and dealing with potential information security threats and vulnerabilities.

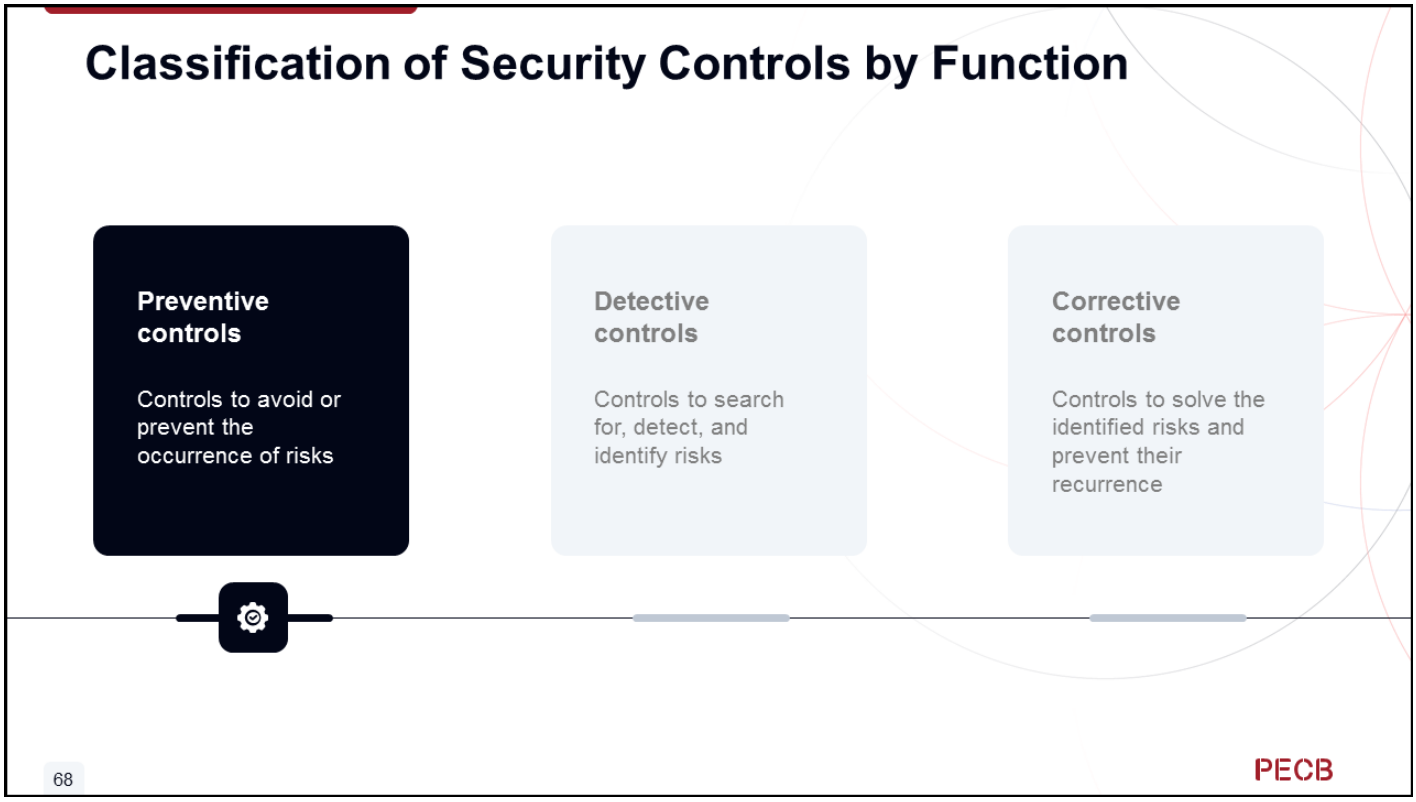
PECB



Controls for information security include any process, policy, procedure, guideline, practice, or organizational structure that can be administrative, technical, managerial, or legal in nature and that can modify information security risks.

Note:

- An administrative control is more related to the structure of the organization as a whole without being applied by a particular person, while a managerial control is to be applied by managers.
- The differences between the types of security controls are explained only for understanding. An organization does not need to determine the nature of the security controls it implements.



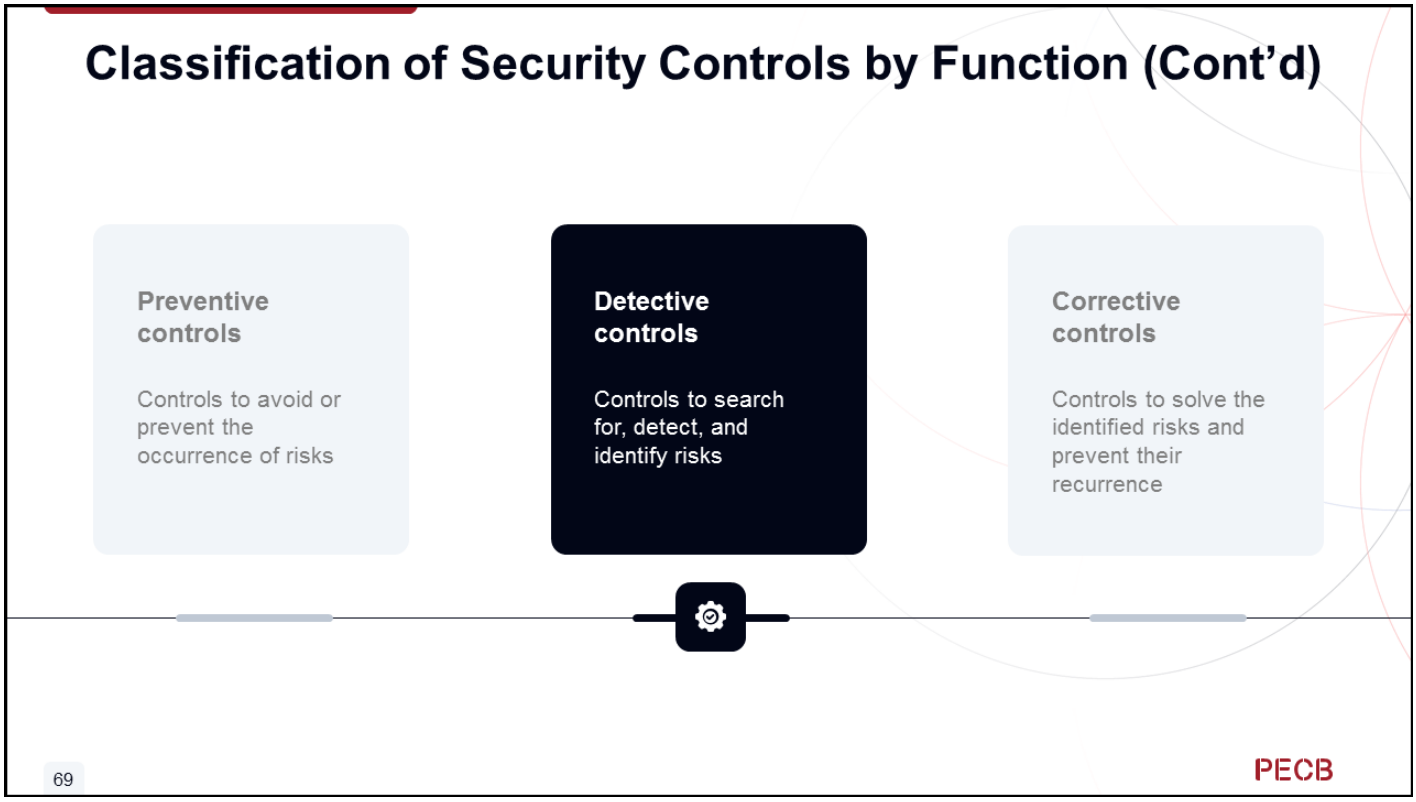
Goal: Avoid or prevent the occurrence of incidents

- Detect incidents before they occur
- Control operations
- Prevent errors, omissions, or malicious acts

Examples:

- Establish an information security policy
- Sign a confidentiality agreement
- Hire only qualified personnel
- Identify third party risks
- Assign duties appropriately
- Separate the development, testing, and operating equipment
- Secure offices, rooms, and equipment
- Use clearly defined procedures (to prevent errors and mistakes)
- Use cryptography
- Use an access control software that only allows authorized personnel to access sensitive files

Note: The types of controls are interrelated. For example, implementing an antivirus can be considered as a preventive control because the antivirus provides protections against malware. Similarly, the antivirus can be considered as a detective control because it detects malware. In addition, the antivirus can also be considered as a corrective control because it deletes any suspicious files or quarantines them.

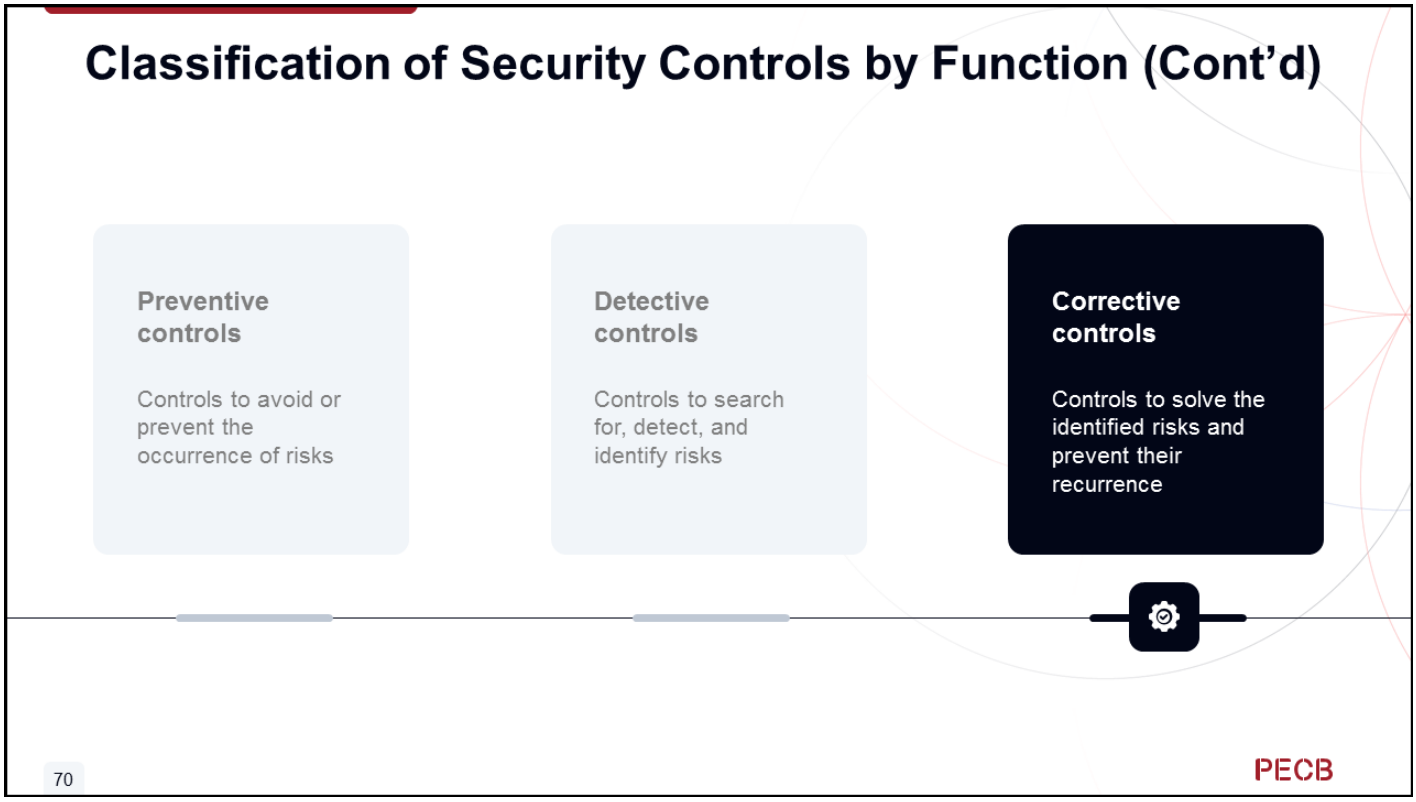


Goal: Search for, detect, and identify incidents

- Use controls that detect and report the occurrence of an error, omission, or malicious act

Examples:

- Monitor and review third party services
- Monitor the resources used by systems
- Use trigger alarms, e.g., fire alarm
- Review user access rights
- Analyze audit logs
- Integration of checkpoints in the applications in production
- Echo control in telecommunications
- Alarms to detect risks related to heat, smoke, fire, or water
- Verification of duplicate calculations in data processing
- Detection of break-ins with video cameras
- Detection of potential intrusions on networks with an intrusion detection system (IDS)
- Review of user access rights
- Technical review of applications after a modification of the operating system



Goal: Solve the identified incidents and prevent their recurrence

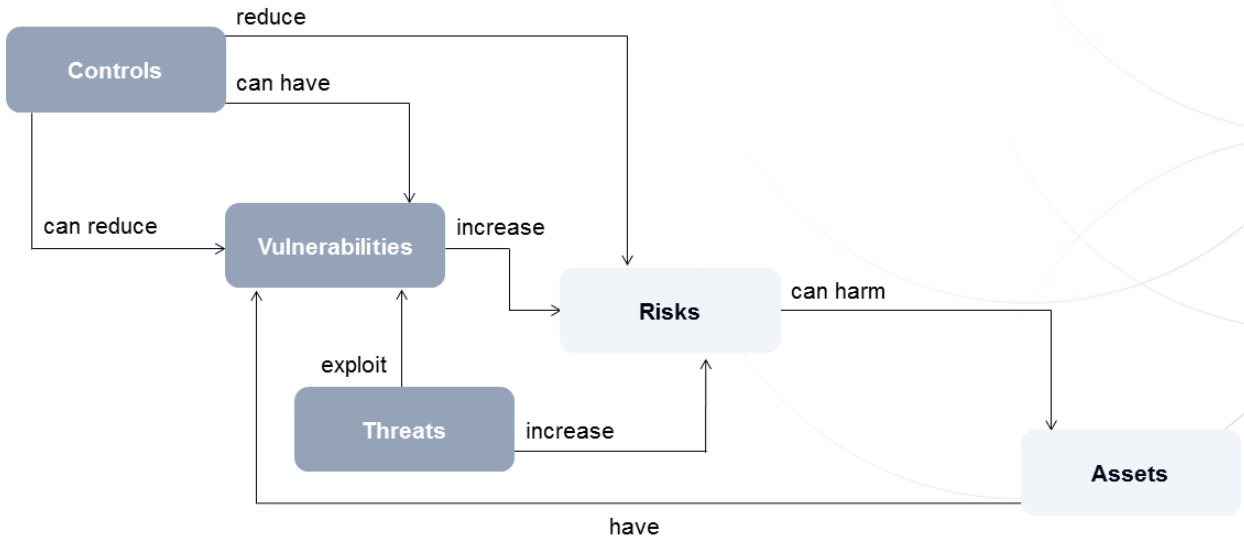
- Minimize the impact of a threat
- Solve the incidents discovered by detection controls
- Identify the causes of an incident
- Modify the processing system to reduce future incidents to a minimum

Examples:

- Conduct technical and legal investigation following an incident
- Enable the business continuity plan after the occurrence of a disaster
- Implement patches following the identification of technical vulnerabilities
- Review the security policy after the integration of a new division in the organization
- Appeal to authorities to report a computer crime
- Change all passwords of all systems when a computer network intrusion has been detected
- Recover the transactions with the backup procedure after discovering that some data has been corrupted
- Automatically disconnect idle sessions
- Implement patches following the identification of technical vulnerabilities

Relationships between Information Security Elements

Overview



71

PECB

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 risks.
3. Controls address vulnerabilities; however, 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.

Cybersecurity

ISO/IEC TS 27100, clause 3.2

Definition: *Safeguarding of people, society, organizations and nations from cyber risks*

- *Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.*

72

PECB

Cybersecurity includes the protection of information and systems against unauthorized access. Considering the high impact cybersecurity risks have on assets, organizations should assess and treat risks associated with their assets accordingly.

In addition to the involvement of the organization and its management in ensuring cybersecurity, the involvement of stakeholders is also important. They are expected to contribute actively in maintaining security in the cyberspace.

