Version 7.1

Document number: ISMSLID3V7.1

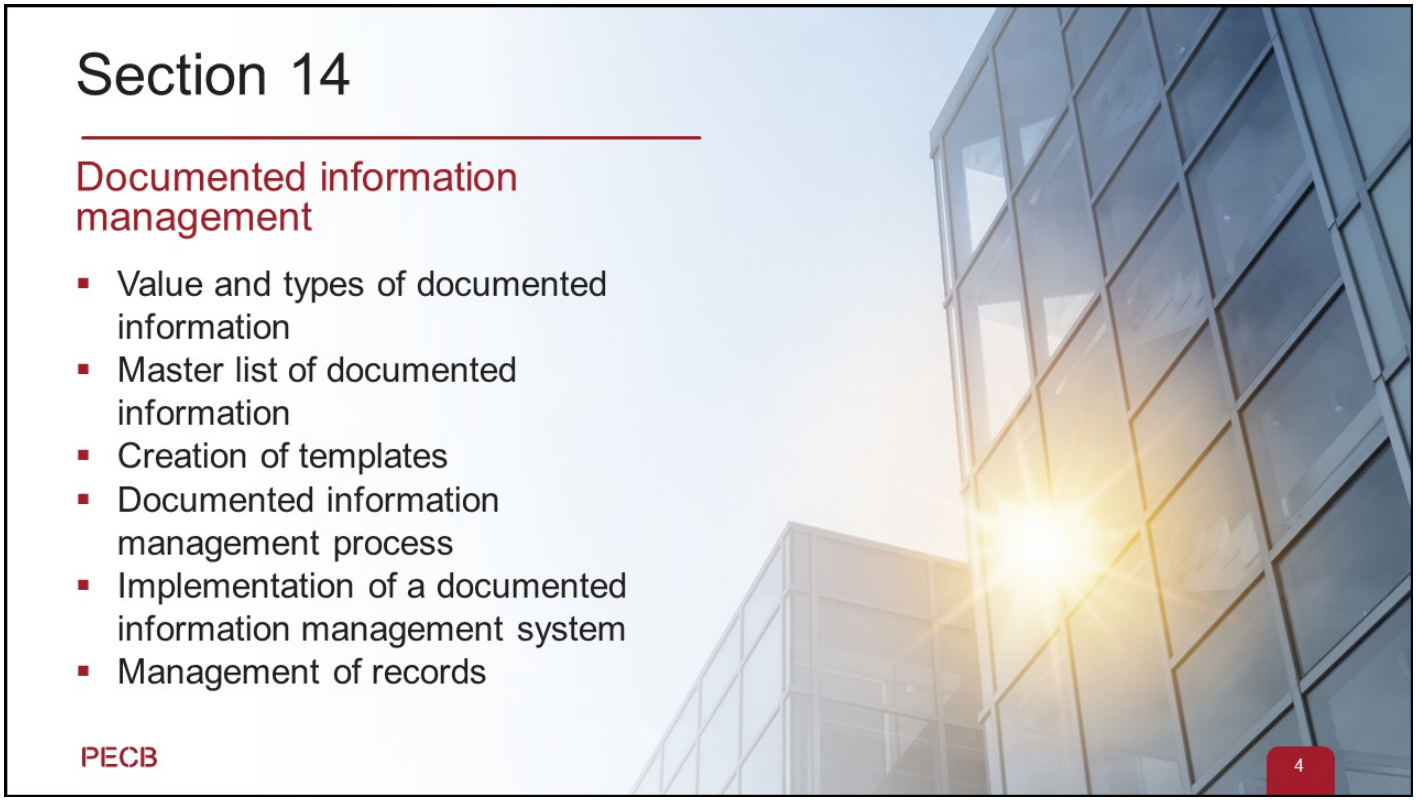
Schedule of the Day

- 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

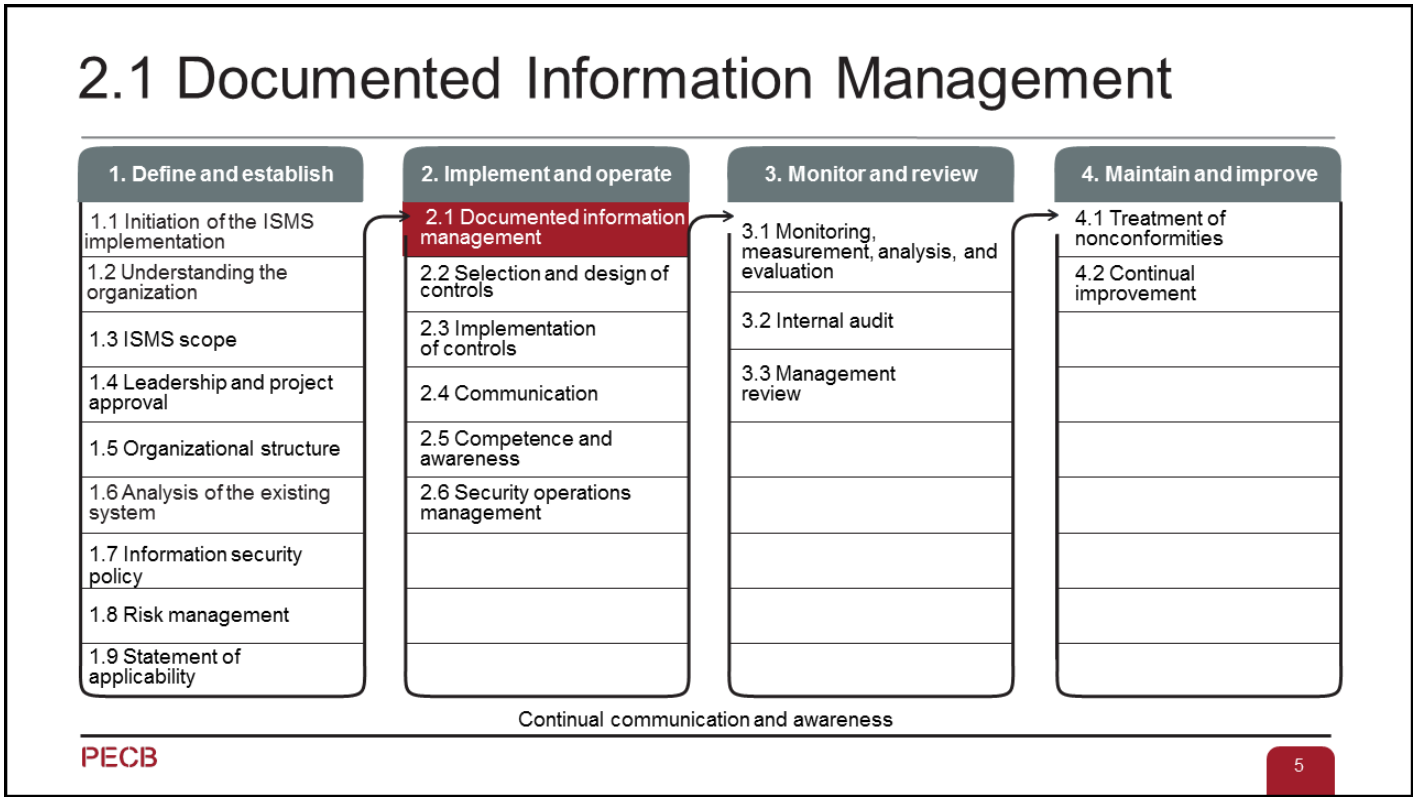
PECB

Learning Objectives of the Day

1. Acquire knowledge on how to design and describe processes and controls
2. Acquire knowledge on how to draft policies and procedures
3. Acquire knowledge on how to develop and implement the documented information management process
4. Acquire knowledge on how to design, plan, and provide the training program
5. Acquire knowledge on how to plan the operations management
6. Acquire knowledge on how to create an incident management policy, and measure and review the incident management process



This section provides information that will help the participants gain knowledge on the documented information management process, including the value and types of documented information, the creation of templates, the management of documented information and records, the implementation of a documented information management system, and the master list of documented information.



This step will help the organization develop and maintain the necessary documented information to ensure an effective management system, tailored to the specific needs of the organization. It will also ensure control and adequacy of the ISMS-documented information and records.

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.5.1

The organization's information security management system shall include:

a) documented information required by this International Standard; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

PECB

6

It is important that the entire ISMS documented information is coherent and complete. In addition, the documented information is crucial in demonstrating that the organization's security controls are implemented based on risk scenarios identified in the risk assessment.

