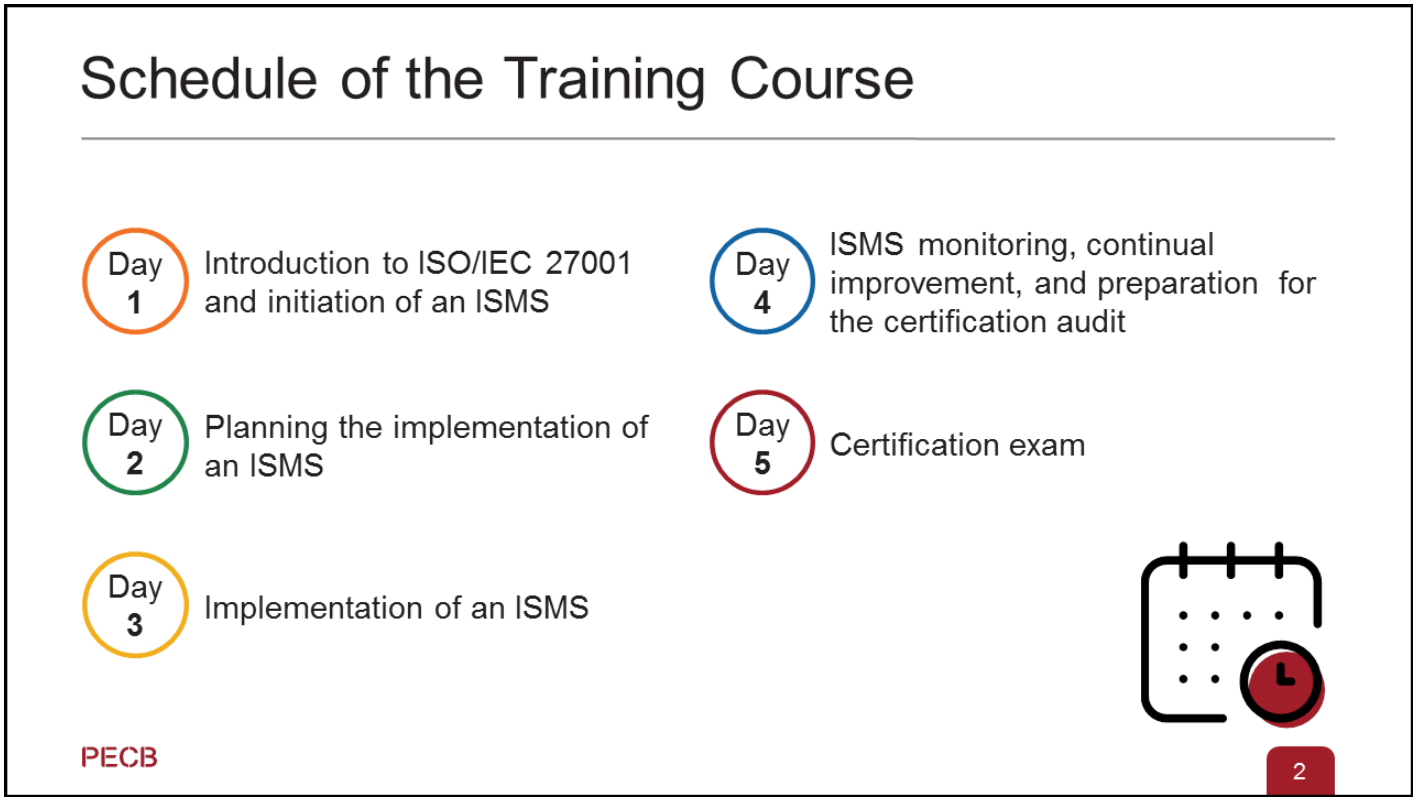
Version 7.1

Document number: ISMSLID1V7.1

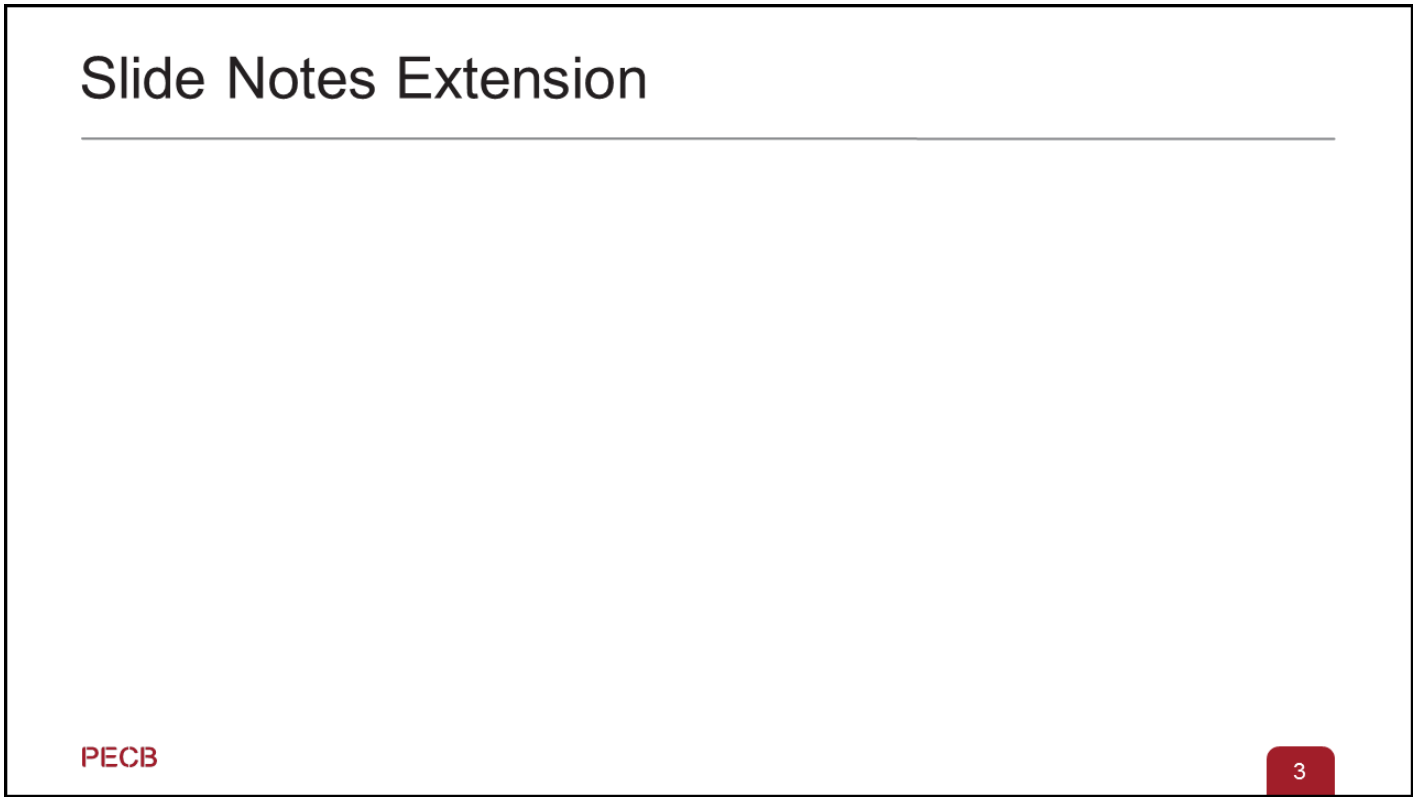


Day 1: Introduction to ISO/IEC 27001 and initiation of an ISMS

- Section 1: Training course objectives and structure
- Section 2: Standards and regulatory frameworks
- Section 3: Information Security Management System (ISMS)
- Section 4: Fundamental information security concepts and principles
- Section 5: Initiation of the ISMS implementation
- Section 6: Understanding the organization and its context
- Section 7: ISMS scope

Day 2: Planning the implementation of an ISMS

- Section 8: Leadership and project approval
- Section 9: Organizational structure
- Section 10: Analysis of the existing system
- Section 11: Information security policy
- Section 12: Risk management
- Section 13: Statement of Applicability



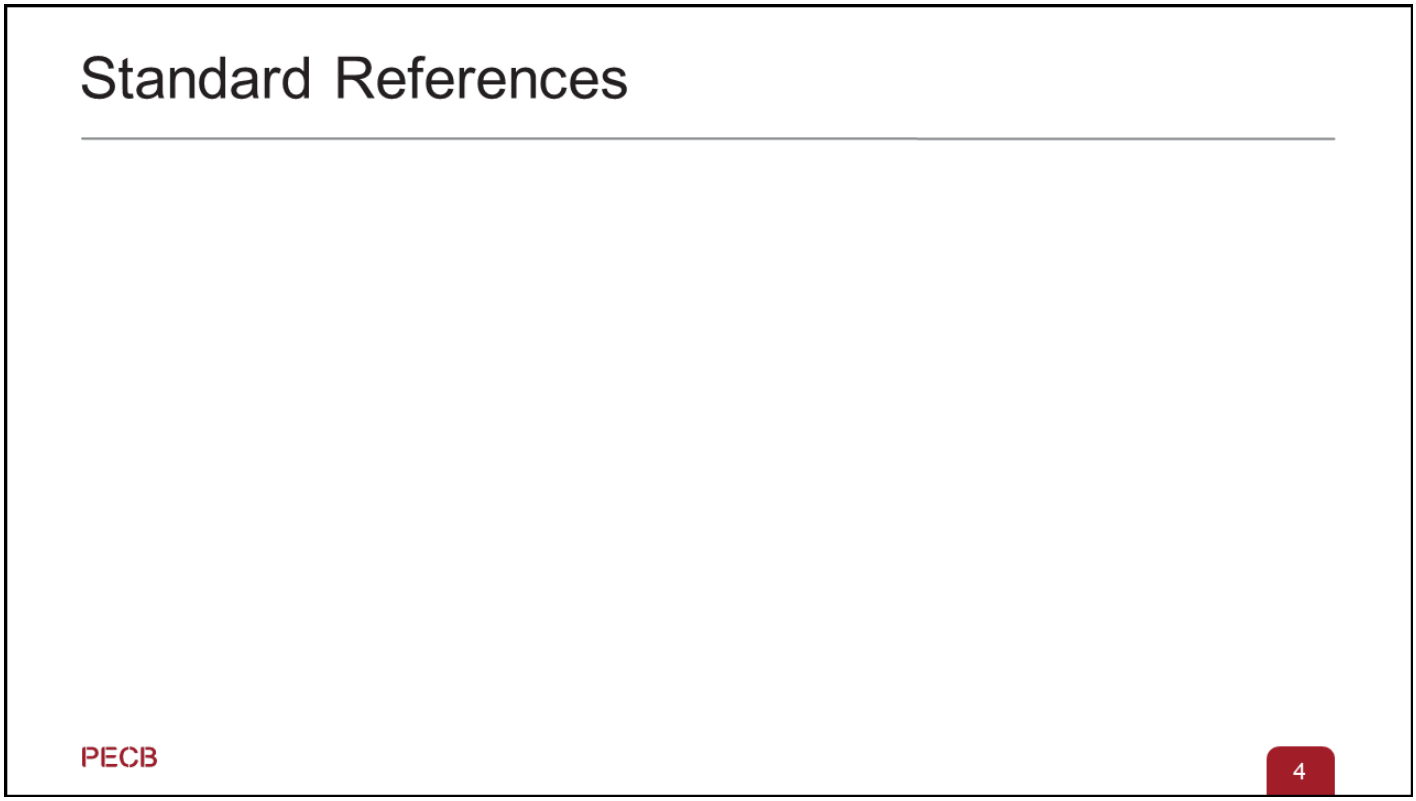
Day 3: Implementation of an ISMS

- Section 14: Documented information management
- Section 15: Selection and design of controls
- Section 16: Implementation of controls
- Section 17: Trends and technologies
- Section 18: Communication
- Section 19: Competence and awareness
- Section 20: Security operations management

Day 4: ISMS monitoring, continual improvement, and preparation for the certification audit

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

Day 5: Certification exam



Standard References

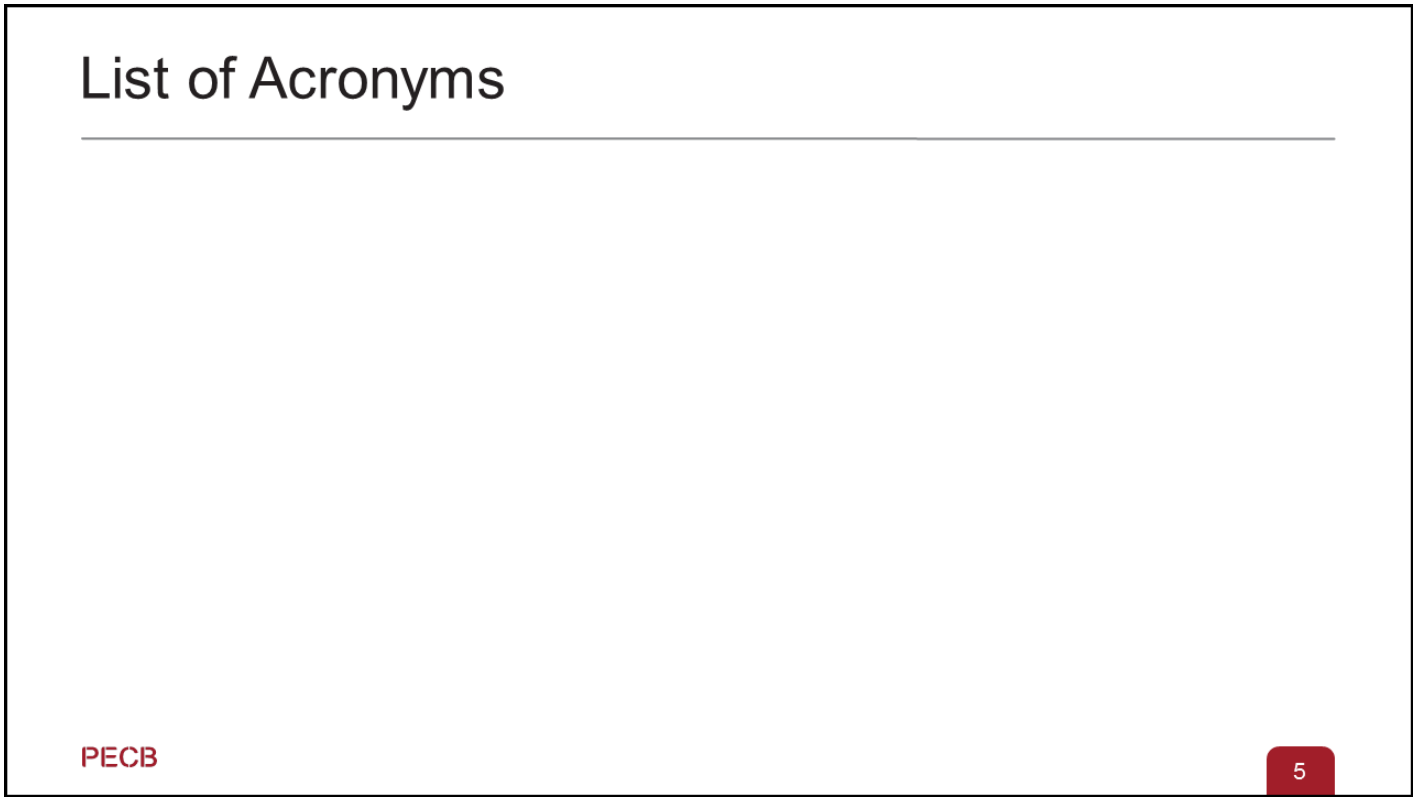
1.Main standard references:

- ISO/IEC 27000: 2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001: 2013, Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002: 2013, Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27003: 2017, Information technology — Security techniques — Information security management systems — Guidance
- ISO/IEC 27004: 2016, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005: 2018, Information technology — Security techniques — Information security risk management
- ISO/IEC 27021: 2017, Information technology — Security techniques — Competence requirements for information security management systems professionals

2. Other standard references:

- ISO 9000: 2015, Quality management systems — Fundamentals and vocabulary
- ISO 10015: 2019, Quality management — Guidelines for competence management and people development
- ISO/IEC 17011:2017, Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies
- ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
- ISO 17024: 2012, Conformity assessment — General requirements for bodies operating certification of persons
- ISO/ IEC 17065: 2012, Conformity assessment — Requirements for bodies certifying products, processes and services
- ISO/IEC 27006: 2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

- ISO/IEC 27007: 2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
- ISO/IEC TS 27008: 2019, Information technology — Security techniques — Guidelines for the assessment of information security controls
- ISO/IEC 27035-1: 2016, Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management
- ISO/IEC 27035-2: 2016, Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- ISO Guide 73: 2009, Risk management — Vocabulary
- ISO 31000: 2018, Risk management — Guidelines
- IEC 31010: 2019, Risk management — Risk assessment techniques
- ISO/IEC Directives, Part 1: 2019, Procedures for the technical work
- ISO 19011: 2018, Guidelines for auditing management systems



List of Acronyms

BCMS: Business Continuity Management System

BS: British Standard

CERT: Computer Emergency Response Team

CFO: Chief Financial Officer

CMM: Capability Maturity Model

CMS: Content Management System

CobiT: Control Objectives for Business and related Technology

COSO: Committee of Sponsoring Organizations of the Treadway Commission

CPD: Continuing Professional Development

CRO: Chief Risk Officer

CSIRT: Computer Security Incident Response Team

DMS: Document Management System

EA: European Co-operation for Accreditation

EDM: Electronic Document Management System

FISMA: Federal Information Security Management Act

GAAS: Generally Accepted Auditing Standards

GLBA: Gramm-Leach-Bliley Act

HIPAA: Health Insurance Portability and Accountability Act

IAF: International Accreditation Forum

IAS: International Accreditation Service

IDS: Intrusion Detection System

IFAC: International Federation of Accountants

IMS2: Integrated Implementation Methodology for Management Systems and Standards

IRM: Information Resources Management

IRT: Incident Response Team

ISMS: Information Security Management System

ISO: International Organization for Standardization

ITIL: Information Technology Infrastructure Library

LA: Lead Auditor

LI: Lead Implementer

NC: Nonconformity

NIST: National Institute of Standards and Technology

OECD: Organization for Economic Co-operation and Development

PCI-DSS: Payment Card Industry Data Security Standard

PDCA: Plan-Do-Check-Act

PIMS: Privacy Information Management System

PECB: Professional Evaluation and Certification Board

RFC: Request for Change

ROI: Return on Investment

ROSI: Return on Security Investment

RSO: Reduced-Sign-On

SABSA: Sherwood Applied Business Security Architecture

SMS: Service Management System

SoA: Statement of Applicability

SOC: Security Operations Center

SOX: Sarbanes-Oxley Act

SSO: Single-Sign-On

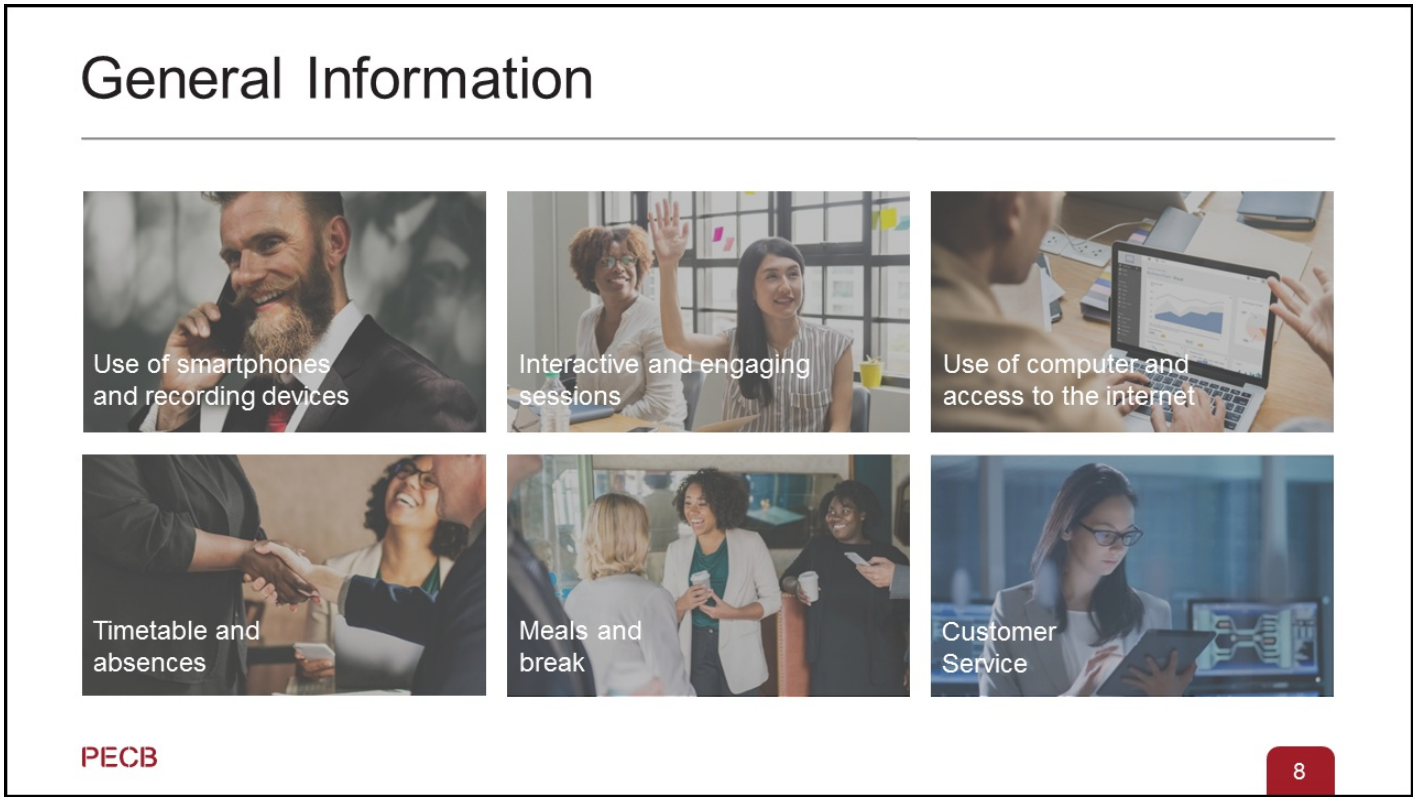
TOGAF: The Open Group Architecture Framework

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

To break the ice, participants introduce themselves stating their:

- Name
- Current position
- Knowledge of and experience with information security management
- Knowledge of and experience with ISO/IEC 27001 and other standards of the ISO/IEC 27000 family (ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, etc.)
- Knowledge of and experience with other management systems (ISO 9001, ISO 14001, ISO/IEC 20000, ISO 22301, etc.)
- Training course expectations

Duration of the activity: 20 minutes



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

Customer Service

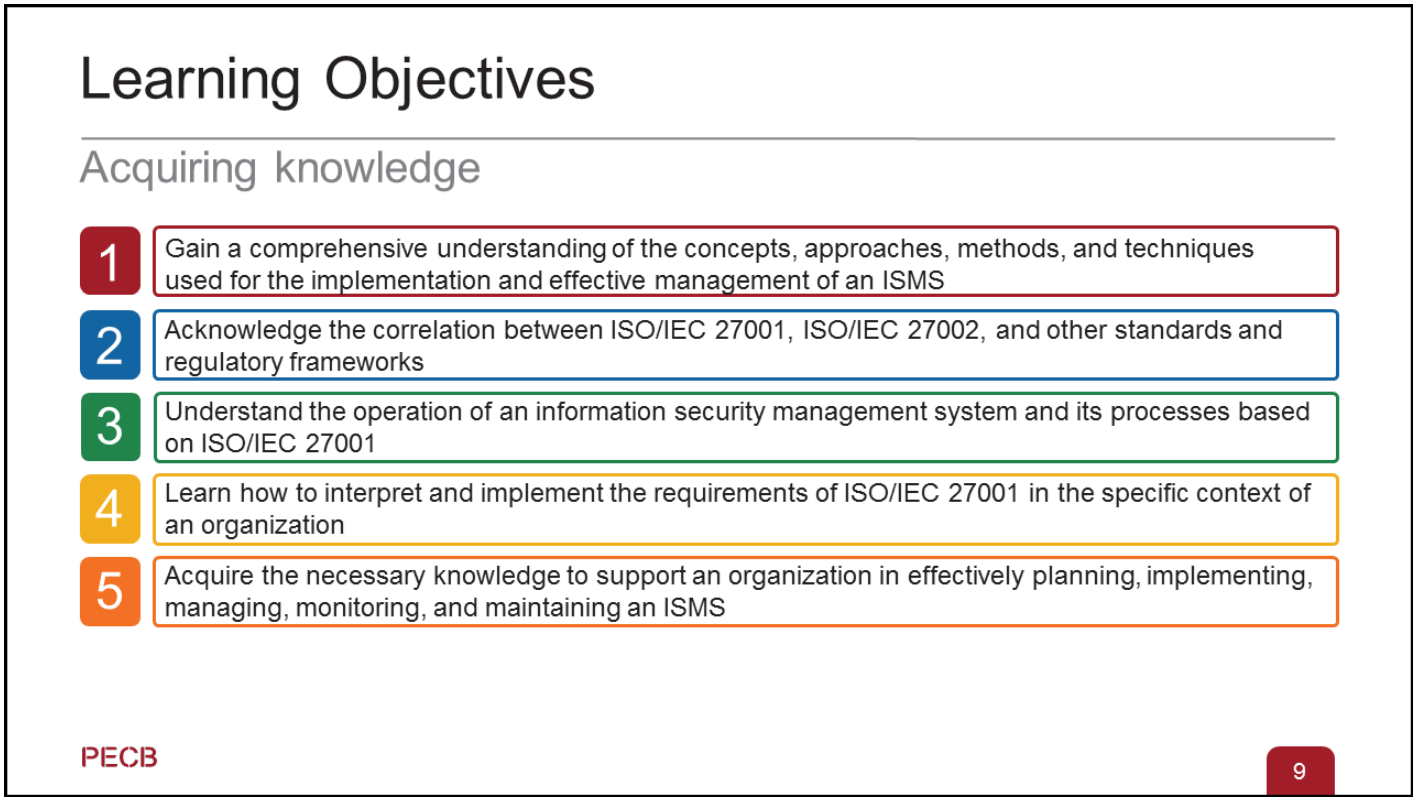
To ensure customer satisfaction and continual improvement, the PECB Customer Service has established a support ticket system for handling complaints of our clients.

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

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

If you have suggestions for improving PECB's training course materials, we would like to hear from you. We read and evaluate the input we get from our clients. You can do so directly from our KATE application, or you can open a ticket directed to the Training Development Department on the PECB Help Center (www.pecb.com/help).

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

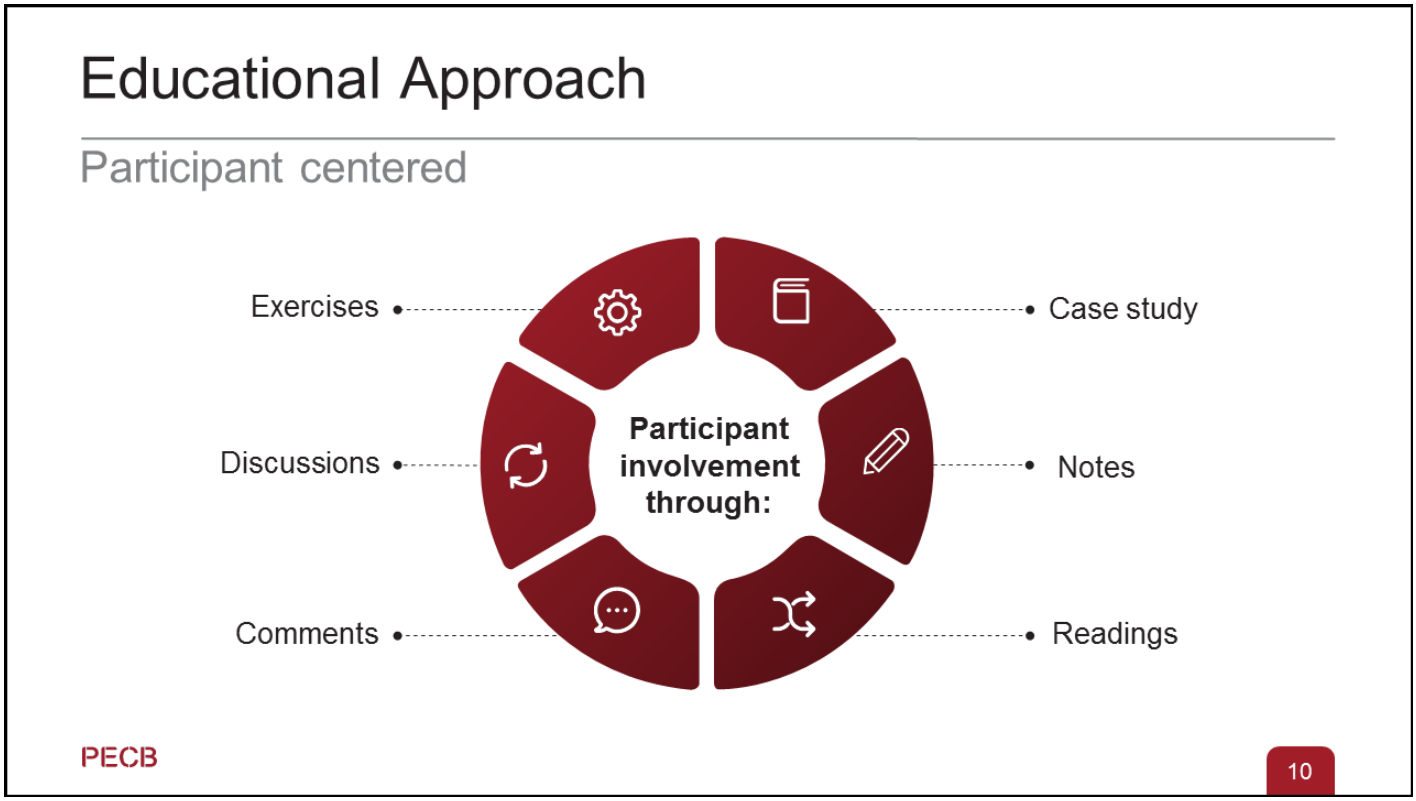


The training course is designed to help the participants acquire or enhance their competency to participate in the implementation of an information security management system (ISMS). From an educational perspective, competency consists of the following three elements:

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

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

To obtain more in-depth knowledge of an ISMS audit process, including the audit principles, techniques, and best practices, it is recommended to take the PECB Certified ISO/IEC 27001 Lead Auditor training course.