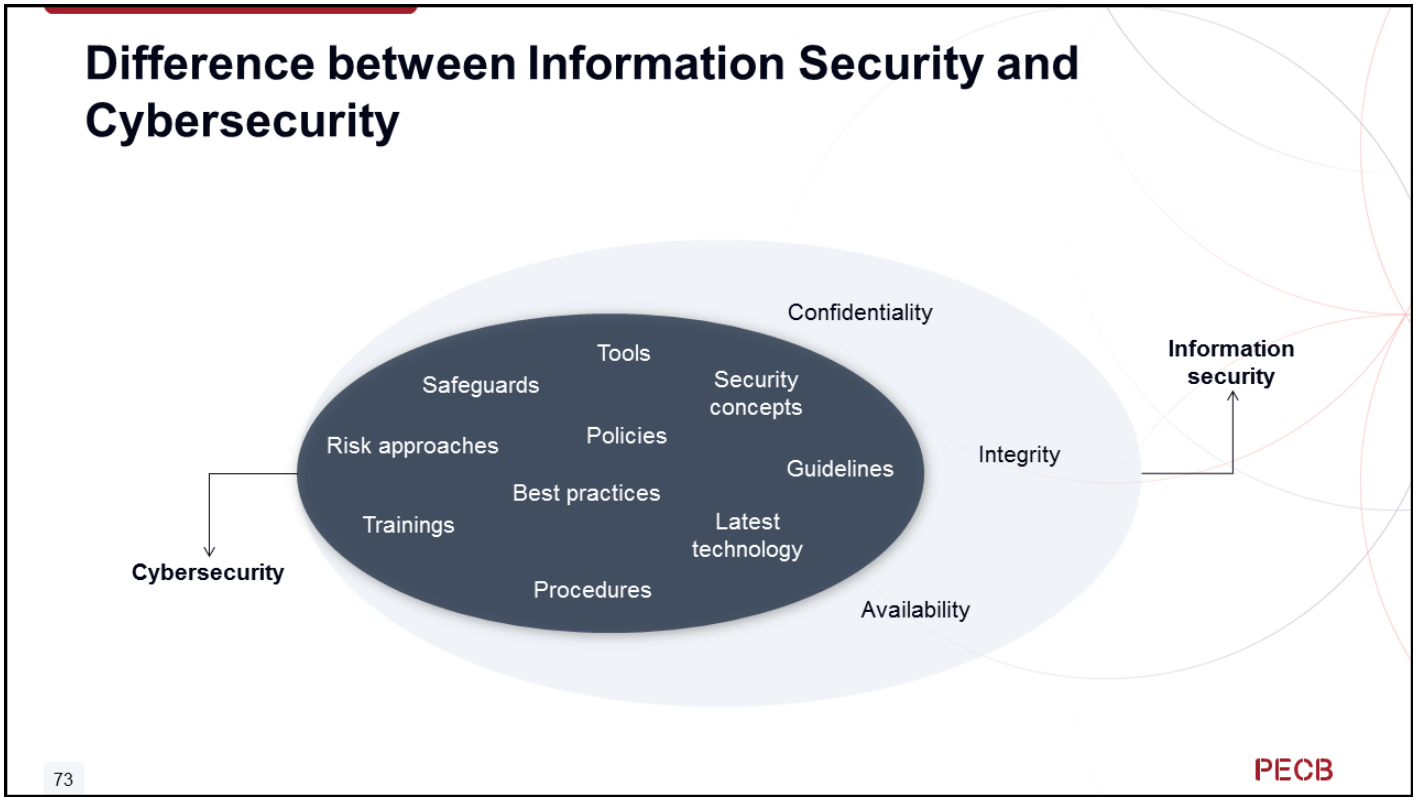
ISO/IEC TS 27100, clause 4.2 Cybersecurity

The objective of adequate cybersecurity is to maintain an acceptable level of stability, continuity and safety of entities operating in cyberspace. While it is not possible to always achieve these objectives, cybersecurity aims to reduce cyber risks to a tolerable level.

Areas of concern for cybersecurity include:

a. *stability and continuity of society, organizations and nations;*
b. *property (including information) of people and organizations; and*
c. *human lives and health.*

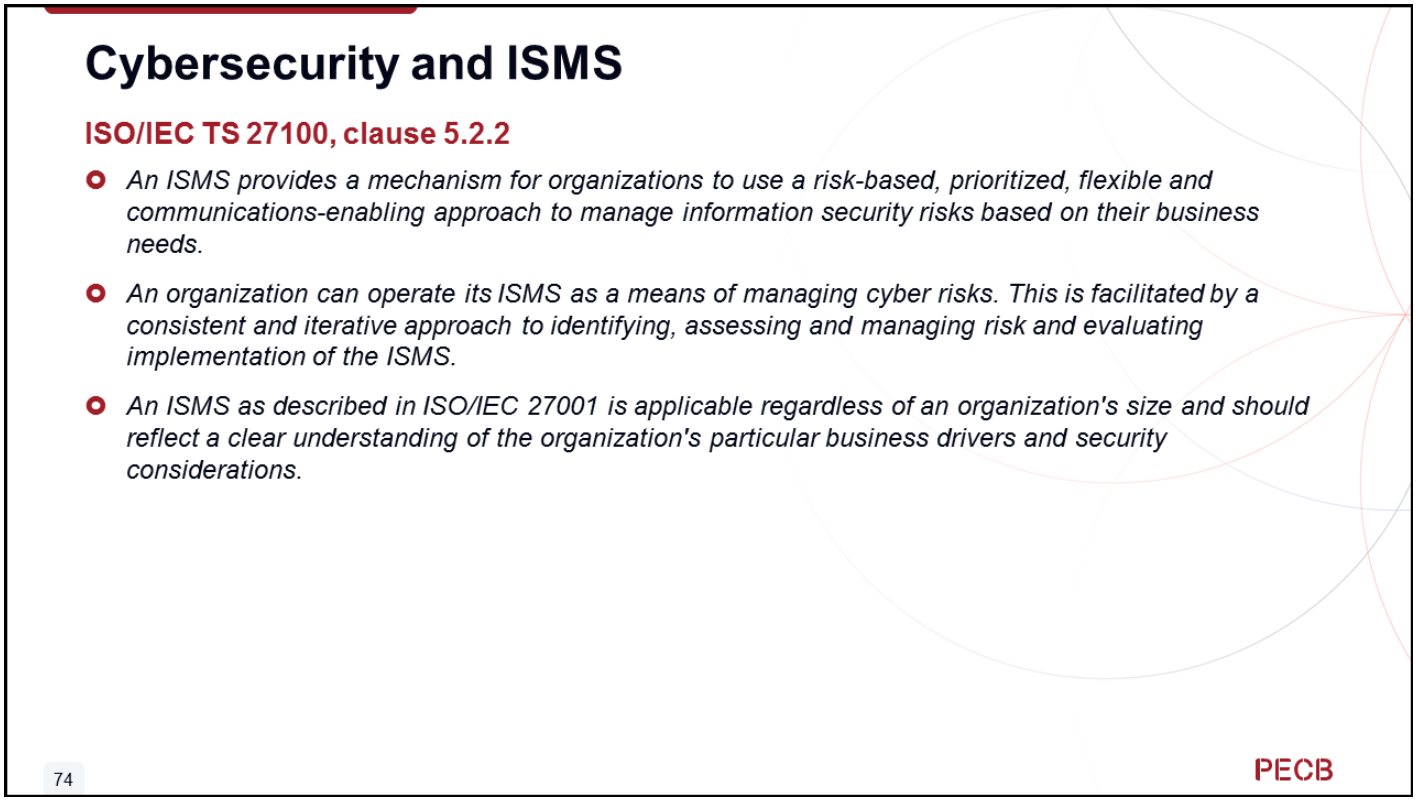
Cybersecurity with these characteristics is implemented by individual organizations. In cyberspace, organizations need to consider not only themselves, but also other parties who share cyberspace. While an organization needs to manage its vulnerabilities to ensure that the organization does not adversely affect other actors, it needs to work with others to reduce cyber risks. In addition, cybersecurity needs to reduce social and human losses in real space caused by cybersecurity incidents in cyberspace. Therefore, immediate detection and appropriate response of information security incidents are important elements of cybersecurity.



The term cybersecurity is frequently used interchangeably with information security due to their close association. There are also technical definitions derived from it, including cyberwarfare and protection of critical infrastructure. However, it is crucial to note that there are significant distinctions between the concepts of information security and cybersecurity.

Information security covers the protection of information by ensuring its confidentiality, integrity, and availability (CIA). It protects information systems and prevents any type of unauthorized access, use, or modification of different formats of information, such as paper documents, digital and intellectual property, etc.

Cybersecurity refers to the ongoing effort to protect digital assets like networks, servers, hardware, or any type of data that is stored and transported through these assets. Cybersecurity is an essential and diverse part of information security.



ISO/IEC TS 27100, clause 5.2.2 ISMS in support of cybersecurity (cont'd)

An ISMS facilitates communication about the implementation of desired outcomes and associated information security activities across the organization, from the top management level by using the management system requirements, to the implementation and operations levels by using the controls. The application of ISMS does not only provide a clear and understandable set of controls as an outcome but also provide a clear scope, boundaries and dependencies of cybersecurity activities in the organization.

An example of using an ISMS in support of cybersecurity is the use of ISO/IEC 27001 with ISO/IEC 27019 to establish, implement, maintain and continually improve an ISMS for the energy utility supplier. The ISMS supports the stability of the energy supply and, hence, contributes to the cybersecurity of a nation.

Information Privacy

- Information privacy determines how to protect personally identifiable information (PII), the reason why it should be protected, and what to protect it from.
- Protection of privacy during the processing of PII ensures that organizations comply with applicable laws and regulations.
- In order to ensure information privacy, organizations have to implement security controls.

The protection of PII has become a serious concern that requires commitment from organizations in order to prevent PII breaches.

PECB

Section 4 Summary

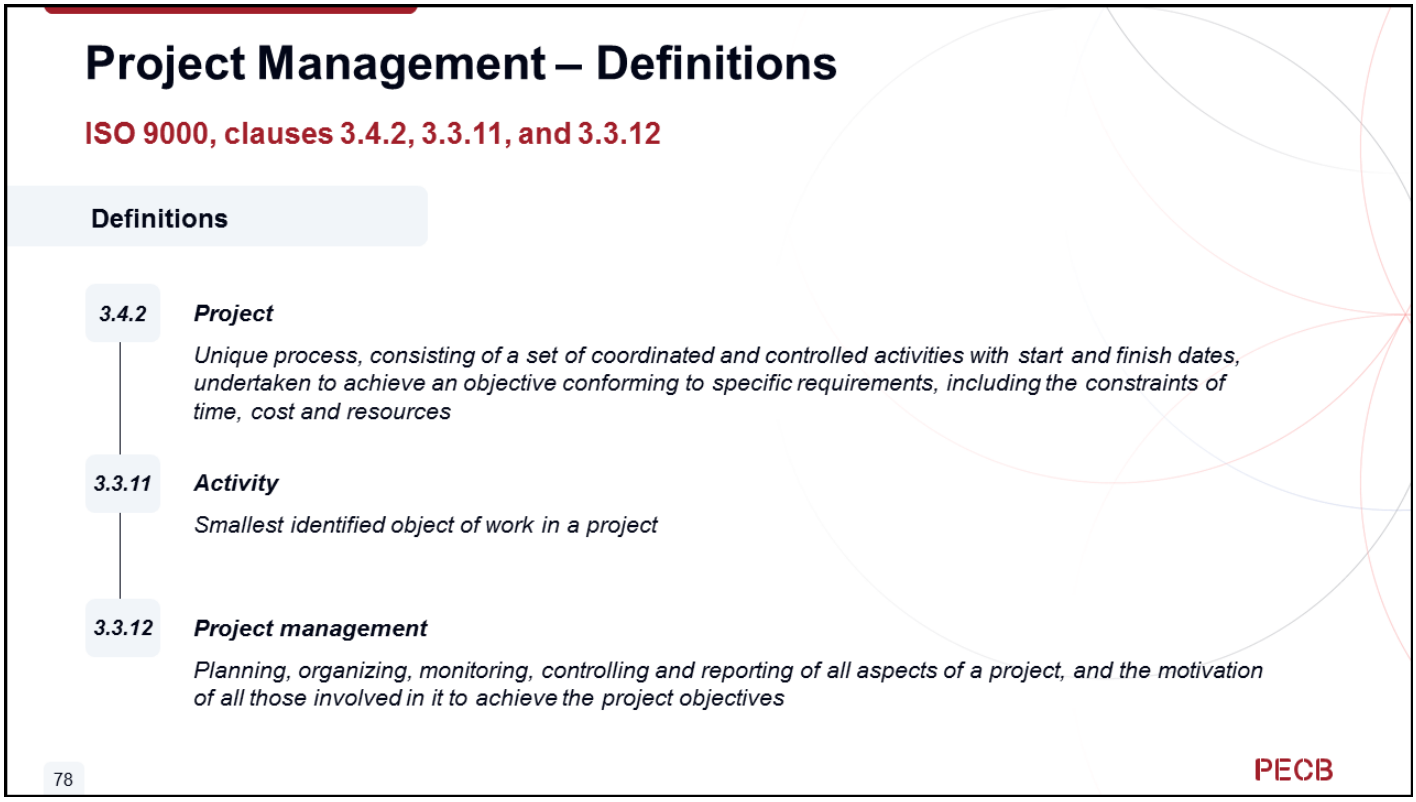
- Information is meaningful data, whereas an asset represents an item, thing, or entity that has potential or actual value to an organization.
- Information security covers all types of information regardless of its format. It determines what information needs to be protected, why it should be protected, how to protect it, and what to protect it from.
- Three main pillars of information security are confidentiality, integrity, and availability.
- 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.
- By type, security controls are classified into technical, legal, administrative, and managerial controls. By function, security controls are classified into preventive, detective, and corrective controls.

Questions?

Quiz 3

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

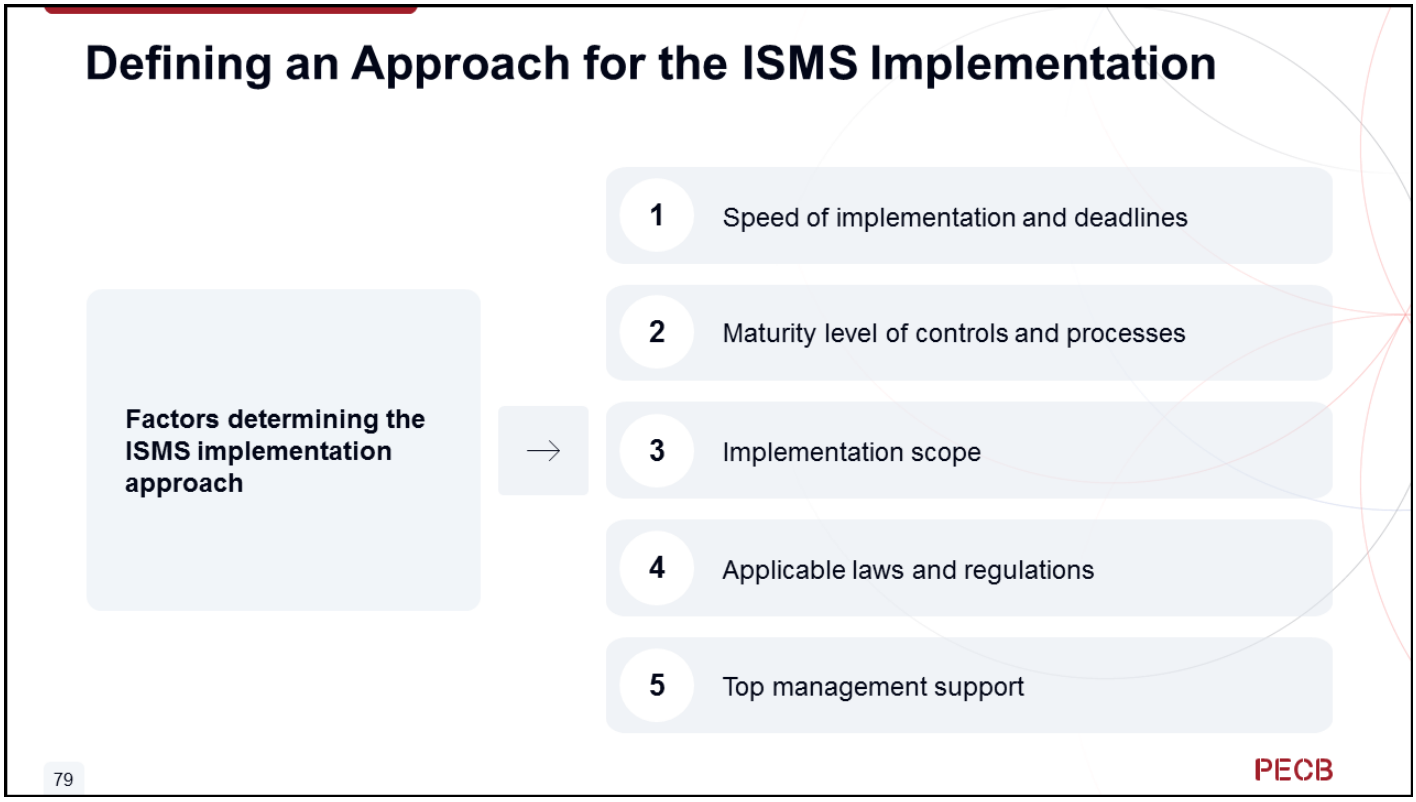
This section provides information that will help the participant gain knowledge on the process of finding an approach to successfully implement the ISMS.



Notes on terminology:

1. Projects are temporary; they continue for only a limited period of time.
2. An individual project may be part of a larger project structure.
3. The complexity of the interactions among project activities is not necessarily related to the project size.
4. It is important to differentiate between conducting the ISMS project and managing the ISMS operations. The former refers to the implementation of the ISMS, while the latter to the management of the ISMS daily operations.

Note: This training course focuses on explaining the methodology for the implementation of the ISMS, not on the management of the ISMS's daily operations.



The project may last for a period of 6 to 12 months from the first process of planning the project to the conclusion of the first cycle of audits and the monitoring of the management system.

However, if a limited scope for the ISMS is considered at the start of the project and it is implemented in a relatively less complex environment, organizations may complete such projects in a shorter time.