The sufficiency and appropriateness of the documented information in the context of the organization should be determined with reasonable judgment and based on the perception of the situation.

Slide Notes Extension

PECB

7

ISO/IEC 27003, clause 7.5.1 General

Explanation

Documented information is needed to define and communicate information security objectives, policy, guidelines, instructions, controls, processes, procedures, and what persons or groups of people are expected to do and how they are expected to behave. Documented information is also needed for audits of the ISMS and to maintain a stable ISMS when persons in key roles change. Further, documented information is needed for recording actions, decisions and outcome(s) of ISMS processes and information security controls.

Guidance

Examples of documented information that can be determined by the organization to be necessary for ensuring effectiveness of its ISMS are:

- *the results of the context establishment;*
- *the roles, responsibilities and authorities;*
- *reports of the different phases of the risk management;*
- *resources determined and provided;*
- *the expected competence;*
- *plans and results of awareness activities;*
- *plans and results of communication activities;*
- *documented information of external origin that is necessary for the ISMS;*
- *process to control documented information;*
- *policies, rules and directives for directing and operating information security activities;*
- *processes and procedures used to implement, maintain and improve the ISMS and the overall information security status;*
- *action plans; and*
- *evidence of the results of ISMS processes (e.g. incident management, access control, information security continuity, equipment maintenance, etc.).*