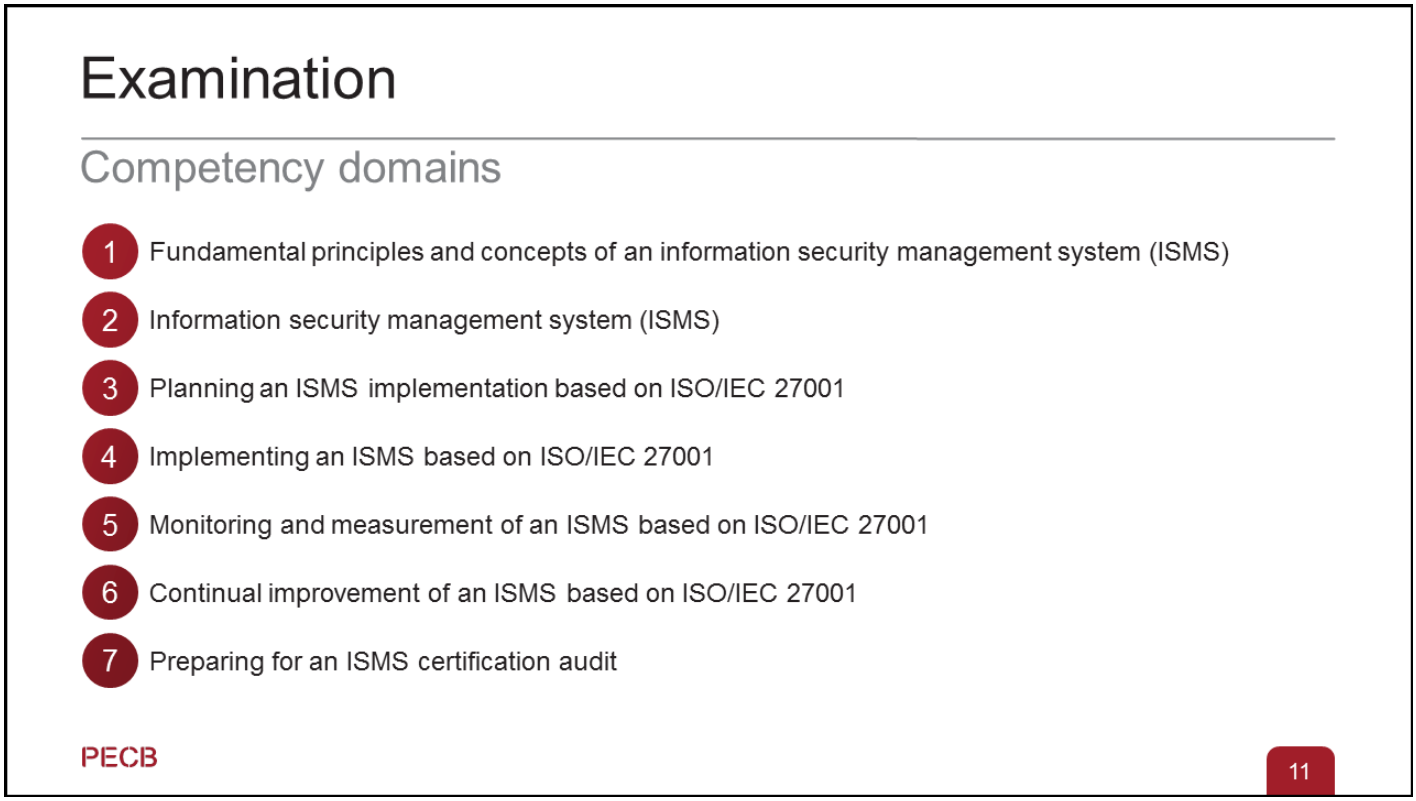
This course is primarily based on:

- Trainer-led sessions, where interaction by means of questions and suggestions is highly encouraged
- Participant involvement through various interactive exercises, case studies, notes, discussions (participant experiences), and so on

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

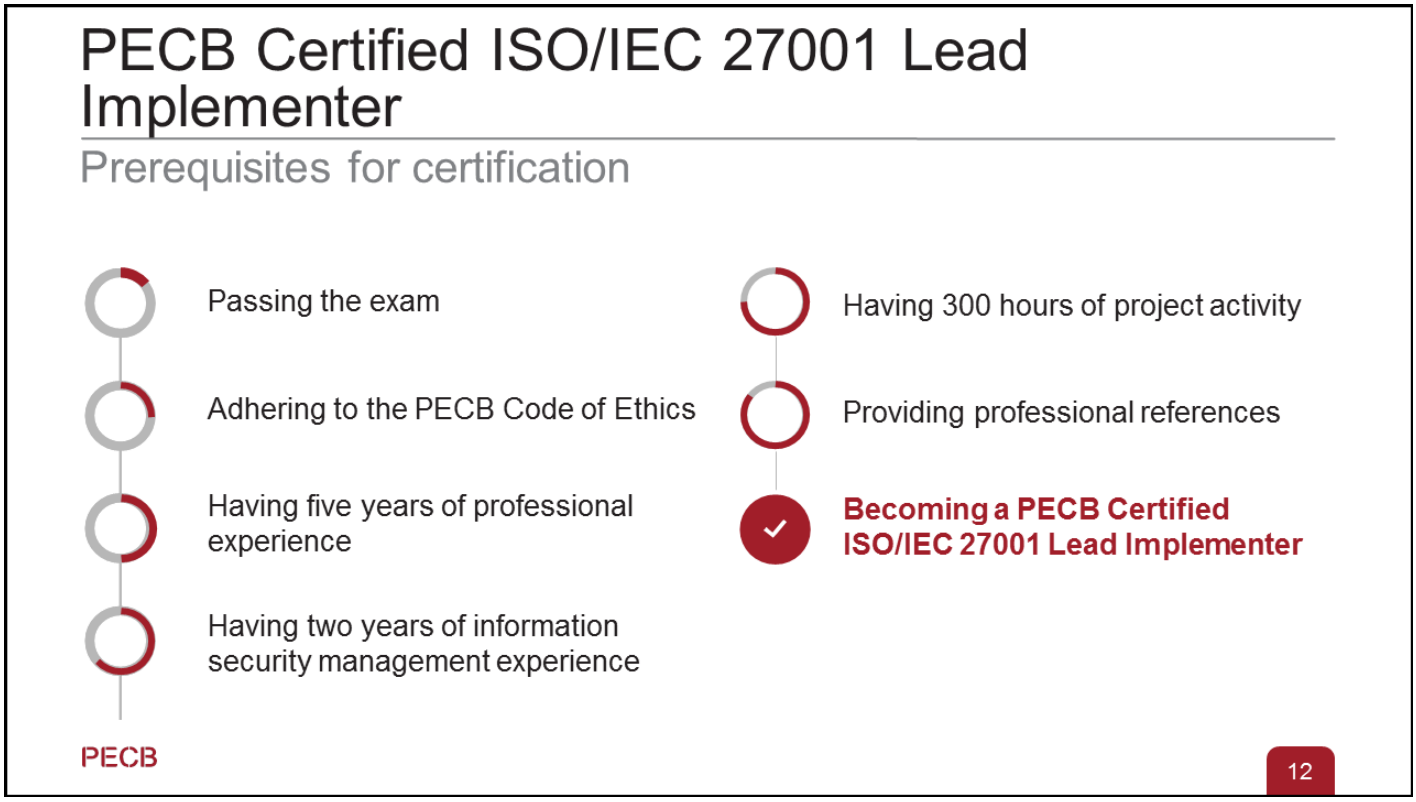
Participants are encouraged to take additional notes.

Exercises are essential for the acquisition of the skills required to properly implement a management system. The participants are recommended to do the exercises conscientiously, considering that they will help them prepare for the certification exam.



The objective of the certification exam is to ensure that the candidates have mastered the information security management concepts and techniques so that they are able to participate in ISMS project assignments. The PECB Examination Committee ensures that the adequacy of the exam questions are maintained based on current professional practice.

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



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

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

The set of criteria and the certification process will be explained in detail during the last day of this training course.

Important note: Certification fees are included in the exam price. The candidate will not have to pay any additional fees when applying for certification to receive one of the following professional credentials: PECB Certified ISO/IEC 27001 Provisional Implementer, PECB Certified ISO/IEC 27001 Implementer, PECB Certified ISO/IEC 27001 Lead Implementer, or PECB Certified ISO/IEC 27001 Senior Lead Implementer.

PECB Certificate

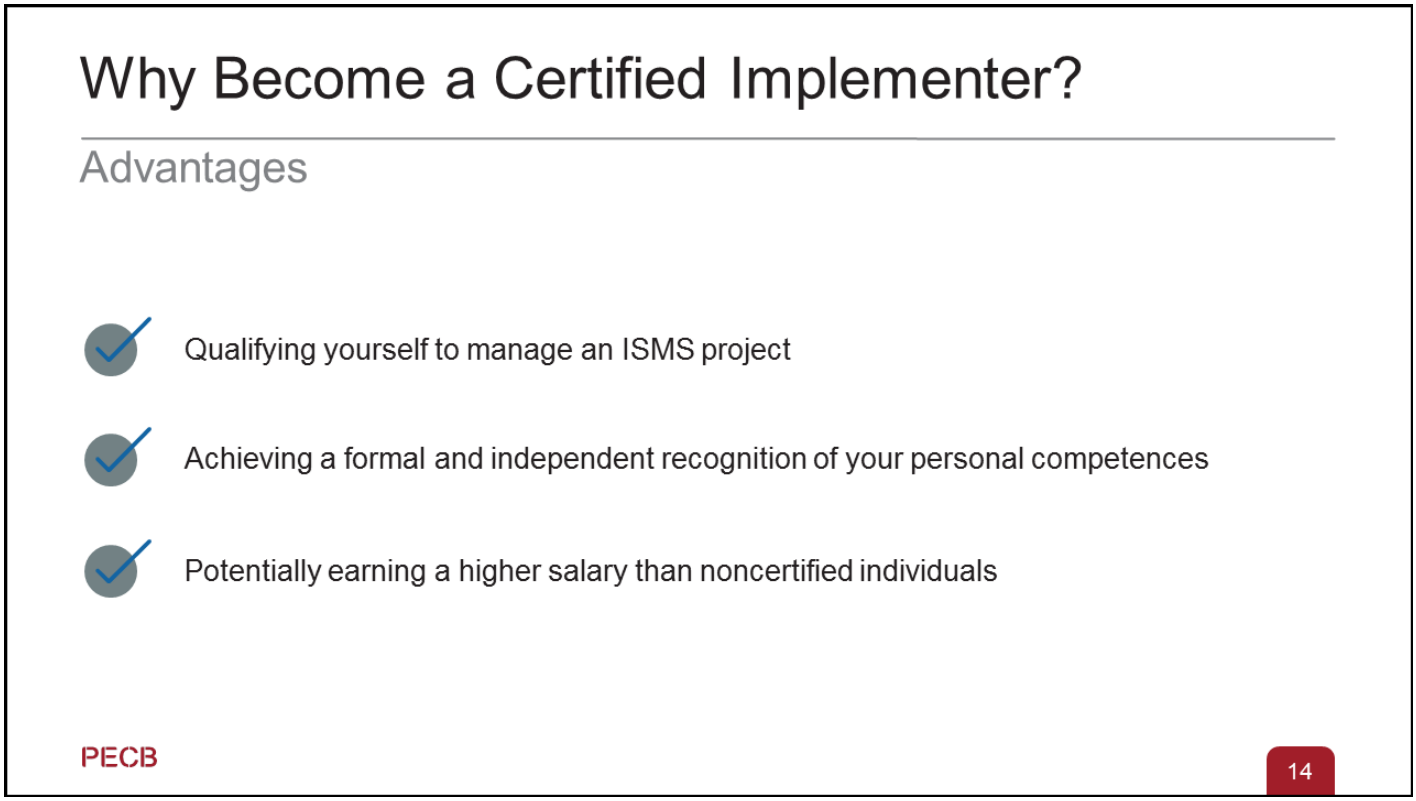
Candidates who meet all the prerequisites for certification will receive a certificate.

PECB

13

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

Upon certification, the candidates will receive a notification from PECB that the certificate can be downloaded on the PECB Member Dashboard. The certificate is valid for three years. To maintain the certification, the candidates must demonstrate every year that they are satisfying the requirements and adhering to the PECB Code of Ethics. To learn more about certificate maintenance and renewal procedure, please visit the PECB website.



- An internationally recognized certification can help you **maximize your career potential** and reach your professional objectives.
- An international certification is a **formal recognition** of one's professional competences.
- According to salary surveys conducted over the last five years, certified implementers earn considerably higher average salaries than their noncertified counterparts.

As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including, but not limited to, Information Security, Information Technology, Business Continuity, Service Management, Quality Management, Risk Management, Health, Safety, and Environment.

We help professionals and organizations show commitment and competence by providing them with valuable education, evaluation, and certification against internationally recognized standards. Our mission is to provide our clients with comprehensive services that inspire trust, demonstrate recognition, and benefit the society as a whole.

The principal objectives of PECB include:

1. Establishing the minimum requirements necessary to certify professionals, organizations, and products
2. Reviewing and verifying the qualifications of candidates to ensure that they are eligible to apply for a PECB certificate
3. Developing and maintaining reliable, valid, and current PECB certificate application processes
4. Granting certificates to qualified candidates, organizations, and products; maintaining records; and publishing a directory of the candidate who hold valid PECB certificates
5. Establishing requirements for the periodic renewal of PECB certificates and ensuring compliance with those requirements
6. Ascertaining that certified individuals meet ethical standards and adhere to the PECB Code of Ethics
7. Promoting the benefits of certification for organizations, employers, public officials, practitioners in related fields, and the public

Certification Body

- ISO/IEC 17021-1 specifies the principles and requirements needed to provide audit and certification of all types of management systems.
- ISO/IEC 17024 specifies the criteria for an organization that conducts certification of persons in relation to specific requirements, including developing and maintaining a certification scheme for persons.
- ISO/IEC 17065 specifies the requirements that should be considered as general criteria for certification bodies operating product, process, or service certification schemes.
- PECB is accredited by the International Accreditation Service (IAS) against ISO/IEC 17024, ISO/IEC 17021-1, and ISO/IEC 17065.

PECB

16

ISO/IEC 17024, Introduction

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

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

Important note:

Only a certification body accredited under ISO/IEC 17024 ensures an international recognition. It is important to validate the status of a certification body with the associated accreditation authority such as IAS, ANSI, and UKAS. For further information regarding the PECB's accreditation, please visit: www.pecb.com/en/affiliations.

ISO/IEC 17021-1, Introduction

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

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

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

Slide Notes Extension

PECB

17

ISO/IEC 17065, Introduction

The overall aim of certifying products, processes or services is to give confidence to all interested parties that a product, process or service fulfils specified requirements. The value of certification is the degree of confidence and trust that is established by an impartial and competent demonstration of fulfilment of specified requirements by a third party. Parties that have an interest in certification include, but are not limited to:

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

Interested parties can expect or require the certification body to meet all the requirements of this International Standard as well as when relevant, those of the certification scheme.

This section provides information that will help the participant gain knowledge on the ISO structure and management system standards, the ISO/IEC 27000 family, and the advantages of ISO/IEC 27001.

What is ISO?

- ISO is an international organization of national standards bodies from over 160 countries.
- The final results of ISO works are published as international standards.
- ISO has published over 22,000 standards since 1947.

PECB

20

Key principles in standard development:

1.ISO standards respond to a need in the market.

ISO only develops standards for which a market demand exists, as a response to formal requests from industry sectors or stakeholders (e.g., consumer groups). Typically, the request for a standard is communicated to national members who then contact the International Organization for Standardization (ISO).

2.ISO standards are based on global expert opinion.

ISO standards are developed by various technical committees (TCs) which comprise experts from all over the world. These experts negotiate all aspects of the standard, including its scope, key definitions, and content.

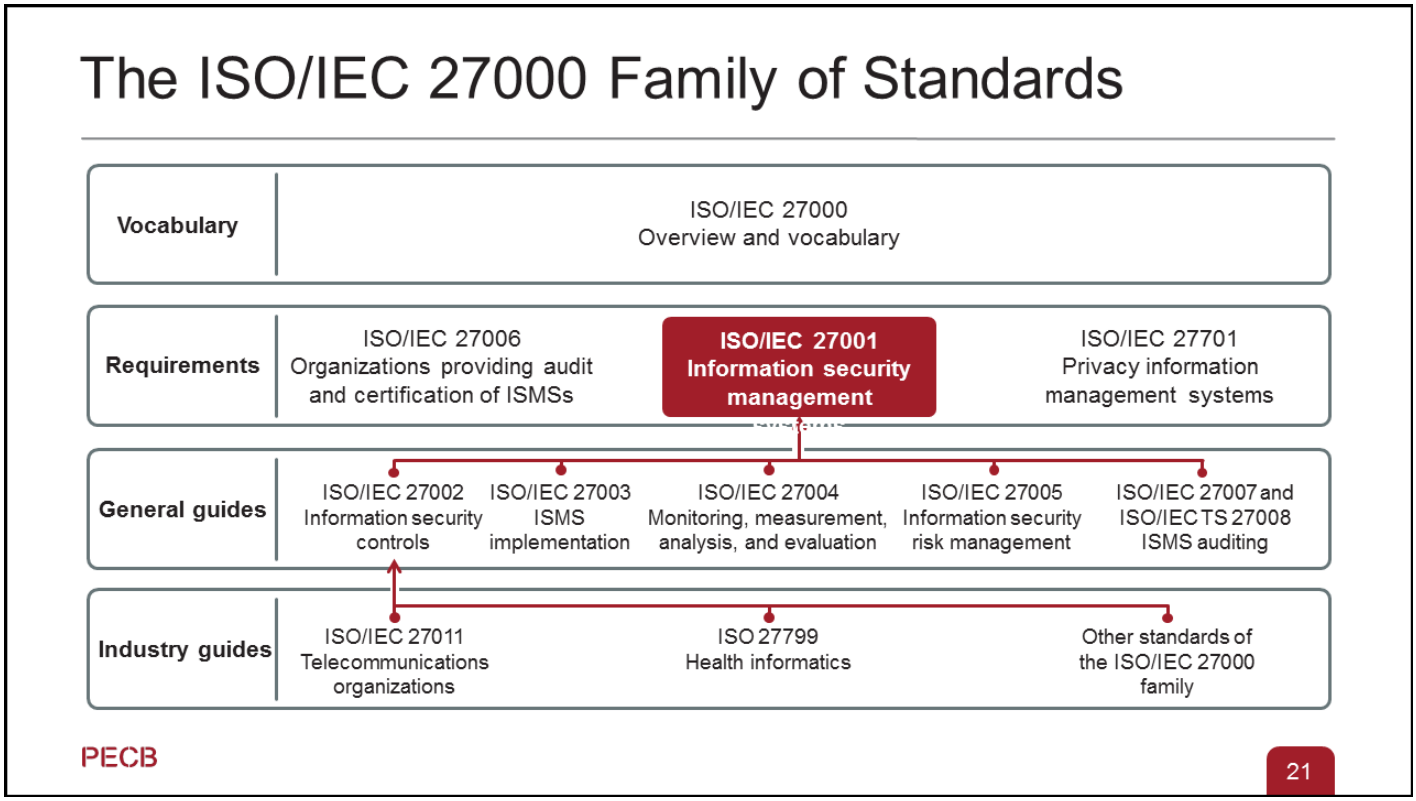
3.ISO standards are developed through a multi-stakeholder process.

The technical committees are made up of experts from the relevant industry, but also from consumer associations, academia, NGOs, and governments.

4.ISO standards are based on a consensus.

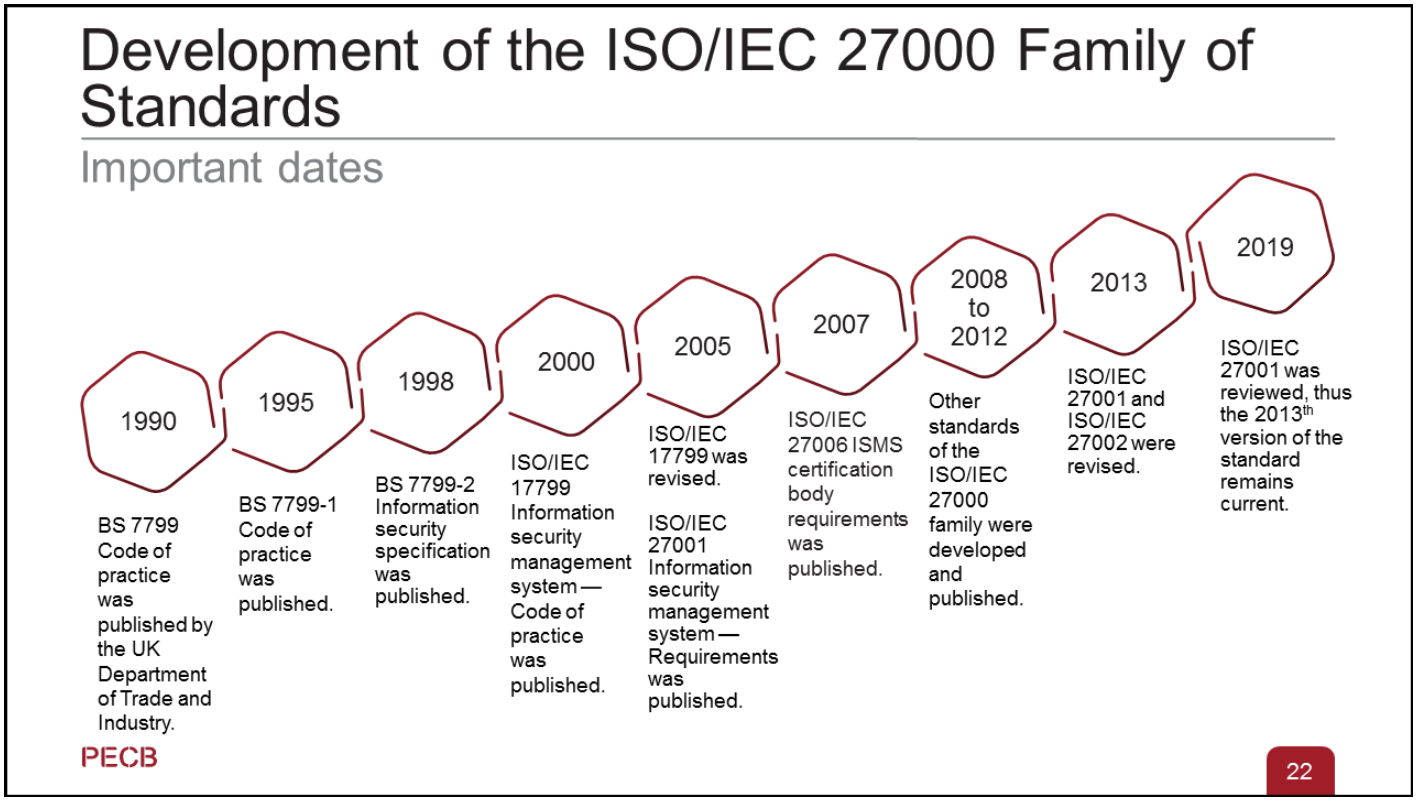
The development of ISO standards is based on a consensus approach, and comments from all stakeholders are taken into account. All ISO country members, regardless of the size or strength of the economy, are on the same footing in terms of their influence in standard development.

For more information, please visit: www.iso.org.



The ISO/IEC 27000 family of standards is a series of information security standards. It includes the following:

- **ISO/IEC 27000:** Presents the basic concepts and the vocabulary that applies when establishing an information security management system (A free copy of this standard can be downloaded on the ISO website.)
- **ISO/IEC 27001:** Defines the requirements for an information security management system (ISMS) and provides a reference set of security controls in its Annex A
- **ISO/IEC 27701:** Specifies the requirements and provides guidance for establishing, maintaining, and continually improving a privacy information management system (PIMS) as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management (as a result of the processing of PII)
- **ISO/IEC 27002 (previously ISO 17799):** Code of practice for the management of information security (This standard provides objectives and implementation guidelines for the information security controls set out in ISO/IEC 27001, Annex A and it is intended to meet the needs of organizations of all types and sizes.)
- **ISO/IEC 27003:** Guidance on implementing or setting up an ISMS
- **ISO/IEC 27004:** Guidance on monitoring and measuring information security performance and ISMS effectiveness
- **ISO/IEC 27005:** Guidance on information security risk management which complies with the concepts, models, and general processes of ISO/IEC 27001
- I**SO/IEC 27006:** Requirements for organizations auditing and certifying an ISMS
- **ISO/IEC 27007:** Guidance for information security management systems auditing
- **ISO/IEC TS 27008:** Guidance for auditors on information security controls
- **ISO/IEC 27011:** Guidance on the use of ISO/IEC 27002 in the telecommunications industry
- **ISO 27799:** Guidance on the use of ISO/IEC 27002 in health informatics



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

- A need for better practices and controls to support trade and governments in the implementation and improvement of information security was expressed.
- The United Kingdom's Department of Trade and Industry formed a working group consisting of information security specialists.
- A "Code of practice," essentially a set of controls (BS 7799), was published. Many of these are recognizable in today's ISO/IEC 27002.
- This was followed up with an "Information security specification" (BS 7799-2, the former BS 7799 that initially 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 standards undergo revision every five years so as to keep up with the developments in various industries. ISO/IEC 27001 was last reviewed and confirmed in 2019; therefore, this version remains current.

ISO/IEC 27001

- The standard specifies requirements for an ISMS (clauses 4 to 10).
- Requirements (clauses) are expressed with the verb “shall.”
- Annex A contains 14 clauses, 35 control objectives, and 114 controls.
- Organizations can obtain certification against this standard.

PECB

23

ISO/IEC 27001:

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

ISO/IEC 27001, clause 0.1 General

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

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

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

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

ISO/IEC 27701

- The standard is an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.
- This standard specifies requirements and provides guidance for a PIMS.
- The standard's requirements (clauses) are written using the imperative verb "shall."
- Organizations can obtain certification against this standard.

PECB

24

ISO/IEC 27701, clause 1 Scope

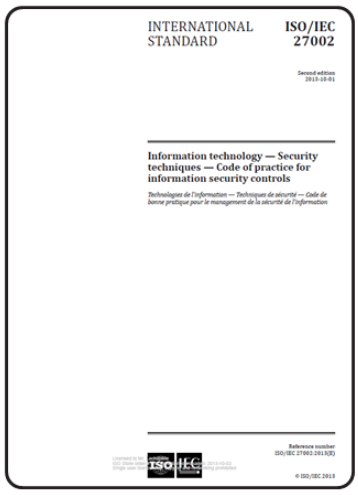
This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

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.

ISO/IEC 27002

- The standard provides guidance for codes of practice for information security controls (reference document).
- Clauses are expressed with the verb “should.”
- Organizations cannot obtain certification against this standard.



PECB

25

ISO/IEC 27002:

- ISO/IEC 27002 is a guide of information security management controls.
- The standard provides a list of security objectives and controls generally practiced in the information security industry.
- Clauses 5 to 18, in particular, provide detailed guidance to support the controls specified in Annex A of ISO/IEC 27001 (control groups A.5 to A.18).

ISO/IEC 27002, clause 1 Scope

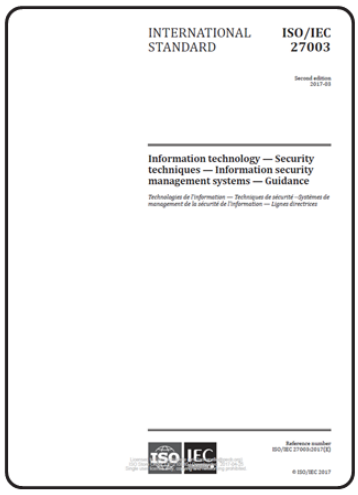
This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization’s information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a. *select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;*
b. *implement commonly accepted information security controls;*
c. *develop their own information security management guidelines.*

ISO/IEC 27003

- The standard provides guidance on the requirements for an information security management system.
- It serves as a reference document to be used with ISO/IEC 27001 and ISO/IEC 27002 standards.
- It is composed of 10 clauses.
- Organizations cannot obtain certification against this standard.



PECB

26

ISO/IEC 27003, clause 1 Scope

This document provides explanation and guidance on ISO/IEC 27001:2013.

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.

Clauses 4 to 10 of this document mirror the structure of ISO/IEC 27001:2013.

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

The Payment Card Industry Data Security Standard (PCI DSS)

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

PECB

27

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

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

The mapping of PCI DSS and ISO/IEC 27001 can be found in the following link: https://www.isaca.org/Journal/archives/2016/Volume-1/Documents/Comparison-of-PCI-DSS-and-ISO-IEC-27001-Standards_joa_Eng_0116.pdf

The Cloud Security Alliance (CSA)

- The Cloud Security Alliance (CSA) is an organization committed to define the best practices of ensuring a secure cloud computing environment.
- CSA has a three-tiered cloud provider assurance program known as the CSA Security, Trust, and Assurance Registry (STAR) program. STAR consists of self-assessment, third party audit, and continuous monitoring. Its primary purpose is to aid customers with the assessment of cloud service providers.

PECB

28

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

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

The General Data Protection Regulation

- The General Data Protection Regulation (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/eli/reg/2016/679/oj


EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

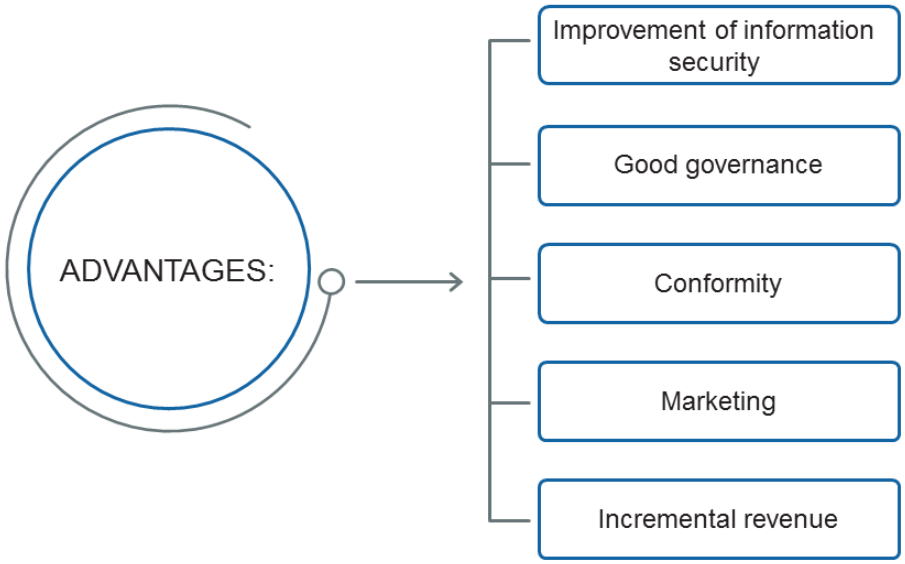
PECB

29

ISO/IEC 27001 is the leading international standard for information security. The implementation of ISO/IEC 27001 is accepted to cover Article 32 of the GDPR. Thus, the ISO/IEC 27001 framework can be used to support compliance with the GDPR. Furthermore, ISO/IEC 27001 and the GDPR overlap in many areas, such as data confidentiality, availability, and integrity, as well as risk assessment, etc.

The mapping of the GDPR and ISO/IEC 27001 can be found in the following link: https://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.docx

Advantages of ISO/IEC 27001



PECB

30

1. **Improvement of information security:**
   - General improvement of information security effectiveness
   - Independent review of your information security management system
   - Enhanced information security awareness
   - Established mechanisms to measure the effectiveness of the management system
   - The opportunity to identify the weaknesses in the ISMS and suggest corrective actions for improvement
2. **Good governance:**
   - Awareness and empowerment of personnel regarding information security
   - Fewer lawsuits against the company in virtue of the ‘‘due care’’ and ‘‘due diligence’’ principles
   - Increase of the top management’s accountability regarding information security
3. **Conformity:**
   - Conformity to ISO/IEC 27001
   - Conformity to OECD (Organization for Economic Co-operation and Development) principles
   - Conformity to industry standards, for example: PCI-DSS (Payment Card Industry Data Security Standard), Basel II (for banking industry)
   - Conformity to national and regional laws
4. **Marketing:**
   - Increased competitive advantage
   - Increased of customer and interested party satisfaction
5. **Incremental revenue:**
   - Increased business opportunities
   - Reduced costs as a result of data breaches

1.Which standard below provides requirements for an information security management system (ISMS)?

A. ISO/IEC 27001
B. ISO/IEC 27002
C. ISO/IEC 27000

2.Which of the statements below is correct?

A. Organizations can obtain certification against ISO/IEC 27001
B. Organizations can obtain certification against ISO/IEC 27005
C. Organizations cannot obtain certification against ISO/IEC 27001

3.Which international standard provides guidelines for codes of practice for information security controls?

A. ISO/IEC 27002
B. ISO/IEC 27003
C. ISO/IEC 27005

4.In what areas do ISO/IEC 27001 and the General Data Protection Regulation (GDPR) overlap?

A. PII collection and processing and the rights of data subjects
B. Data confidentiality, availability, and integrity, and risk assessment
C. Physical security, access control, and continual improvement

5.What does STAR stand for in the cloud security alliance (CSA)?

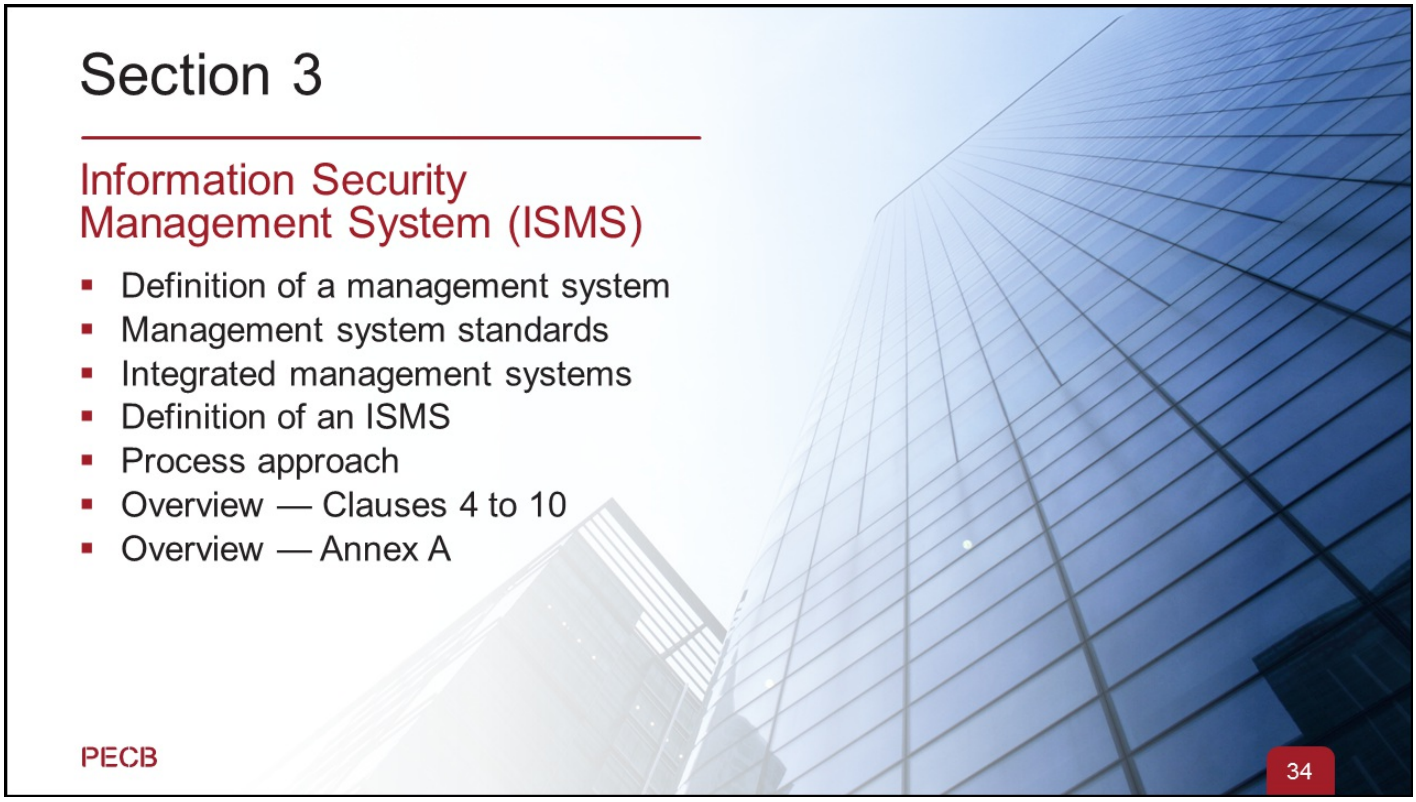
A. Security, Trust, and Assurance Registry
B. Security, Task, Action, and Results
C. Security, Transparency, Assurance, and Response

6.Which of the following is NOT an advantage of ISO/IEC 27001?