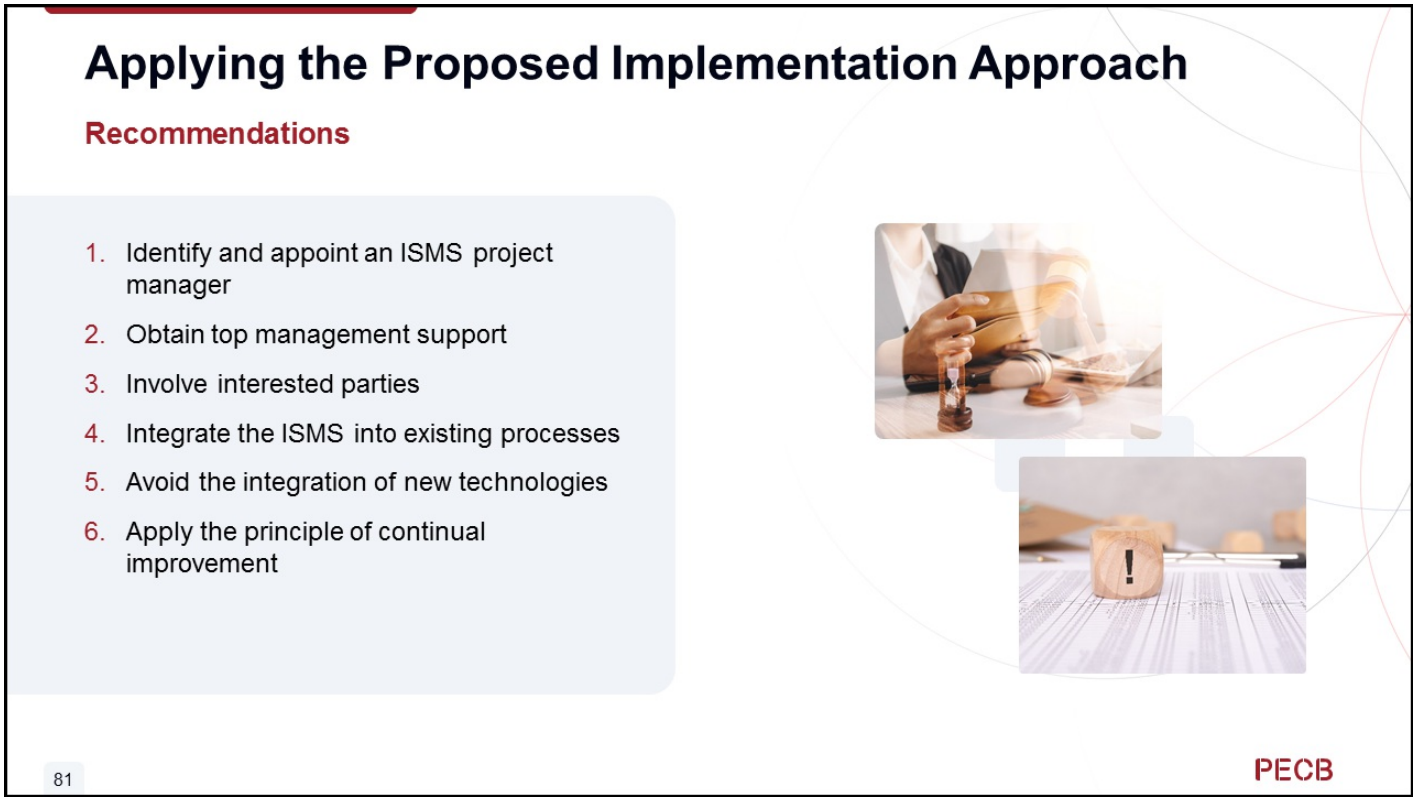
Proposing Implementation Approaches

1. **Business approach:** Integration of the ISMS into the context of commercial activities across the organization
2. **Systems approach:** Overall implementation of the ISMS processes, not by isolating certain processes
3. **Systematic approach:** Application of best practices in project management, such as ISO 10006
4. **Integrated approach:** Integration or adjustment of the ISMS with other management systems or requirements established within the organization
5. **Iterative approach:** Rapid implementation of the ISMS by adhering to the minimum requirements of the standard and proceeding with continual improvement thereafter

PECB

The proposed approaches for an ISMS are implemented in a chronological order. For instance, an organization's project plan is devised before a project of the ISMS. Likewise, the monitoring and improvement phases begin only after identifying the location of the system components. During each phase, the ISMS processes and controls are implemented in succession. However, the implementation of these approaches is time-consuming and resource-intensive, be it for planning or implementing the system "piece by piece." Another drawback is that the approach does not allow organizations to experience any instant positive results from implementing the management system, since a considerable period of time should pass before results can be noticed. This approach also exhausts the participants during the implementation process, which may lead to them abandoning the project altogether.

The approaches described in the slide are proposed by PECB as a response to overcome the difficulties mentioned above.



The following is a list of recommendations to consider when applying the proposed implementation approach in practice:

1. **Identify and appoint an ISMS project manager:** Organizations should identify and appoint an individual responsible for implementing the project. The project manager's responsibility is to ensure that the project runs smoothly in terms of time and support (budget, approvals, etc.).
2. **Obtain top management support:** The top management's support is essential in the success of the implementation of ISMS. As such, it is important to obtain their support. They are responsible for providing the resources needed to implement the information security management system and for conducting regular reviews of the management system in order to ensure its ongoing efficiency.
3. **Involve interested parties:** Organizations should define the roles and responsibilities of the interested parties early in the implementation process. In addition, it is also important that they are involved in the project and that their support is maintained and their needs analyzed.
4. **Integrate the ISMS into existing processes:** Organizations should integrate the ISMS into already existing processes and ensure that these processes are adjusted in accordance with the framework of ISMS. Organizations should avoid creating processes that do not fit with their context and culture.
5. **Avoid the integration of new technologies:** Organizations should implement the ISMS initially with the technology already in place (most of them have the necessary technology to do so). If organizations want to upgrade their technology, they may do so during continual improvement.
6. **Apply the principle of continual improvement:** Organizations should apply the principle of continual improvement and should consider any opportunities or recommendations for improvement by the interested parties. They should set achievable goals at the beginning of a project and should target continual improvement for the longer term.

The most common purpose of a business case is to determine the financial consequences of a decision. It should answer the question, “What are the financial consequences if we choose X over Y?”

A well-structured business case must indicate what benefits can be expected from a decision on a given period of time. It also includes the methods and the logic used to calculate those benefits. All in all, a business case will be helpful for an organization’s management to have better decisions on the investments of certain resources and achieve positive outcomes.

The business case must describe the overall impact of the implementation of a particular project, program, or portfolio in easily understandable terms. It should address the critical success factors and contingencies. It should also identify significant risks that might occur and cues that would signal any change in the results.

It should answer the following questions:

- What is the purpose of the project?
- What are the solutions that have been studied?
- Why is this particular solution chosen? What are its risks and constraints?
- How much does it cost? Who is responsible for this project?
- How will this project affect my work?
- How to tell if the project is successful?

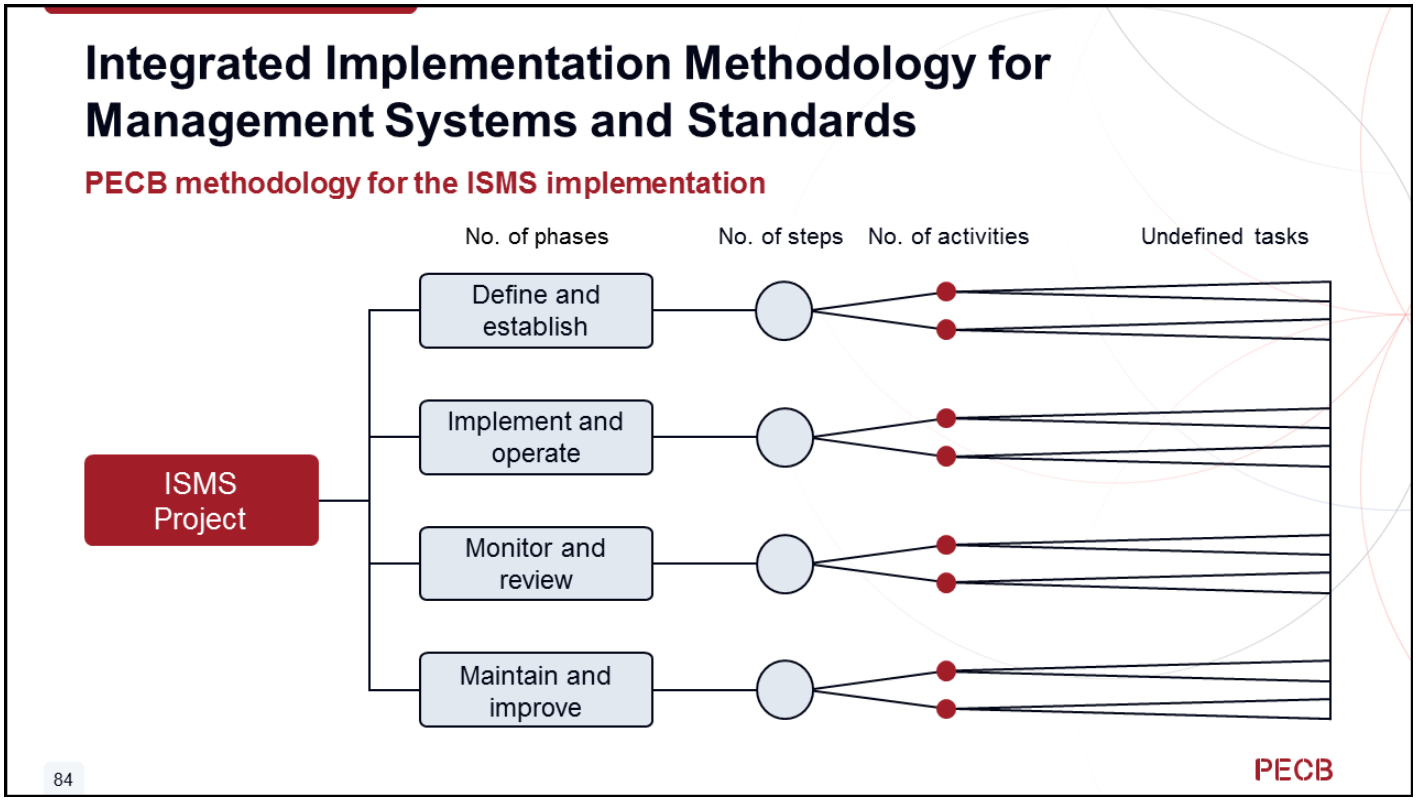
Content of a Business Case

1. **Environment:** List of factors that justify the existence of the project, the economic, commercial, and competitive environments, the opportunities
2. **Purpose and objectives:** Project vision, general and strategic objectives, specific and tactical objectives, operational objectives (technical, economic, and temporal)
3. **Project summary:** A summary of the contents of the project in a few words: name/project reference, origin, environment, current status
4. **Expected benefits:** Intended outcomes, financial benefits, financial scenarios, cost/ROI, risks/costs of not acting, project risks (for the project itself, for the profits, and for the business)
5. **Preliminary scope:** Action framework, perimeter, and boundaries, prerequisites
6. **Critical success factors:** Material and human resources, context of the organization
7. **Preliminary project plan:** The project approach, definitions of phases, reports, deliverables
8. **Deadlines and milestones:** Activities and modifications of project activities, technical distribution, project planning
9. **Roles and responsibilities:** Functions, roles, resources to cover the workload
10. **Resources:** Resources needed for the project, funds
11. **Budget:** Project controls, financial plans
12. **Constraints:** Expected problems and solutions, assumptions, identified and assessed options, magnitude, scale, complexity rating

PECB

To these 12 elements of the development plan of the project, the two items below can be added and considered as part of a “facilitation plan” of the project.

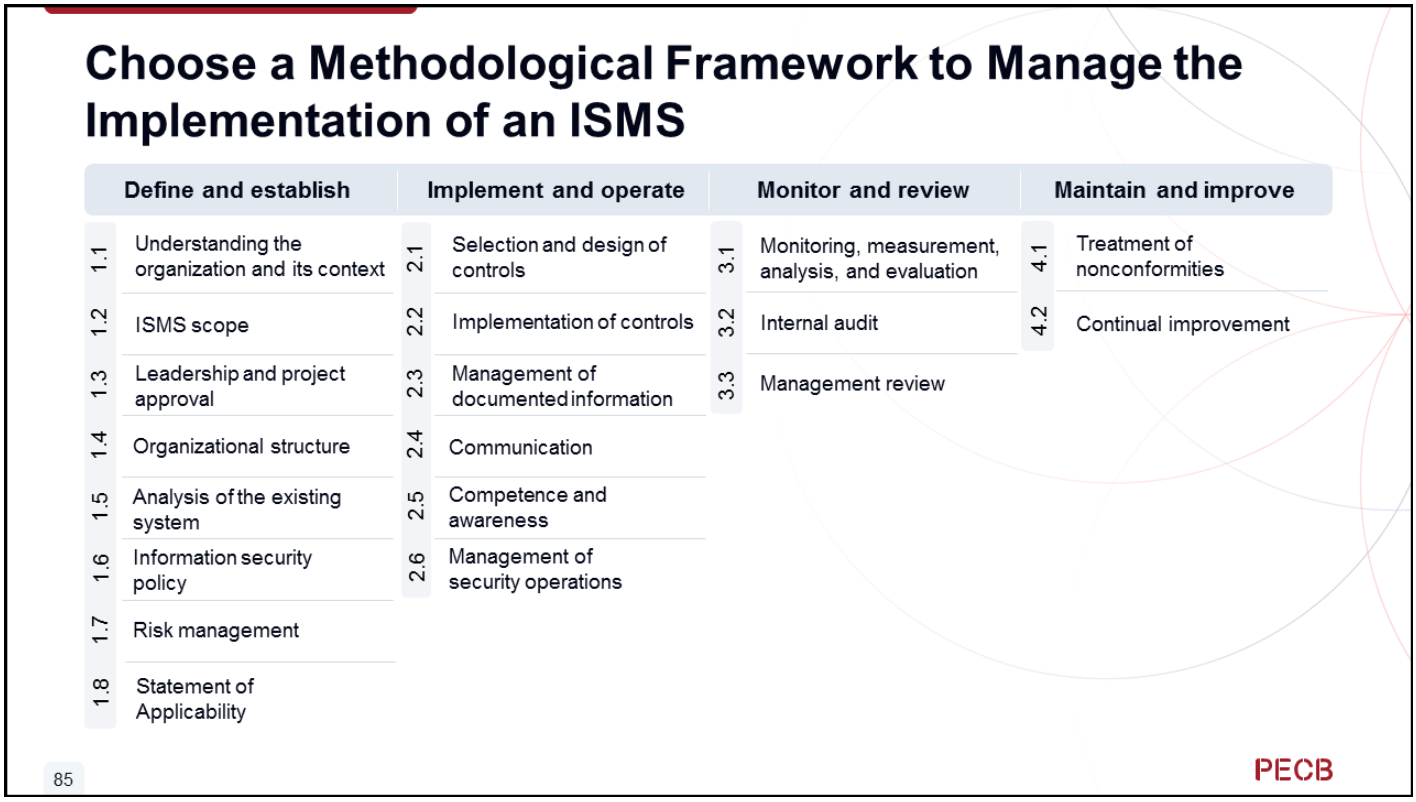
- **Communication:** Operational (media selection, target audience) or promotional (internal or external)
- **Project monitoring:** Indicators, dashboards, reporting, project reviews, traceability



PECB has developed a methodology based on best practices for implementing a management system, known as the "Integrated Implementation Methodology for Management Systems and Standards (IMS2)." This methodology is also based on the guidelines of ISO standards and meets the requirements of ISO/IEC 27001.

Based on this methodology the project is divided into phases, phases into steps, steps into activities, and activities into tasks. During the training course, the steps and activities will be presented in the chronological order of the course of an implementation project.

Tasks will not be detailed because they are specific for each project and depend on the organization's context. For example, the activities 1.4.2 (Establish the ISMS project team) will involve a series of tasks such as the job description, interviewing candidates, signing of a contract, etc.



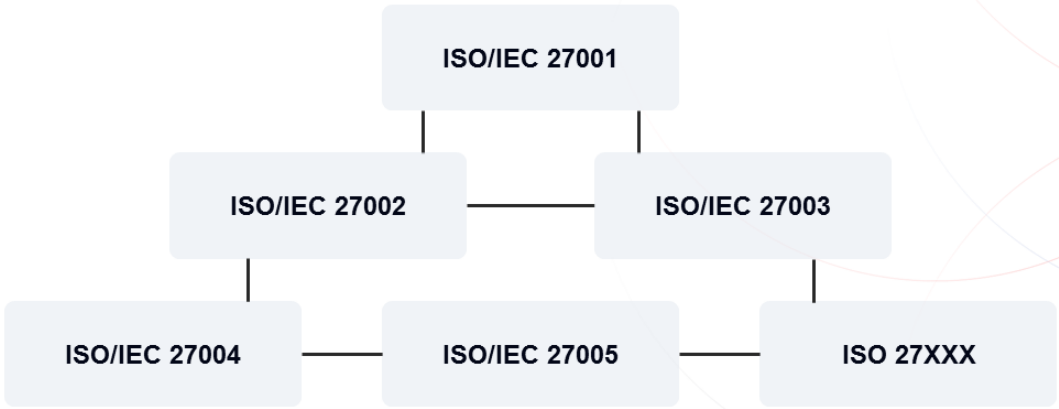
By following a structured and effective methodology, an organization can cover the minimum requirements for the implementation of a management system.

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).

Aligning with Best Practices

Use of ISO standards



Note: ISO 27XXX refers to standards that will be developed in the future.