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.5.2

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

PECB

8

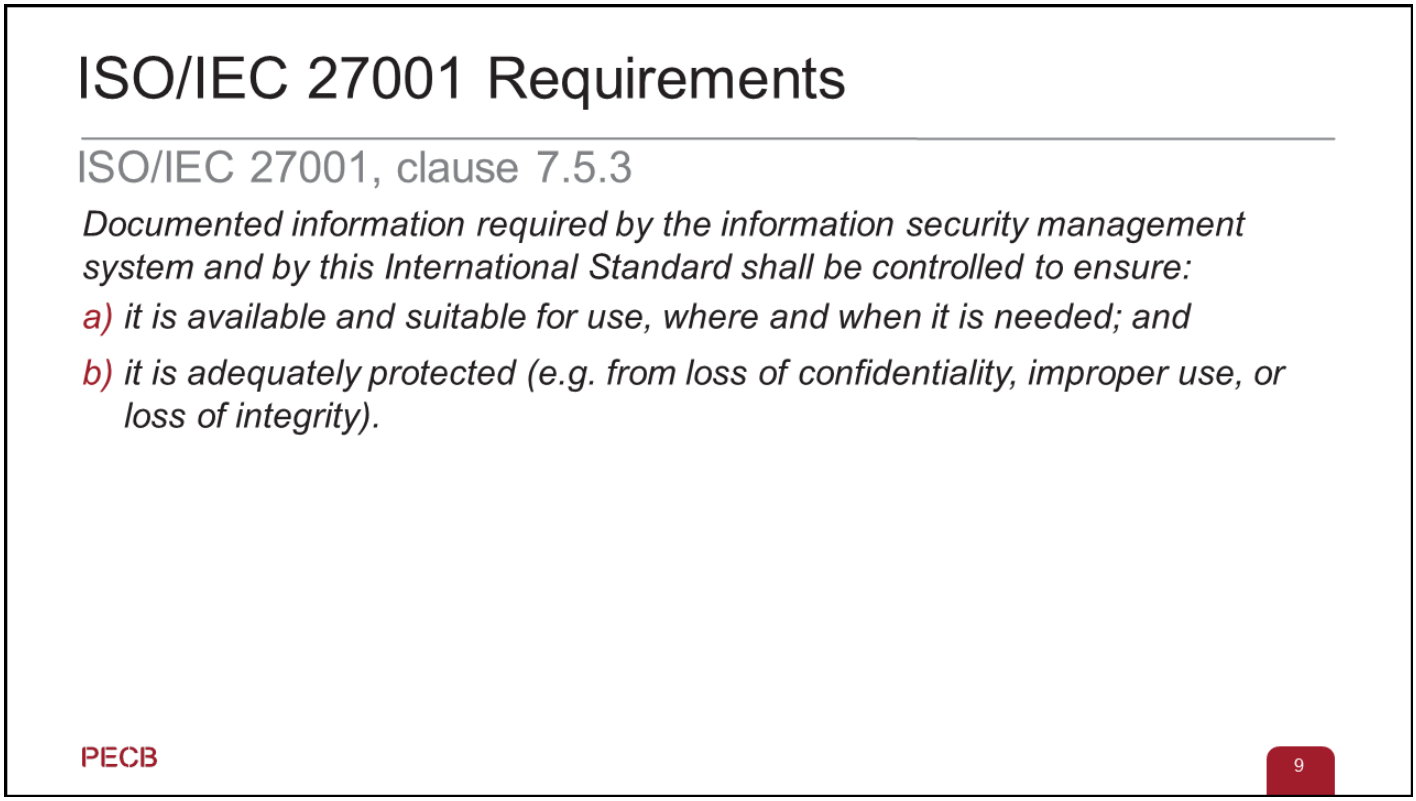
ISO/IEC 27003, clause 7.5.2 Creating and updating

Guidance

Documented information may be retained in any form, e.g. traditional documents (in both paper and electronic form), web pages, databases, computer logs, computer generated reports, audio and video. Moreover, documented information may consist of specifications of intent (e.g. the information security policy) or records of performance (e.g. the results of an audit) or a mixture of both. The following guidance applies directly to traditional documents and should be interpreted appropriately when applied to other forms of documented information.

Organizations should create a structured documented information library, linking different parts of documented information by:

a. *determining the structure of the documented information framework;*
b. *determining the standard structure of the documented information;*
c. *providing templates for different types of documented information;*
d. *determining the responsibilities for preparing, approving, publishing and managing the documented information; and*
e. *determining and documenting the revision and approval process to ensure continual suitability and adequacy.*



The control of documented information is ensured through effective management of the records' life cycle from creation to destruction.

ISO/IEC 27003, clause 7.5.3 Control of documented information

Guidance

A structured documented information library can be used to facilitate access to documented information.

All of the documented information should be classified in accordance with the organization's classification scheme. Documented information should be protected and handled in accordance with its classification level.

A change management process for documented information should ensure that only authorised persons have the right to change and distribute it as needed through appropriate and predefined means. Documented information should be protected to ensure it keeps its validity and authenticity.

Documented information should be distributed and made available to authorized interested parties. For this, the organization should establish who are the relevant interested parties for each documented information (or groups of documented information), and the means to use for distribution, access, retrieval and use (e.g. a web site with appropriate access control mechanisms). The distribution should comply with any requirements related to protecting and handling of classified information.