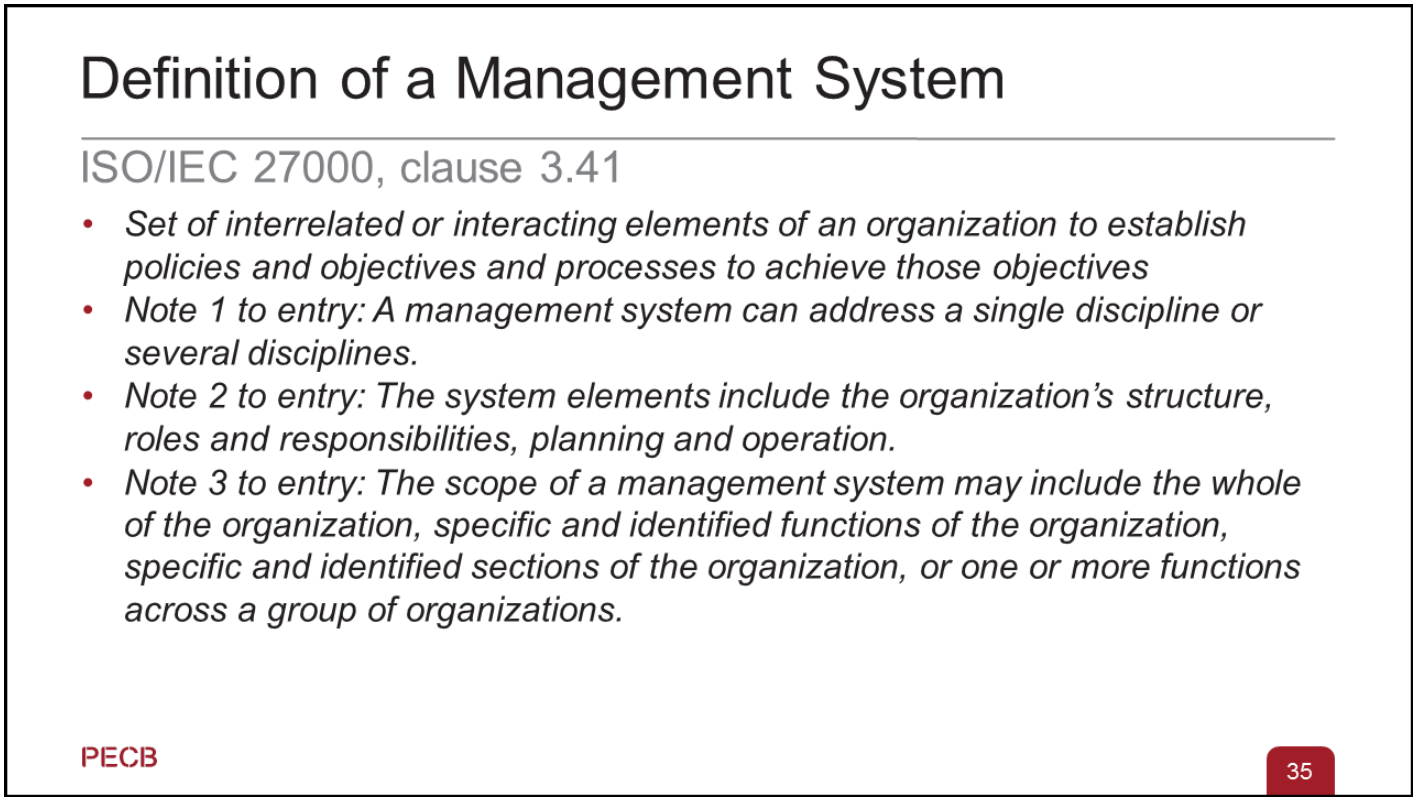
A. Marketing
B. Incremental revenue
C. Performance evaluation

Section summary

- The International Organization for Standardization (ISO) publishes standards in response to a market demand. ISO standards are based on global expert opinion and consensus and are developed through a multi-stakeholder process.
- The ISO/IEC 27000 family of standards includes information security standards.
- ISO/IEC 27001 is the main standard of the family that specifies the requirements for an ISMS.
- ISO/IEC 27701 specifies the PIMS requirements and provides guidance to PII controllers and processors to hold responsibility and accountability for PII processing.
- ISO/IEC 27002 is a guideline standard of information security management best practices.
- In a normative standard, requirements (clauses) are written using the imperative verb “shall.” On the other hand, in a guideline standard, clauses are written using the verb, “should.”
- ISO/IEC 27003 is a standard against which organizations cannot obtain certification. It provides guidance on the implementation of the ISMS requirements as specified in ISO/IEC 27001.
- The advantages of having an ISMS in place are manifold: improved information security, good governance, international recognition, competitive advantage, incremental revenue, etc.



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



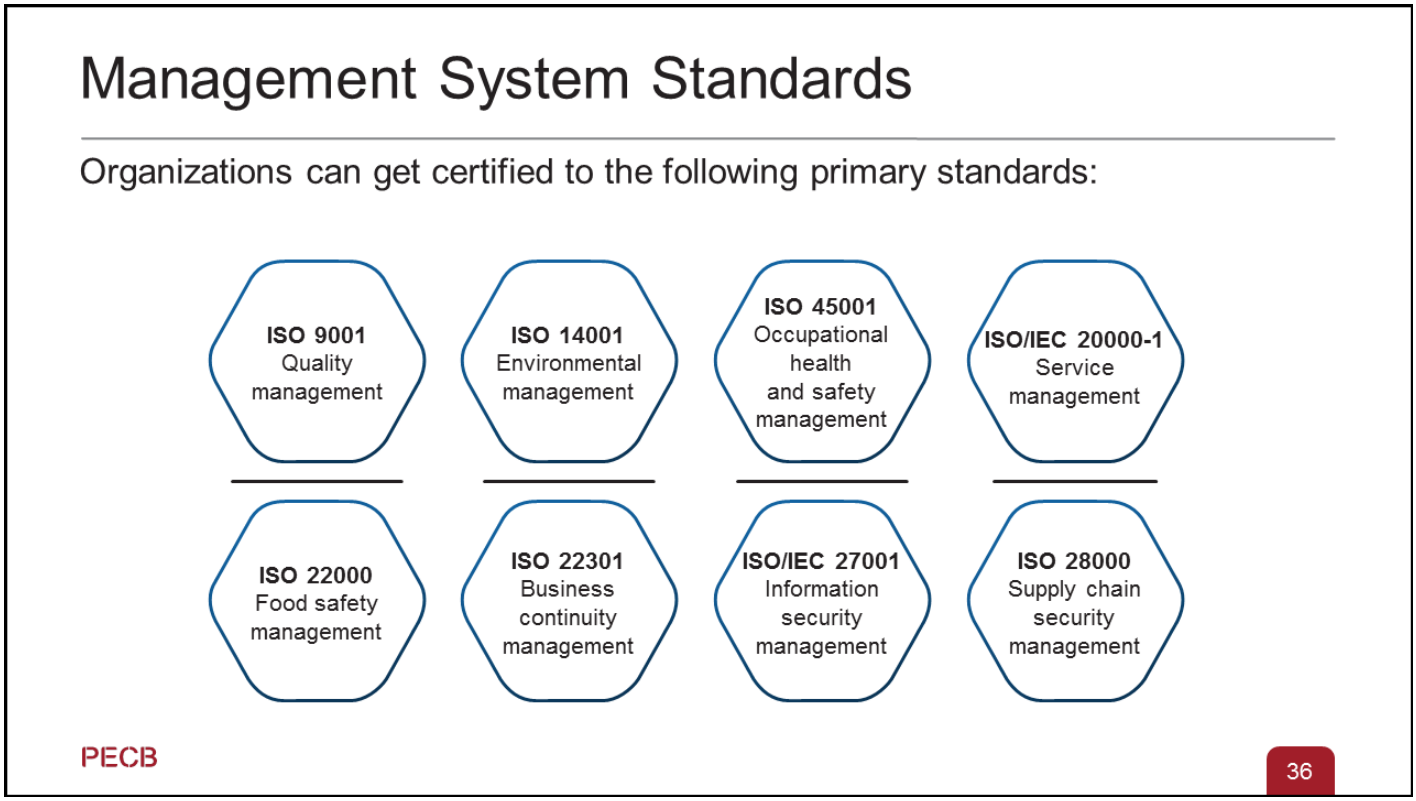
A management system is a system that allows organizations to establish policies and objectives and to subsequently implement them. The management system of an organization may include management systems in different fields, including quality, information security, environment, etc.

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

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

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

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



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

ISO 9000 and ISO 14000 families of standards are among the best known ISO standards. The ISO 9001 standard has become an international reference with regard to quality. The ISO 14001 standard, for its part, is used to help 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 www.pecb.com or www.iso.org

Integrated Management Systems

Common structure of ISO standards

Requirements	ISO 9001:2015	ISO 14001:2015	ISO 55001:2014	ISO 22301:2019	ISO/IEC 27001:2013
Leadership and commitment	5.1	5.1	5.1	5.1	5.1
Policy of the management system	5.2	5.2	5.2	5.2	5.2
Objectives of the management system	6.2	6.2	6.2	6.2	6.2
Documented information	7.5	7.5	7.6	7.5	7.5
Internal audit	9.2	9.2	9.2	9.2	9.2
Management review	9.3	9.3	9.3	9.3	9.3
Continual improvement	10.3	10.3	10.3	10.2	10.2

PECB

37

As organizations increasingly manage several compliance frameworks simultaneously, it is recommended to implement an integrated management system. An integrated management system (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.

There are several good reasons for integration, including to:

- Harmonize and optimize practices
- Eliminate conflicting responsibilities and relationships
- Balance conflicting objectives
- Formalize informal systems
- Reduce duplication and therefore costs
- Reduce risks and increase profitability
- Shift focus toward business goals
- Create consistency
- Improve communication
- Facilitate training and awareness

Slide Notes Extension

PECB

38

ISO/IEC Directives (Part 1), Annex L.1 General

Whenever a proposal is made to prepare a new management system standard (MSS), including sector-specific MSS, a justification study (JS) shall be carried out in accordance with Appendix 1 to this annex.

NOTE No JS is needed for the revision of an existing MSS whose development has already been approved and provided the scope is confirmed (unless it was not provided during its first development).

To the extent possible, the proposer shall endeavour to identify the full range of deliverables which will constitute the new or revised MSS family, and a JS shall be prepared for each of the deliverables.

ISO/IEC Directives (Part 1), Appendix 1 Justification criteria questions

Each general principle should be given due consideration and, ideally, when preparing the JS, the proposer should provide a general rationale for each principle, prior to answering the questions associated with the principle. The principles to which the proposer of the MSS should pay due attention to when preparing the justification study are:

1. *Market relevance*
2. *Compatibility*
3. *Topic coverage*
4. *Flexibility*
5. *Free trade*
6. *Applicability of conformity assessment*
7. *Exclusions*

Definition of an ISMS

ISO/IEC 27000, clause 4.2.1

- *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.*

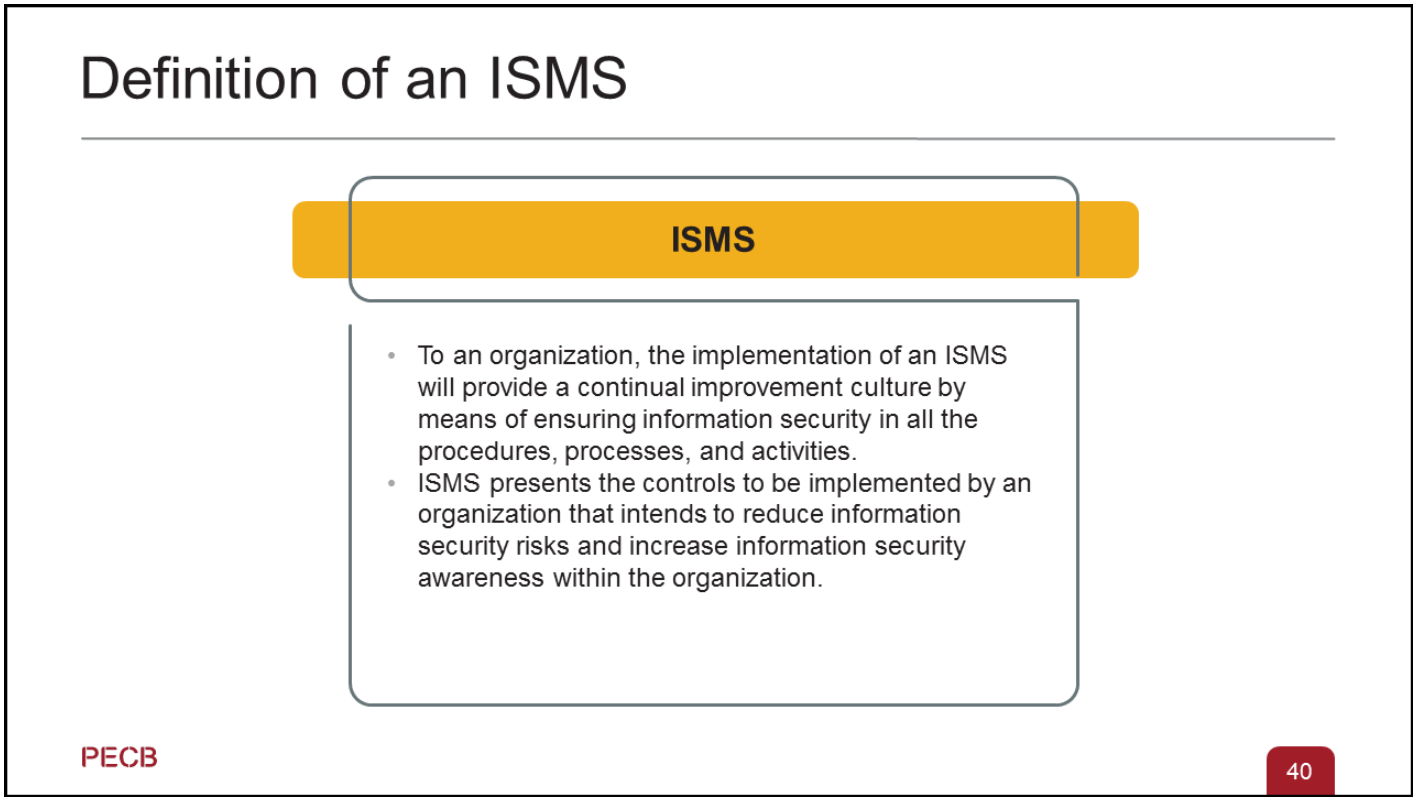
- *An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.*

PECB

39

ISO/IEC 27000, clause 3.28 Information security

Preservation of confidentiality, integrity and availability of information

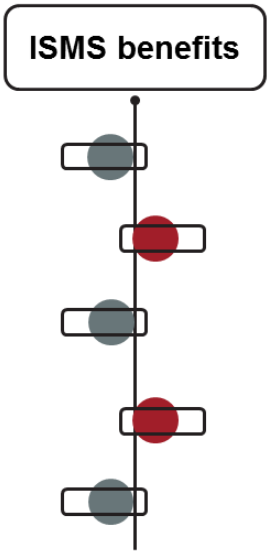


As defined in ISO/IEC 27001, the establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used, and the size and structure of the organization.

Benefits of the ISMS

Having an effective ISMS in place helps an organization in:

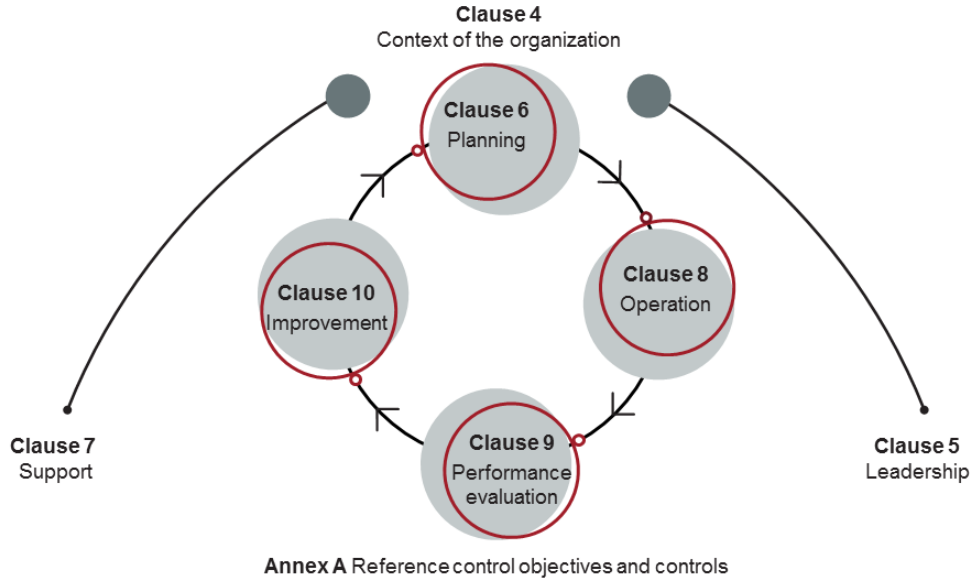
- Reducing information security risks and minimizing exposure to information security breaches
- Protecting assets and sensitive information
- Creating competitive advantage
- Improving reputation and increasing customer confidence
- Protecting the confidentiality, availability, and integrity of information



PECB

41

Structure of ISO/IEC 27001



PECB

42

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

Context of the Organization

ISO/IEC 27001, clause 4

4.1 Understanding the organization and its context

The organization shall establish the external and internal factors related to the ISMS that can affect the achievement of the ISMS intended outcome(s).

4.2 Understanding the needs and expectations of interested parties

The organization shall determine the interested parties and the information security requirements relevant to these interested parties.

4.3 Determining the scope of the information security management system

The organization shall establish the ISMS scope by setting its boundaries and applicability. The scope shall be available as documented information.

4.4 Information security management system

The organization shall comply with the standard's requirements to establish, implement, maintain and continually improve an information security management system.

Leadership

ISO/IEC 27001, clause 5

5.1 Leadership and commitment

- Top management shall ensure that the ISMS is compatible with the organization's strategic orientation.
- Top management shall integrate the ISMS requirements into the organization's business processes, determine the necessary resources for the ISMS, and communicate the importance of an effective information security management.

5.2 Policy

- Top management shall create an information security policy that shall be appropriately available and communicated to all interested parties.
- The policy shall be aligned with the purpose of the organization and shall include the information security objectives, a commitment to fulfill the information security requirements and a commitment for continual improvement.

5.3 Organizational roles, responsibilities and authorities

- Top management shall assign the appropriate information security roles and responsibilities in order to ensure that the information security management system conforms to the requirments of ISO/IEC 27001.

Planning

ISO/IEC 27001, clause 6

Actions to addresss risks and opportunities

The organization shall determine the risks and opportunities to achieve the intended outcome(s); prevent or reduce undesired effects; and achieve continual improvement. The organization shall also plan actions to address risks and opportunities, implement those actions, and evaluate their effectiveness.

Information security risk assessment

The organization shall establish and maintain risk criteria; identify, analyze, and evaluate risks; and ensure that the risk assessment process generates consistent, valid, and comparable results.

Information security risk treatment

The organization shall select the risk treatment options, determine the controls needed to implement the risk treatment options, compare the selected controls, produce the Statement of Applicability, formulate the risk treatment plan, and obtain approval for the risk treatment plan as well as for the acceptance of residual risks.

Information security objectives and planning to achieve them

The organization's objectives shall be measurable and consistent with the information security policy. They shall also be aligned with the requirements, and risk assessment and risk treatment results. The objectives shall be appropriately communicated, and updated.

Support

ISO/IEC 27001, clause 7

7.1 Resources

The organization shall determine and provide the necessary resources for the appropriate implementation of the ISMS.

7.2 Competence

The organization shall ensure that it has the competent personnel to perform the tasks related to the ISMS.

7.3 Awareness

The organization shall ensure that its employees are aware of the information security policy, their roles in the ISMS, and the implications of failing to conform to the ISMS requirements.

7.4 Communication

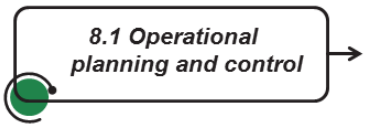
The organization shall establish, implement, and maintain arrangements for communication with relevant external and internal interested parties.

7.5 Documented information

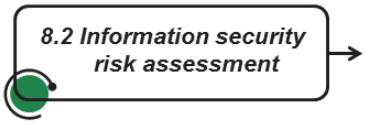
The organization's ISMS shall include documented information required by ISO/IEC 27001 and records to demonstrate the effectiveness of the ISMS.

Operation

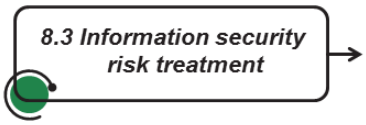
ISO/IEC 27001, clause 8



The organization shall plan, implement, and control the necessary processes to comply with the standard requirments. The organization shall also implement the plans, keep documented information as evidence of the implementation of planned processes, control and review the planned changes, and determine and control the oursourced processes.



The organization shall conduct information security risk assessments at planned intervals and shall keep documented information of the risk assessment results.



The organization shall implement the information security risk treatment plan and shall keep documented information on risk treatment results.

Performance Evaluation

ISO/IEC 27001, clause 9

9.1

Monitoring, measurement, analysis and evaluation

The organization shall evaluate the performance and effectiveness of the information security management system and keep documented information as evidence of the monitoring and measurement outputs.

9.2

Internal audit

The organization shall perform internal audits at planned intervals in order to validate whether the information security management system is effectively implemented, maintained, and remains conform to the organization's own requirements as well as the standard requirements.

9.3

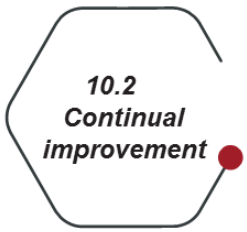
Management review

The top management shall perform reviews of the ISMS at planned intervals in order to ensure its suitability, adequacy and effectiveness. The organization shall keep documented information as evidence of the management review outputs.

Improvement

ISO/IEC 27001, clause 10

The organization shall take the appropriate actions when a nonconformity occurs. It shall evaluate and implement those actions, review their effectiveness and, if necessary, make changes. The organization shall also keep documented information as evidence of the results of corrective actions.



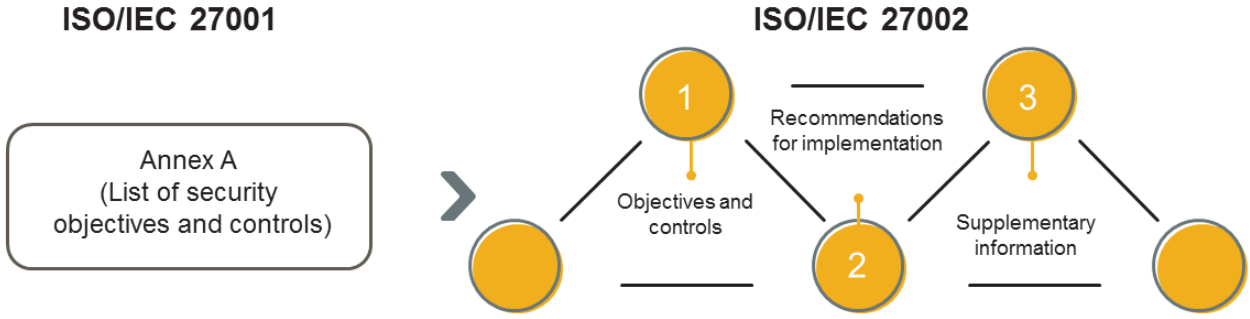
The organization shall ensure the continual improvement of the suitability, adequacy, and effectiveness of the information security management system.

Annex A

- Annex A is part of ISO/IEC 27001 and it is comprised of 114 controls that should be considered when intending to comply with the standard.
- The list of control objectives and 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.

Annex A

Security objectives and controls



Important note: Since ISO/IEC 27002 is a code of practice, there is no requirement to follow its guidance in order to obtain an ISO/IEC 27001 certification.

PECB

51

The objectives and the information security controls listed in Annex A (A.5 to A.18) of ISO/IEC 27001 are aligned with the security objectives and security controls listed in clauses 5 to 18 of ISO/IEC 27002.

114 Security Controls

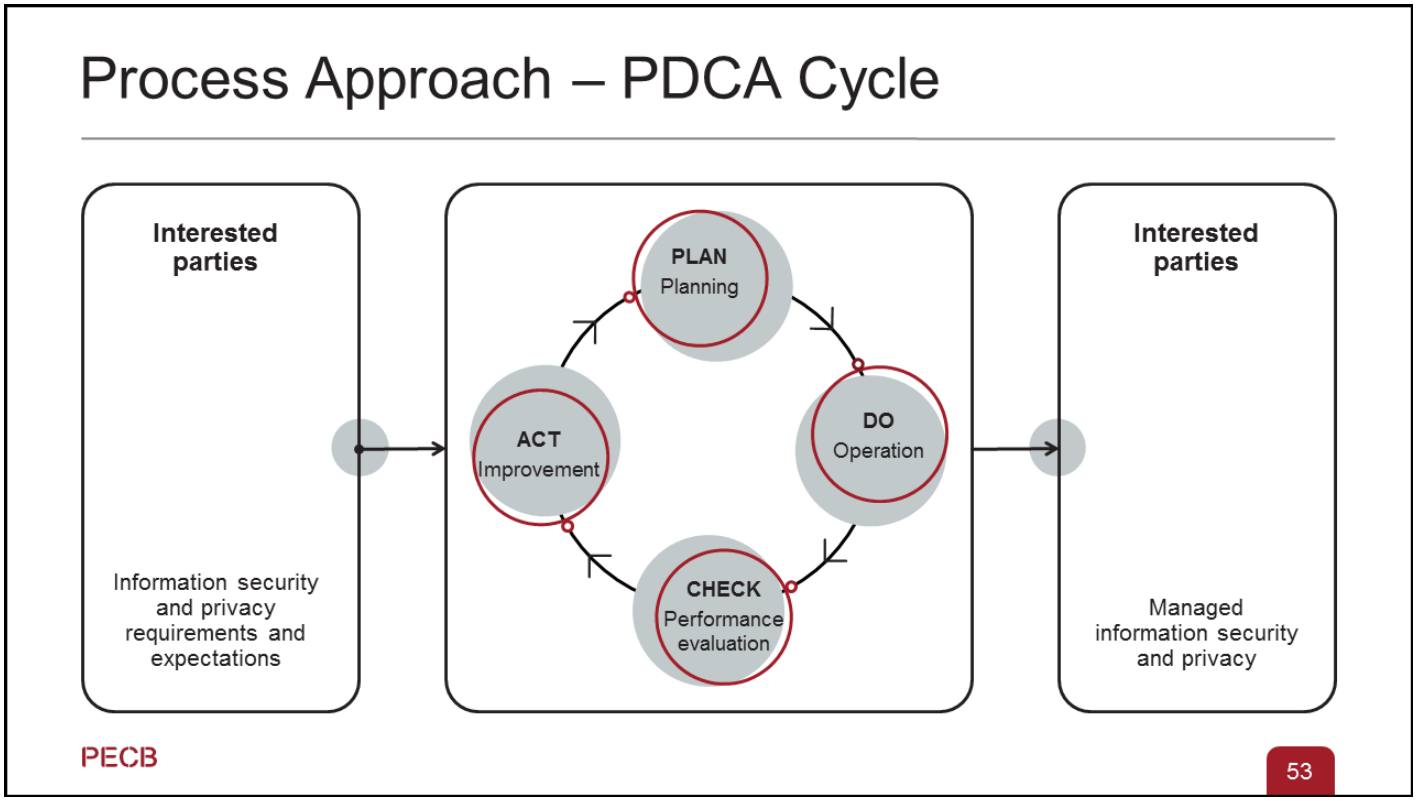
ISO/IEC 27001, Annex A

A.5	Information security policies	2 controls
A.6	Organization of information security	7 controls
A.7	Human resource security	6 controls
A.8	Asset management	10 controls
A.9	Access control	14 controls
A.10	Cryptography	2 controls
A.11	Physical and environmental security	15 controls
A.12	Operations security	14 controls
A.13	Communications security	7 controls
A.14	System acquisition, development and maintenance	13 controls
A.15	Supplier relationships	5 controls
A.16	Information security incident management	7 controls
A.17	Information security aspects of business continuity management	4 controls
A.18	Compliance	8 controls

PECB

52

The objectives and the security controls listed in Annex A (A.5 to A.18) of ISO/IEC 27001 are supported by guidance of ISO/IEC 27002, clauses 5 to 18.



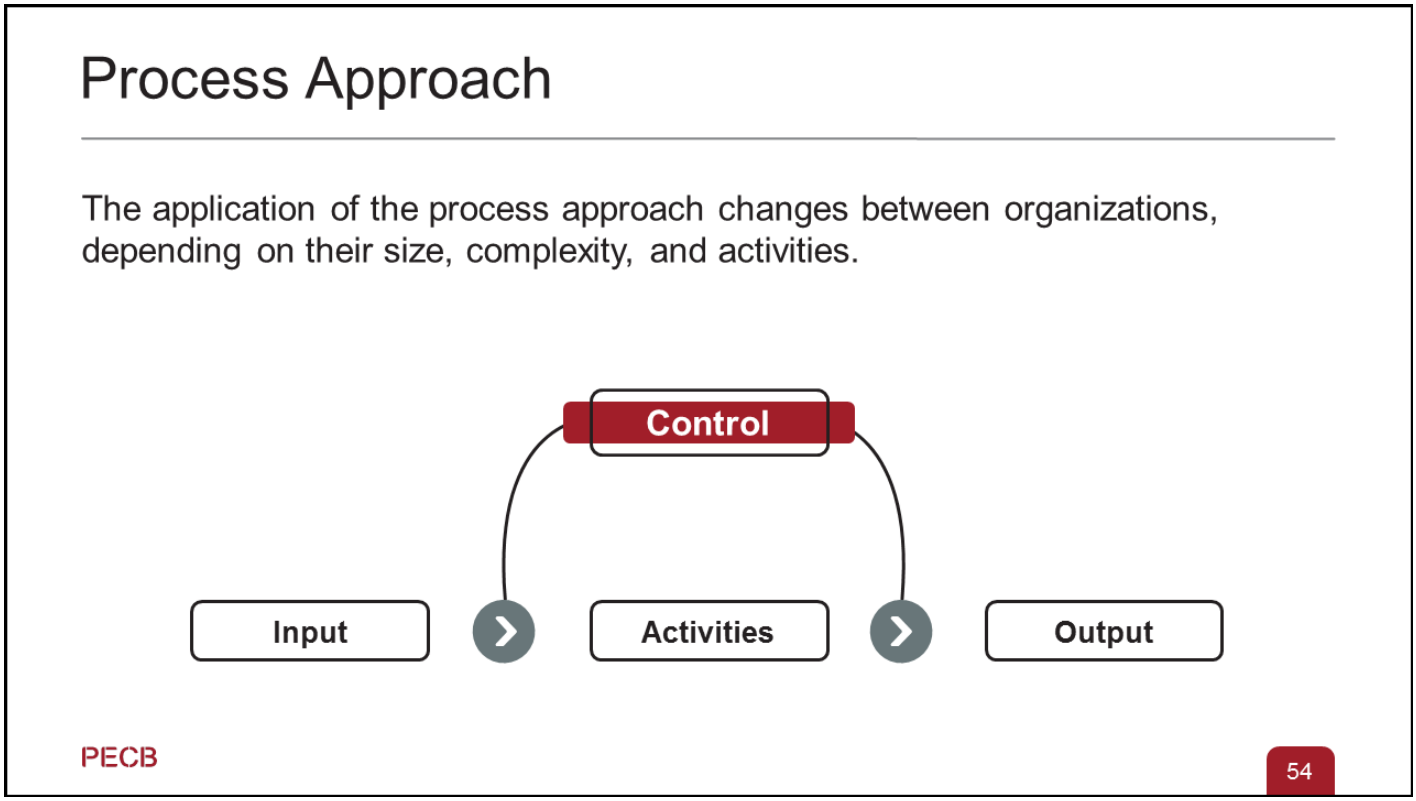
ISO/IEC 27001 adopts the process model “Plan-Do-Check-Act” (PDCA), also known as the Deming wheel. The model is applied to the structure of all the processes in an information security management system. The figure on the slide illustrates how a management system uses the requirements and the expectations of the interested parties as input, and how it produces, with the necessary actions and processes, the information security results that meet the requirements and expectations of interested parties.