86

PECB

The core of best practices included in various ISO standards provides access to knowledge that is consensual among experts in the information security management field. Best practices should not be confused with standard requirements. A good practice is a recommendation, not a requirement. Each organization is free to use them as reference and is not obliged to adopt them.

We present the good practices published in various ISO standards in this training course. However, there are several other sources of good practices available.

Notes on terminology

1. “Good practice” means it is generally recognized that the implementation of said practices corresponds to activities, tools, and techniques widely used by specialists.
2. “Generally recognized” means that the knowledge or the practices presented are usually applicable to most organizations and their value and utility are subject to a fairly broad consensus.

ISO 10006 Quality management systems — Guidelines for quality management in projects: ISO 10006 gives guidance on the application of quality management in projects. It is applicable to projects of varying complexity, small or large, of short or long duration, in different environments, and of all kinds of product or process involved. This can require some tailoring of the guidance to suit a particular project.

Source: www.iso.org

Project Management Body of Knowledge — PMBOK Guide: The PMBOK Guide identifies and describes the knowledge and practices applicable to most projects. It recognizes five basic processes: initiating, planning, implementation, monitoring, and verification, and closing of a project. The processes are described in terms of inputs (documents, plans, designs, etc.), tools and techniques (mechanisms applied to inputs), and outputs (documents, products, etc.). The PMBOK Guide also defines nine knowledge areas: Project Integration Management, Project Scope Management, Project Time Management, Project Cost Management, Project Quality Management, Project Human Resource Management, Project Communications Management, Project Risk Management, and Project Procurement Management.

Source: www.pmi.org

ISO/IEC 27003 Information security management system implementation guidance: ISO/IEC 27003 presents a guidance on the requirements of an information security management system as specified in ISO/IEC 27001 and is intended to be applicable to all organizations, regardless of type, size, or nature. Organizations implementing an ISMS are under no obligation to implement the guidance in this document.

Source: www.iso.org

Section 5 Summary

- There are some activities that should be conducted to initiate the ISMS implementation. These activities include defining the approach to the ISMS implementation, choosing a methodological framework to manage the implementation of an ISMS, and aligning it with best practices.
- There are some factors that should be taken into account when defining the approach for the implementation of the ISMS, such as the speed of implementation, the targeted maturity level of controls, and the expectations and scope.
- Some recommendations that organizations should consider when implementing the ISMS include appointing an ISMS project manager, obtaining top management support, involving interested parties, avoiding the integration of new technologies, integrating the ISMS into existing processes, and applying the principle of continual improvement.

Questions?

Quiz 4

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

This section provides information that will help the participant understand the importance of identifying internal and external factors that may affect the implementation of an ISMS, including determining whether climate change is a relevant issue, the key processes and interested parties involved in the implementation of an ISMS, and the necessary information for planning the ISMS implementation.

Understanding the Organization and Its Context

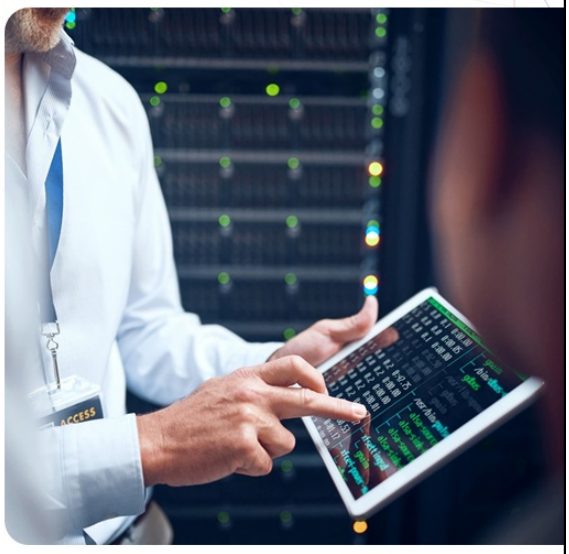
Define and establish		Implement and operate		Monitor and review		Maintain and improve	
1.1	Understanding the organization and its context	2.1	Selection and design of controls	3.1	Monitoring, measurement, analysis, and evaluation	4.1	Treatment of nonconformities
1.2	ISMS scope	2.2	Implementation of controls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

PECB

ISO/IEC 27001's Requirements for Understanding the Organization and Its Context

ISO/IEC 27001, 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.*
- *The organization shall determine whether climate change is a relevant issue.*



91

PECB

An organization aiming compliance with ISO/IEC 27001 should:

1. Demonstrate that their ISMS is aligned with its mission, objectives, and business strategies
2. Identify and document the organization's activities, functions, services, products, partnerships, supply chains, and relationships with interested parties
3. Define the external and internal factors that can influence the ISMS
4. Assess the potential impact of climate change on the organization's ISMS and determine appropriate measures to mitigate risks arising from it
5. Recognize and take into account issues related to information security within their industrial sector, such as risk, legal and regulatory obligations, and customer requirements
6. Establish and document objectives for the ISMS

Note: ISO has initiated the publication of climate action amendments to management system standards to consider climate change. This requires organizations implementing management system standards to determine whether the climate change is relevant to the management system they are implementing. ISO has published an amendment for ISO/IEC 27001:2022 in February, 2024 regarding this. The requirements of this amendment are included in this training course.

Slide Notes Extension

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:

1. 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.
2. The use of “organization” in ISO/IEC 27001 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).
3. 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).

1.1 Understanding the Organization and its Context

List of activities

1.1.1 Understand the mission, objectives, values, and strategies

1.1.2 Determine the ISMS objectives

1.1.3 Determine the preliminary scope

1.1.4 Analyze the internal and external environment

1.1.5 Identify the key processes and activities

1.1.6 Determine climate change implications

1.1.7 Identify and analyze the interested parties

1.1.8 Identify and analyze the business requirements

PECB

1.1.1 Understand the Mission, Objectives, Values, and Strategies

94

PECB

It is necessary to obtain an overview of the organization in order to understand the information security challenges 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 an organization's existence. It serves as a reference point to keep everyone clear on where the organization is headed.

  Implications for the ISMS: The ISMS aims to support the organization in fulfilling its mission by safeguarding 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 the organization that influence the behavior of individuals.

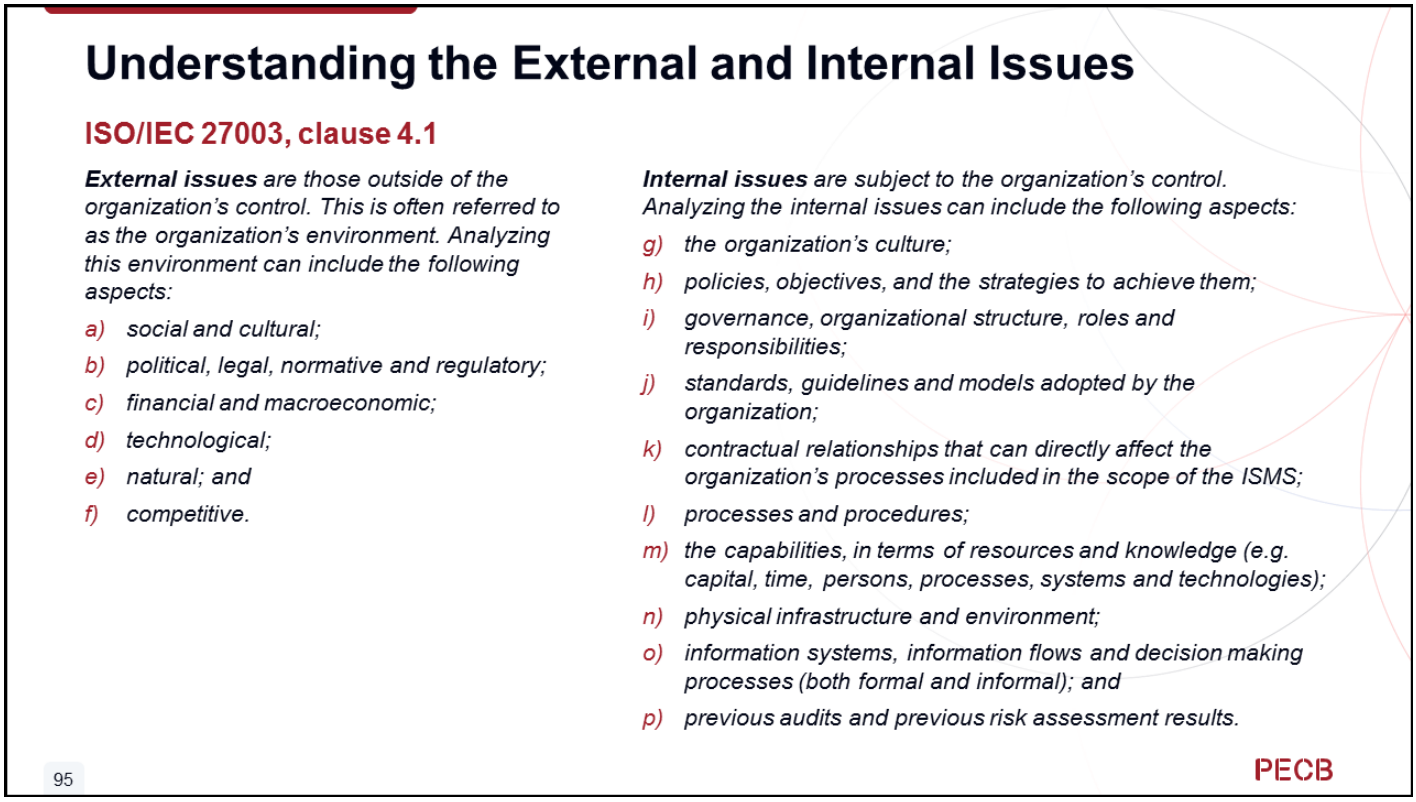
  Implications for the ISMS: The values of the organization influence the choices made by information security professionals. For example, values can impact the process of evaluating information security risks.

- **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 the ISMS: As for strategy, the ISMS must be aligned with the organization's objectives in order to achieve the ultimate objective and ensure information security.

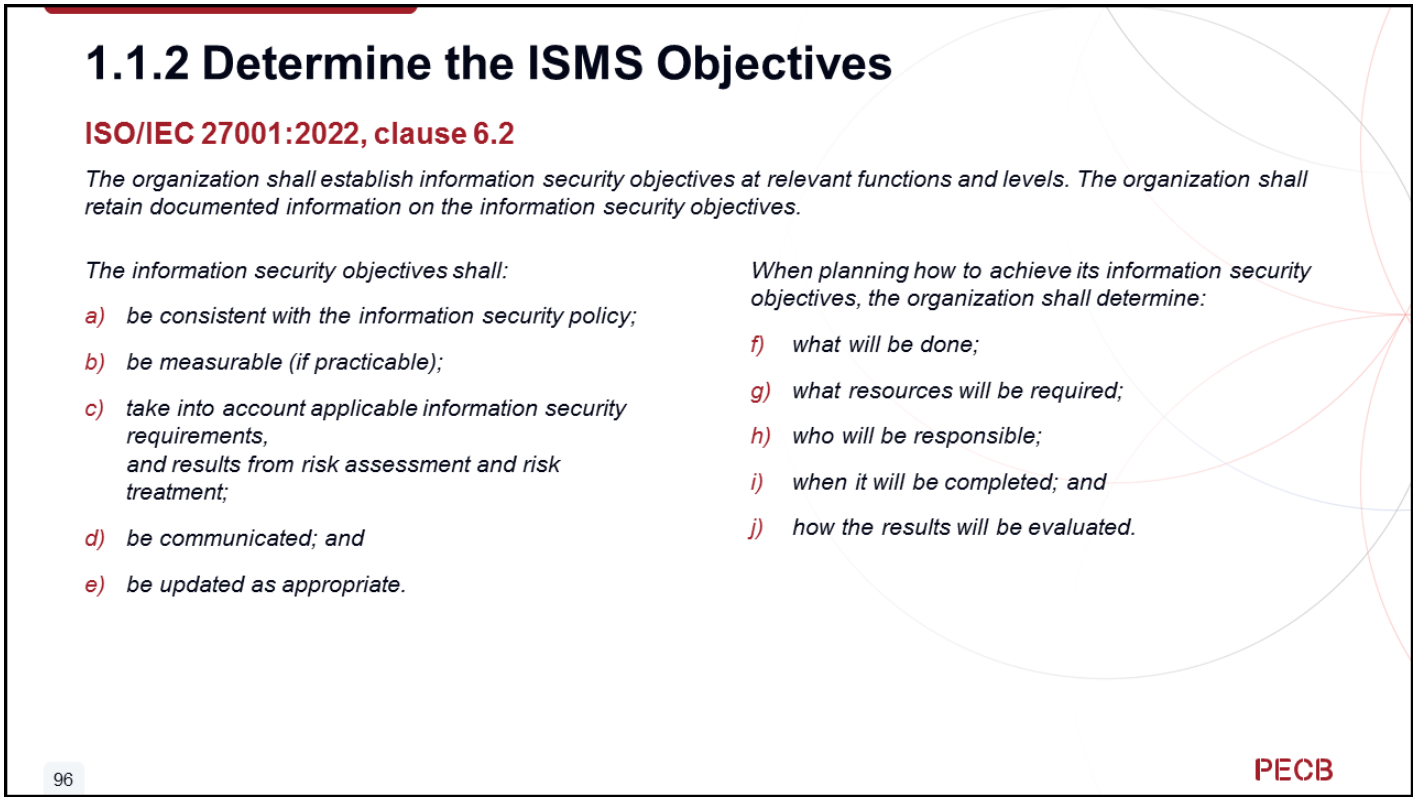
- **Strategies:** The strategy consists of a defined sequence of actions aimed at achieving one or more goals.

  Implications for the ISMS: The choice and results of actions will also depend on the information security strategy defined by the organization.



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.



The objectives of an ISMS are the expression of the organization's intent to treat the identified risks and comply with the set requirements. Nonetheless, it is necessary to first establish the ISMS objectives in collaboration with interested parties.

The ISMS objectives are important for determining the scope and must be validated at the highest level of the organization. Objectives can be modified as the project progresses, particularly after the completion of the risk analysis. Objectives must be documented properly.

Aspects and questions to consider when establishing information security objectives:

- **Improved risk management –** Can the implementation of the ISMS improve risk management?
- **Effective information security management –** Can the implementation of the ISMS improve information security?
- **Competitive advantage –** Can the implementation of the ISMS offer the organization competitive advantage?

Examples of ISMS Objectives

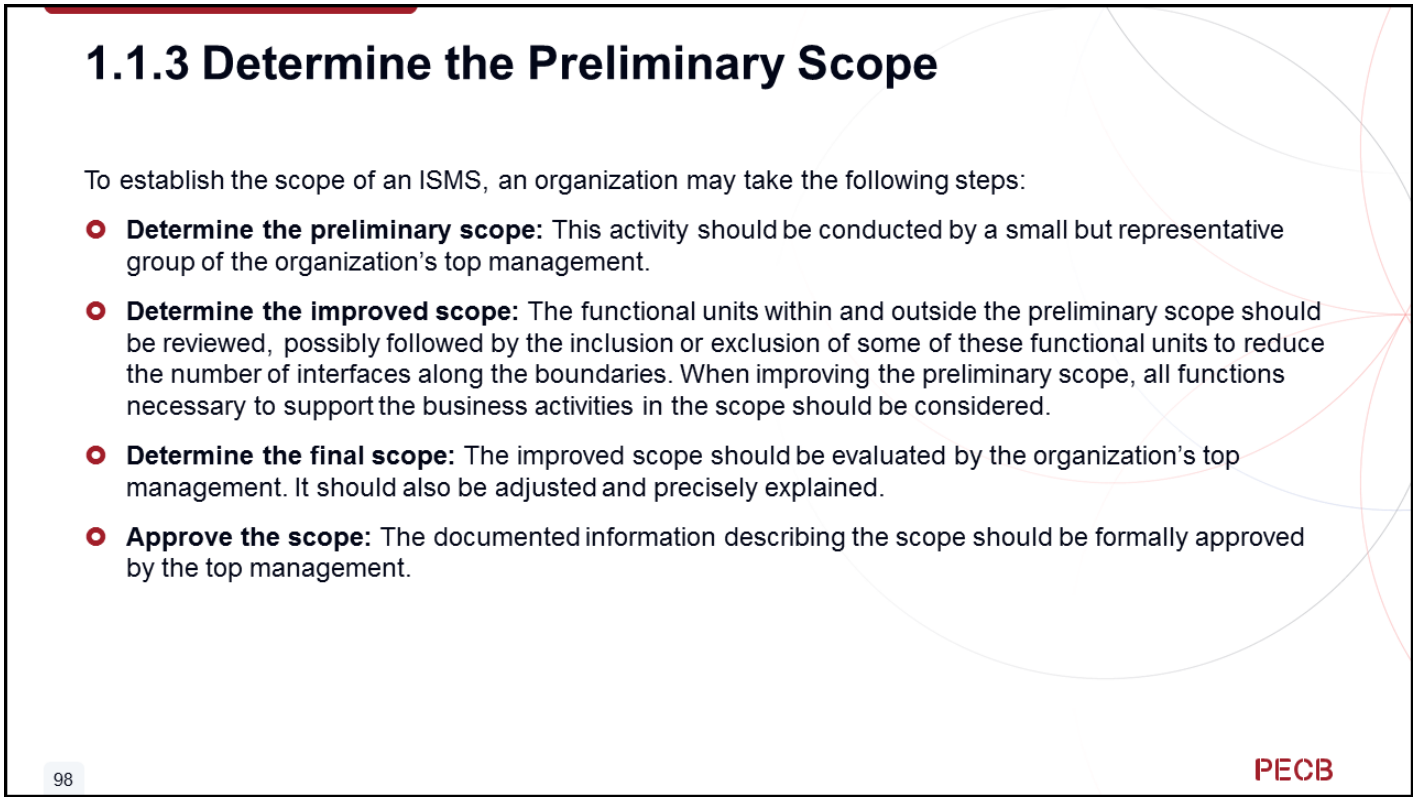
Examples of objectives related to the ISMS implementation:

- Ensure compliance with legal, regulatory, and contractual obligations
- Demonstrate due diligence
- Inspire confidence among the organization's interested parties
- Protect the organization's critical assets
- Ensure information security by following the best practices
- Improve the response to information security incidents
- Reduce the costs associated with information security incidents
- Facilitate business continuity

The determination of the objectives should take in consideration:

- Historical events within the organization
- Current and emerging risk exposures
- Prior operational disruptions and incidents
- Cost associated with potential disruptions
- Financial costs
- Liabilities
- Social responsibilities
- Success and failure of other information security projects and programs

PECB



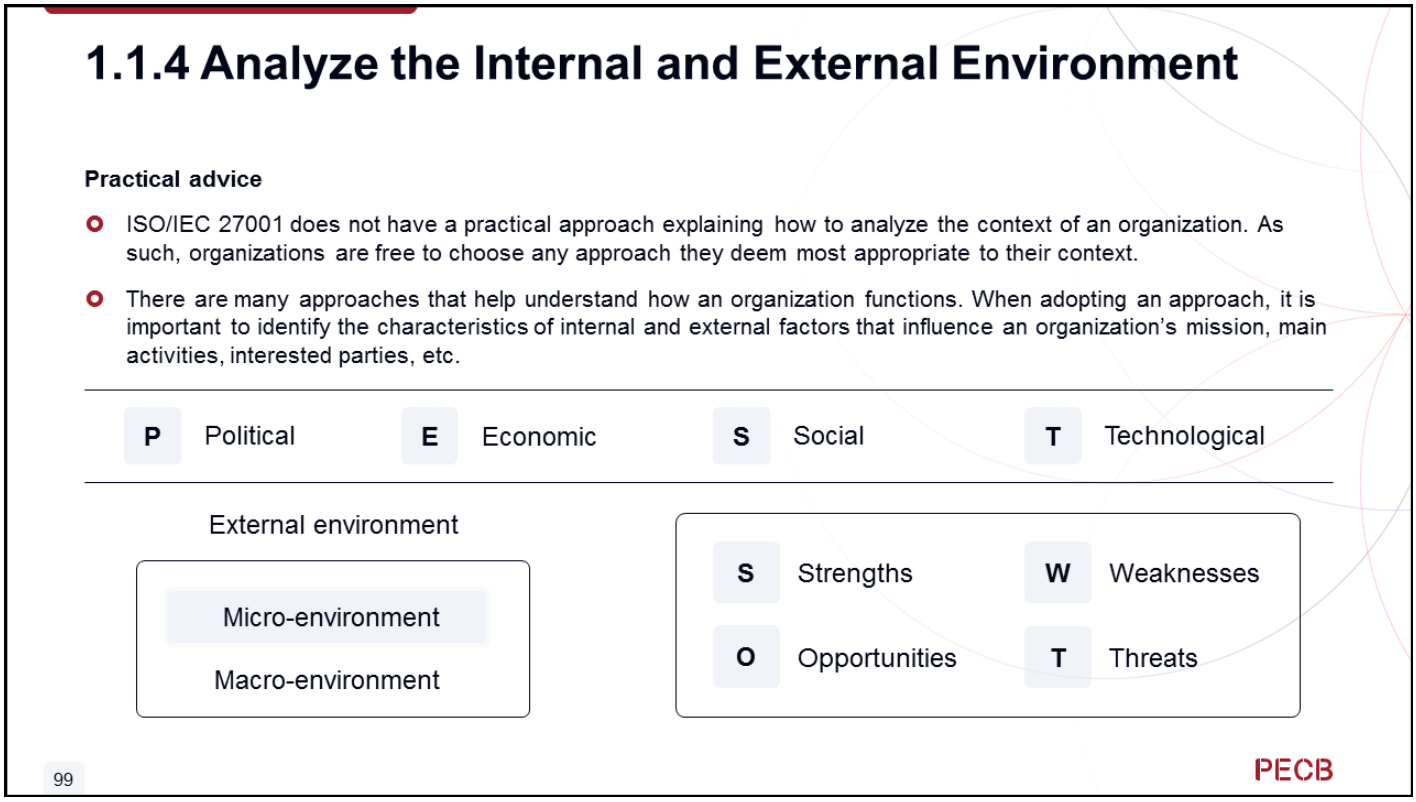
ISO/IEC 27003, clause 4.3 Determining the scope of the information security management system

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.

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

- What are the mandates for information security management established by the organization's 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 departments)?
- How will the ISMS-related documents be communicated throughout the organization (e.g., on paper or through the intranet)?
- Can the current management system support the organization's needs? Is it as fully operational, well-maintained, and functional as it was 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.



Several approaches have been already developed that help analyze and understand the context of an organization. In most organizations, there are studies conducted either internally or by other organizations on their context. It is advisable to collect these studies, analyze them, and interview some key interested parties in order to ensure an adequate understanding of the organization's context. However, it is important to mention that this process is not a project in itself.

The following approaches are particularly helpful in analyzing an organization's context:

SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis: SWOT analysis is used to conduct a thorough analysis of an organization's strengths, weaknesses, opportunities, and threats. The analysis is done with the aim of determining where the organization should invest its resources (take advantage of opportunities, reduce weakness, face threats, etc.). 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: PEST analysis allows organizations 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: 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 or services.

Analyze the Internal and External Environment

Organizational structure and key players

In order to understand the structure and main actors of the organization with regard to the scope, we should look at the following three levels of the organization:

- **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.

100

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 the strategic, administrative, and operational decisions within that unit.
2. **The functional structure:** The functional authority is exercised over proceedings, including planning and decision-making.

Notes:

- A division within the organization can be organized into functions, and vice versa.
- An organization can have a matrix structure, where the entire organization is based on the two structure types (divisional and functional).
- Whatever the structure, the following levels are distinguished:

    1. The strategic level (responsible for policies and strategies)
    2. The steering level (responsible for the coordination and management of activities)
    3. The operational level (responsible for eliminating threats and reducing information security risks)

Other tools used to analyze an organization's internal context include, but are not limited to, the following:

- Capacity assessment grid
- McKinsey's 7S framework
- Appreciative inquiry
- Core competencies technique
- Portfolio analysis

Internal Context — Key Aspects

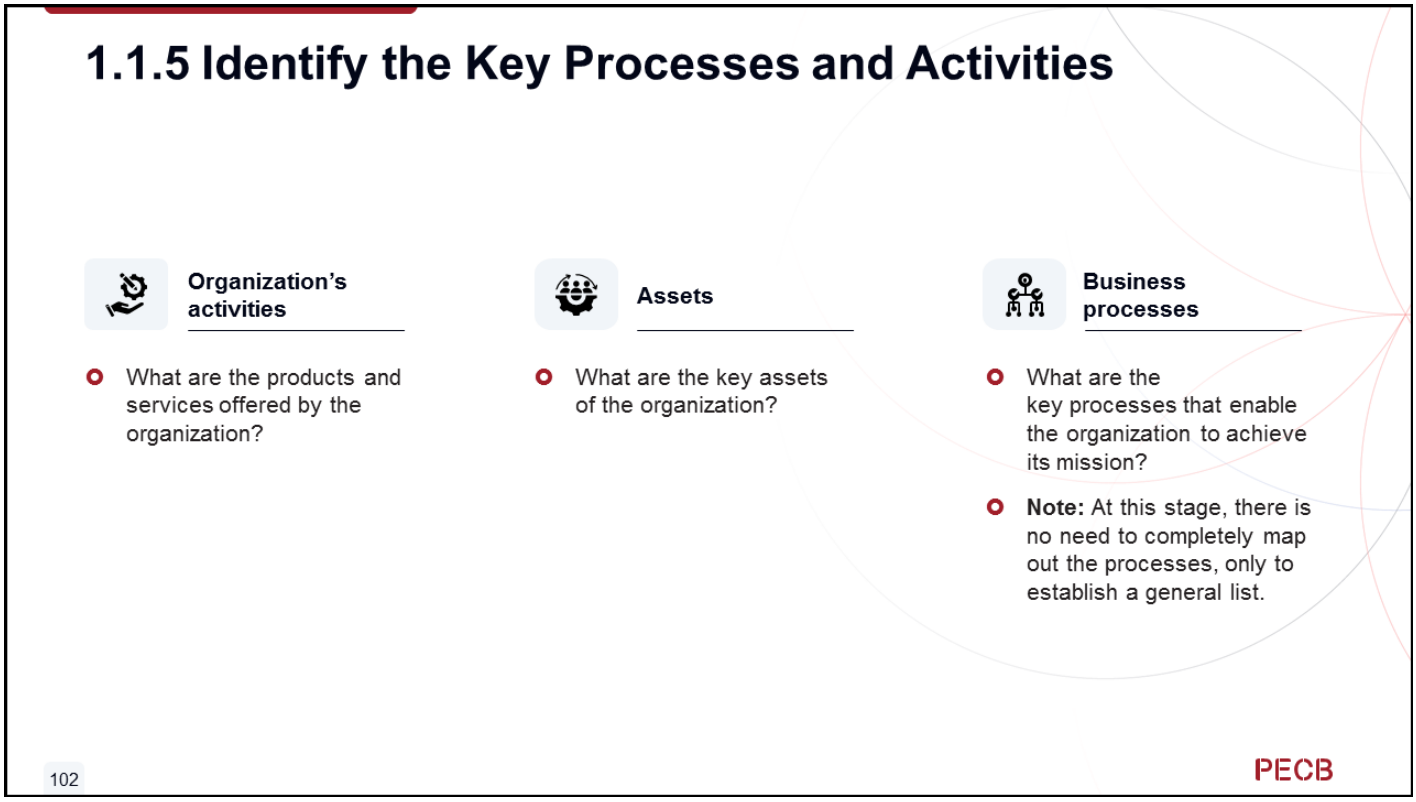
ISO/IEC 27000, clause 3.38

Internal environment in which the organization seeks to achieve its objectives

Note 1 to entry: Internal context can include:

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

PECB

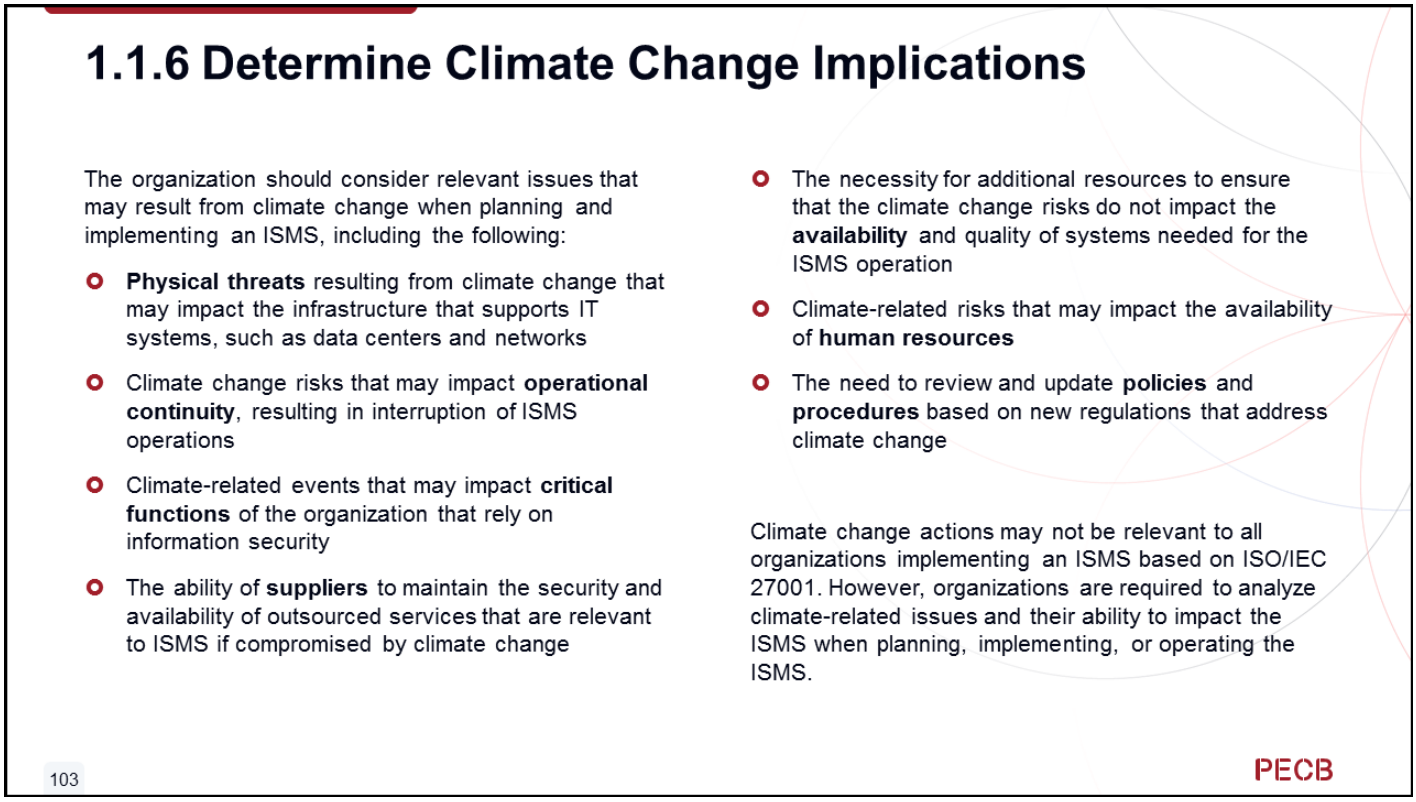


It is essential that the ISMS project manager is familiar with the organization's activities that affect information security. The type of products and services offered by the organization will certainly have a major impact on its business model. These products and services may also expose the organization to special risks, such as information security risks, liabilities, fines.

The ISMS project manager should also be familiar with the organization's business processes since these processes may expose the organization to numerous information security risks. As such, the project manager should analyze and understand the nature of these processes and determine the direct and indirect risks to which the organization is exposed during its activities and processes.

The identification of the organization's assets is crucial when establishing 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, ISMS project managers have to pay particular attention when they:

- Identify the owners of the assets
- Increase the owner's awareness of 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
- Determine the value that the organization attaches to the evaluated assets that can be absolute (e.g., a purchase price or replacement) or relative (direct cost or indirect loss caused by this asset)



What does climate change refer to?

Climate change refers to alterations in the typical weather conditions of a specific region or the entire planet over an extended period, usually spanning decades to centuries. These changes affect various aspects of Earth's climate, including temperature, precipitation patterns, humidity levels, wind patterns, and more. The term encompasses both natural variations and human-induced alterations to the climate system.

As per the 2021 Global Risks Report by the World Economic Forum, the greatest risk confronting communities worldwide is the inability to address and adjust to climate change. Some organizations might be heavily impacted by climate change due to their operations or the industry in which they operate, while others may be less impacted. By determining the degree to which climate change impacts its operations, the organization can determine the extent to which it needs to incorporate climate-related considerations into its decision-making processes, strategies, and actions. [1][2]

Organizations that determine climate change issues not relevant to their management system do not have to make any change to their existing ISMS but should document such decision.

Steps to Determine Climate Change Implications

The following steps can help in determining if climate change is a relevant issue to organization's purpose and if it can impact its ability to achieve the objectives of the ISMS[3]:

1. Conduct a risk assessment
2. Understand the expectations of interested parties
3. Analyze environmental regulatory requirements
4. Assess market trends and consumer preferences
5. Conduct a supply chain analysis
6. Evaluate financial implication
7. Manage reputational risk
8. Incorporate climate change in the long-term strategy

104

PECB

1. **Conduct a risk assessment:** A risk assessment enables organizations to evaluate how climate change could impact the organization's operations, supply chain, infrastructure, and information security. The risk assessment should consider both physical risks (such as extreme weather events, sea-level rise, and temperature changes) and transition risks (such as policy changes, market shifts, and reputational impacts).
2. **Understand the expectations of interested parties:** This step involves identifying key interested parties, including customers, investors, employees, suppliers, regulators, and community members, and assess their concerns and expectations regarding climate change. Their engagement can help the organization understand the impact of climate-related issues to its various interested parties.
3. **Analyze environmental regulatory requirements:** The organization should be aware of relevant climate-related regulations, policies, and international agreements that could affect its operations. This includes evaluating potential compliance requirements and the associated risks and opportunities.
4. **Assess market trends and consumer preferences:** The organization should monitor market trends and consumer preferences related to sustainability and climate change. It should also consider whether there is growing demand for environmentally friendly products.
5. **Conduct a supply chain analysis:** This involves assessing the climate-related risks and opportunities within the organization's supply chain, including potential disruptions, resource constraints, and opportunities for collaboration to address climate-related challenges collectively.
6. **Evaluate financial implications:** This involves the evaluation of potential costs associated with physical damage, regulatory compliance, carbon pricing, and changes in market dynamics. Opportunities for cost savings and revenue generation through investments in sustainability initiatives should also be considered.
7. **Manage reputational risk:** The organization should recognize the importance of reputation and brand image in the context of climate change. Considering how the organization's actions or inactions on climate-related issues could impact its reputation and relationships with interested parties is also important.
8. **Incorporate climate change in the long-term strategy:** Climate change should be considered when establishing the organization's long-term strategic planning process. The organization should identify opportunities to mitigate risks, capitalize on emerging trends, and contribute to global efforts to address climate change while achieving its mission and objectives.