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.5.3

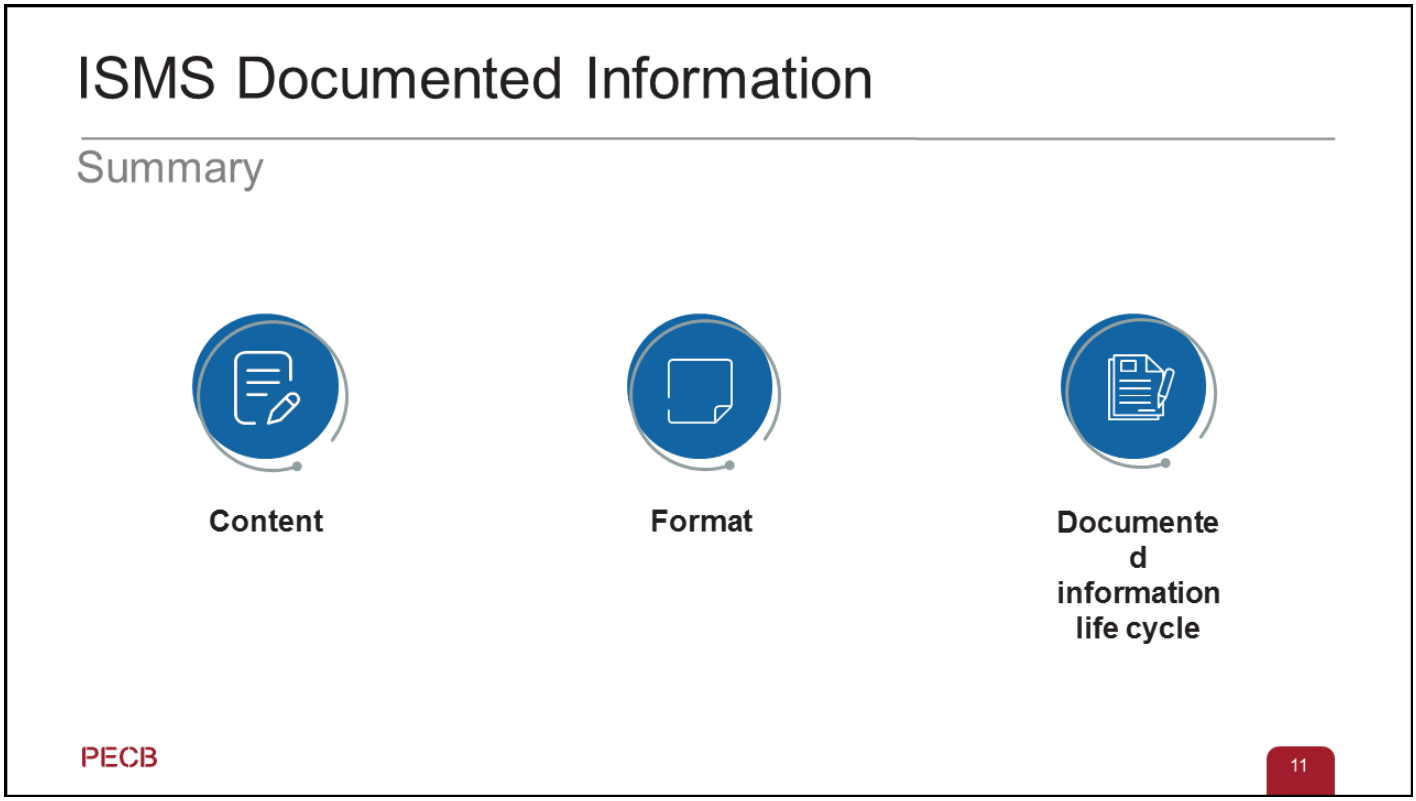
For the control of documented information, the organization shall address the following activities, as applicable:

c) *distribution, access, retrieval and use;*
d) *storage and preservation, including the preservation of legibility;*
e) *control of changes (e.g. version control); and*
f) *retention and disposition.*

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE

Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.



An organization wishing to conform to ISO/IEC 27001 shall:

1. Have and put to use all documented information required by ISO/IEC 27001
2. Develop a procedure for the control of documented information
3. Develop a procedure for the control of records

In summary, this means that the organization must approve its ISMS documented information to ensure conformity according to the three following criteria:

1. **Documented information content:** The organization must ensure that each document contains the information required by the related clause. However, **the document should contain only the minimum required,** not everything that could be added.
2. **Documented information format:** The organization must ensure that each document is consistent in format and includes author identification, production date, version number, approval date of the latest revision, etc.
3. **Documented information life cycle:** The organization must ensure that there is a document life cycle management that conforms to ISO/IEC 27001, clause 7.5.3.

Slide Notes Extension

PECB

12

Definitions related to documented information management

ISO 9000, clause 3.8.2 Information

Meaningful data

ISO 9000, clause 3.8.5 Document

Information and the medium on which it is contained

ISO 9000, clause 3.8.7 Specification

Document stating requirements

ISO 9000, clause 3.6.13 Traceability

Ability to trace the history, application or location of an object

ISO 9000, clause 3.8.10 Record

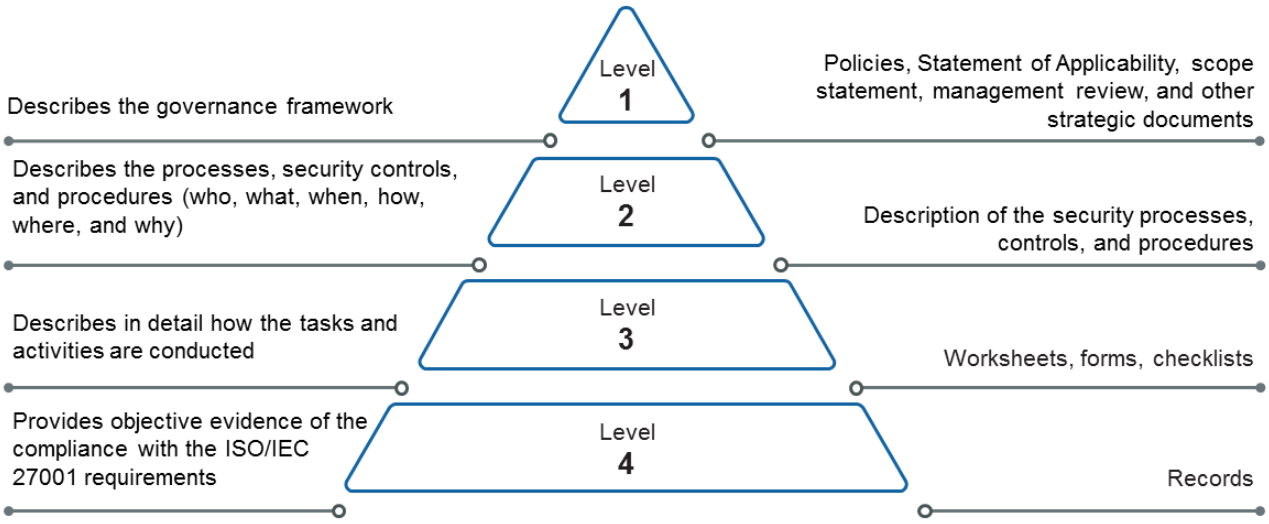
Document stating results achieved or providing evidence of activities performed

Notes on terminology:

1. A management system consists of several types of documents, such as policies, procedures, records, specifications, etc.
2. A document is the combination of information with its medium. The medium may be paper, magnetic disk (electronic or optical), photographs, or a combination of these.
3. A set of documents is commonly called documentation.