Plan (establish the management system): Establish the policy, objectives, processes, and procedures related to risk management and the improvement of information security in order to provide results that are in line with the organization’s objectives

Do (implement and operate the management system): Implement and operate the policy, controls, processes, and procedures of the management system

Check (monitor and review the management system): Assess and, if applicable, measure process performances against the policy and objectives, and report the results to top management for review

Act (maintain and improve the management system): Undertake corrective and preventive actions on the basis of the results of the internal audit, management review, or other relevant information to continually improve the management system



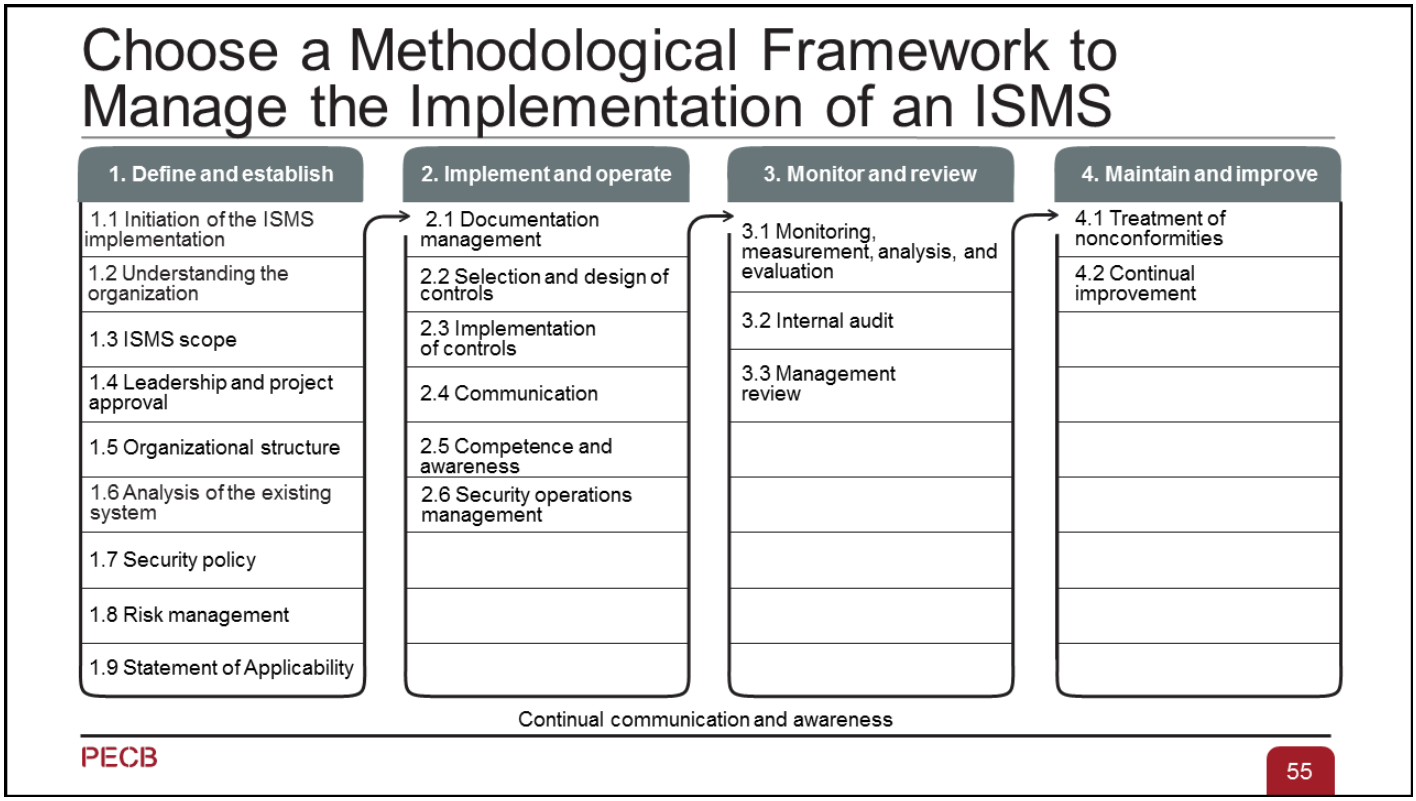
A process can be defined as a logical group of interrelated tasks performed to reach a defined objective. It is a sequence of structured and measured activities designed to create a product or service for a specific purpose, typically for a market sector or a particular client.

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.



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).

Exercise 1: Reasons to adopt ISO/IEC 27001

After reading the section “Introduction and history” in the case study, present the three most significant advantages of implementing an information security management system (ISMS) based on ISO/IEC 27001 to the CEO of *e-Scooter*.

Duration of the exercise: 30 minutes

Comments: 15 minutes

1.A management system is a system that allows organizations to establish policies and objectives and to subsequently implement them.

A. True
B. False

2.What is an integrated management system (IMS)?

A. A management system that integrates all the guidelines and best practices so as to enable the achievement of its purpose and mission
B. A management system that integrates all the components of a business into a coherent system so as to enable the achievement of its purpose and mission
C. A management system that integrates all frameworks and resources so as to enable the achievement of its purpose and mission

3.Which of the options below is a benefit of an effective ISMS?

A. Reducing information security risks and minimizing exposure to information security breaches
B. Processing and removing redundant information
C. Exposing the confidentiality of information

4.Annex A of ISO/IEC 27001 consists of 114 controls that organizations do not have to consider when intending to comply with the standard.

A. True
B. False

5.Which process model does ISO/IEC 27001 adopt?

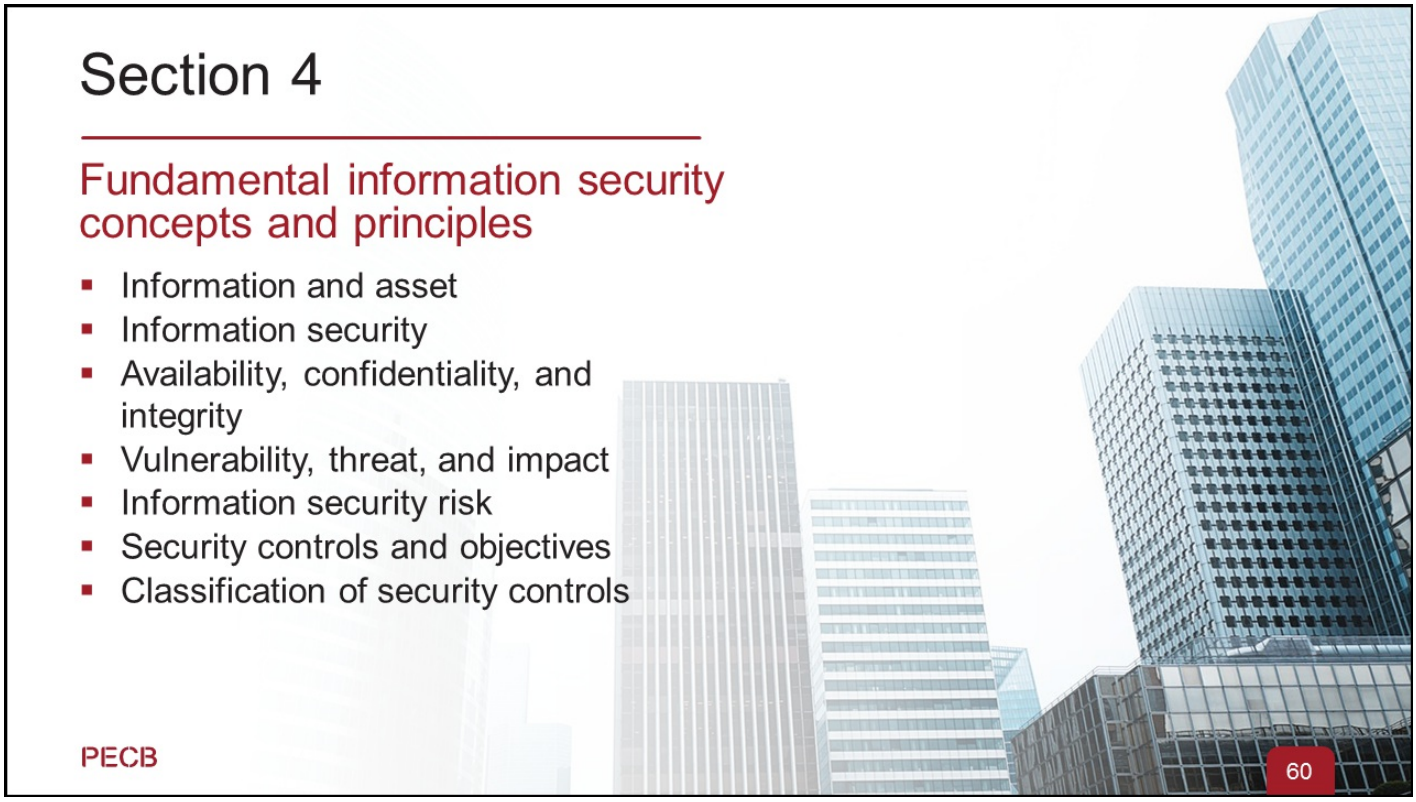
A. Plan, improve, operate, and act
B. Plan, manage, check, and act
C. Plan, do, check, and act

6.Which standard supports the controls of Annex A?

A. ISO/IEC 27002
B. ISO/IEC 27003
C. ISO/IEC 27701

7.What is the term for the identification and orderly management of processes within an organization?

A. Input element
B. Information security control
C. Process approach



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, and controls.

Information and Asset

ISO 9000, clause 3.8.2 and ISO 55000, clause 3.2.1

Information: *meaningful data*

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

There are many types of assets, including:

- Information
- Software, such as computer programs
- Physical assets, such as computers
- Services
- People and their qualifications and skills
- Intangibles, such as reputation and image

PECB

61

ISO/IEC 27000, clause 3.35 Information system

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

ISO/IEC 27001, Annex A.8 defines the objectives for security controls linked to asset management.

ISO/IEC 27001, Annex A.8.1 Responsibility for assets

Objective: *To identify organizational assets and define appropriate protection responsibilities.*

ISO/IEC 27001, Annex A.8.1.1 Inventory of assets

Control: *Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.*

ISO/IEC 27001, Annex A.8.1.2 Ownership of assets

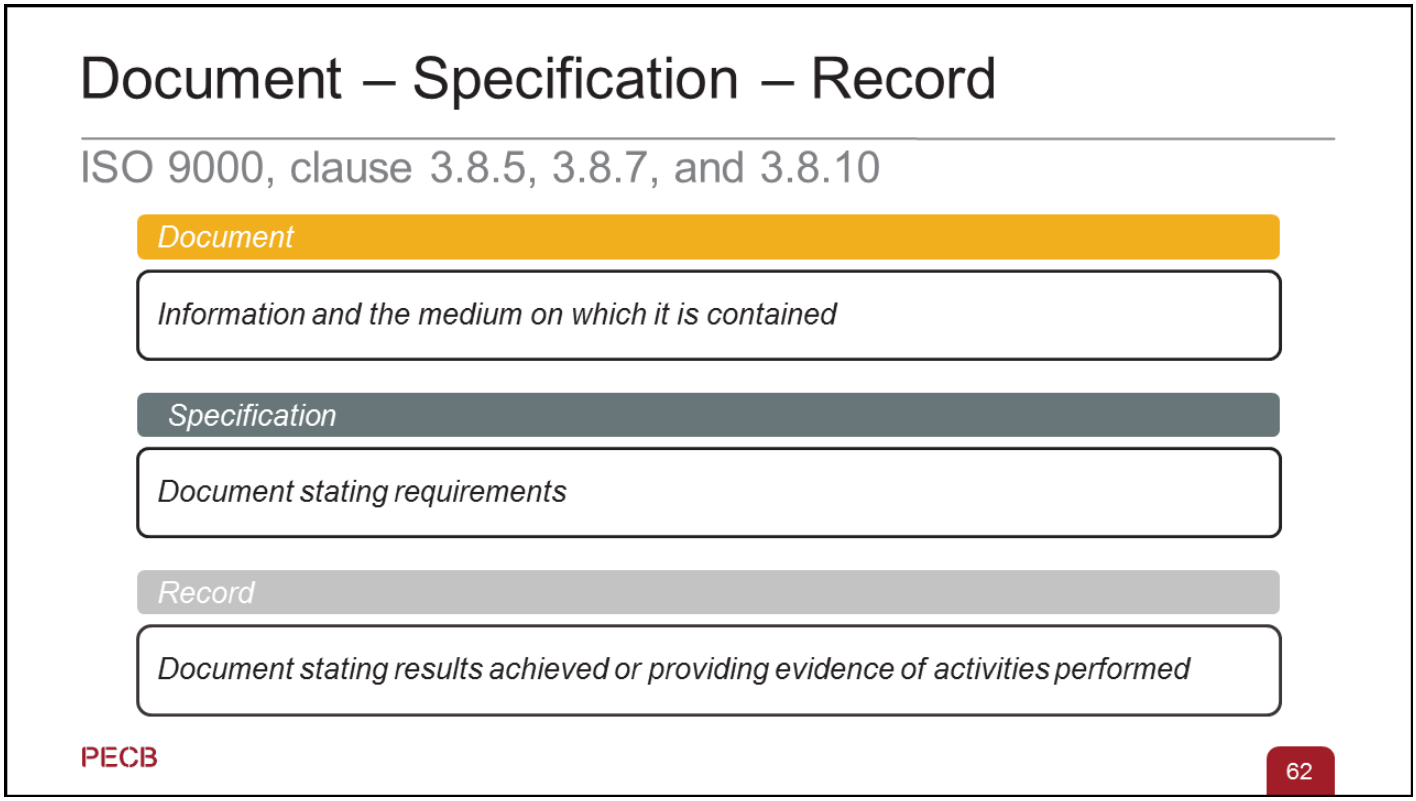
Control: *Assets maintained in the inventory shall be owned.*

ISO/IEC 27001, Annex A.8.1.3 Acceptable use of assets

Control: *Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.*

ISO/IEC 27001, Annex A.8.1.4 Return of assets

Control: *All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.*



ISO 9000, clause 3.8.5 Document (cont'd)

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

Note 1 to entry: The medium can be paper, magnetic, electronic or optical computer disc, photograph or master sample, or combination thereof.

Note 2 to entry: A set of documents, for example specifications and records, is frequently called "documentation".

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

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

Information Security

- Information security determines what information needs to be protected, the reason why it should be protected, how to protect it, and what to protect it from.
- By protecting the organization against threats and vulnerabilities, information security reduces the risks and the impact of such risks to its assets.
- Information security covers information of all kinds, such as printed or handwritten, transmitted by email or website, mentioned during conversations, etc.

PECB

63

ISO/IEC 27001 applies to the protection of information regardless of its type and form, be it numeric, paper, electronic, or verbal human communication.

ISO/IEC 27002, clause 0.2 Information security requirements

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

a. *the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;*
b. *the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;*
c. *the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.*

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

Slide Notes Extension

PECB

64

Other definitions related to information security:

ISO/IEC 27000, clause 3.27 Information processing facilities

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

ISO/IEC 27000, clause 3.30 Information security event

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

ISO/IEC 27000, clause 3.31 Information security incident

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

ISO/IEC 27000, clause 3.32 Information security incident management

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

ISO/IEC 27000, clause 3.35 Information system

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

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 behaviour and results

Annex A includes control objectives related to the classification of information:

ISO/IEC 27001, Annex A.8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

ISO/IEC 27001, Annex A.8.2.1 Classification of information

Control: Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

ISO/IEC 27001, Annex A.8.2.2 Labelling of information

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

ISO/IEC 27001, Annex A.8.2.3 Handling of assets

Control: Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Confidentiality

ISO/IEC 27000, clause 3.10

Confidentiality

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

- Confidentiality requires that only authorized users have access to protected and sensitive data.
- Some of the practices employed to address confidentiality are:
  - An authentication process that requires a user identification and password when addressing confidential data
  - Security methods to ensure viewer authorization
  - Access controls that provide restrictions on the network access based on the employee's roles and responsibilities

PECB

65

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

Example:

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

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

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

Integrity

ISO/IEC 27000, clause 3.36

Integrity

Property of accuracy and completeness

- Integrity:
  - Ensures that information is not modified when in storage or in transit
  - Ensures that only authorized modifications are made
  - Ensures that data is accurate, authentic, and safe from unauthorized access in order for users to be able to rely on the correctness of information when processing it

PECB

66

Integrity: Data must be complete and intact.

Example:

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

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

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

Integrity must be protected by:

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

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

Data can experience changes due to:

- Storage erosion
- Natural or intentional errors
- System damages

Availability

ISO/IEC 27000, clause 3.7

Availability

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

- Information availability is crucial for modern information security.
- Information availability means that the information is accessible:
  - As required
  - When required
  - Where required
  - To the person(s) requiring
- Information security managers usually face three challenges:
  - Denial of service (DoS) as a result of intentional attacks (e.g., a programmer is not aware of a defect that could harm the software due to a specific and unexpected input)
  - Losing protection capacities of information systems due to natural disasters or human activities
  - Equipment failures

PECB

67

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

Example:

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

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

Vulnerability

ISO/IEC 27000, clause 3.77

Vulnerability

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 get implemented incorrectly or malfunction could become vulnerabilities.

PECB

68

The assessment of vulnerabilities can be complicated by a common misperception that weaknesses are always associated with negative characteristics. Many vulnerabilities are indeed negative characteristics, like an information system where “patches” are not updated.

Sometimes, certain vulnerabilities can be accepted for the sake of the positive outcomes associated with the risk we take. For example, purchasing laptops instead of desktop computers can increase the chances of theft but also improves the workers’ mobility.

Vulnerabilities can be divided into intrinsic and extrinsic. 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.

Types of Vulnerabilities

ISO/IEC 27005, Annex D.1

Type	Examples of vulnerabilities
Hardware	*Insufficient maintenance/faulty installation of storage media*
	Lack of periodic replacement schemes
Software	*No or insufficient software testing*
	Complicated user interface
Network	*Unprotected communication lines*
	Single point of failure
Personnel	*Insufficient security training*
	Unsupervised work by outside or cleaning staff
Site	*Unstable power grid*
	Location in an area susceptible to flood
Organization	*Lack of proper allocation of information security responsibilities*
	Lack of information security responsibilities in job descriptions

PECB

69

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

Threats

ISO/IEC 27000, clause 3.74 and ISO/IEC 27005, clause 8.2.3

Threat

Potential cause of an unwanted incident, which can result in harm to a system or organization

A threat has the potential to harm assets such as information, processes and systems and, therefore, organizations.

Threats can be of natural or human origin, and can be accidental or deliberate.

Both accidental and deliberate threat sources should be identified.

PECB

70

ISO/IEC 27005, clause 8.2.3 Identification of threats (cont'd)

A threat can arise from within or from outside the organization. Threats should be identified generically and by type (e.g. unauthorized actions, physical damage, technical failures); then, where appropriate, individual threats within the generic class identified. This means no threat is overlooked, including the unexpected, but the volume of work required is limited.

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

Types of Threats

ISO/IEC 27005, Annex C

Type	Threats
Physical damage	Fire
	Water damage
Natural events	Volcanic phenomenon
	Flood
Loss of essential services	Failure of air conditioning or water supply system
	Loss of power supply
Disturbance due to radiation	Electromagnetic radiation
	Thermal radiation
Compromise of information	Tampering with hardware
	Theft of media or documents
Technical failures	Equipment failure
	Software malfunction
Unauthorized actions	Unauthorized use of equipment
	Corruption of data
Compromise of functions	Error in use
	Abuse of rights

PECB

71

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

Relationship Between Vulnerability and Threat

Examples

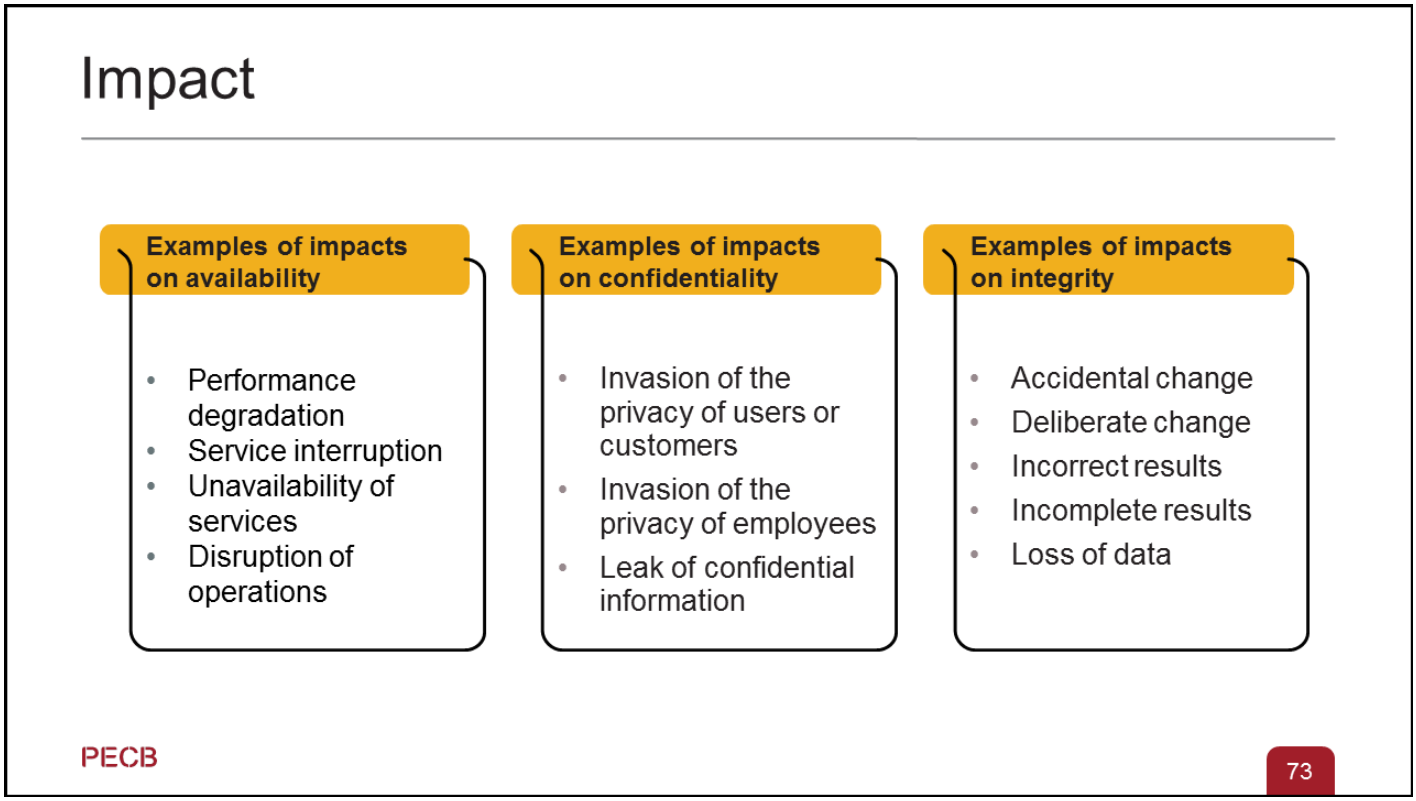
Vulnerabilities	Threats
Warehouse unprotected and without surveillance	Theft
Complicated data processing procedures	Data input error by personnel
No segregation of duties	Fraud, unauthorized use of a system
Unencrypted data	Information theft
Use of pirated software	Lawsuit, virus
No review of access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

PECB

72

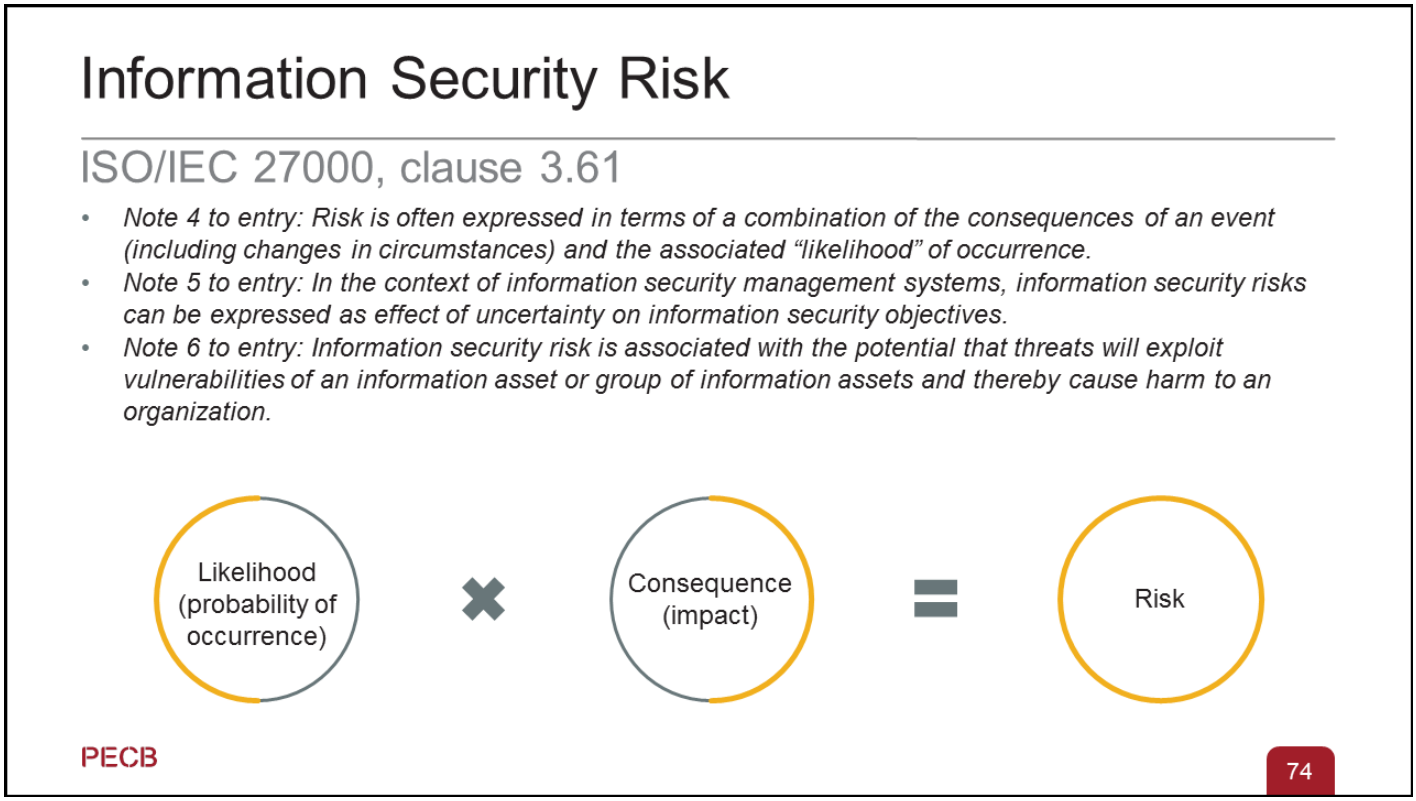
The presence of a vulnerability itself does not produce damage; a threat must exist to exploit it. A vulnerability that does not correspond to a threat may not require the set-up of a control, but it must be identified and monitored in case of changes.

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



The following is a list of potential impacts (see ISO/IEC 27005, Annex B.2) that can affect availability, integrity, or confidentiality, or a combination of them:

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



ISO/IEC 27000 clause 3.57 Residual risk

Risk remaining after risk treatment

Note 1 to entry: Residual risk can contain unidentified risk.

Note 2 to entry: Residual risk can also be referred to as "retained risk".

ISO/IEC 27000, clause 3.61 Risk

Effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" and "consequences" or a combination of these.

ISO/IEC 27000, clause 3.62 Risk acceptance

Informed decision to take a particular risk

Note 1 to entry: Risk acceptance can occur without risk treatment or during the process of risk treatment.

Note 2 to entry: Accepted risks are subject to monitoring and review.

ISO/IEC 27000, clause 3.63 Risk analysis

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

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

Note 2 to entry: Risk analysis includes risk estimation.

ISO/IEC 27000, clause 3.64 Risk assessment

Overall process of risk identification, risk analysis and risk evaluation

Slide Notes Extension

PECB

75

ISO/IEC 27000, clause 3.66 Risk Criteria

Terms of reference against which the significance of risk is evaluated

Note 1 to entry: Risk criteria are based on organizational objectives, and external context and internal context.

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

ISO/IEC 27000, clause 3.67 Risk evaluation

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

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

ISO/IEC 27000, clause 3.68 Risk identification

Process of finding, recognizing and describing risks

Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

ISO/IEC 27000, clause 3.69 Risk management

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

ISO/IEC 27000, clause 3.70 Risk management process

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

Note 1 to entry: ISO/IEC 27005 uses the term "process" to describe risk management overall. The elements within the risk management process are referred to as "activities".

ISO/IEC 27000, clause 3.71 Risk owner

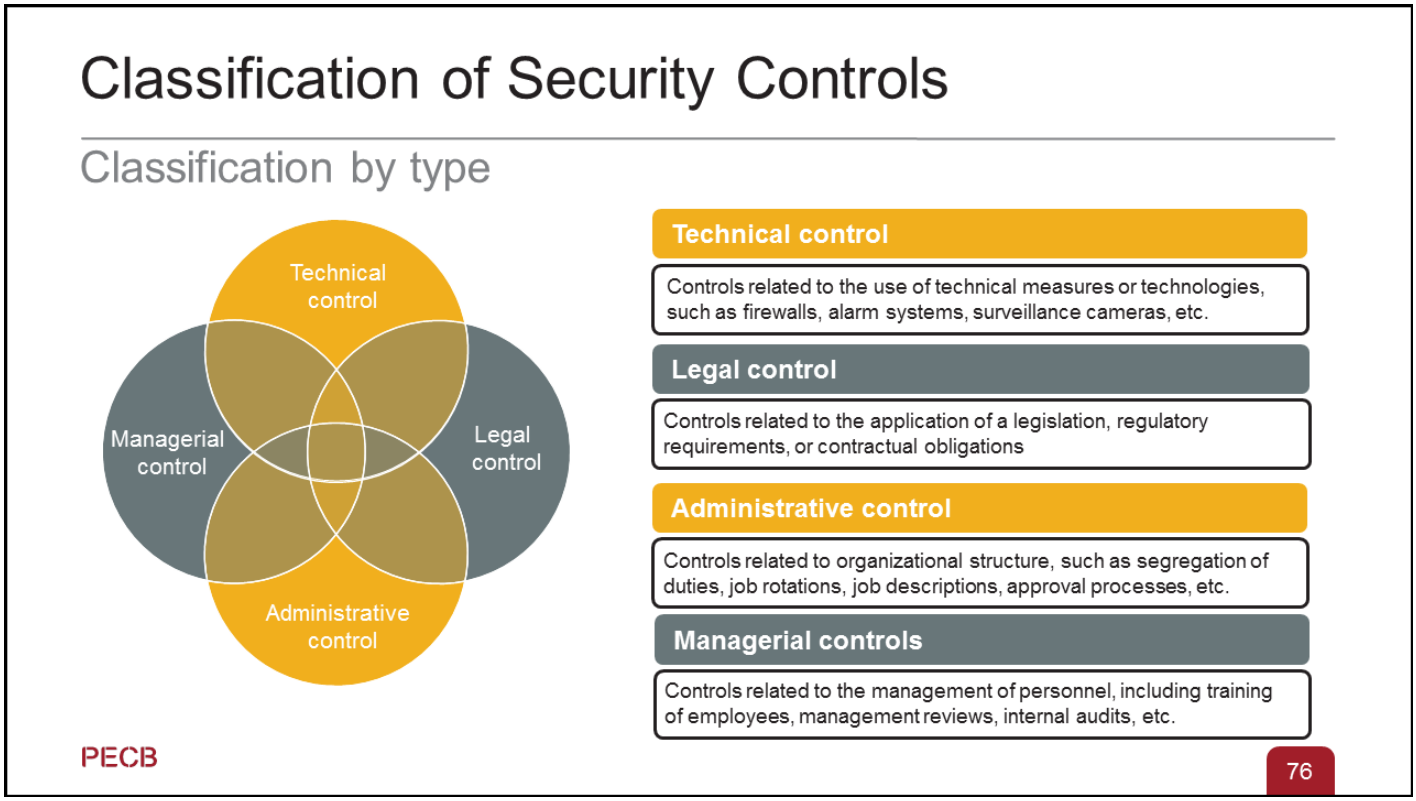
Person or entity with the accountability and authority to manage a risk

ISO/IEC 27000, clause 3.72 Risk treatment

Process to modify risk

Note 1 to entry: Risk treatment can involve:

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



ISO/IEC 27000, clause 3.14 Control

Measure that is modifying risk

ISO/IEC 27000, clause 3.15 Control objective

Statement describing what is to be achieved as a result of implementing controls

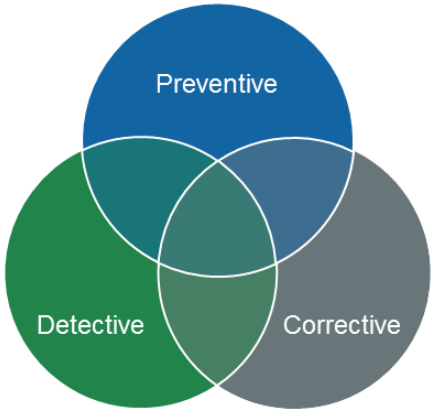
Controls for information security include any process, policy, procedure, guideline, practice, or organizational structure that can be administrative, technical, managerial, or legal in nature, and that can modify information security risks.