1.1.7 Identify and Analyze the Interested Parties

ISO/IEC 27001, clause 4.2

The organization shall determine:

a) interested parties that are relevant to the information security management system;

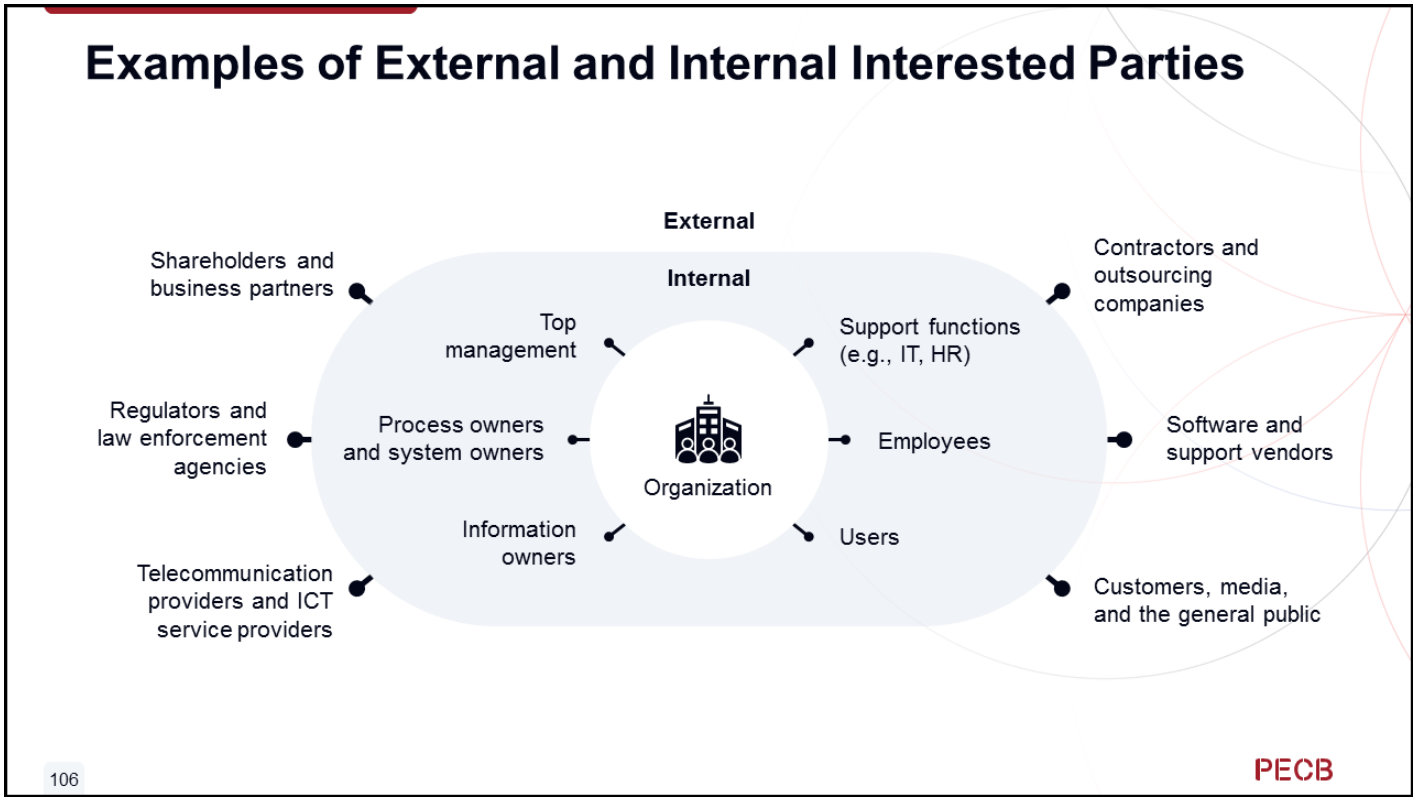
b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

NOTE 1 *The requirements of interested parties can include legal and regulatory requirements and contractual obligations.*

NOTE 2 *Relevant interested parties can have requirements related to climate change.*

PECB



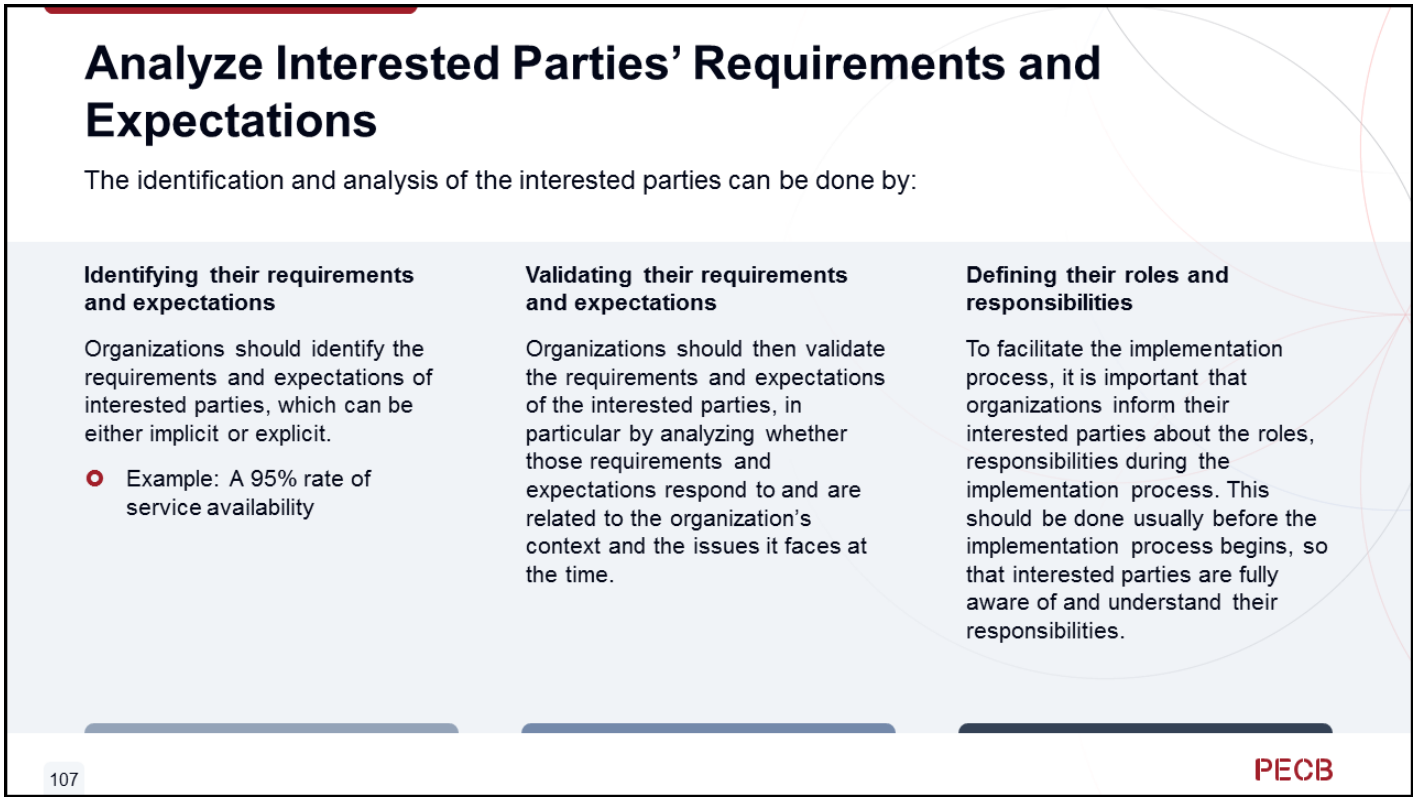
ISO/IEC 27003, clause 4.2 Understanding the needs and expectations of interested parties

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.

Identifying and analyzing interested parties can be challenging due to many issues that may arise, including conceptual ones, such as dealing with cultural or procedural differences:

- How to approach the interested parties and how to manage them in the long term
- How to balance the different opinions and needs of interested parties
- How to categorize the interested parties when there are no clear boundaries between them, when multiple interested parties groups exist, or when there is a coalition between some of the groups



There are six stages to conducting an interested parties analysis[5]:

1. Map interested parties relations
2. Map interested parties coalitions
3. Assess the nature of each interested party's interest
4. Assess the nature of each interested party's power
5. Construct a matrix of interested parties priorities
6. Monitor shifting coalitions

Note: The organization is obliged to inform all the interested parties of the actions taken regarding the ISMS and of the impact and responsibilities they have in it.

Understand Climate-Related Requirements of Interested Parties

The organization should identify and analyze the relevant requirements of interested parties related to climate change and determine which of these requirements need to be addressed through the ISMS. Such requirements of interested parties may include:

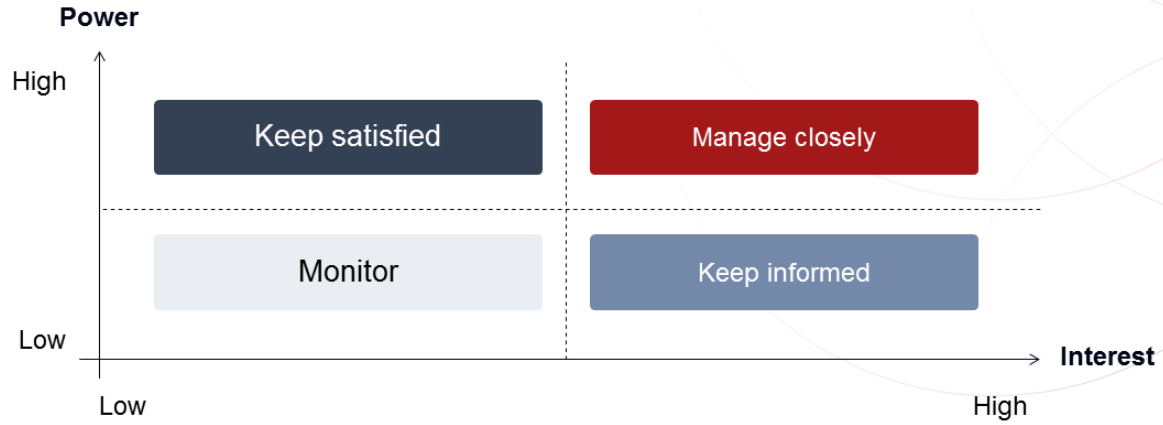
- **Regulatory compliance:** New laws and regulations required by regulatory bodies regarding climate change, industry standards, and other practices
- **Agreements between parent companies:** Changes to business plans of holding companies and contracting obligations
- **Customer requests:** New climate-related requirements of customers for products or services offered by the organization
- **Corporate social responsibility:** Meeting societal expectations for environmental management

PECB

Incorporating climate-related requirements into an ISMS means addressing environmental management in parallel with information security efforts. This process could involve adopting energy-efficient technologies to minimize IT operations' carbon footprint, implementing sustainable practices like recycling and waste reduction, assessing and mitigating risks associated with climate change impacts, and communicating with stakeholders about climate issues and sustainability progress. Through these actions, organizations can address environmental concerns within their ISMS framework, ensuring a comprehensive approach to both information security and environmental sustainability.

Power/Interest Matrix of Interested Parties

The Power/Interest matrix, developed by Johnson and Scholes[5], is a tool that assists in determining and managing the interested parties.



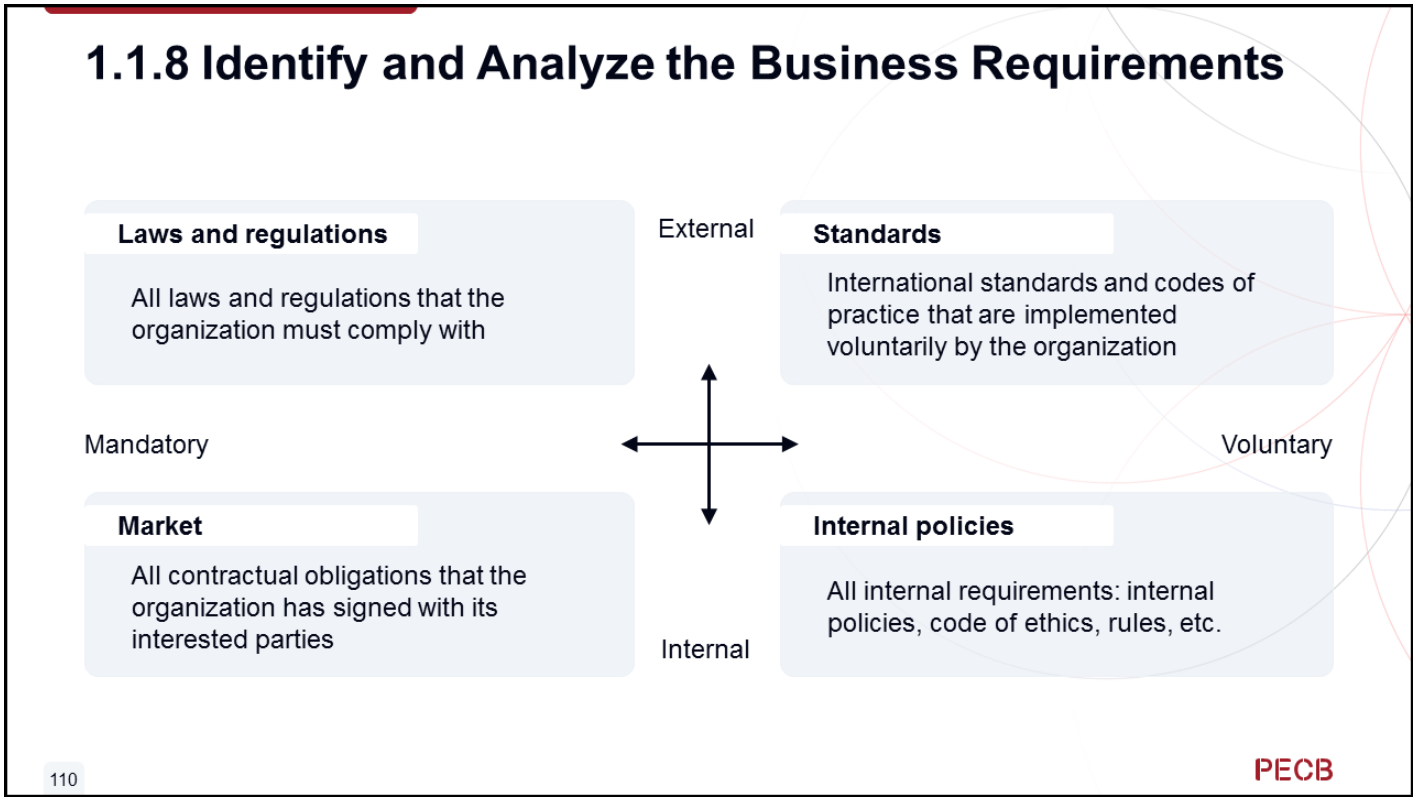
109

PECB

The matrix illustrated on the slide shows the relationship between two significant variables (interest and power). On one hand, the interest variable shows the interest of the interested parties in the organization's decisions and activities. On the other hand, the power variable shows how much power interested parties have on the organization's decisions and activities. Through the matrix, organizations can prioritize the effort required to meet the needs and expectations of interested parties.