ISMS Documented Information

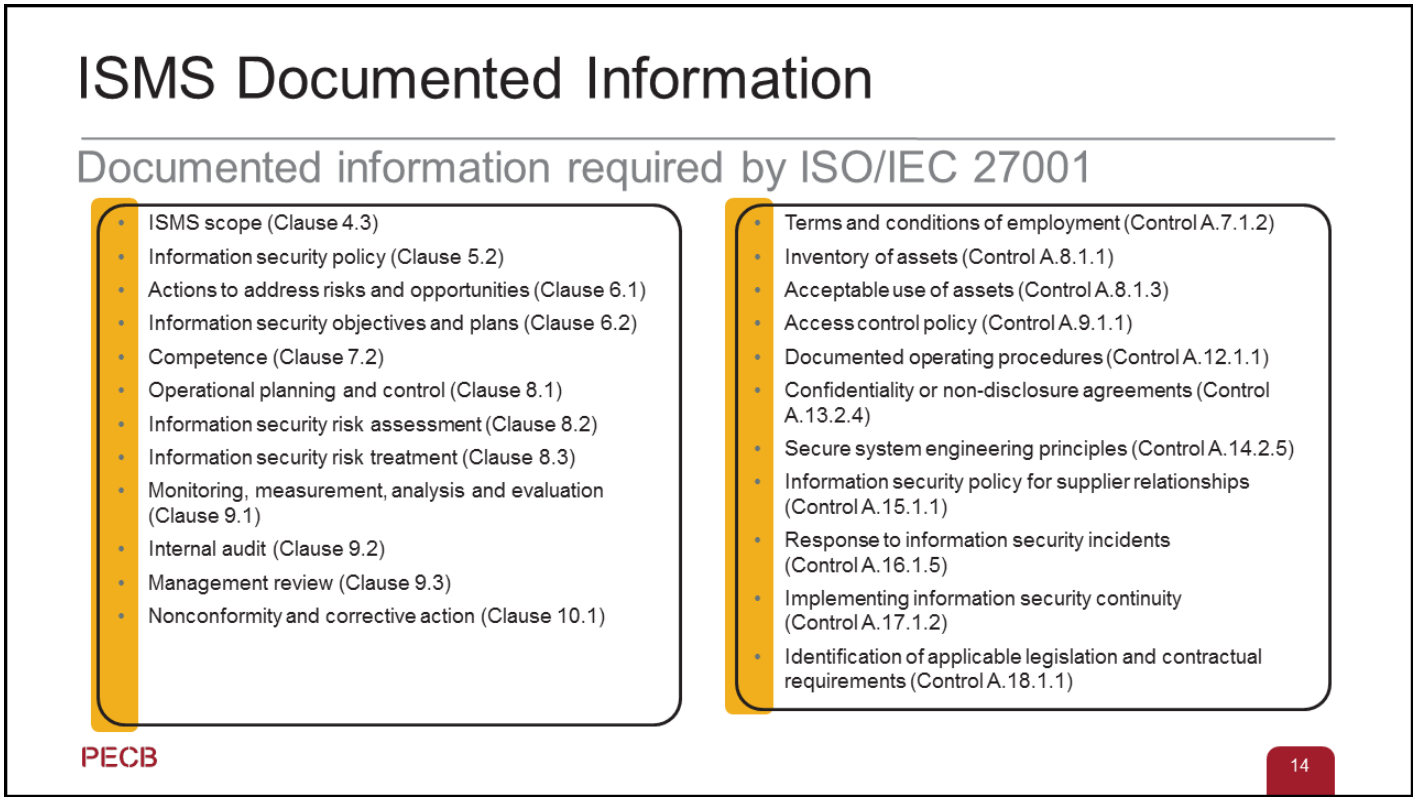
Types of documents



PECB

13

There is no mandatory requirement on how to document processes and security controls. This can be done using diagrams, textual descriptions, spreadsheets, etc.



The following documented information is implicitly required to demonstrate the conformity of the ISMS to the requirements of ISO/IEC 27001. The availability of these documents supports operations and helps ensure conformity during the certification audit.

1. Communication (Clause 7.4)
2. Procedure for document control (Clause 7.5)
3. Organizational roles, responsibilities, and authorities (Clause 5.3)
4. Leadership and commitment (Clause 5.1c)
5. Improvement (Clause 10)
6. Mobile devices and teleworking (Control A.6.2)
7. Information classification (Control A.8.2)
8. User access management (Control A.9.2)
9. Disposal of media (Control A.8.3.2)
10. Secure disposal or re-use of equipment (Control A.11.2.7)
11. Working in secure areas (Control A.11.1.5)
12. Clear desk and clear screen policy (Control A.11.2.9)
13. Change management (Control A.12.1.2)
14. Restrictions on changes to software packages (Control A.14.2.4)
15. Information backup (Control A.12.3.1)
16. Information transfer (Control A.13.2)
17. Information security continuity (Control A.17.1)
18. Redundancies (Control 17.2)

Vocabulary

Term	Explanation
Requirement	The terms **"shall"** and **"shall not"** indicate requirements that are to be strictly followed in order to conform to the standard and from which no deviation is permitted.
Recommendation	The terms **"should"** and **"should not"** indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.
Permission	The terms "**may**" and "**need no**" indicate a course of action permissible within the limits of the standard.
Possibility	The terms "**can**" and **"cannot"** indicate a possibility of something occurring.