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.

Classification of Security Controls

Classification by function



Preventive control

Controls to avoid or prevent the occurrence of incidents

Detective control

Controls to search for, detect, and identify incidents

Corrective control

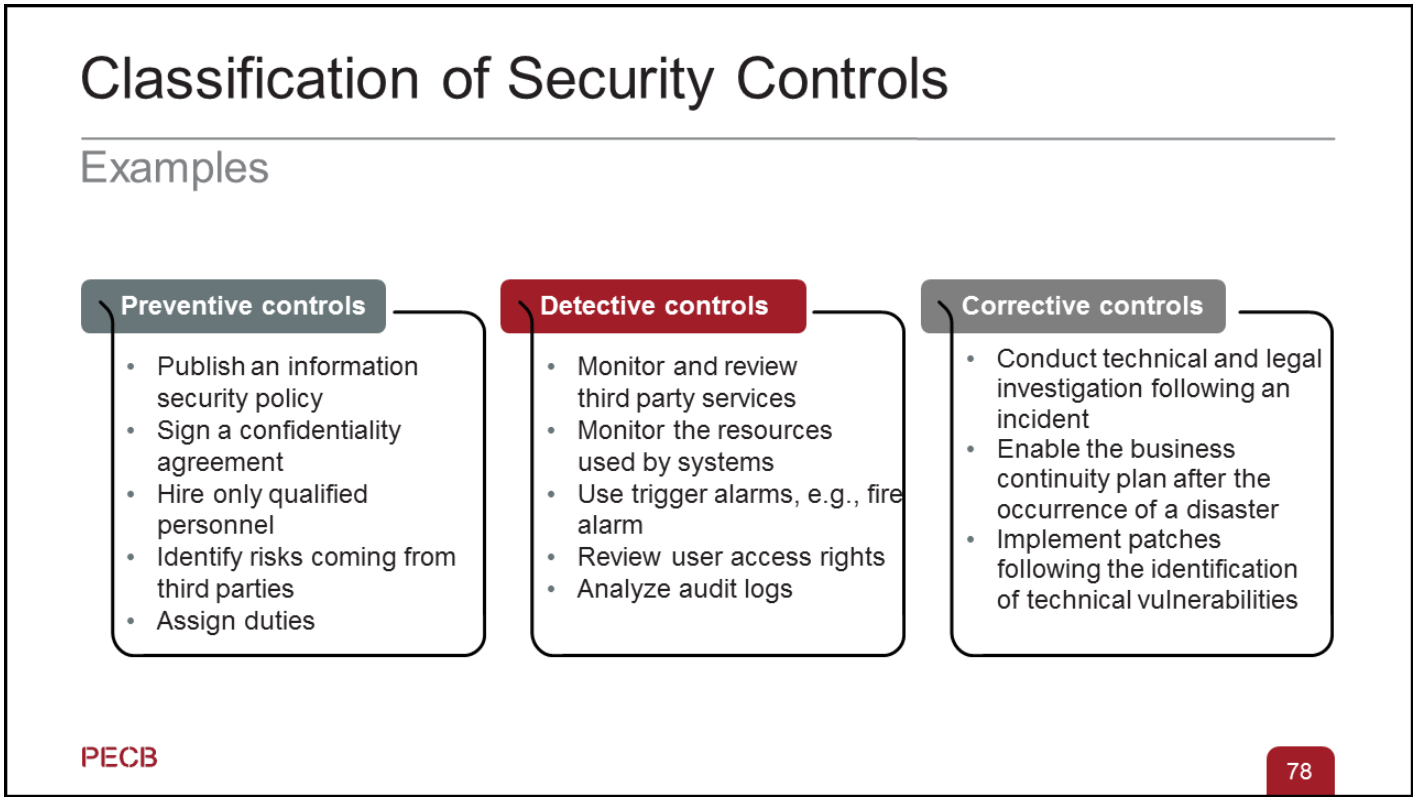
Controls to solve the identified incidents and prevent their recurrence

PECB

77

Information security controls can be classified into preventive, detective, and corrective. Several information security reference frameworks use classifications with more categories.

Important note: These different types of controls are connected with one another. For example, the implementation of an antivirus is a preventive control because it provides protection against malware. At the same time, the antivirus serves as a detective measure when it detects a potential virus and provides a corrective measure when a suspicious file is quarantined or deleted.



1.Preventive control
Goal: Avoid or prevent the occurrence of incidents

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

Examples:

- 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

Slide Notes Extension

PECB

79

2.Detective control
Goal: Search for, detect, and identify incidents

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

Examples:

- 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

3.Corrective control
Goal: Solve the identified incidents and prevent their recurrence

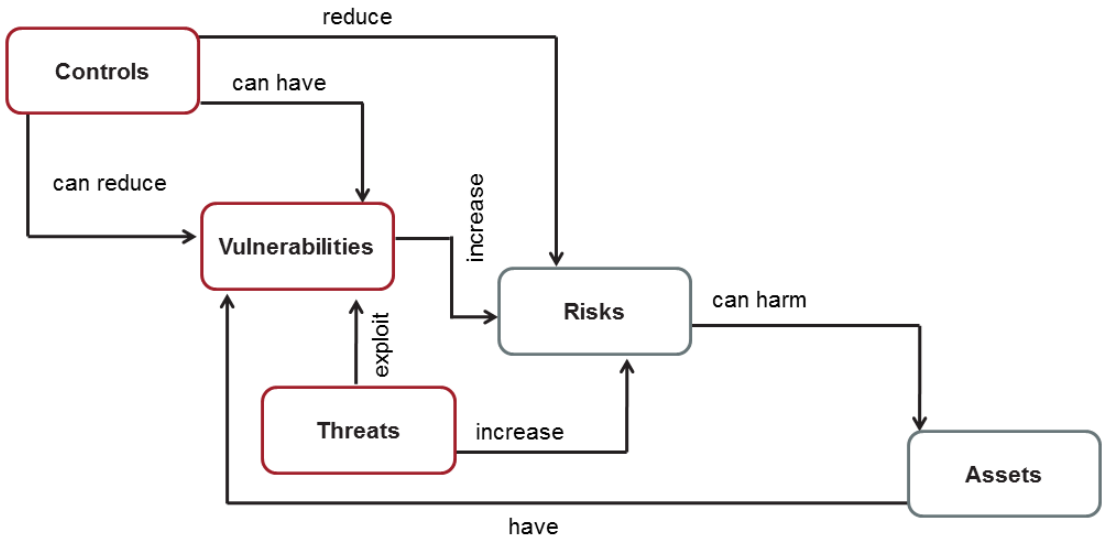
- Minimize the impact of a threat
- Solve the incidents discovered by detection controls
- Identify the causes of an incident
- Modify the processing system to reduce future incidents to a minimum

Examples:

- 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



PECB

80

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

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

Exercise 2: Classification of controls

For each of the following information security controls, determine their type (administrative, technical, managerial, or legal) and their function (preventive, corrective, or detective). Elaborate on your answer.

Example: The installation of a wire fence around the company's site

By function, the installation of a wire fence is a preventive control that helps secure the company's site, especially the information processing facilities, against unauthorized physical access. By type, it is a technical control.

1. Segregation of information security duties
2. Installation of a fire alarm system
3. Encryption of electronic messaging
4. Investigation of security incidents
5. Consideration of applicable legislation

Duration of the exercise: 20 minutes

Comments: 15 minutes

1.What are information, software, services, and people considered as?

A. Inventories
B. Assets
C. Information

2.Which of the following statements regarding information security is correct?

A. Information security protects the confidentiality, integrity, and availability of information regardless of its type and form
B. Information security protects the confidentiality, integrity, and availability of information only in an electronic form
C. Information security protects the organization against threats by only identifying the threat source

3.What does confidentiality ensure?

A. That the information is accessible to the authorized individuals
B. That the information is accurate and complete
C. That the information is available

4.Which of the following is NOT an example of a threat?

A. Theft of media or documents
B. Complicated user interface
C. Unauthorized use of equipment

5.Performance degradation can have an impact on the _____ of information.

A. Availability
B. Confidentiality
C. Integrity

6.Vulnerability is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.

A. True
B. False

7.What type of controls are the segregation of duties, job rotations, and approval processes?

A. Technical controls
B. Managerial controls
C. Administrative controls

8.What type of control is the separation of development, testing, and operating environment?

A. Preventive control
B. Detective control
C. Corrective control

9.An organization has installed a fire alarm in its premises. What type of control is this?

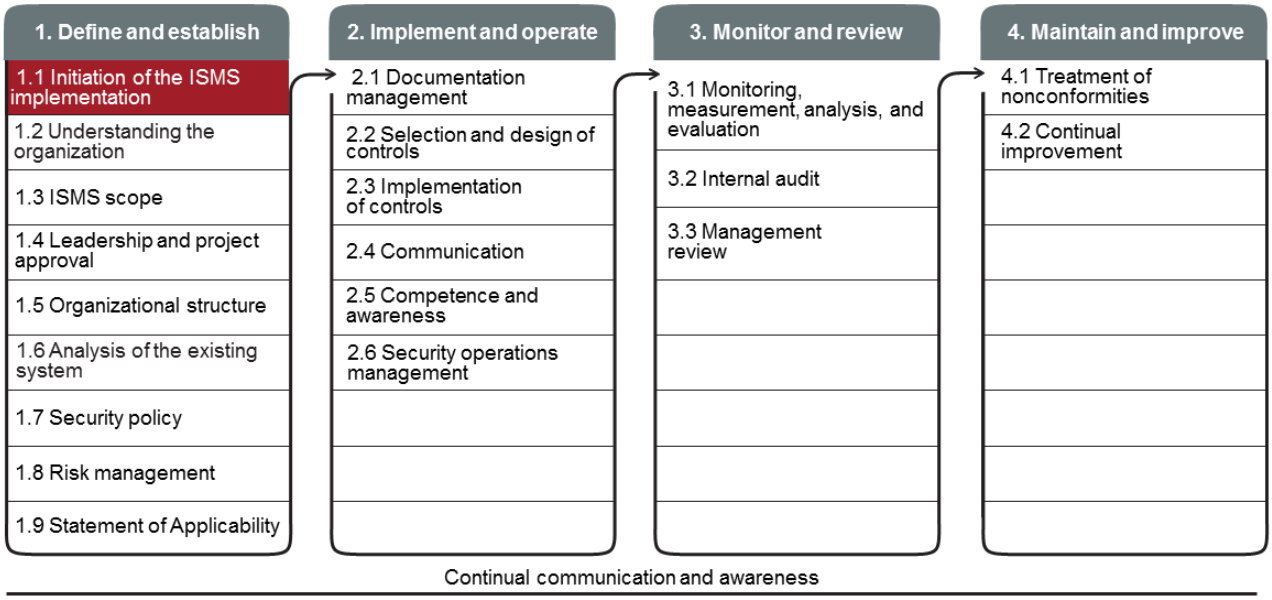
A. Preventive and administrative
B. Corrective and managerial
C. Detective and technical

10.Assets and controls can present _____ that can be exploited by _____.

A. Threats, vulnerabilities
B. Vulnerabilities, threats
C. Threats, risks

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

1.1 Initiation of the ISMS implementation



Project Management – Definitions

ISO 9000 definitions related to project management

ISO 9000, clause 3.4.2 Project

Unique process, consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources

ISO 9000, clause 3.3.11 Activity

Smallest identified object of work in a project

ISO 9000, clause 3.3.12 Project management

Planning, organizing, monitoring, controlling and reporting of all aspects of a project, and the motivation of all those involved in it to achieve the project objectives

PECB

87

Notes on terminology:

1. Projects are temporary in that they have a defined beginning and end in 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. We must distinguish between conducting the ISMS project and managing the ISMS operations. Conducting an ISMS project refers to implementing an ISMS. Managing the ISMS operations, on the other hand, refers to the daily management and maintenance of the ISMS.

Important note: This training course aims to explain the methodology for the implementation of the ISMS, and not the management of the ISMS's daily operations.

1.1 Initiation of the ISMS implementation

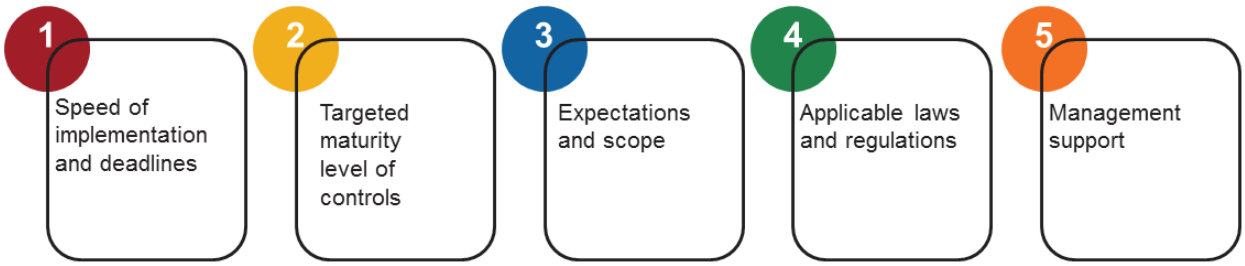
List of activities

1.1.1 Define the approach to the ISMS implementation

1.1.2 Align with best practices

1.1.1 Define the Approach to the ISMS Implementation

Factors determining the ISMS implementation approach



PECB

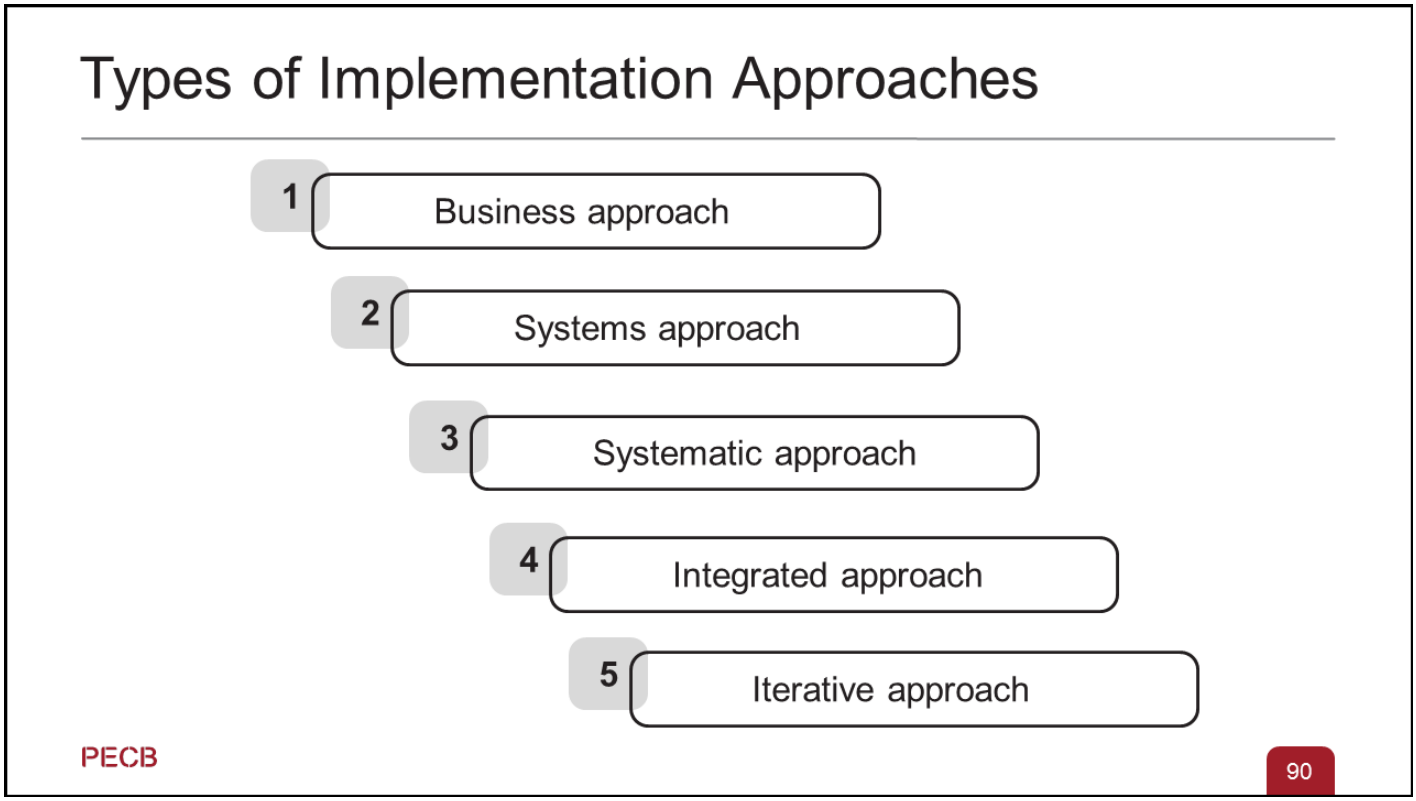
89

An organization wishing to comply with ISO/IEC 27001 may consider several approaches based on the following:

- Speed of implementation and deadlines
- Targeted maturity level of controls
- Expectations and scope
- Applicable laws and regulations
- Management support

It is reasonable to consider a period of 6 to 12 months for the project from its conception to the completion of the first cycle of audits and the monitoring of the system.

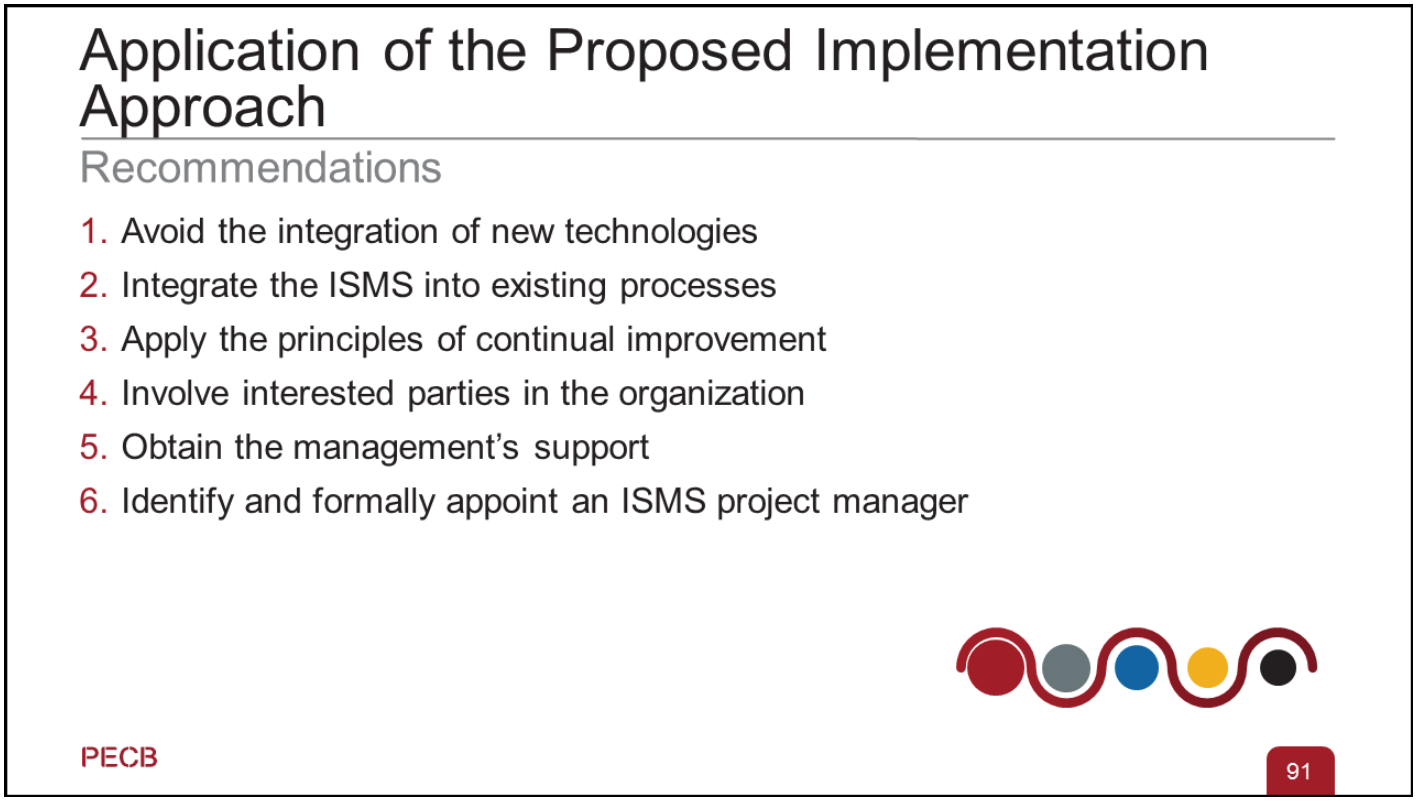
When a limited scope for the ISMS is considered at the start of the project, for example the approach “IT governance fast track” (approach to achieve the goal very quickly in a given business context), a medium-sized organization could complete such projects in 4 to 7 months.



The implementation approaches proposed for an ISMS are usually sequential. The organization's project plan is completed prior to the establishment of a project dedicated to the ISMS. Likewise, the monitoring and improvement phases begin only after the location of system components has been identified. In each phase, the ISMS processes or controls may be implemented sequentially. A major drawback of this approach is that it is time-consuming and resource-intensive, whether for planning, approving, or implementing the system "piece by piece." This approach does not allow the organization to immediately experience any positive outcomes from the implementation of a management system, since a certain period of time needs to pass before such an effect can be noticed. Another drawback of this approach is "the exhaustion" of the participants during the implementation process, thus posing a major risk of abandonment during the project.

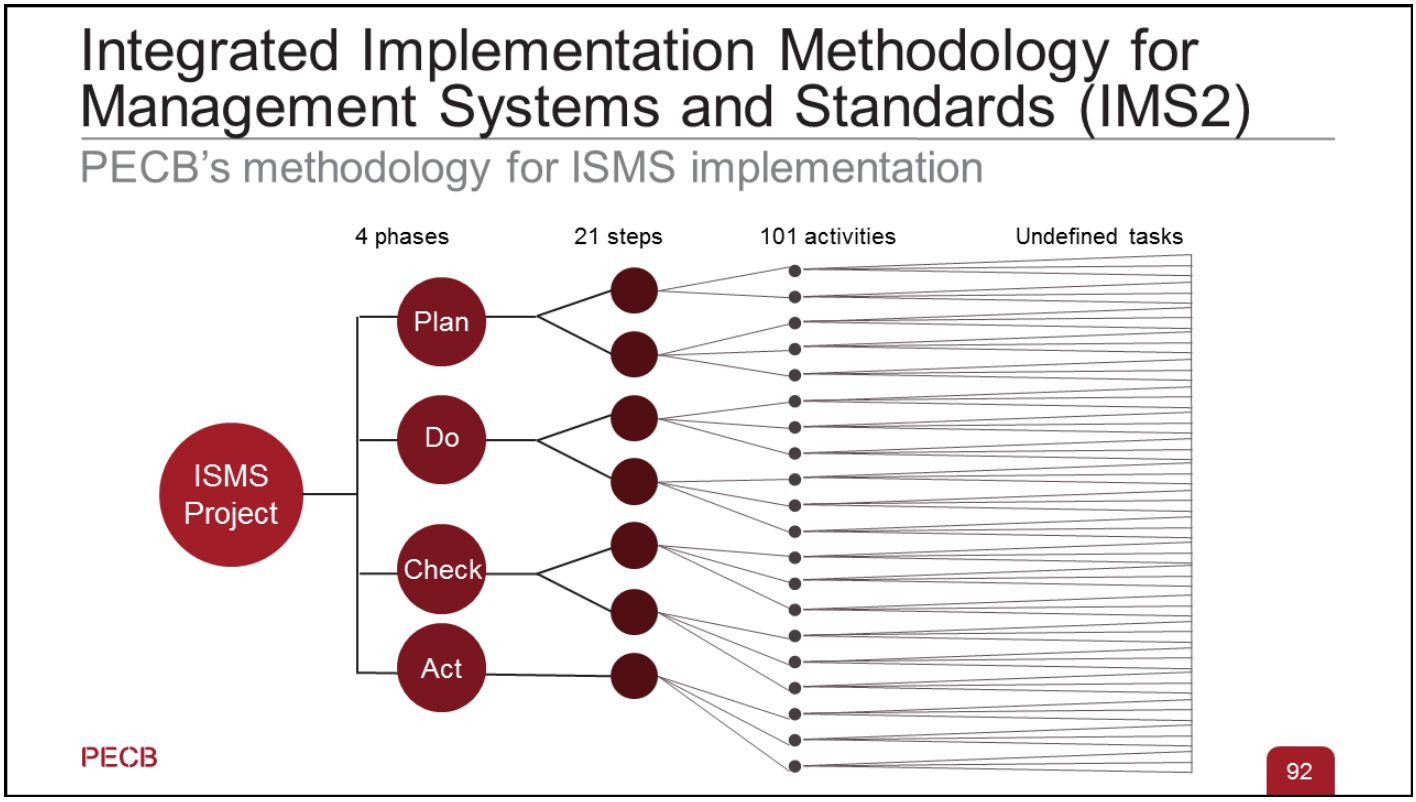
The approach proposed in this training course attempts to circumvent this difficulty by suggesting a philosophy based on the following approaches to initiate such a system within a reasonable period:

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 the best practices in project management such as ISO 10006
4. **Integrated approach:** Integration or harmonization 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



Some recommendations to consider when applying the proposed implementation approach in practice:

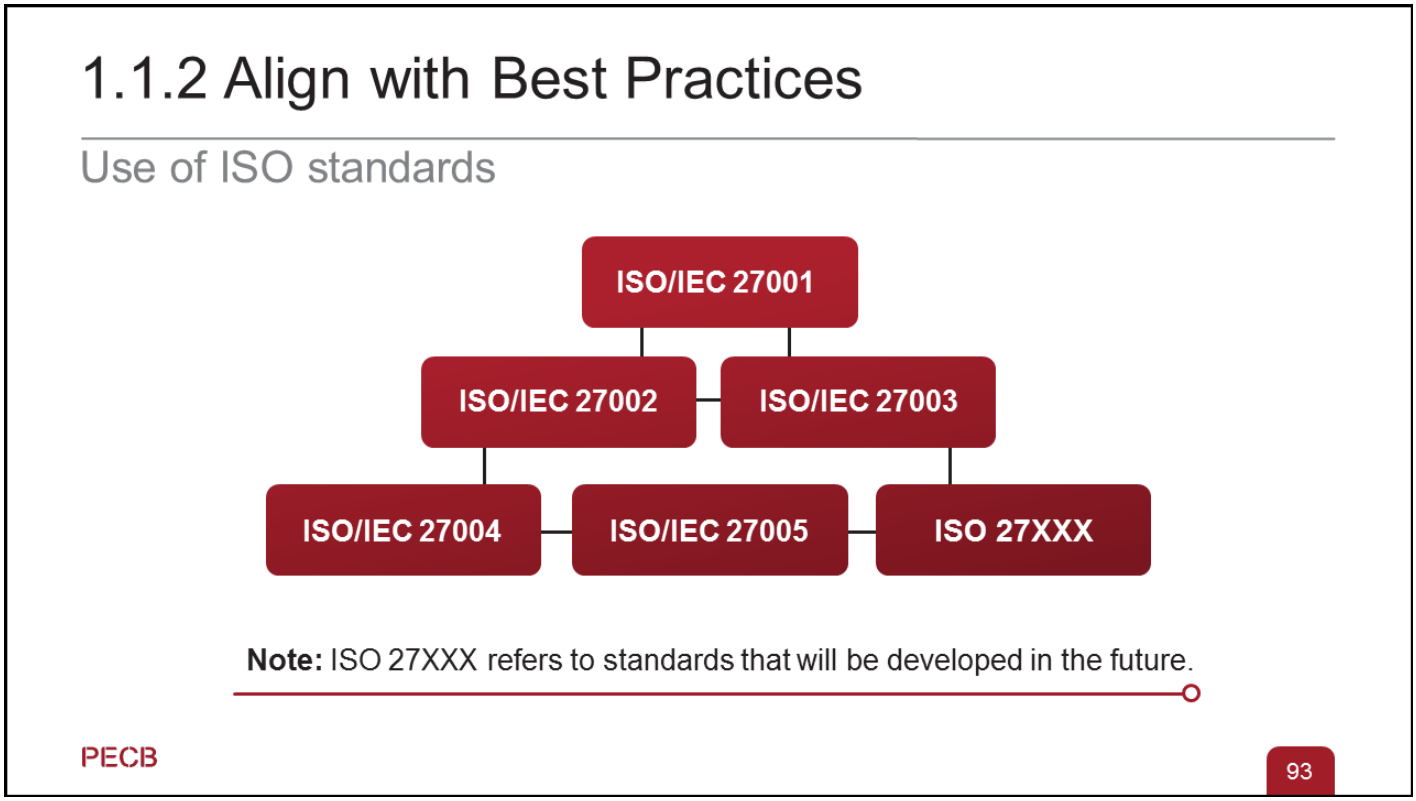
1. **Avoid the integration of new technologies:** The initial system should be designed with the technology that is already in place within the organization. Most organizations already have established the necessary technology needed to implement an ISMS. The optimization of the ISMS with more efficient technologies can be completed in the continual improvement phase.
2. **Integrate the ISMS into existing processes:** The existing customized processes should be adjusted in accordance with the requirements of the ISMS's framework. In addition, creating processes that do not fit with the organization's culture should be avoided.
3. **Apply the principles of continual improvement:** The principles of continual improvement should be applied. Any improvement suggestions recommended by the interested parties should be taken into account. Minor goals should be envisaged at the beginning of the project and a progressive improvement must be a target for the longer term.
4. **Involve interested parties in the organization:** The roles and responsibilities of all interested parties should be defined early in the implementation process. After ensuring their involvement, their support in the organization should be analyzed and maintained.
5. **Obtain the management's support:** It is important to ensure that the management understands and supports the project. Their role in the implementation of the management system is detrimental. They are responsible not only for providing resources to successfully implement ISMS but also for performing regular reviews of the management system so as to ensure ongoing success.
6. **Identify and formally appoint an ISMS project manager:** It is important to identify and appoint an individual who will be responsible for the project implementation. The Project Manager's appointment will guarantee the smooth running of operations including the timing and support of the implementation process (budget, approvals, etc.).



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

IMS2 is based on the PDCA cycle divided into four phases: Plan, Do, Check, and Act. In turn, these phases are divided 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 description of the job, interview candidates, signing a contract, etc.