Organizations may also categorize the different interested parties in the matrix, depending on the priority of:

- Identifying and listing relevant interested parties
- Determining the needs and expectations of interested parties by using different research methods
- Ranking the interested parties in terms of power and interest
- Setting priorities and objectives and reducing the risk of not meeting their needs and expectations

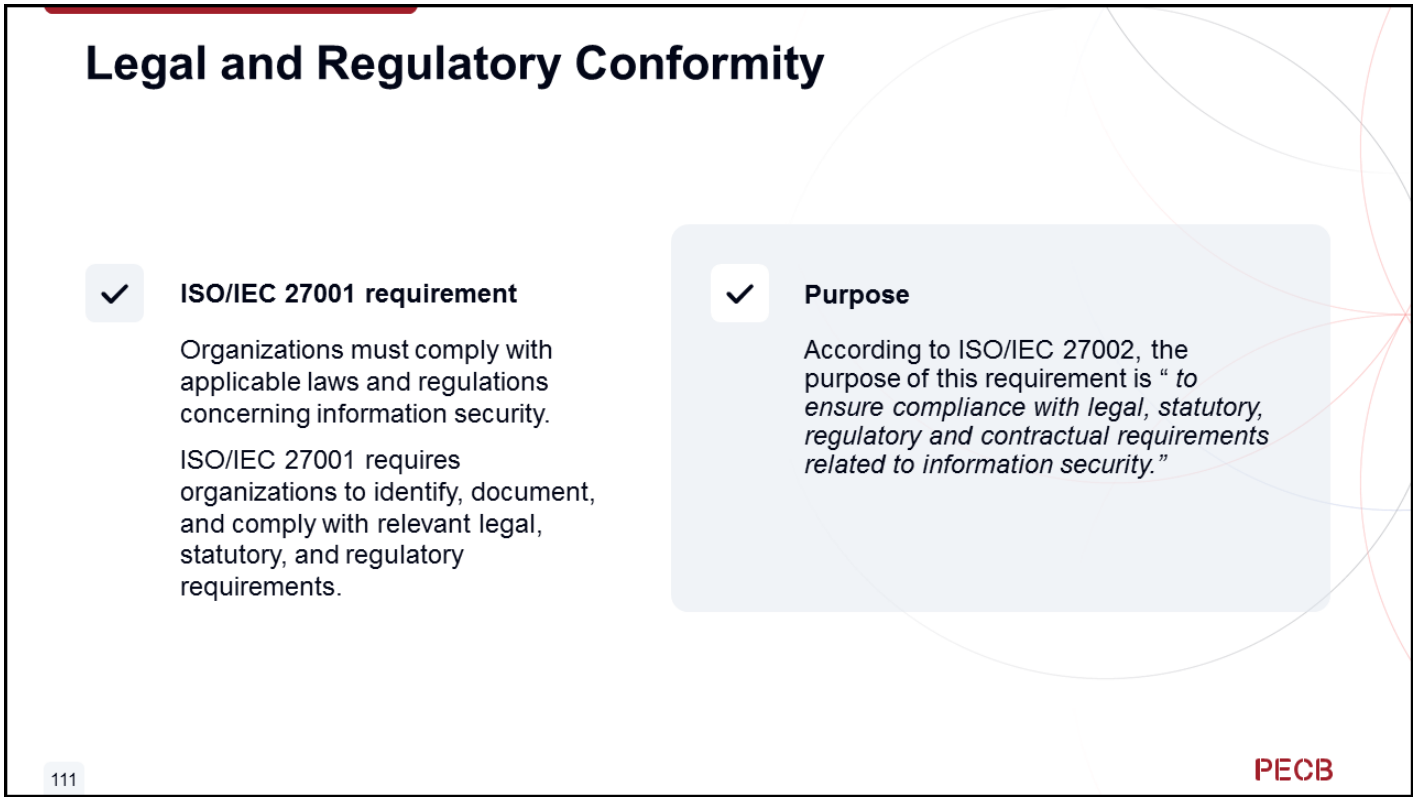


The organization must take into account the business, legal, or regulatory requirements and contractual obligations agreed upon with interested parties. To do so, it is important to identify and take into account all the requirements of the organization that could affect the ISMS implementation. They must be included in the risk assessment 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, for example, suited to analyze the legal implications and may, as a result, fail to identify the legal and contractual requirements.

The information security requirements for all organizations are mainly determined from four sources:

1. **Laws and regulations:** This will be discussed in the following slides.
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 an organization has no contractual obligation to deliver its products as planned, it goes without saying that this is a commercial policy 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 principles, rules, and guidelines that include all the requirements defined within the organization: internal policies, ethical codes, work rules, etc. It is worth noting that not complying with internal policies does not necessarily involve any legal implications.



ISO/IEC 27002, clause 5.31 Legal, statutory, regulatory and contractual requirements

Control

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.

Guidance

Legislation and regulations

The organization should:

a. *identify all legislation and regulations relevant to the organization's information security in order to be aware of the requirements for their type of business;*
b. *take into consideration compliance in all relevant countries, if the organization:*
   - *conducts business in other countries;*
   - *uses products and services from other countries where laws and regulations can affect the organization;*
   - *transfers information across jurisdictional borders where laws and regulations can affect the organization;*
c. *review the identified legislation and regulation regularly in order to keep up to date with the changes and identify new legislation;*
d. *define and document the specific processes and individual responsibilities to meet these requirements.*

Legal and Regulatory Conformity

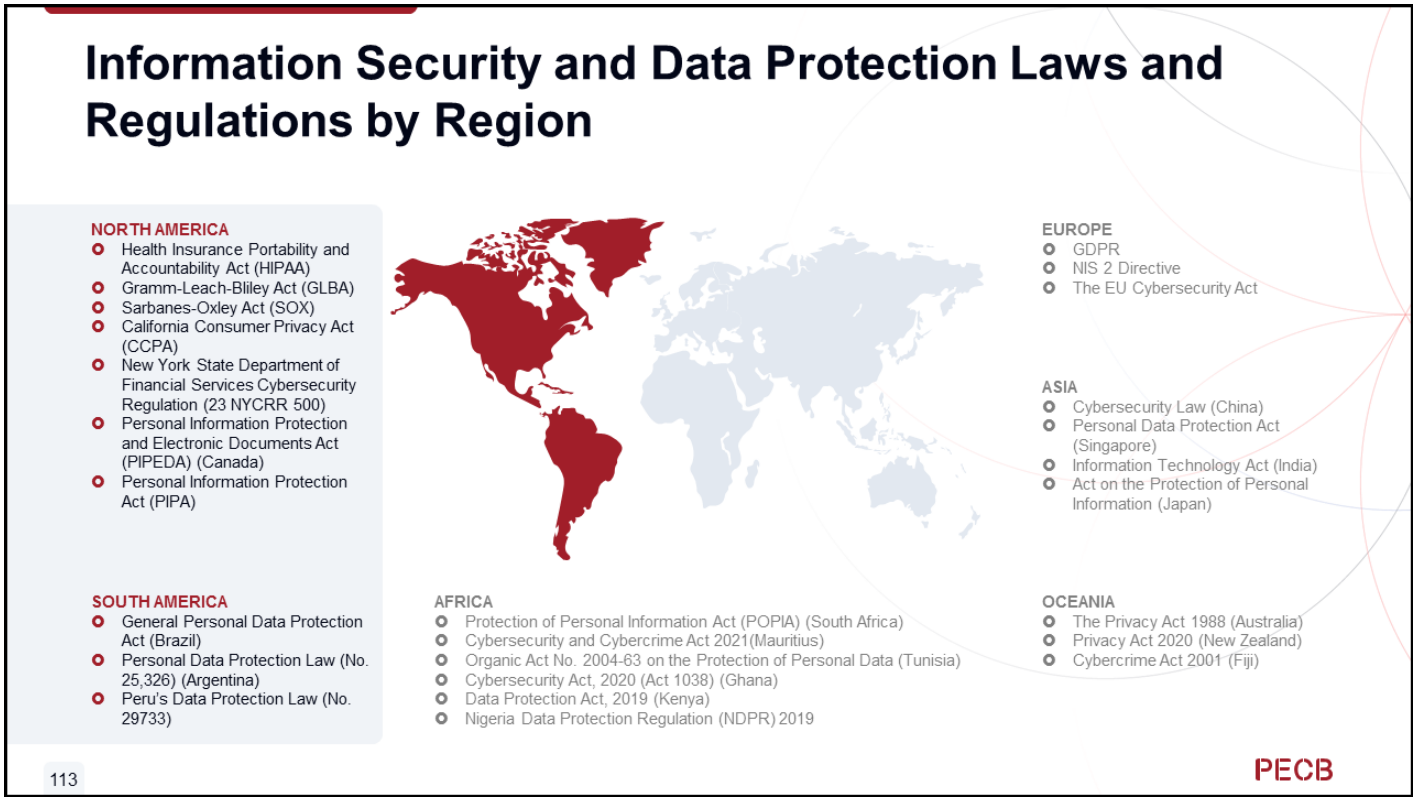
Key areas to monitor

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

112

PECB

1. **Data protection:** Many countries have established data protection laws and regulations that aim to safeguard 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.
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 the transfers of funds 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.

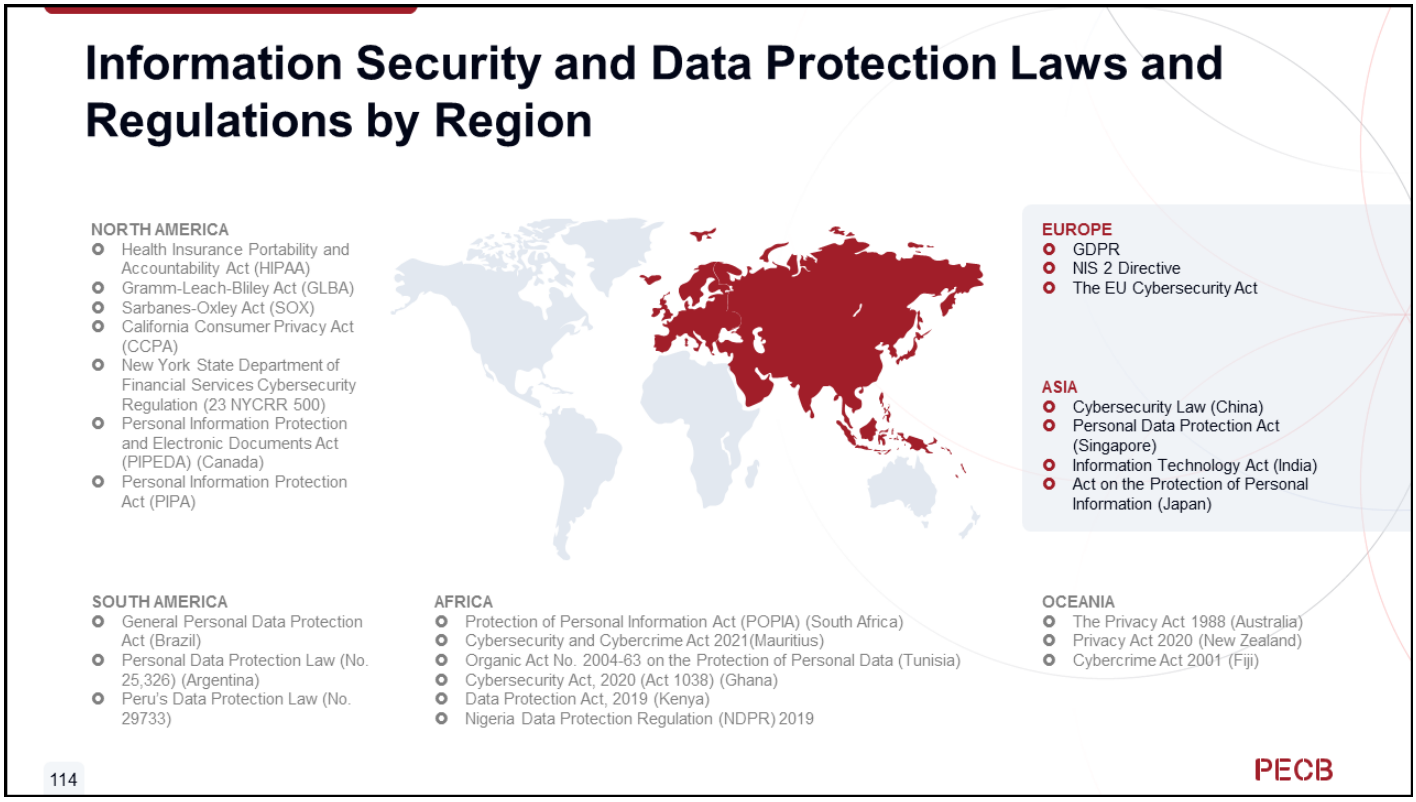


NORTH AMERICA:

- **Health Insurance Portability and Accountability Act (HIPAA)** regulates the privacy and security of medical information in the United States.
- **Gramm-Leach-Bliley Act (GLBA)** requires financial institutions to protect consumer financial information.
- **Sarbanes-Oxley Act (SOX)** regulates financial reporting and auditing requirements for public organizations in the United States.
- **California Consumer Privacy Act (CCPA)** regulates how organizations handle California residents' personal information.
- **New York State Department of Financial Services Cybersecurity Regulation (23 NYCRR 500)** requires financial institutions to establish and maintain a cybersecurity program.
- **Personal Information Protection and Electronic Documents Act (PIPEDA)** regulates how Canadian private sector organizations collect, use, and disclose personal information.
- **Personal Information Protection Act (PIPA)** is a privacy law that governs the collection, use, and disclosure of personal information by private sector organizations in British Columbia, Canada.

SOUTH AMERICA:

- **General Personal Data Protection Act (Brazil)** is a data protection law that regulates the processing of personal data in Brazil. It applies to both Brazilian and foreign organizations that process personal data of individuals located in Brazil.
- **Personal Data Protection Law (No. 25,326) (Argentina)** addresses the collection, processing, storage, and transfer of personal data. Under the law, individuals have the right to access, modify, and delete their personal data held by data controllers, as well as the right to object to the processing of their data.
- **Peru's Data Protection Law (No. 29733)** is a Peruvian law that regulates the processing of personal data by individuals and organizations. The law aims to protect the privacy of individuals by establishing principles and requirements for the collection, use, storage, and transfer of personal data.

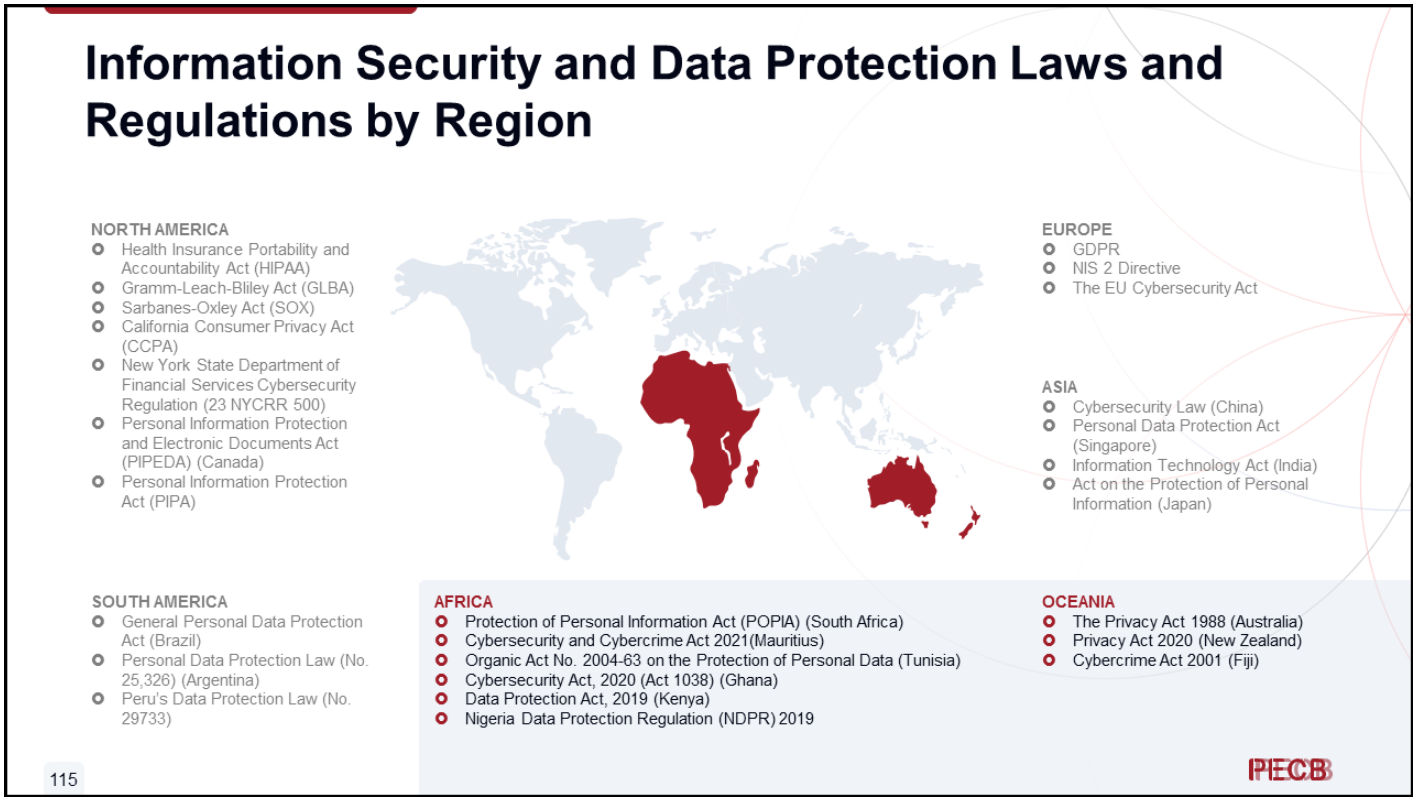


EUROPE:

- **GDPR** regulates the privacy and security of personal information for individuals within the European Union.
- **NIS 2 Directive** is the initial EU-wide legislation on cybersecurity, designed to attain a uniform and elevated level of cybersecurity throughout the member states.
- **The EU Cybersecurity Act** creates a unified system for certifying ICT products, services, and processes related to cybersecurity in Europe.

ASIA:

- **Cybersecurity Law (China)** regulates the security of networks and personal information in China.
- **Personal Data Protection Act (Singapore)** regulates the collection, use, and disclosure of personal data in Singapore.
- **Information Technology Act (India)** regulates electronic transactions and digital signatures in India.
- **Act on the Protection of Personal Information (Japan)** regulates the handling of personal information in Japan.
- **The Basic Act on Cybersecurity (Japan)** establishes a basic policy for Japan's cybersecurity efforts, formulates a cybersecurity strategy, and effectively advances cybersecurity initiatives.



AFRICA:

- **Protection of Personal Information Act (POPIA) (South Africa)** is a data protection law in South Africa and it applies to any individual or legal entity that handles personal data.
- **Cybersecurity and Cybercrime Act 2021 (Mauritius)** is a law in Mauritius that deals with cybercrime and cybersecurity. The act provides for different penalties based on the severity of the offense committed, it can include a fine not exceeding two million rupees and imprisonment for a term not exceeding 25 years.
- **Organic Act No. 2004-63 on the Protection of Personal Data (Tunisia)** is the primary legal framework for data protection in Tunisia.
- **Cybersecurity Act, 2020 (Act 1038) (Ghana)** promotes a safe and secure digital environment, protects critical information infrastructure, and combats cybercrime in Ghana.
- **Data Protection Act, 2019 (Kenya)** regulates the processing of personal data and seeks to safeguard the privacy and data protection rights of individuals in Kenya.
- **Nigeria Data Protection Regulation (NDPR) 2019** is the first comprehensive data protection regulation in Nigeria, and it sets out the legal framework for the protection of personal data in Nigeria.