PECB

15

During the implementation of a management system, particular attention should be given to the use of verbal expressions to indicate the nature of specific provisions.

The organization shall ensure that a requirement of a standard expressed by the use of the verb "shall" is strictly followed in the management system.

The organization can use recommendations in a form of a guideline that users **should** follow, rather than adopt them as requirements.

However, if a process or a control that is not a requirement of the standard is documented by the organization with the verb "shall," it becomes a requirement of the management system of the organization. Such an obligation may be imposed, e.g., by law, through a policy or by a contract. For example, if a procedure of the organization indicates that backups **shall** be checked every morning at 10:00 but the auditor finds during the audit that this is not followed, this presents a nonconformity. However, if the same procedure was written with the verb "should," there is no need to issue a nonconformity, because it would be seen as a guideline followed by the organization.

ISO/IEC Directives (Part 2), clause 3.3.3 Requirement

Expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled and from which no deviation is permitted if conformance with the document is to be claimed

ISO/IEC Directives (Part 2), clause 3.3.4 Recommendation

Expression, in the content of a document, that conveys a suggested possible choice or course of action deemed to be particularly suitable without necessarily mentioning or excluding others

Value of Documented Information

Important note

- The preparation of documents should not be a target itself. This must be a value-adding activity to the ISMS.
- Highly voluminous documented information is unnecessary because it is difficult to manage and, often, not understood by users.
- Each organization determines the necessary documented information and media for the communication of information.

PECB

16

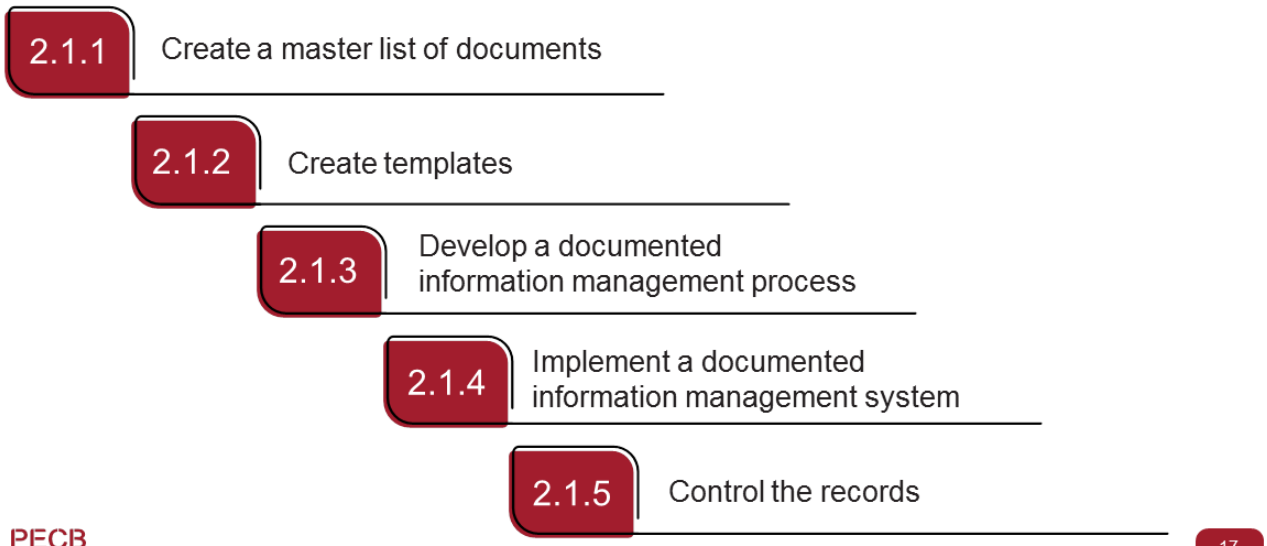
The extent of the necessary documentation and media types to use depends on factors such as the type and size of the organization, the complexity and interaction of processes, information systems and technologies available, the stakeholders' (customers, suppliers, etc.) requirements, and the applicable regulatory requirements.

The primary value of documented information is to communicate the ISMS implementation and ensure consistency in the actions taken. It is used to:

a. Achieve compliance with legal, regulatory, and contractual obligations
b. Achieve conformity with ISO/IEC 27001 and other normative standards
c. Provide media for communication and training
d. Ensure the repeatability and traceability of actions taken
e. Provide evidence for a certification audit
f. Evaluate the effectiveness and relevance of the ISMS
g. Improve ISMS processes and security controls

2.1 Documented Information Management

List of activities



PECB

17

2.1.1 Create a Master List of Documents

It is recommended to make a list of all documented information related to the ISMS with basic information, such as:

- Unique identifier (e.g., 05010-Physical Security Policy, where 05010 is the unique identifier)
- Title
- Document type
- Functions and names of authors
- Function and name of the approver and the date of approval
- Date of issue
- Version and revision date
- Page number
- Classification

PECB

18

Several organizations integrate the main list of documents with the Statement of Applicability in a single document that includes a description of security controls and related documentation.

It is preferable to refer to authors and approval bodies by their role instead of their name. Their role, name, and date should be recorded when each formal version or release of a document is made.

For electronic filing purposes, assigning dates in the format YYYY-MM-DD is recommended. This format is easier to search, because it arranges files in order of date.