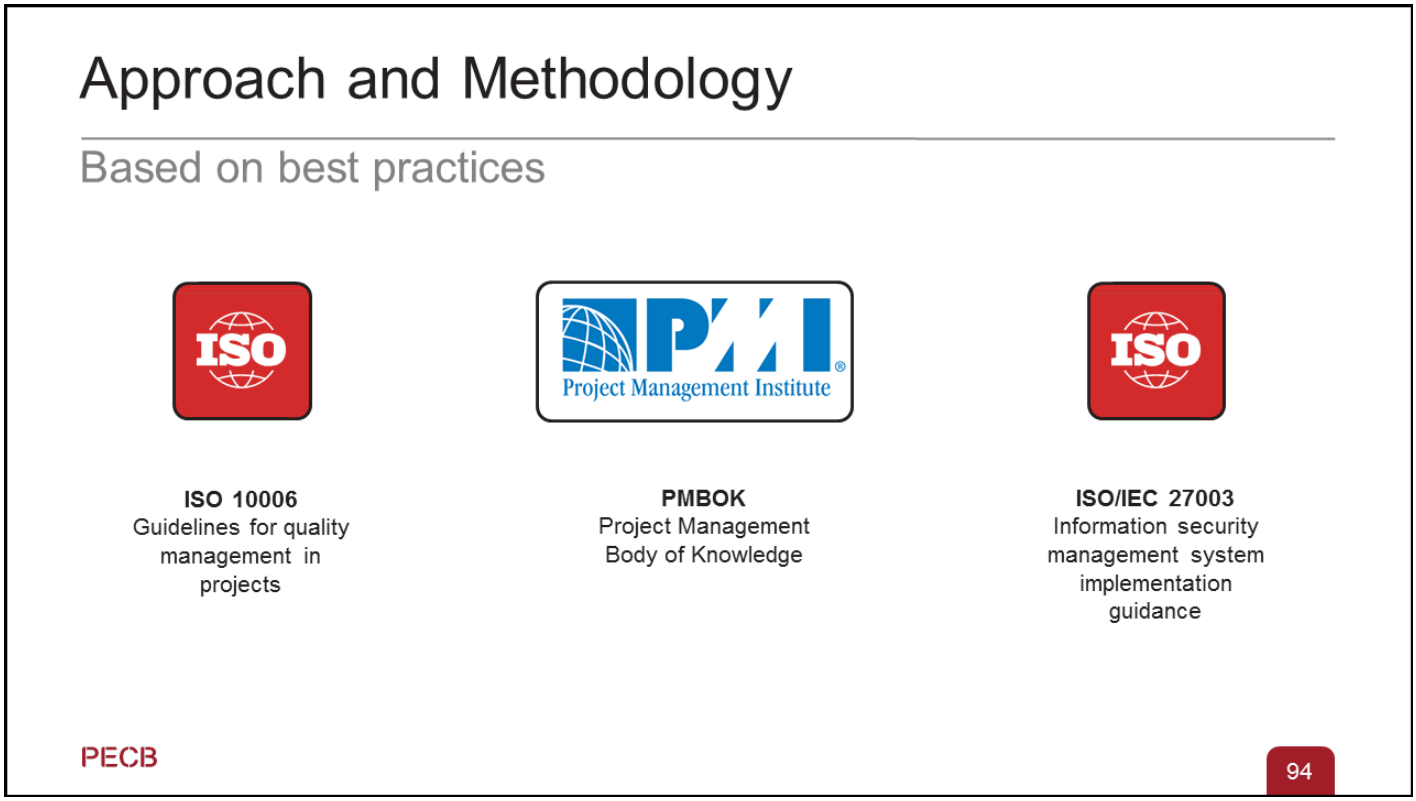


The core of best practices included in various ISO standards provide access to knowledge which has a large consensus among experts in the information security management field. These notions of best practices should not be confused with the standard requirements. A good practice is a recommendation, not a requirement. This means that each organization is free to use it as a reference or choose whether to apply it or not.

In this training, it was a conscious choice to present the good practices published in various ISO standards. However, there are several other sources of good practices, such as ANSI or the ITIL library. An organization may also refer to ISO/IEC 27035 to develop its incident management process. It could equally well be based on ITIL or on CERT guides in that domain.

Note on terminology

1. “Good practice” means it is generally recognized that the implementation of recommendations related to the described 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. 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.

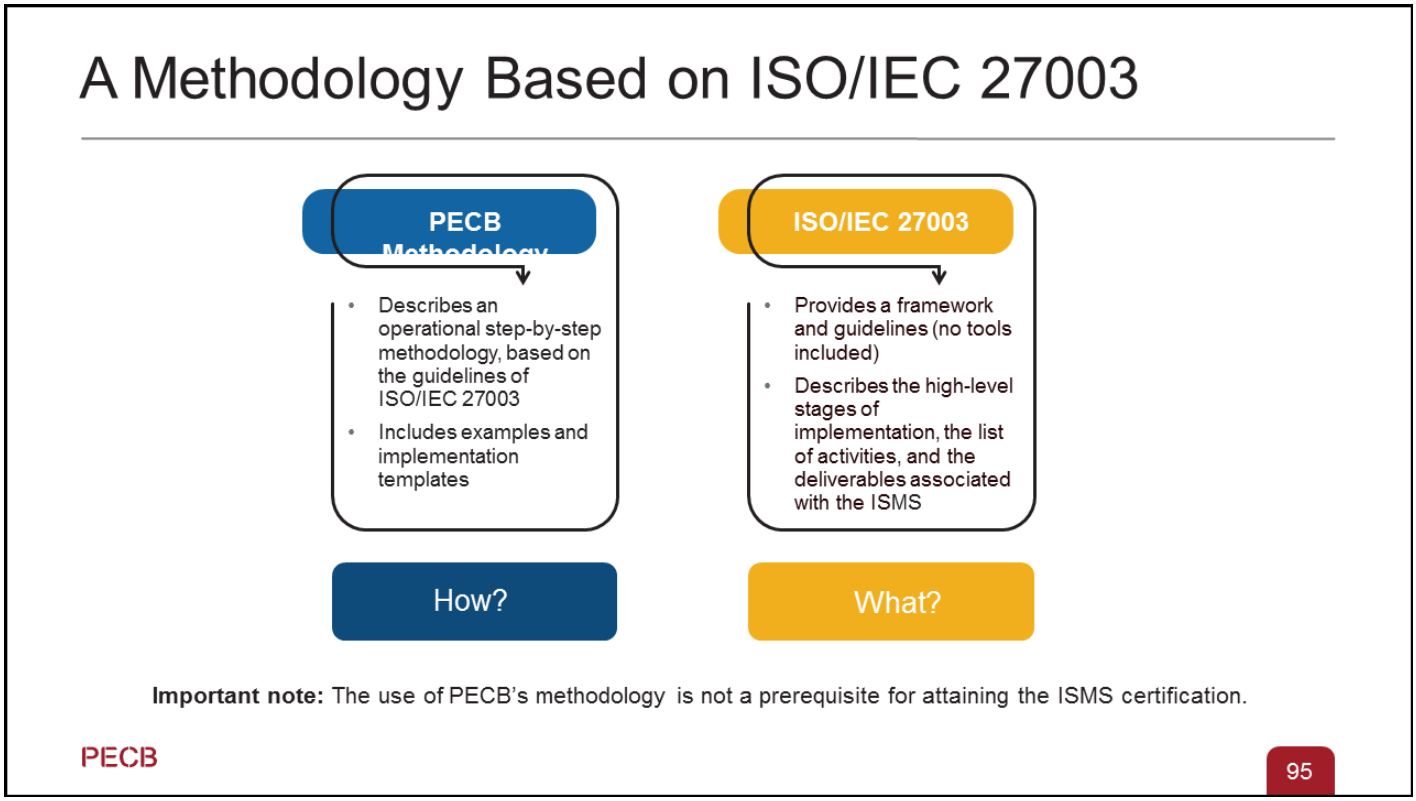
Source: www.iso.org

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: initiation, 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 observe the guidance in this document.

Source: www.iso.org



ISO/IEC 27003 outlines the major steps in implementing an ISMS. It guides the user throughout and facilitates the effective implementation of the ISMS. The standard contains the following clauses:

1. Introduction
2. Scope
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

The methodological framework proposed by ISO/IEC 27003 is generic and applicable to all types of organizations, regardless of their size, type, or activity. Nonetheless, it is not an exhaustive reference and does not claim to be universal. This framework is not a formal methodology because it does not contain an equipped operational approach. It should be noted that its use is not a requirement in itself that can lead to the ISO/IEC 27001 certification.

The methodology proposed by PECB is partially based on the approach described in ISO/IEC 27003, but does not necessarily substitute it. The objective of this methodology is to introduce an operational step-by-step implementation of the ISMS. The PECB methodology explains using examples and tools, the "how" starting from the "what" as described in ISO/IEC 27001.

Important note: Please note that, during this training course, not all subjects are discussed in detail. Nonetheless, subjects briefly mentioned here should not be regarded as unimportant.

1._____ includes the application of best practices in project management.

A. Business approach
B. Iterative approach
C. Systematic approach

2.What is the correct definition of the term project?

A. A unique process consisting of a set of coordinated and controlled activities
B. A small identified object of work
C. The process of planning, organizing, and controlling a set of activities

3.Which of the following statements is correct?

A. The ISMS should be implemented with new technology because this helps the optimization of the processes
B. The roles and responsibilities of interested parties should be defined after the implementation process
C. The ISMS should be integrated into existing processes of the organization

4.Which step follows the initiation of the ISMS implementation according to the PECB framework?

A. Organizational structure
B. Risk management
C. Understanding the organization

5.What does the iterative approach include?

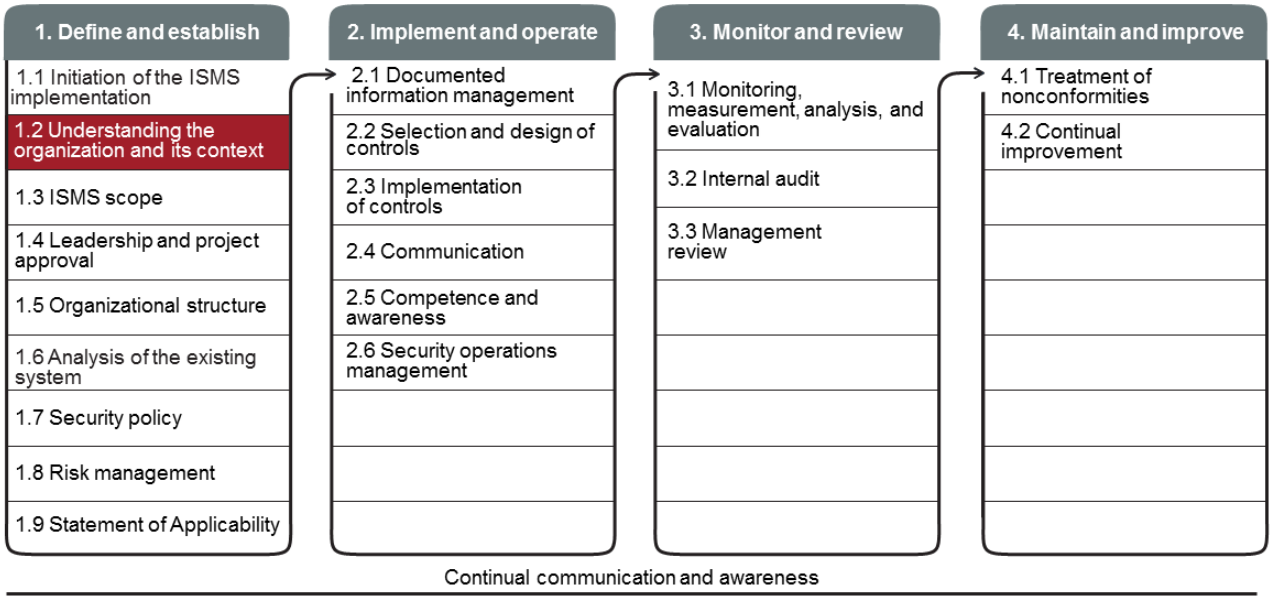
A. Integration of the ISMS into the context of commercial activities across the organization
B. Rapid implementation of the ISMS by adhering to the minimum requirements of the standard and proceeding with continual improvement thereafter
C. Harmonization of the ISMS with other management systems established in the organization

Section summary

- There are some activities that should be followed to initiate the ISMS. 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.

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, the key processes involved in the implementation of an ISMS, the interested parties involved in the implementation of an ISMS, and the necessary information for planning the ISMS implementation.

1.2 Understanding the Organization and its Context



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 4.1

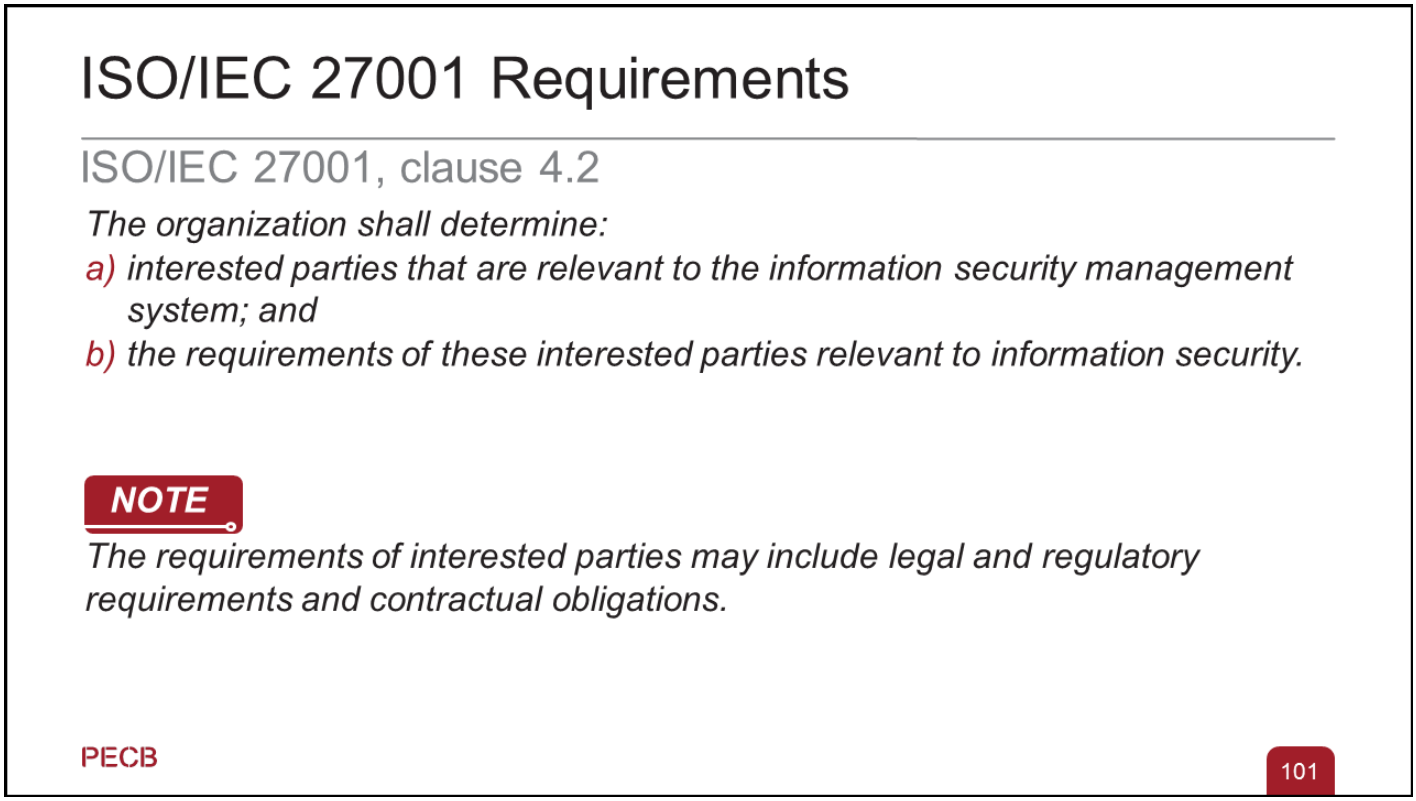
The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

PECB

100

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

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. Recognize and take into account issues related to information security within their industrial sector, such as risk, legal and regulatory obligations, and customer requirements
5. Establish and document objectives for the ISMS



Definitions related to the concept of organization

ISO 9000, clause 3.2.1 Organization

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

ISO 9000, clause 3.5.2 Infrastructure

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

ISO 9000, clause 3.6.4 Requirement

Need or expectation that is stated, generally implied or obligatory

Notes on terminology:

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. “Infrastructure” can be used as a synonym of “supporting asset,” as defined by ISO/IEC 27005.
4. 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).

Slide Notes Extension

PECB

102

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

External issues are those outside of the organization's control. This is often referred to as the organization's environment. Analysing this environment can include the following aspects:

a. *social and cultural;*
b. *political, legal, normative and regulatory;*
c. *financial and macroeconomic;*
d. *technological;*
e. *natural; and*
f. *competitive.*

Internal issues are subject to the organization's control. Analysing the internal issues can include the following aspects:

k.*the organization's culture;*
l.*policies, objectives, and the strategies to achieve them;*
m.*governance, organizational structure, roles and responsibilities;*
n.*standards, guidelines and models adopted by the organization;*
o.*contractual relationships that can directly affect the organization's processes included in the scope of the ISMS;*
p.*processes and procedures;*
q.*the capabilities, in terms of resources and knowledge (e.g. capital, time, persons, processes, systems and technologies);*
r.*physical infrastructure and environment;*
s.*information systems, information flows and decision making processes (both formal and informal); and*
t.*previous audits and previous risk assessment results.*

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.

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

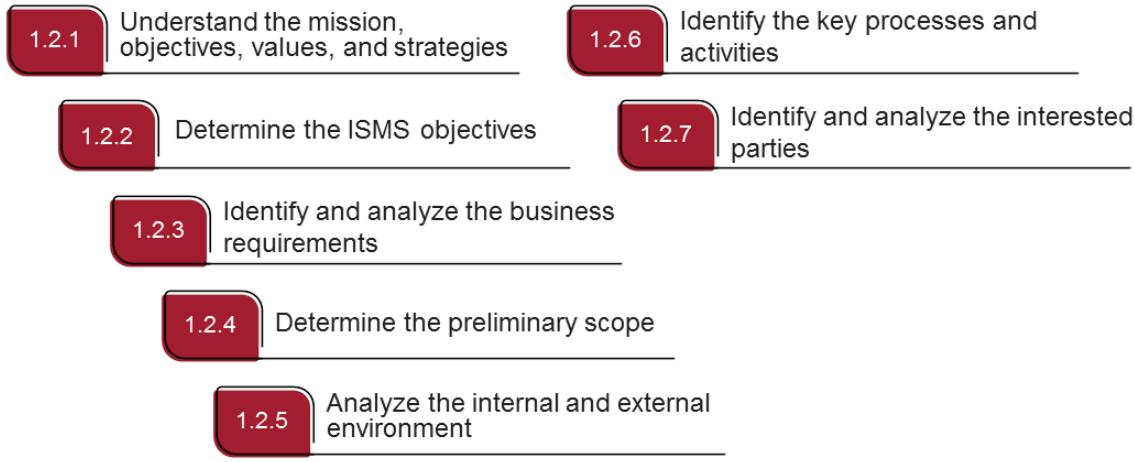
External interested parties can include: a) regulators and legislators; b) shareholders including owners and

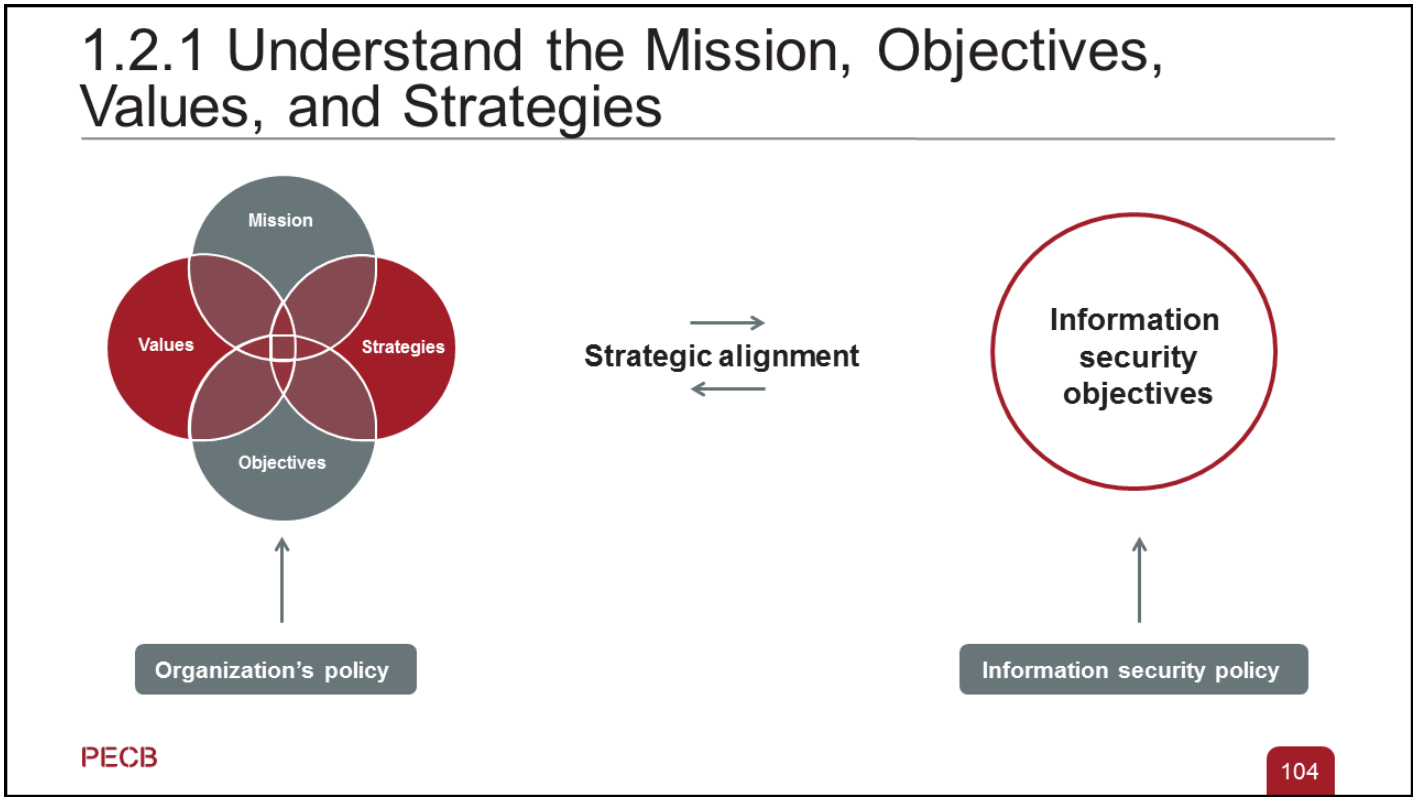
investors; c) suppliers including subcontractors, consultants, and outsourcing partners; d) industry associations; e) competitors; f) customers and consumers; and g) activist groups.

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.

1.2 Understanding the Organization and its Context

List of activities





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

Mission: The mission is what justifies and defines the organization's existence. It serves as a reference point to keep everyone clear on where the organization is headed.
Implications for information security management: The information security management aims to support the organization in fulfilling its mission, that is the protection of its information assets. The ISMS must, therefore, be aligned with the organization's mission.

Values: Values are the fundamental and enduring beliefs that are shared by all the members of an organization which influence the behavior of individuals.

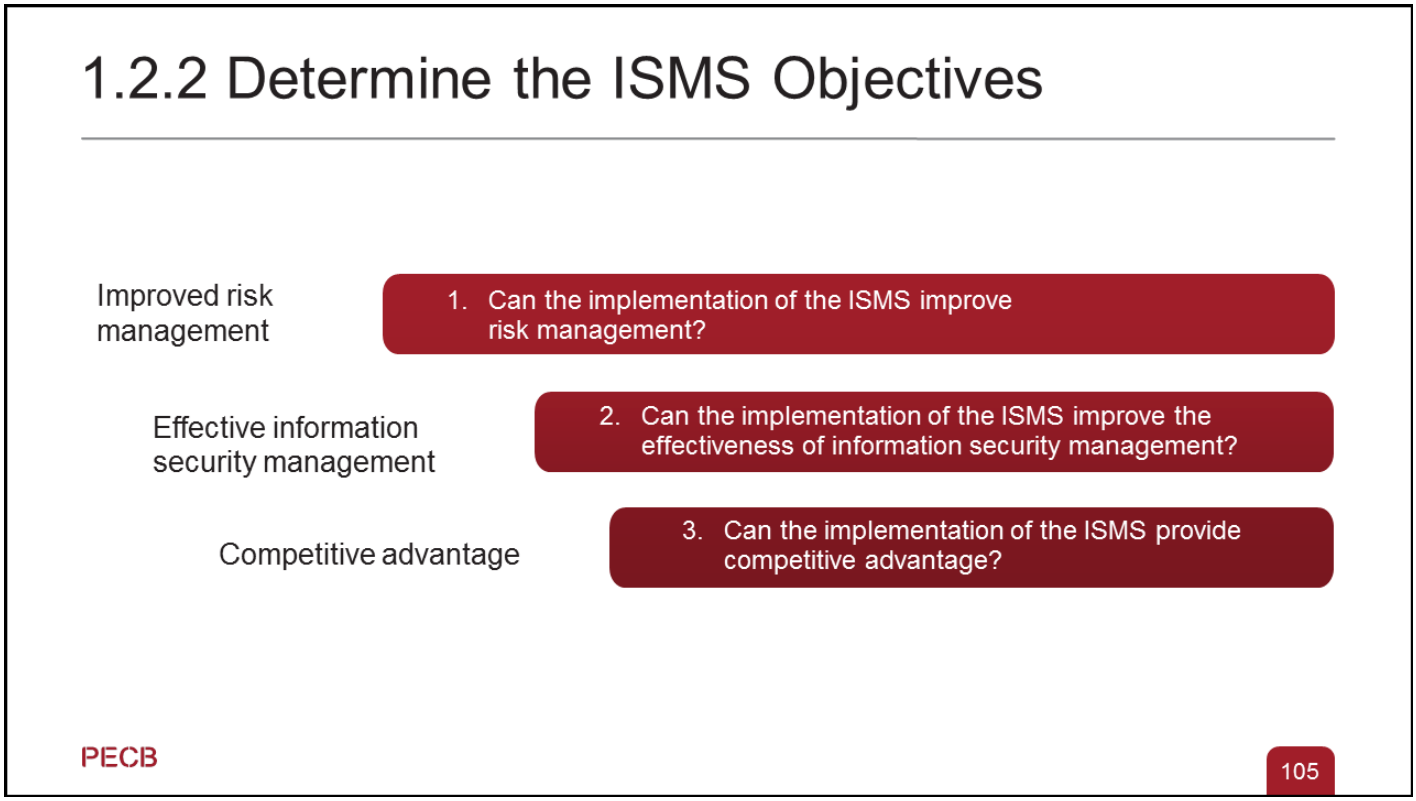
Implications for information security management: The values of the organization influence the choices made by professionals in information security management. For example, values can influence the priorities and policies in terms of evaluating information security risks.

Objectives: An objective is the result that the organization intends to achieve. Objectives are generally predetermined, quantified, and time-bound (e.g., increase the market share by 5% in the upcoming 24 months).

Implications for information security management: As for strategy, information security management system must be aligned with the organization's objectives so as to achieve the ultimate objective and ensure that information security is achieved.

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

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



The objectives of an ISMS management program 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 with interested parties.

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

For example, the ISMS objective can be restoring 5GB of data within 24 hours. This objective is specific and measureable, because its successful backup can be tested by monitoring the hard drive disk (HDD) of the server and determining the amount of GB that have been added in the period of 24 hours.

ISO/IEC 27001, clause 6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a. *be consistent with the information security policy;*
b. *be measurable (if practicable);*
c. *take into account applicable information security requirements, and results from risk assessment and risk treatment;*
d. *be communicated; and*
e. *be updated as appropriate.*

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

f. *what will be done;*
g. *what resources will be required;*
h. *who will be responsible;*
i. *when it will be completed; and*
j. *how the results will be evaluated.*

Determine the 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

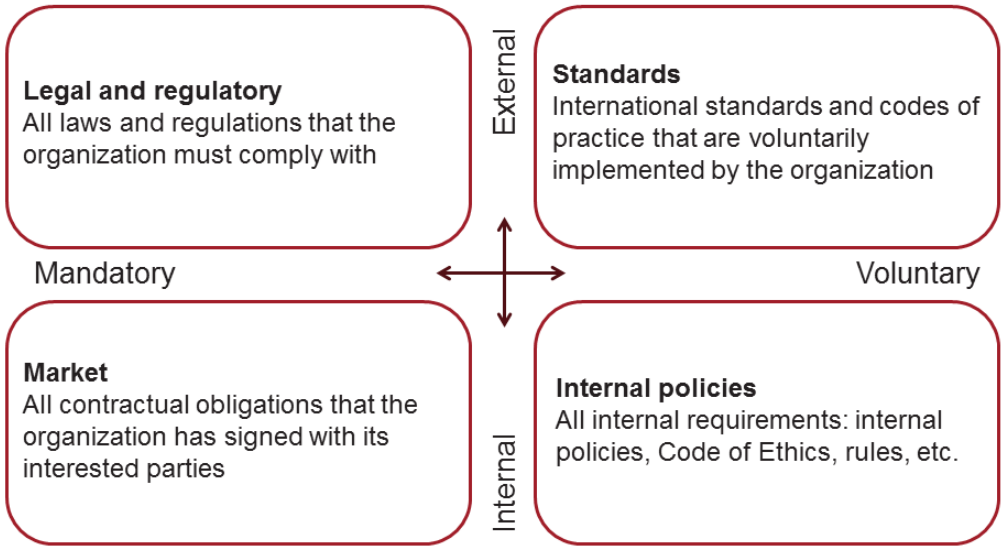
PECB

106

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

1.2.3 Identify and Analyze the Business Requirements



PECB

107

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

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

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

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

Laws and Regulations

Legal compliance

- The organization must comply with the applicable laws and regulations.
- In most countries, the implementation of an ISO standard is a voluntary decision, not a legal requirement.
- In all cases, laws take precedence over standards.

PECB

108

ISO/IEC 27002, clause 18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

ISO/IEC 27002, clause 18.1.1 Identification of applicable legislation and contractual requirements

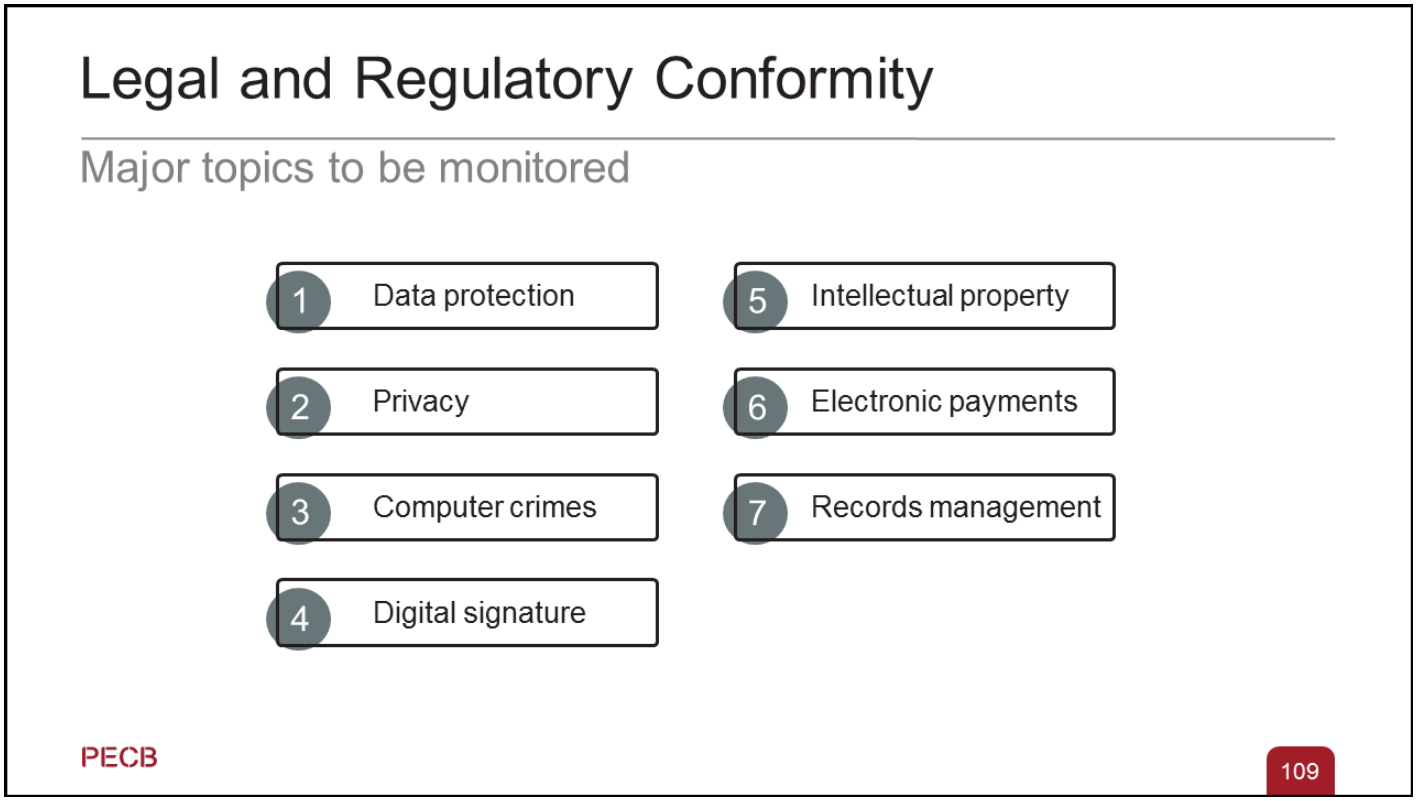
Control

All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization.