OCEANIA:

- **The Privacy Act 1988** governs the handling of personal information by Australian government agencies and private organizations. It requires organizations to have a privacy policy, obtain consent for collecting personal information, provide access to individuals to their personal information, and ensure the accuracy and security of personal information.
- **Privacy Act 2020 (New Zealand)** regulates the collection, use, and disclosure of personal information in New Zealand. It applies to all organizations, including government agencies and businesses.
- **Cybercrime Act 2001 (Fiji)** was enacted by the Fiji government, which criminalizes a range of cyber offenses, including unauthorized access to computer systems, cyberstalking, and cyberbullying.

Section 6 Summary

- To understand the organization and its context, it is necessary to obtain general information regarding its mission, strategies, purpose, and values. This helps to ensure the alignment of information security objectives and the organization's mission.
- The structure of the organization may be divisional and functional.
- The internal context can include governance, organizational structure, policies, objectives, the organization's culture, etc.
- The organization can identify and analyze the interested parties by identifying and validating their requirements and expectations and defining their roles and responsibilities.
- The ISMS requirements for all organizations are mainly derived from four sources: laws and regulations, market, internal policies, and standards.
- The organization must adhere to the applicable laws and regulations.

Questions?

Quiz 5

Note: To complete Quiz 5, please go to the Quizzes Worksheet.

This section provides information that will help the participant gain knowledge on the ISMS, organizational, information security, and physical boundaries. In addition, the participant will also learn more about the ISMS scope statement.

ISMS Scope

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

PECB

ISO/IEC 27001's Requirements for Determining the ISMS Scope

ISO/IEC 27001, clause 4.3

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) *the external and internal issues referred to in 4.1;*

b) *the requirements referred to in 4.2;*

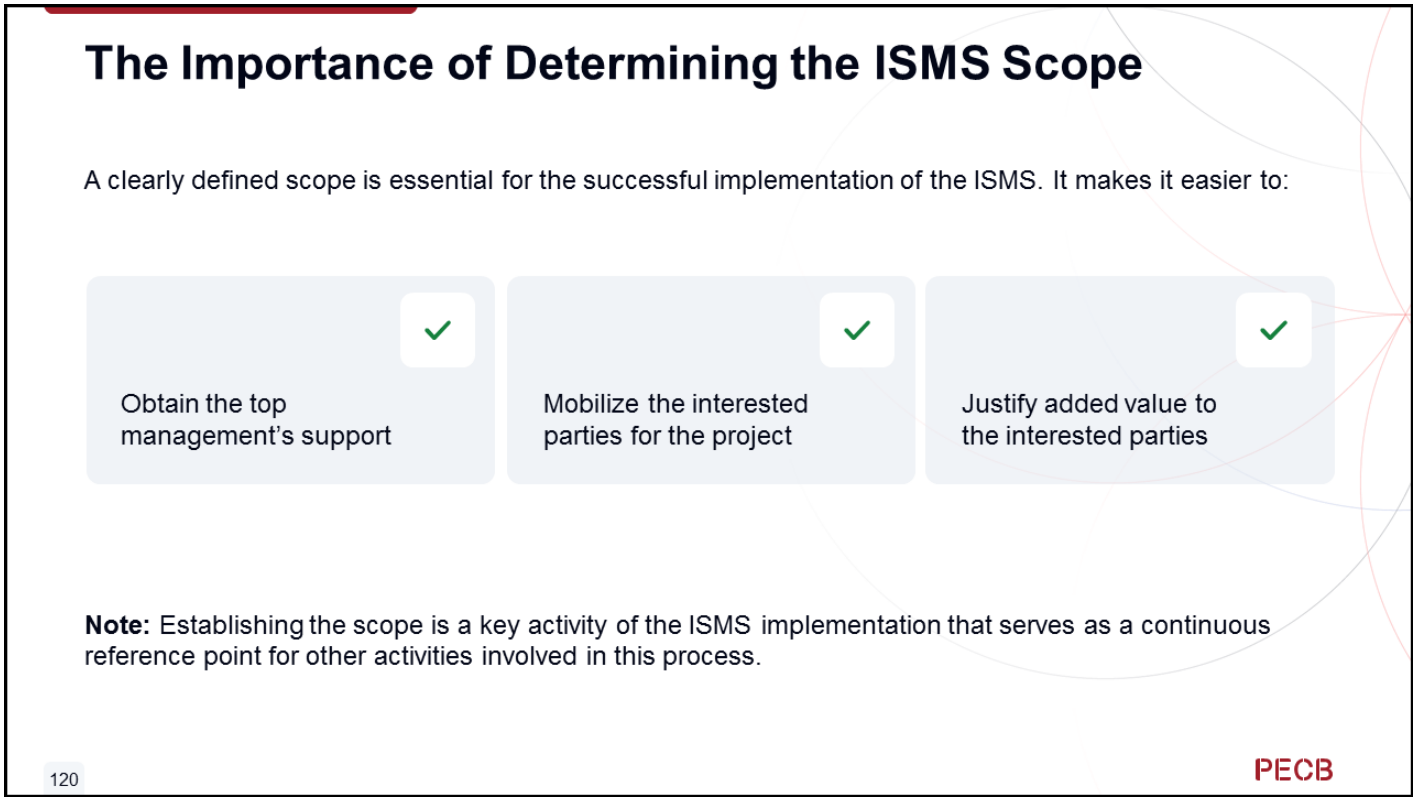
c) *interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.*

119

PECB

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

1. Document the ISMS scope
2. Define the boundaries of the management system
3. Justify and document exclusions



Application areas which provide no value to the interested parties and do not match their expectations should be excluded from the scope. For example, a bank that is having its training center certified to ISO/IEC 27001 may not create value for its customers or increase their perception of security. If this is the case, this can even be regarded as deception.

The extent of the scope will be the primary factor influencing the amount of effort required by the project. Obviously, for an organization of 20,000 employees with 30 divisions spread over six countries, it will be easier, faster, and less expensive to certify just one division or a key process rather than the whole organization.

If there is already a management system implemented within the organization, such as a quality management system (QMS) based on ISO 9001, the ISMS scope may cover the same area, partly overlapping the first system or be completely independent of it.

1.2 ISMS Scope

List of activities

Define the organizational boundaries

Define the information system boundaries

Define the physical boundaries

Define the ISMS scope

PECB

Boundaries of the ISMS

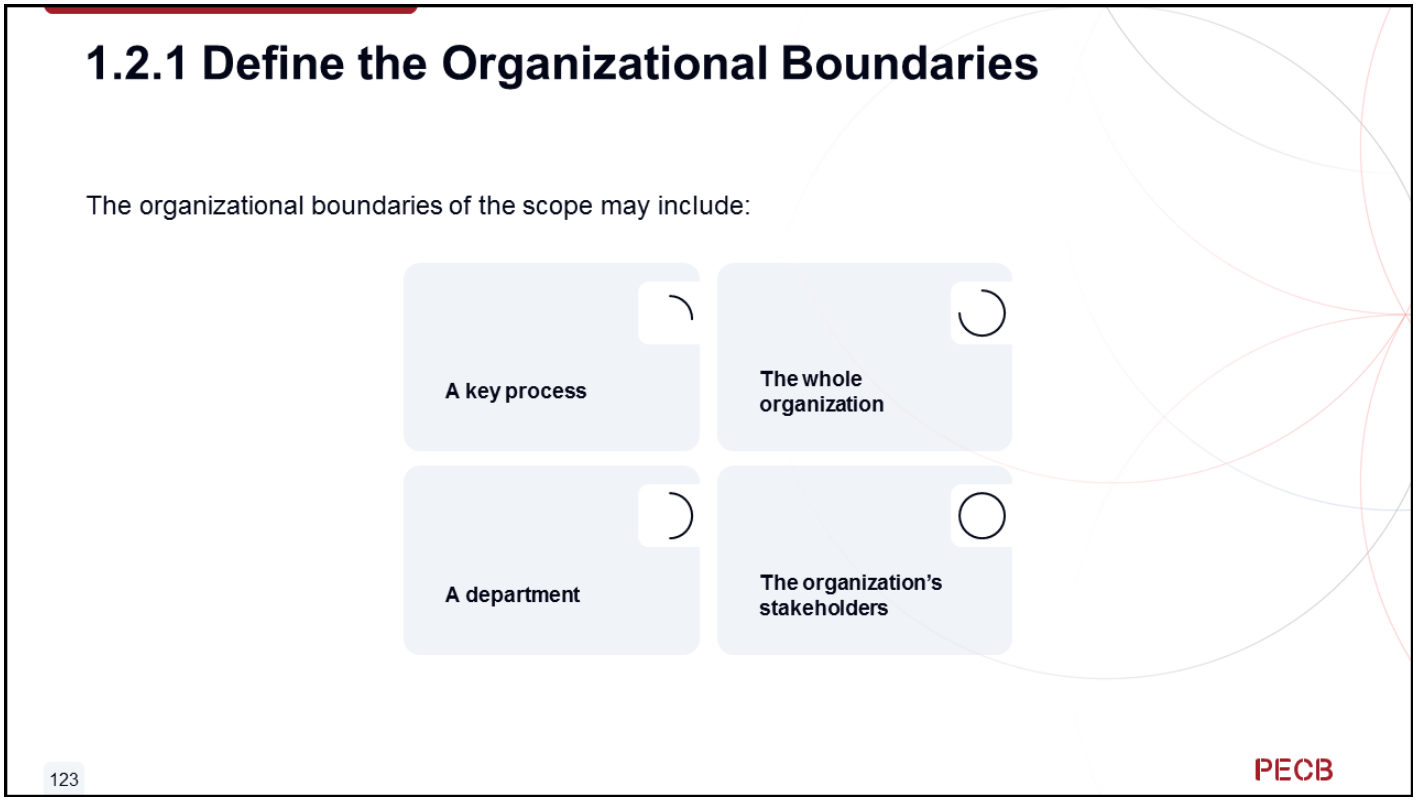
There are three dimensions to consider when defining the boundaries of the ISMS scope:

Organizational boundaries

Information system boundaries

Physical boundaries

PECB



Two approaches to the definition of "boundary" are commonly binding. The realistic approach adopts the definition of boundary used by the users themselves. In contrast, a common approach is that the program manager will choose a boundary that reaches their analytical objectives. The geographical boundaries (office of the organization, etc.) and temporal boundaries (time, desktop programs) are practical methods to define the organizational boundaries.

When defining the organizational boundaries, the following have to be considered:

1. Organizational units: departments, service projects, subsidiaries, etc.
2. Organizational structures and the responsibilities of managers
3. Business processes: sales, procurement, etc.

An efficient method for determining organizational boundaries is to evaluate decision-makers' responsibilities and their areas of influence within the organization. For instance, an organization is planning to implement an ISMS in its finance department; by analyzing key processes and services that fall under the CFO (chief financial officer), the boundaries can be proposed at the organizational level. As a result, if employee compensation is managed by the HR Department (rather than by the Finance Department), this responsibility is to be documented as excluded from the scope.

The deliverables for this activity are:

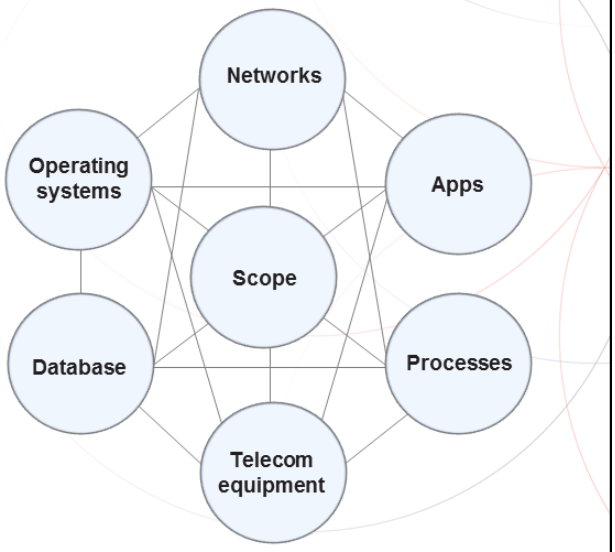
1. Description of the organizational boundaries with documented justification of exceptions
2. Description of organizational structures included in the ISMS
3. Identification of business processes and information assets (with their owners)
4. Identification of the "decision-making direction and processes"

Note: In a highly decentralized organization, it may be desirable to establish a different ISMS for each division and then have each of them certified independently. In contrast, a highly centralized organization will tend to have only one ISMS directed and controlled from headquarters.

1.2.2 Define the Information System Boundaries

- All system components should be taken into account; the focus is not to be limited to hardware components only.
- In terms of information system boundaries, all system components should be taken into account and not be limited to hardware such as servers and telecommunications equipment only. The technological constraints and contractual obligations of the organization should also be considered.

Note: In theory, the lack of technical infrastructure does not prevent an organization from obtaining an ISO/IEC 27001 certification.



124

PECB

The boundaries of information systems in particular are defined in terms of:

1. Networks: internal networks, wireless networks, etc.
2. Operating systems: Windows, Linux, etc.
3. Applications: CRM (customer relationship management), software management payroll, ERP (enterprise resource planning), utilities, database
4. Database: customer records, medical data, research and development, etc.
5. Processes: Consider processes that transport, store, or process information
6. Telecom equipment: routers, firewalls, etc.

The information systems supporting business processes should at least be included in the organizational boundaries of the scope. For example, it would be inappropriate to exclude customer databases and the CRM application if it includes accounts receivable management and the Customer Service Department. All the activities of a process and the exchange of information contained within the scope, including the inputs and outputs, should be taken into consideration. For instance, an organization plans to have its “checks servicing” certified. Internally, there is a program used to capture data and transfer information to a third party who issues the checks. As such, the organization must ensure the security of information, not just during the input phase, but also during the transfer and treatment process by the external party. For example, this insurance could take the form of a contractual agreement.

1.2.3 Define the Physical Boundaries

- All physical locations, both internal and external, included in the ISMS should be taken into account.
- The sites include all locations within the scope or part of the scope and the physical means required for them to work.
- In the case of leased sites, the interfaces with the ISMS and the applicable service agreements have to be considered. For instance, if a data processing center is leased, the organization must consider the geographic location where the center is located, even if they are not the owner.

125

PECB

The physical boundary of a system can be as simple as a socket on the wall, a port on a switch or the perimeter of a firewall. For example, in a metropolitan system, the physical boundaries could be defined by the particular building in the city where the system is used exclusively. On a more systemic basis, a system can also be defined by a particular set of servers connected to workstations in different geographical locations, and where everyone shares the same database. Thus, the physical boundaries tend to be more concrete than the logical borders, because they are tangible.

1.2.4 Define the ISMS Scope

ISO/IEC 27003, clause 4.3

The scope of an ISMS can be very different from one implementation to another. For instance, the scope can include:

a) *one or more specific processes;*

b) *one or more specific functions;*

c) *one or more specific services;*

d) *one or more specific sections or locations;*

e) *an entire legal entity; and*

f) *an entire administrative entity and one or more of its suppliers.*

The organization should also consider activities with 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.

PECB

Scope Statement

The organization should prepare a statement that defines the scope of the ISMS that is appropriate to the size, nature, and complexity of the organization. The statement should be available to interested parties. The scope statement should be:

1. As simple as possible
2. Understandable by external parties and those with limited knowledge about the organization
3. Precise enough to show what is covered by the ISMS, if the organization wishes to go through a formal certification process

Note: The process of defining a scope statement for the ISMS is completed at top management level; subject matter experts, such as consultants and business analysts, may assist.

PECB

Changes in the Scope

The scope can change over time so the ISMS continues to enable the organization to achieve its information security objectives.

Changes in the scope may be necessary due to:

- Changes in the internal environment (reorganization, new products, services, work methods, processes, etc.)
- Changes in the external environment (legal, competitive, technological)
- The emergence of new risks and opportunities
- Continual improvement activities

Any change in scope must be evaluated, approved, and documented.

PECB

Organizations should establish a process for change requests. Any change request should be justified and approved during a management review. If the organization is certified by a conformity assessment body (CAB), changes to the scope may require a review and approval by the CAB.

Documenting the Scope

ISO/IEC 27001, 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

Section 7 Summary

- A clear definition of the scope is an important success factor for the ISMS implementation.
- There are three types of boundaries of an ISMS that should be considered: physical boundaries, organizational boundaries, and boundaries of information systems.
- The scope of an ISMS can vary significantly between implementations, encompassing specific processes, functions, services, sections or locations, entire legal or administrative entities, and their suppliers.
- The scope statement for the ISMS should be completed at top management level; subject matter experts, such as consultants and business analysts, may assist.

Questions?

Quiz 6

Note: To complete Quiz 6, please go to the Quizzes Worksheet.

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

Day 1 Summary

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

- Training course objectives and structure
- Advantages of an ISMS based on ISO/IEC 27001
- Overview of the ISO/IEC 27001
- Confidentiality, integrity, and availability
- Vulnerability, threat, and impact
- Information security risk
- Classification of security controls
- ISMS implementation approach
- Context of the organization
- ISMS scope

Note: To complete Homework 1-3, please go to the Exercises Worksheet.