2.1.2 Create Templates

Types of documents

Type of document	Objectives
Policy	Statement of overall intentions and the strategic direction of an organization as formally expressed by its management
Procedure	Specific instructions on the steps to be taken
Guidelines	General guidance on good practices to be followed in order to achieve the policy objectives
Security manual	Consolidation of different types of documents related to information security and data protection
Charter	Description of agreements in place between the organization and groups of actors such as users, employees, suppliers, service providers, etc.
Schematic diagram	Schema illustrating how a process works
Narrative processes	Detailed explanation of the functioning of a process as a narrative description
Form	Form, in electronic or hard copy format, which is designed to provide or record information about an operation (request for change, request for authorization, incident reporting, etc.)
Guide	Practical document giving detailed instructions on the use or installation, maintenance, or operation of something
Datasheet	Document that summarizes the technical information (specifications) needed to install, use, maintain, etc. equipment, software, etc.

PECB

19

- **Policy:** A policy represents the overall intentions and strategic direction of an organization as expressed formally by its management.
- **Procedure:** A procedure contains specific instructions that explain clearly the steps to determine how the policy, guidelines, and supporting standards will be actually implemented in an operational environment. It describes an ordered sequence of actions aimed at achieving a goal.
- **Guidelines:** Guidelines provide guidance on good practices to be followed in order to achieve the policy objectives. Although not mandatory, guidelines are important documents that should be respected.
- **Security manual:** A security manual is a collection of either actual description of or references to policies, practices, processes, procedures, and checklists relating to information security, within the scope of the information security management system (ISMS).
- **Charter:** A charter is a description of agreements in place between the organization and a group of actors, such as users, employees, suppliers, service providers, etc. A charter defines the rights and duties of the involved parties.
- **Schematic process:** A schematic process illustrates the working of a process.
- **Narrative process:** A narrative process presents a detailed explanation of the functioning of a process as a narrative description.
- **Form:** A form, be it in electronic or hard copy format, is designed to provide or record information about an operation (request for change, request for authorization, incident reporting, etc.). The use of electronic forms can facilitate the capturing of inputs, control of records, approval processes, and reuse of information (synonym: template or pro forma).

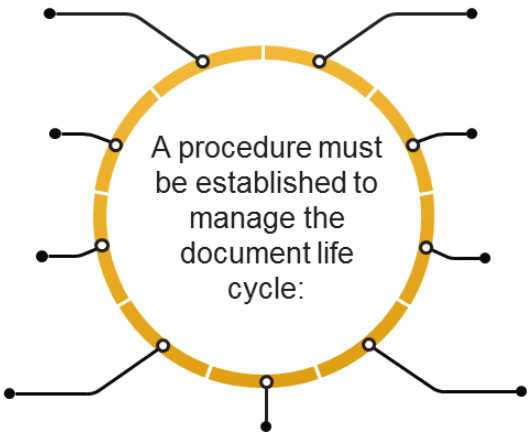
Slide Notes Extension

PECB

20

- **Guide:** A guide is a practical document that gives detailed instructions on the installation, use, maintenance, or operation of something. In practice, although they denote different concepts, the generic terms guide and manual are often used under the same circumstances. Thus, they lead to many expressions that are virtually synonymous. The guide should be adapted to the target audience (e.g., a guide aimed at all users must contain simple and easily understandable technological terms).
- **Data sheet:** A data sheet is a document that summarizes the technical information (specifications) needed to install, operate, or maintain equipment, software, etc. It is generally used for technical equipment and software products in simple series and standards found in the organization. A datasheet can contain, among other things, physical description, information on the product operating characteristics, and installation conditions.

2.1.3 Develop a Documented Information Management Process



1. Creation
2. Identification
3. Classification
4. Modification
5. Approval
6. Distribution
7. Adequate use
8. Archiving
9. Disposal

PECB

21

Establishing procedures for controlling and managing documents is essential for maintaining, communicating, and further improving the management systems with all people involved.

1. **Identification —** The document that needs to be produced has been identified.
2. **Creation of a draft** — A draft document is produced.
3. **Classification —** The draft document is classified and determined to whom it will be accessible.
4. **Review —** The draft is shared for formal review or revision. (The document may take several cycles between this stage and stage 2.)
5. **Approval —** The document is finalized and signed off.
6. **Distribution —** The document is distributed to all interested parties.
7. **Adequate use** — The document is available for use and accessible when needed.
8. **Archiving —** The document is archived.
9. **Disposal** — The organization disposes the unneeded and obsolete documents after their retention period has expired.

2.1.4 Implement a Documented Information Management System

- Facilitating access, referencing, dissemination, and archiving of documented information
- Managing the entire document life cycle
- Ensuring traceability
- Securing document access

PECB

22

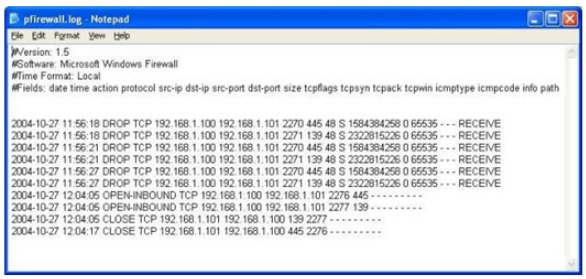
A documented information management system ensures traceability and secures access to documents by managing the different levels of authorization to access, use, and disseminate the data.

Types of available solutions:

1. **Electronic document management system (EDM):** EDM is a computerized system for the acquisition, classification, storage, and archiving of documents (example of use: mass digitization of paper documents). An example is SharePoint (Microsoft).
2. **Content management system:** Content management systems (CMS) are a family of software design and dynamic updating of web sites or multimedia applications to manage content. An example is any “Wiki” application type, such as Wikipedia.