Implementation guidance

The specific controls and individual responsibilities to meet these requirements should also be defined and documented.

Managers should identify all legislation applicable to their organization in order to meet the requirements for their type of business. If the organization conducts business in other countries, managers should consider compliance in all relevant countries.



It is generally desirable that the expert in information security works with legal advisers to identify the subjects to be analyzed and explain the security issues involved. For example, they should explain to the lawyer involved in this analysis the operational mode of the network monitoring system, so the latter can better assess whether it violates a privacy law or any internal regulation of the organization.

Moreover, new laws related to privacy issues, financial obligations, and corporate governance require experts to monitor the IT infrastructure with more responsiveness and effectiveness than before. Several public and private organizations that work with different organizations are mandated to ensure a minimum level of safety. In the absence of proactive security, business executives may be exposed to lawsuits (civil or even criminal) for breaching their fiduciary and legal responsibilities. In larger organizations, the demand for legal advice may focus on:

1.Data protection

In several countries, specific laws exist that cover the safeguarding of confidentiality and data integrity, often limited to control of personal data (for example, the General Data Protection Regulation in Europe). In the same way that security incidents must be related to the individuals who caused it, personal information should be subject to management and adequate recording. A structured approach for incident management related to information security should, therefore, manage the most appropriate measures to protect the privacy and personal data of individuals.

2.Privacy

In compliance with applicable laws, many organizations choose to establish a policy for the protection of privacy, often designed to achieve the following objectives:

- Increase awareness of regulatory, legal, and business requirements regarding the treatment and protection of personal information
- Establish a clear and complete policy for the treatment of personal information
- Define the responsibilities to all persons dealing with personal information
- Enable the organization to meet their commercial liability and their legal and regulatory obligations in respect of personal information

Slide Notes Extension

PECB

110

3.Computer crimes
Cyber crime represents a significant threat via internet for information systems of an organization. The damage can be really devastating and can result in direct financial costs, loss of reputation, or significant time wasted for an organization. It has many faces and knows no borders. Its generic and unstable nature requires the head of the organization (with virtually any structure being connected to an external network) to have the necessary awareness and implement the adequate countermeasures in compliance with applicable laws.
4.Digital signature
Today, the law recognizes the validity of agreements on the evidence as was already the case based on the non-mandatory rules on evidence. The drafting of these agreements cannot be done by any types of means; it should proceed in respect to the context in which they fall to be considered valid in case of litigation. 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., in France, the AFNOR NF Z 42—013, or, more internationally, the standard ISO 14721 for the "transfer systems and spatial information—System Open Archival Information—Reference Model").
5.Intellectual property
The result of intellectual effort is often recognized by national and international conventions as an intellectual property right to protect certain intangible assets. For small and medium organizations, the efficient use of human intellectual property can help compete with bigger organizations. Intellectual property has great potential in terms of legal protection, information technology, and competitive advantage. The goal here is to strengthen the competitive position of the organization.
6.Electronic payments
From a legal standpoint, in most countries, it is quite essential to prove in court that a customer bought the product or service sold by the organization. It should also be possible to satisfy the tax authority to demonstrate the time in which the individual transactions took place. The big difference between electronic commerce and trade by paper is the medium in which transactions are stored. With proof on paper, a physical change is difficult, while a change to an electronic file is easier. Another aspect is the possibility that a competitor may offer the same products from a server located in a tax haven. Finally, when a customer buys a product on a website, it is not always easy to determine which national law applies.
7.Records management
Some national laws require that organizations maintain updated records regarding their activities and review them through a process of annual audit. Similar requirements exist at the governmental level. In some countries, organizations are obliged by law to issue such reports or to provide records for legal purposes (for example, in a case that could be the result of an offense involving penetration into a sensitive government system).

1.2.4 Determine the Preliminary Scope

ISO/IEC 27003, clause 4.3

The organization determines the boundaries and applicability of the ISMS to establish its scope.
The following factors can affect the determination of the scope:

a) the external and internal issues described in 4.1;
b) the interested parties and their requirements that are determined according to ISO/IEC 27001:2013, 4.2;
c) the readiness of the business activities to be included as part of ISMS coverage;
d) all support functions, i.e. functions that are necessary to support these business activities (e.g. human resources management; IT services and software applications; facility management of buildings, physical zones, essential services and utilities); and
e) all functions that are outsourced either to other parts within the organization or to independent suppliers.

PECB

111

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

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

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

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

Slide Notes Extension

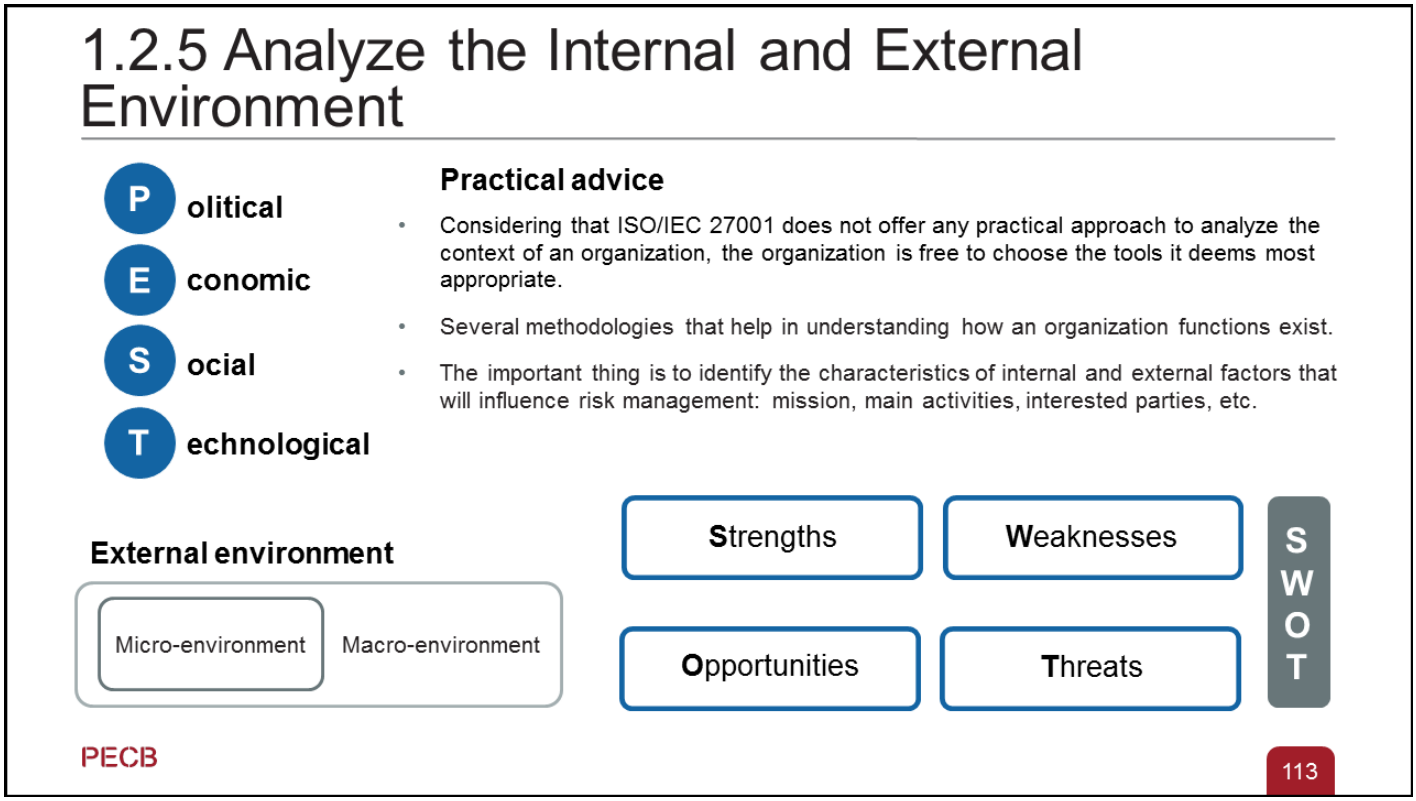
PECB

112

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.

Documented information describing the scope should include:

j. The organizational scope, boundaries, and interfaces
k. The information and communication technology scope, boundaries, and interfaces
l. The physical scope, boundaries, and interfaces



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

The following are some of the frequently used models:

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

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

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

Analyze the Internal and External Environment

Organizational structure and key players

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

- Strategy (who sets the strategic directions?)
- Steering (who coordinates and manages the operations?)
- Operational (who is involved in production and support activities?)

PECB

114

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.

The structure of the organization may be of different types:

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

Notes:

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

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

Internal Context – Key Aspects

ISO/IEC 27000, clause 3.38

Internal environment in which the organization seeks to achieve its objectives

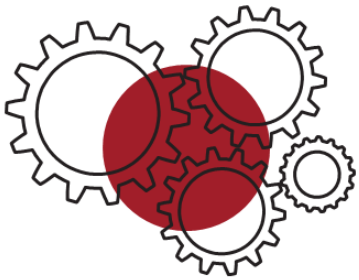
Note 1 to entry: Internal context can include:

- *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.*

1.1.6 Identify the Key Processes and Activities

Assets

What are the key assets of the organization?



Organization's activities

What are the goods and services produced by the organization?

Business processes

What are the key processes that enable the organization to achieve its mission?

NOT

At this stage, there is no need to completely map out the processes, only to establish a general list.

PECB

116

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

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

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

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

Identification of Infrastructure

Category	Definition	Examples
Hardware	Physical components that support the process	Server, laptop, printer, CD-ROM, etc.
Software	Programs that contribute to data processing	Operating system, word processer, accounting software, etc.
Networks	Telecommunications equipment used to physically connect the elements in an information system	Router, firewall, network cable, switch, bridge, etc.
Sites	Physical locations where operations take place	Office, server room, employees residence, secure area, air conditioning system, etc.
Third party supplier	Organization that provides a product not supplied by the main organization	Telephone company, marketing agency, etc.

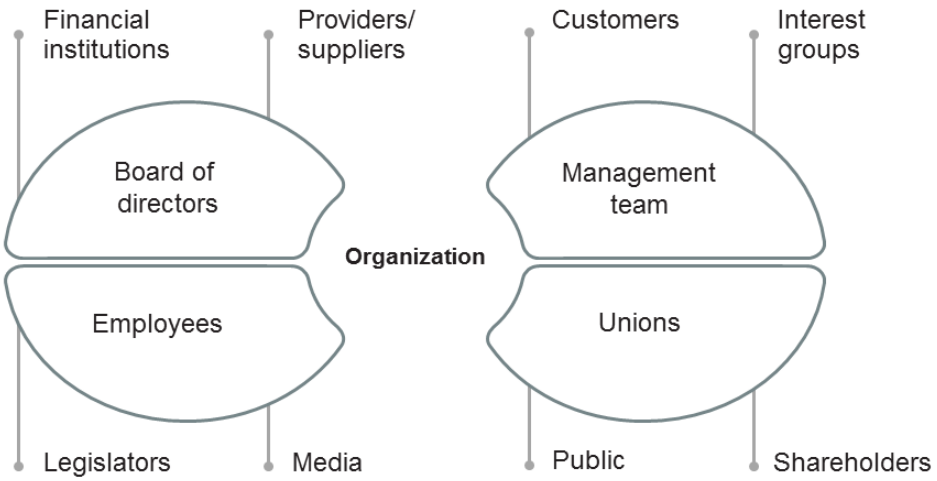
PECB

117

Despite the fact that ISO/IEC 27001 is concerned with protecting all information assets, the ISMS project manager must understand the process and IT infrastructure of the organization because these processes play a vital part in the processing, transfer, and maintenance of organizational information.

In ISO/IEC 27005, the IT infrastructures belong to the category of the supporting assets. In Annex B.1.3., the sub-categories are defined for each asset category with examples. During the second day of this training, we will cover the identification and analysis of risks related to the assets in more detail.

1.2.7 Identify and Analyze the Interested Parties



Note: The term "interested party" is synonymous with the term "stakeholder." Therefore, these terms are used interchangeably.

PECB

118

ISO/IEC 27001 often raises the topic of the interested parties, which, in this context, denotes both the internal and external interested parties of the organization with interests in the process of information security management.

ISO/IEC 27001 also stipulates that the ISMS is intended to ensure the selection of appropriate and proportional security controls to protect the assets and give confidence to interested parties.

Note on terminology: ISO/IEC 27005 also uses the term "stakeholders" without classification. Some experts define stakeholders as a sub-category of the interested parties. Stakeholders are those who take direct action in relation with the ISMS (such as employees, customers, or suppliers). The media or legislators would only be interested parties because they do not generally work directly in relation to the ISMS.

Definitions

ISO 9000, clause 3.2.3 Interested party

Stakeholder

Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

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

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

ISO 9000, clause 3.2.4 Customer

Person or organization that could or does receive a product or a service that is intended for or required by this person or organization

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

Note 1 to entry: A customer can be internal or external to the organization.

Slide Notes Extension

PECB

119

ISO 9000, clause 3.2.5 Provider

Supplier

Organization that provides a product or a service

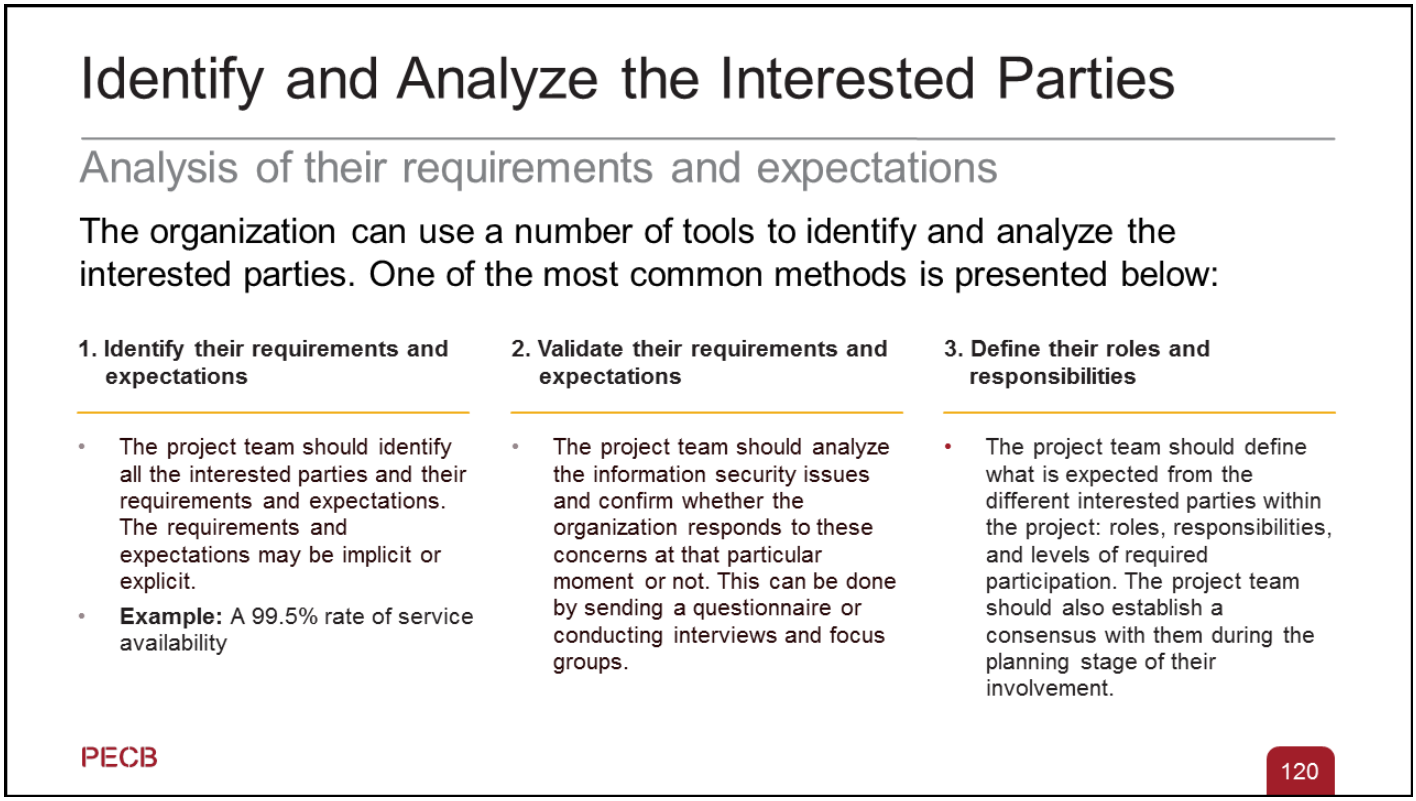
EXAMPLE Producer, distributor, retailer or vendor of a product or a service.

Note 1 to entry: A provider can be internal or external to the organization.

Note 2 to entry: In a contractual situation, a provider is sometimes called "contractor".

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

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

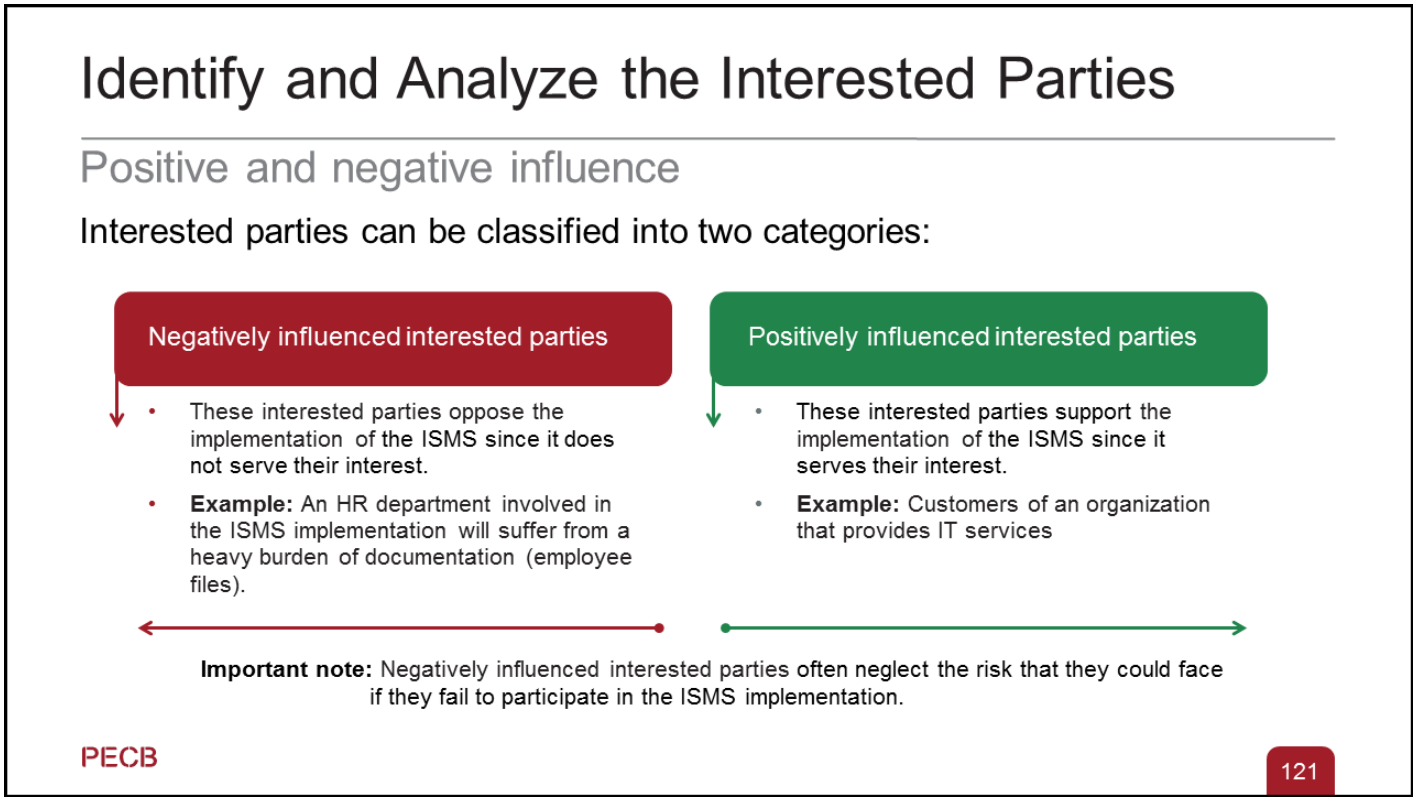


The organization must dedicate a considerable amount of time in the project to support the interested parties in their assigned tasks (answering questions, consolidating reports, presenting project progress, etc.).

William C. Frederick, James E. Post, and Keith Davis state in their book Business and Society: Corporate Strategy, Public Policy, Ethics that there are six stages to conducting an interested parties analysis, as follows:

- Map interested parties relations
- Map interested parties coalitions
- Assess the nature of each interested party's interest
- Assess the nature of each interested party's power
- Construct a matrix of interested parties priorities
- Monitor shifting coalitions

Important 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.



Negative interested parties impede the smooth running of the project.

For example, the head of a department in charge of managing users' access rights would not be pleased to see that additional security controls are being established, because they could undermine their team's effectiveness to grant access rights on time or because it might cause their team to work overtime.

Strategy: Contact the interested parties about the objectives, highlight the best interests for them and the organization, compromise or neutralize their influence as a measure of last resort

Positive interested parties help in the implementation of the ISMS.

For example, the CIO of an organization might consider that ISMS will bring new dimensions of action to the management team, which will facilitate the assessment of security incidents. Thus, it is perceived that this may positively improve the reporting to the management.

Strategy: Active involvement as an interested party

Slide Notes Extension

PECB

122

Other examples for positive interested parties:

- The CFO thinks that the ISMS is a useful instrument for assessing the value (even relative) of intangible assets of the organization.
- The quality manager is motivated by the fact that complying with ISO/IEC 27001 will help reactivate the quality management process that has been somewhat neglected since the last ISO 9001 certification. Combining both standards also seems to be a good strategy to develop internally effective economic practices.
- The organization's customers perceive compliance to ISO/IEC 27001 as a better guarantee that their personal data will be more effectively protected by the supplier.

Other examples for negative interested parties:

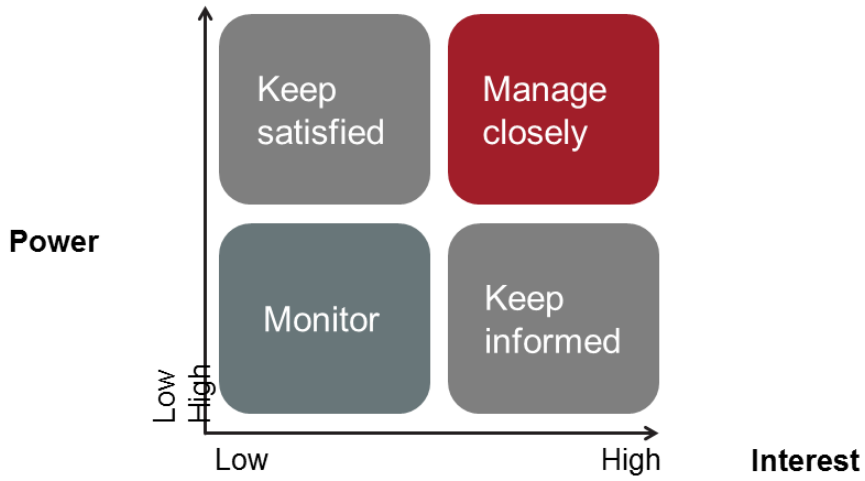
- The HR manager sees the ISMS as a vector with a certain heaviness and impact on the effective functioning of their department.
- The head of physical security (managed by an external organization) identifies the ISMS as a disruptive element in their role, because the ISMS system distributes the roles and responsibilities to a larger number of people; thus, they perceive that their contribution will not be as substantial as it used to be.

One possible way to deal with negative attitudes in relation to the establishment of the ISMS may be to assign an "ISMS champion." This person, usually a member of the leading team, or a person with considerably high responsibilities in the organization, could be the leader of the ISMS project and guarantee its success.

This person should embody the will of the management to lead the implementation of the system. As such, they have full power and authority to support and help finalize the project. In contrast to the role of the protector, we sometimes develop a kind of "anti-champion" or "negative leader," who symbolizes the conflicting interests to realize the project, for whatever reasons. The role of the champion is, therefore, quite useful to counter hostile actions against the project that could come from negative interested parties represented by one or more leaders.

Identify and Analyze the Interested Parties

Power/interest matrix



PECB

123

The Power/Interest matrix, developed by Johnson and Scholes, is a tool that assists in determining and managing the interested parties. This matrix shows the relationship between two significant variables (interest and power). On the one hand, the interest variable shows the interest of the interested parties in the organization's decisions and activities whereas, 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 map the different interested parties in the matrix depending on priority:

- 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/Interest
- Setting priorities and objectives and thus reducing the risk of not meeting their needs and expectations

Slide Notes Extension

PECB

124

ISO/IEC 27001 and Regulatory Frameworks

Examples

United States:

- **Federal Information Security Management Act (2002):** FISMA (legislation on information security management) imposes a series of processes that must be followed for any information system used by the American Federal Government, its contractors, or suppliers.
- **NIST 800-53:** NIST 800-53 (National Institute for Standards and Technology) provides guidelines to secure information systems within the federal government by choosing and specifying security controls. These guidelines apply to every part of an information system that processes, stores, or transmits federal information. It is issued by the U.S. Department of Commerce.

Note that NIST 800-53 includes a “crosswalk” between its controls and those in ISO/IEX 27001 Annex A.

Europe:

- **General Data Protection Regulation—GDPR:** This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- **Regulation (EC) n°45/2001:** Regulation concerning the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The text includes provisions that guarantee a high level of protection of personal data processed by the community institutions and bodies. It also provides for the establishment of an independent supervisory body to monitor the application of these provisions.

International and industry repositories:

- **OECD Principles (2002):** OECD (Organization for Economic Cooperation and Development) has developed guidelines regulating the security of information systems and networks based on nine principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment.
- **COBIT (1994+):** Developed by the ISACA and the ITGI, CobiT (Control Objectives for Business and

related Technology) is a reference frame to manage the governance of information systems. CobiT provides information technology managers, auditors, and users with indicators, processes, and best practices to help them maximize advantages stemming from the information technologies recourse and the elaboration of the governance and the control of an organization.

Exercise 3: Establishing the ISMS context

While proud of their rapid growth rate, the executives of e-Scooter are, nevertheless, concerned about control and security aspects. Their concerns grew after the occurrence of a few security incidents recently. Knowing you and your expertise on information security, *e-Scooter* has decided to trust you with the assignment of assisting them with the implementation of an ISMS and the preparation for an ISO/IEC 27001 certification.

The first step of your assignment is to establish the context of the ISMS within the company. To *e-Scooter*, this task seems to require a person specialized in the respective field. They see that in you and want you to propose a version that they plan to approve later. To achieve this, use the information contained in the case study to identify two potential sources of compliance requirements for the company that you consider to be most important. In addition, identify the company's two most critical information assets and business processes.

Duration of the exercise: 30 minutes

Comments: 15 minutes

1.Why is it important to understand the mission, objectives, values, and strategies of an organization?

A. To facilitate the internal audit process
B. To create a map of all the processes
C. To understand the information security challenges the organization faces

2.Which of the options below represents an ISMS objective?

A. Integration of new technologies
B. Protection of critical assets
C. Improvement of the information security incidents

3.Which of the following statements is correct?

A. Standards take precedence over laws
B. The implementation of an ISO standard is not a legal requirement
C. Compliance with the ISO/IEC 27001 ensures compliance with data protection laws and regulations

4.Do outsourcing activities of an organization impact its ISMS?

A. No, because outsourcing activities should not be included in the ISMS scope
B. Yes, because outsourcing activities do not directly support the business activities
C. Yes, because outsourcing activities can affect the determination of the ISMS scope

5.What can be included when analyzing the internal environment of an organization?

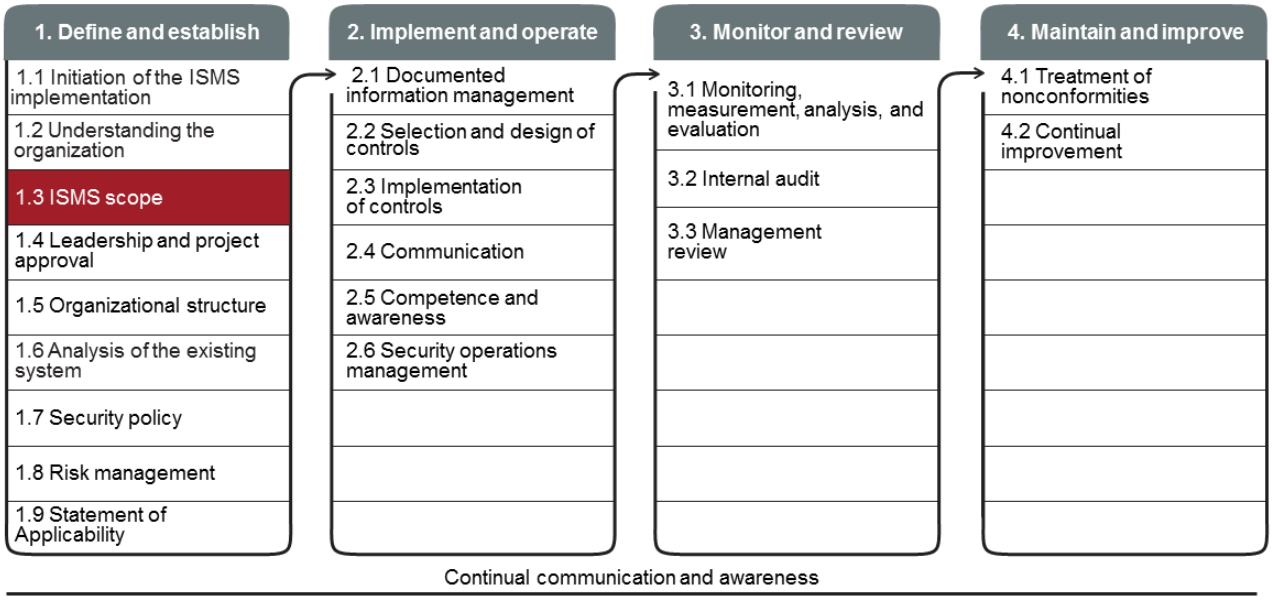
A. Information systems, information flow, and decision-making processes
B. Segregation of duties, responsibilities of the interested parties, and information systems
C. Trends having impact on the objectives of the organization

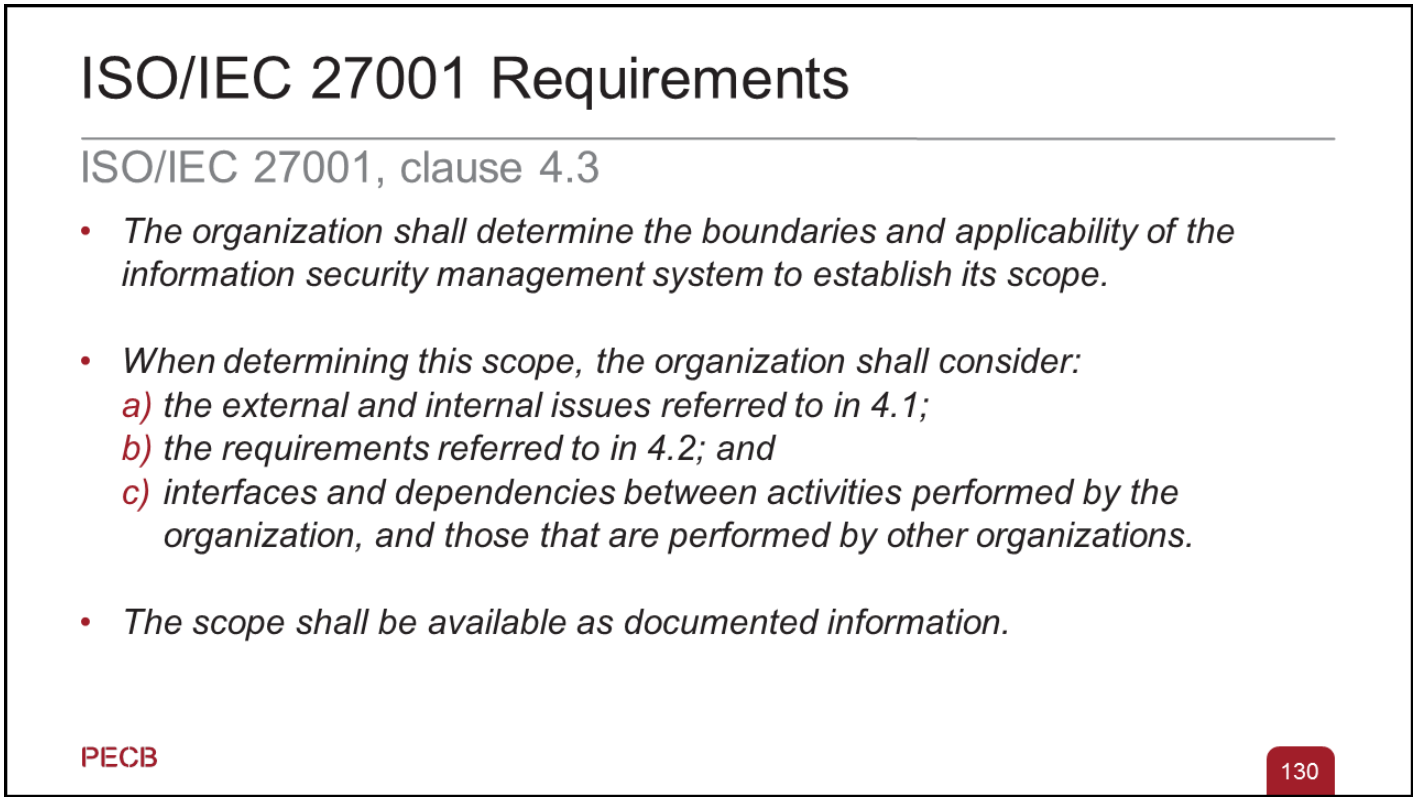
Section summary

- 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.
- In order to identify and analyze the interested parties, the organization uses a number of tools, such as identifying and validating their requirements and expectations, and defining their roles and responsibilities.
- The interested parties can be classified into two categories: negatively and positively influenced interested parties.
- The ISMS requirements for all organizations derive from four sources: laws and regulations, market, internal policies, and standards.
- The organization must adhere to the appropriate laws and regulations.

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.

1.3 Scope





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

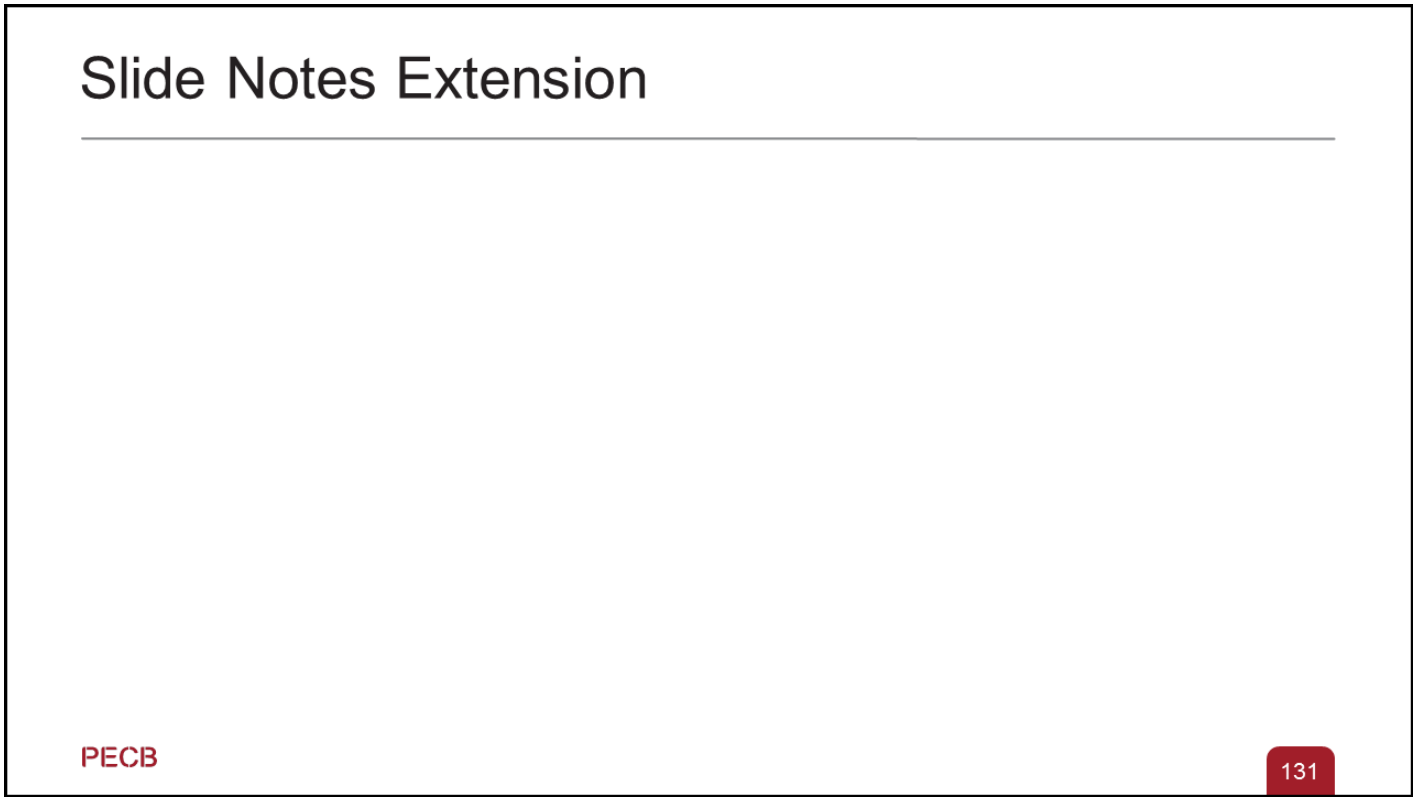
1. Document the ISMS scope
2. Define the boundaries of the management system
3. Justify and document exclusions

Note: We will, when discussing Annex A and Statement of Applicability, see some controls that can be excluded although not all of them can.

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

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

- *one or more specific processes;*
- *one or more specific functions;*
- *one or more specific services;*
- *one or more specific sections or locations;*
- *an entire legal entity; and*
- *an entire administrative entity and one or more of its suppliers.*

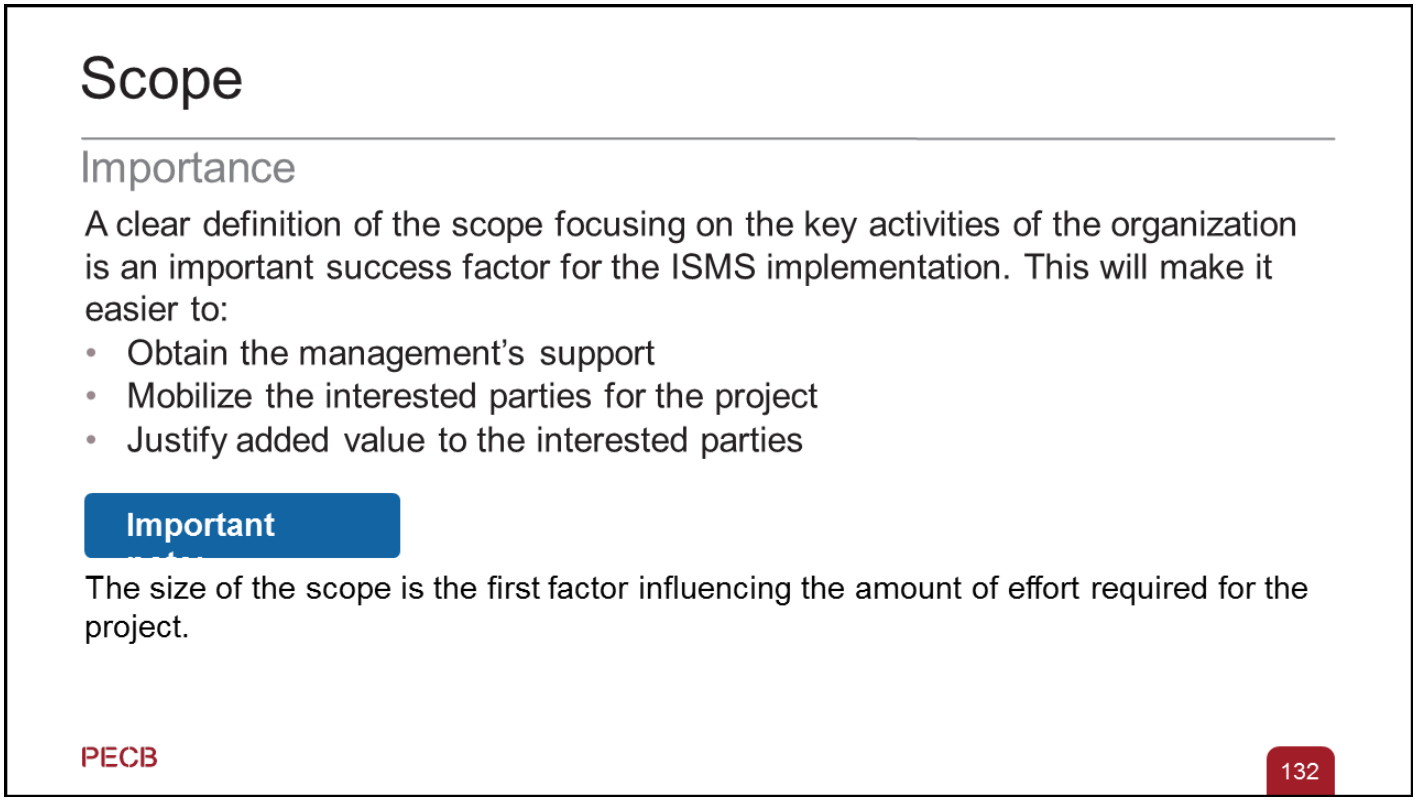


ISO/IEC 27003, clause 4.3 Determining the scope of the information security management system (cont'd)

Guidance

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

f)*determine the preliminary scope: this activity should be conducted by a small, but representative group of management representatives;*
g)*determine the refined scope: the functional units within and outside the preliminary scope should be reviewed, possibly followed by inclusion or exclusion of some of these functional units to reduce the number of interfaces along the boundaries. When refining the preliminary scope, all support functions should be considered that are necessary to support the business activities included in the scope;*
h)*determine the final scope: the refined scope should be evaluated by all management within the refined scope. If necessary, it should be adjusted and then precisely described; and*
i)*approval of the scope: the documented information describing the scope should be formally approved by top management.*



By defining a scope, which is a continuation of the mission of the organization, it is easier to obtain management support and interested parties commitment in the project.

Application areas which provide no value to the interested parties and do not match their expectations should be avoided. 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, the ISMS scope may cover the same area, partly overlapping the first system or be completely independent of it.

1.3 Scope

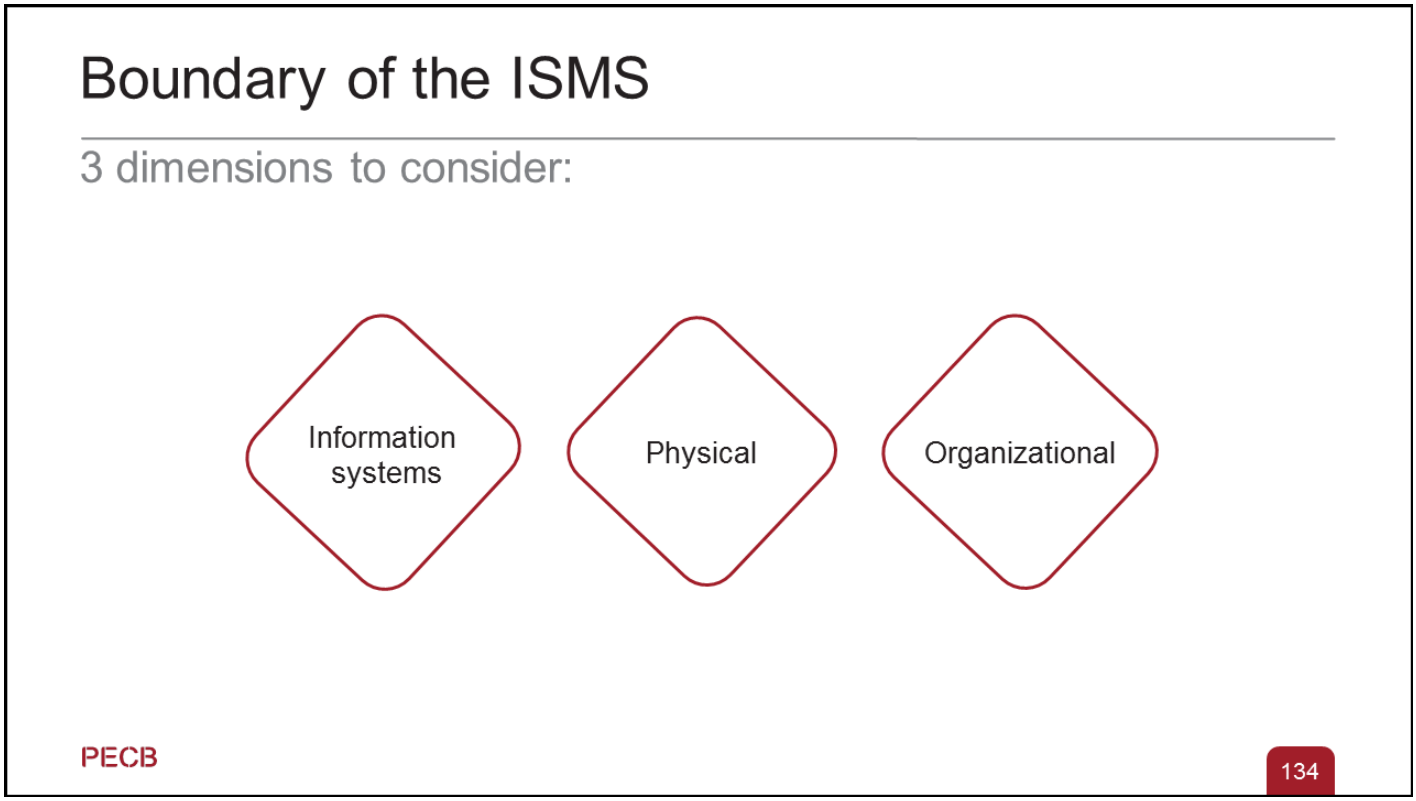
List of activities

1.3.1 Define the organizational boundaries of the scope

1.3.2 Define the information security boundaries

1.3.3 Define the physical boundaries

1.3.4 Define the ISMS scope



1.Information systems boundaries

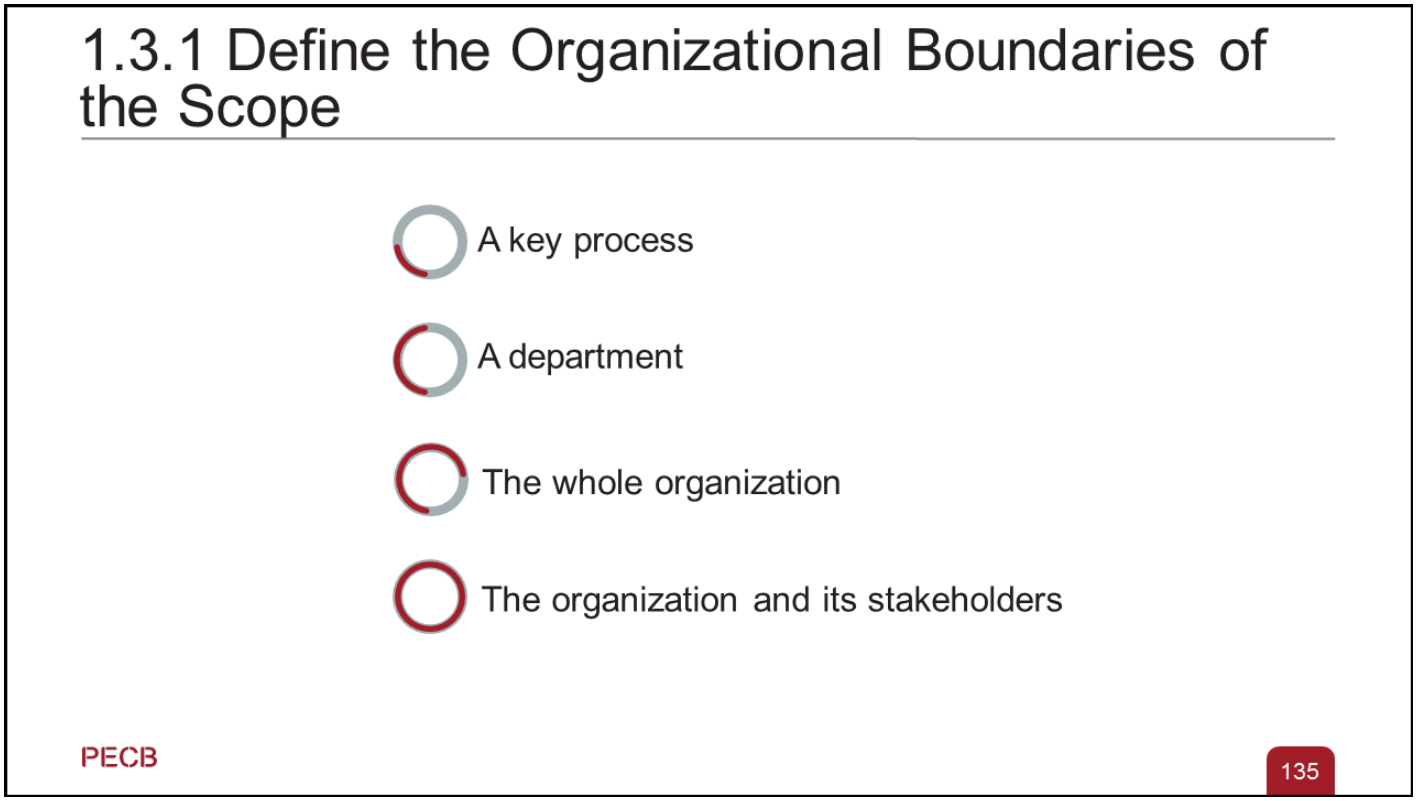
- The identification of information resources in an information system defines the security boundary for this system. The organizations have, in fact, a considerable flexibility in determining what constitutes an information system (for example, a major application or general support system). If a set of information resources is identified as an information system, these resources should generally be under the same direct management authority. Complex information systems may contain multiple subsystems, each with their own boundaries. **Note:** The information resources consist of information they contain and the associated resources, such as personnel, equipment, budget, and dedicated information technology used in support of the resource.

2.Physical boundaries

- 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.

3.Organizational boundaries

- 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.



The following have to be considered:

1. Organizational units: department, service project, subsidiary, etc.
2. Organizational structures and responsibilities of managers
3. Business process: sales management, procurement process, hiring, etc.

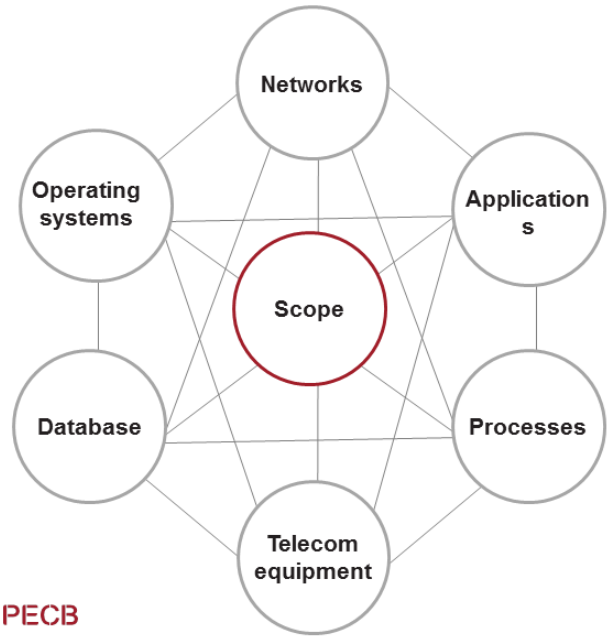
One efficient method for determining organizational boundaries is to evaluate decision-makers' responsibilities and their areas of influence within the organization. For instance, an organization is planning to implement an ISMS in its finance department; by analyzing key processes and services that fall under the CFO, 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 create 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.

1.3.2 Define the Information Security Boundaries



- All system components are to be taken into account; the focus is not to be limited to hardware components only.
- **Note:** In theory, the lack of technical infrastructure does not prevent an organization from obtaining an ISO/IEC 27001 certification.

PECB

136

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.

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, software management payroll, ERP, utilities, database
4. Data: customer records, medical data, research and development, etc.
5. Processes: Consider processes that transport, store, or process information
6. Telecommunications 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 (Customer Relationship Management) 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. This insurance could take the form of, for example, a contractual agreement.

Note: In theory, an ISMS without technical infrastructure can be ISO/IEC 27001-certified, because the standard is concerned about the information security and not about computer systems. One could cite the example of an archive that has no (or almost no) technology installed.

1.3.3 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 within part of the scope and the physical means required for them to work.
- In the case of outsourced physical sites, the interfaces with the ISMS and the applicable service agreements have to be considered.

PECB

137

It is important to consider the interfaces with the ISMS and the applicable service agreement in the case of outsourced physical sites. For instance, if a data processing center is outsourced, the organization must consider the geographic location where the center is located, even if they are not the owner.

1.3.4 Define the ISMS Scope

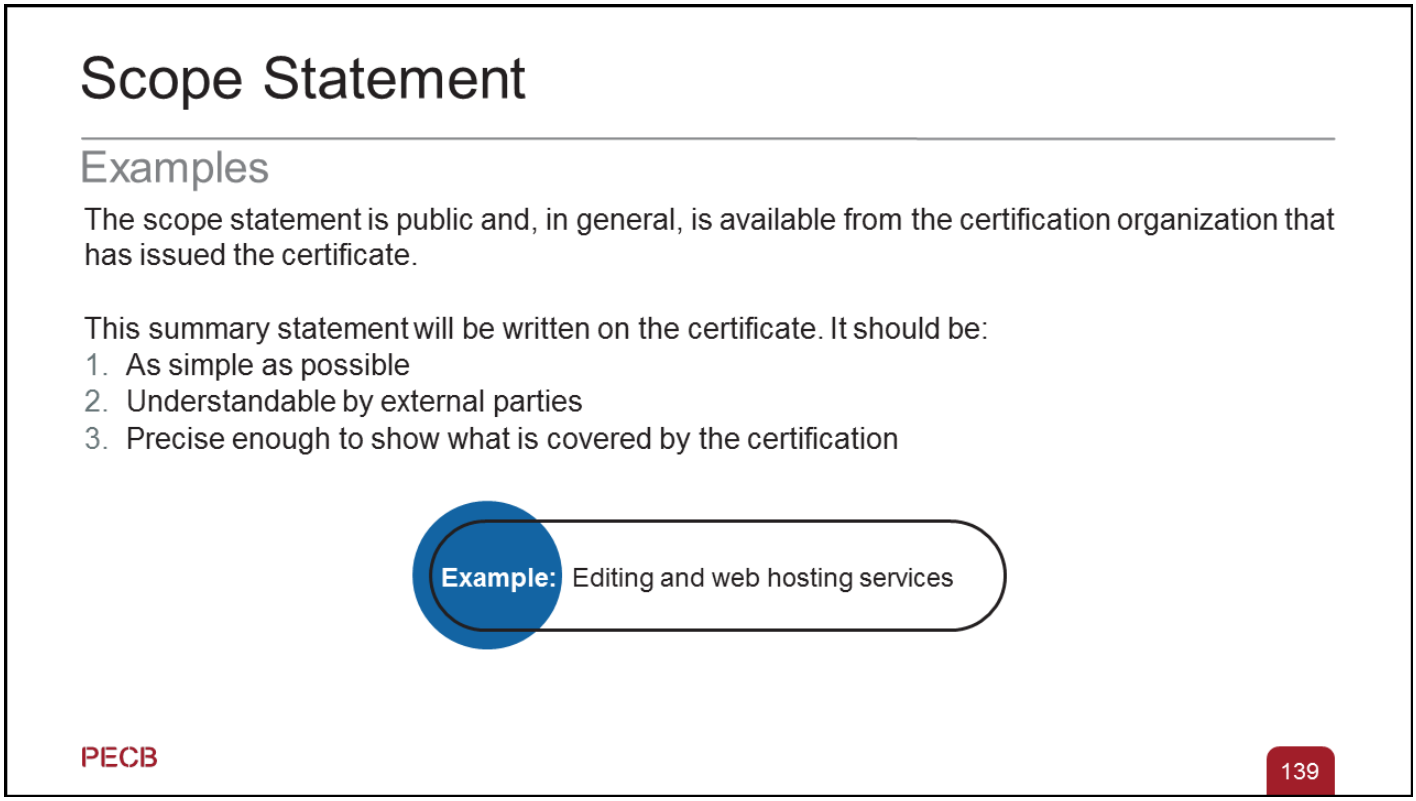
The scope should include:

1. Key characteristics of the organization
2. Organizational processes
3. Descriptions of the roles and responsibilities related to the ISMS
4. List of information assets
5. List of information systems
6. Maps of geographic locations
7. Details and reasons for exclusions

PECB

138

After having the boundaries defined, the different components of the scope should be integrated and documented.



Some examples are:

2e2 IOM Ltd (UK): The provision and installation of IT hardware, software and cabling services, including consultation, training, support, maintenance, and disaster recovery facilities for the Isle of Man Government in accordance with the latest version of the Statement of Applicability.

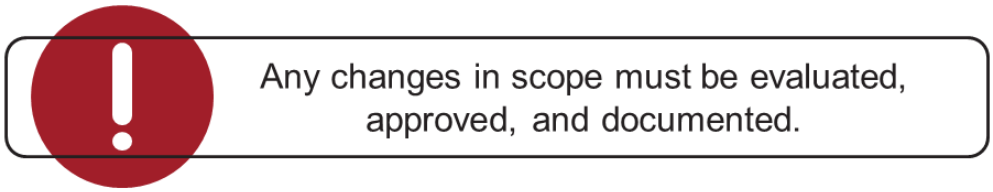
AAD Co., Ltd (Japan): Printing and planning, producing and designing related thereof. Planning for websites and implementation thereof. Statement of Applicability, issued on 19/Jul/2011, Version 3 Other location(s): Kawaguchi Plant.

Citigroup Technology Infrastructure's (USA): This ISMS applies to Citigroup Technology Infrastructure's (CTI's) Global Information Security (GIS) group. GIS is responsible for the provision of information security programs for CTI that meets all of the relevant information security controls, policies, and practices that govern Citigroup business, as they relate to technology infrastructure and operational risk management in the infrastructure environment. This is in accordance with the Statement of Applicability, version 2.4, dated 2017/08/03.

Microsoft, Global Foundation Services Division (USA): The management of information security for Microsoft Global Foundation Services Infrastructure encompassing data centers listed in this report (Seattle, Quincy, San Antonio, Tokyo, Singapore, etc.) and specific teams comprised of Online Services Security and Compliance, Data Center Services, Global Networking Services, Data Center Software Services, OpsCenter Service Desk, Operations Systems Support Group, and Asset Management and Deployment, in accordance with Microsoft GFS ISMS Statement of Applicability, dated 5/15/2017.

CIIC HR Management Consulting Co., Ltd. (China): Provision of Network Teaching Service And The Related Facilities And Infrastructure For Above Services. This Is In Accordance With The Latest Version Statement of Applicability.

Change in Scope



PECB

140

It is common that the scope can change over time in order for the ISMS to continue to allow the organization to achieve their information security goals. The change request can be caused by, among others, the following:

- Extension of the scope to other units of the organization
- Changes in the external environment (legal, competitive, technological)
- Consideration of new risk scenarios

The change request should be made through a pre-defined process that will usually require filing the change request. Any change request should be justified and accepted by the ISMS steering committee at a management review.

In case of an important change, an analysis of the impacts of the change on the ISMS should be conducted before final acceptance. Indeed, a change may result in the need for a risk reassessment and implementing new security controls that were not foreseen in the initial ISMS.

Furthermore, special attention should be paid to changes in scope, since a change to it may invalidate any certification which is reliant upon the terms of the scope statement. Care is therefore necessary in drafting a scope statement in the first place.

Extension of the Scope

- There are cases when organizations prefer to define a reduced scope of certification and apply for an extension in the upcoming years.
- If the extension is not granted, the organization does not lose its current certificate.

PECB

141

ISO/IEC 17021-1, clause 9.6.4.1 Expanding scope

The certification body shall, in response to an application for expanding the scope of a certification already granted, undertake a review of the application and determine any audit activities necessary to decide whether or not the extension may be granted. This may be conducted in conjunction with a surveillance audit.

Exercise 4: Definition of the scope

Referring to the context of the information security management system within the company from Exercise 3 and the case study, provide a scope for the company's ISMS and determine its boundaries. The management wishes to choose a scope that will be perceived as having an added value to its customers and, at the same time, delimit it as much as possible for the initial certification of the ISMS.

Duration of the exercise: 20 minutes

Comments: 15 minutes

1. **What should an organization do when establishing its ISMS scope?**
   A. Determine the amount of effort required for the ISMS implementation
   B. Determine the internal and external information security risks
   C. Determine the boundaries and applicability of the ISMS
2. **Which of the following is considered an ISMS boundary?**
   A. Information systems boundaries
   B. Critical assets boundaries
   C. Information security incident boundaries
3. **In which of the ISMS boundaries below should the evaluation of the responsibilities of decision-makers and their areas of influence in the organization be done?**
   A. Organizational
   B. Physical
   C. Information systems
4. **Which of the following is included in the ISMS scope?**
   A. The description of the changes in the external environment
   B. The description of the information security risks related to the ISMS
   C. The description of the roles and responsibilities related to the ISMS
5. **Which of the following statements regarding the ISMS scope is correct?**
   A. The ISMS scope should be categorized as confidential information
   B. The ISMS scope should not consider the information systems
   C. The ISMS scope should be available as documented information
6. **When can an organization make a change in the ISMS scope?**
   A. When the organization is applying for certification
   B. When new risk scenarios are to be considered
   C. When the list of information assets has been modified

Section summary

- A clear definition of the scope is an important success factor for the ISMS implementation.
- There are three boundaries of an ISMS that should be considered: physical boundaries, organizational boundaries, and boundaries of information systems.
- The scope should include: key characteristics of the organization, organizational processes, description of the roles and responsibilities related to the ISMS, list of information assets and systems, and more.

YoMedia is a marketing agency that primarily collects and analyzes customer and business data for targeted advertising campaigns. This is done to keep the data complete and accurate. Recently, *YoMedia* has decided to implement an information security management system (ISMS) to better protect its confidential information. The team assigned to implement the ISMS dedicated their time and resources to analyze the existing system by conducting interviews with the employees of the company and using various techniques to gather information on the existing processes, procedures, policies, and controls. They found out that the company uses an access control software that allows only authorized users to access sensitive information. However, their software application and programs have a complicated user interface that causes a lot of data input errors by the personnel on a daily basis. While conducting interviews, they learned that there were at least two employees of each department who did not receive any security trainings in the last two years. The team assigned to implement the ISMS concluded that the company should redefine the training needs and simplify its user interface.

Based on the above-mentioned scenario, answer the following questions:

1.*YoMedia* has implemented an access control software that allows only authorized users to access sensitive data. What is the purpose of this information security control?

A. To avoid or prevent errors or malicious acts
B. To detect the occurrence of errors or malicious acts
C. To correct the identified errors or malicious acts and prevent their recurrence

2.What controls should the company implement to ensure that the information is complete and accurate?

A. Data encryption controls
B. Data integrity controls
C. Backup and recovery controls

3.Which of the situations presented in the scenario is considered a threat?

A. The data input error by the personnel
B. The complicated user interface
C. The use of programs or applications by personnel on a daily basis

4.By analyzing the existing system and conducting interviews with the employees, *YoMedia* conducted a:

A. Risk management process
B. Security control designation
C. Gap analysis process

5.What does the fact that at least two employees of each department in *YoMedia* did not receive any security trainings in the last two years indicate?

A. The presence of a threat that is related to the possible functions of the company
B. The presence of an information security risk expressed as the combination of the impact and occurrence of an incident in the company
C. The presence of a vulnerability in the existing personnel procedures of the company

Slide Notes Extension

PECB

147

Summary of Day 1

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

- Definition of the ISMS and its importance
- Overview of the ISO/IEC 27001 clauses and Annex A
- Fundamental concepts and principles of information security
- Confidentiality, integrity, and availability
- Vulnerability, threat, and impact
- Information security risk
- Security objectives and controls
- Classification of security controls
- Approach to the ISMS implementation
- Mission, objectives, values, and strategies of the organization
- ISMS scope statement
- Boundary of ISMS
- Information security and physical boundaries

Blank Page for Note Taking

Blank Page for Note Taking