2.1.5 Control the Records

- The identification, storage, protection, availability, retention, and disposal of records must be documented and implemented.
- Records must be protected and remain legible, readily identifiable, and accessible.



PECB

23

Records of information systems, register of visitors, audit reports, and completed forms for authorizing access are examples of records.

Records Register

Example

Identification	Stored	Responsibility	Retention	Classification
Visitor log	Reception	Administrative assistant	One year	Internal use
Incidents report sheet	Service Center	Service center director	Three years	Confidential
Employee record	HR Department	HR director	Five years after the termination of employment	Highly confidential
Management review	Executive Committee	Secretary of the executive committee	Seven years	Highly confidential

Documented Information Management

Most common problems

Problems:

- Difficulty in finding or managing a document
- Inability to quickly extract useful information from a document
- Inefficient update of documents
- Incoherence between records and actual business processes
- Ambiguous or incomprehensible texts or graphics
- Proliferation of document versions

Potential cause:

- A large number of misclassified and not indexed documents
- Voluminous documents, too literary, often with multiple annexes
- Document management processes not established or poorly exploited
- Employees not being involved in drafting the documents
- No validation with users, lack of training and awareness, incompetent editors
- No documented information management system in place

Exercise 10: Master list of documented information

The top management of e-Scooter has decided to implement all the information security controls on business continuity management (ISO/IEC 27001, Annex 17).

Propose a list of documented information that should be generated to ensure conformity to the information security controls of Annex 17.

Duration of the exercise: 30 minutes

Comments: 15 minutes

1. **What should an organization do in order to comply with ISO/IEC 27001?**
   A. Develop a procedure for the control of the documented information
   B. Develop a form for the control of the documented information that is visible only to the top management
   C. Develop a guideline for the control of the documented information only when requested by an executive
2. **In order to comply with ISO/IEC 27001, organizations should fulfill some mandatory requirements on how to document controls.**
   A. True
   B. False
3. **What does a master list of documents in the context of ISMS contain?**
   A. All documentation related to the ISMS in a single list
   B. Key parts of the documentation related to the ISMS in single lists
   C. A group of the most accessed documents in a single list
4. **What does a procedure describe?**
   A. An orderly sequence of actions aimed at achieving a goal
   B. A guide to an actual description of policies
   C. A detailed explanation of the functioning of a process

5.Which is the correct sequence of actions when establishing a procedure to manage the document life cycle?

A. Approval, identification, classification, modification, disposal, archiving, adequate use, and distribution
B. Creation, identification, classification, modification, approval, distribution, adequate use, archiving, disposal
C. Distribution, identification, modification, classification, disposal, archiving, adequate use, and creation

6.During which of the following cases is the implementation of a documented information management system especially useful?

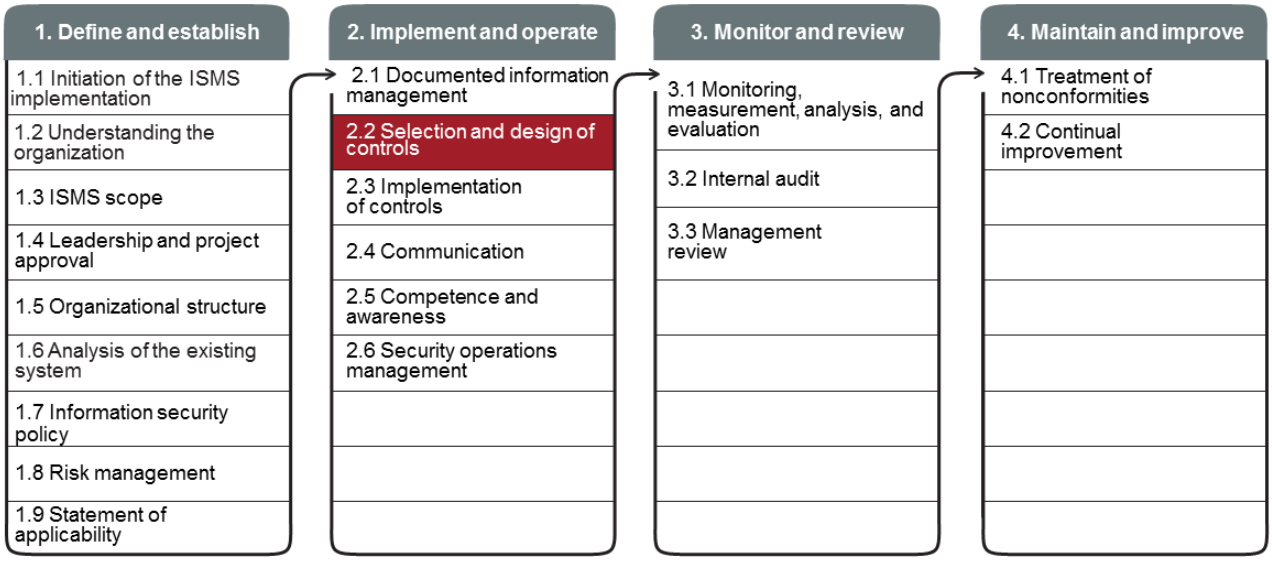
A. Facilitating access to, referencing, disseminating, and archiving documents
B. Losing traceability of the documented information
C. Managing parts of the document life cycle

Section summary

- ISMS documented information is needed to comply with the ISO/IEC 27001 requirements.
- Every document shall have a title, date, author, or reference number.
- Organizations should develop procedures for the control of documents and records.
- There is no requirement on how to document processes and security controls or the types to be used. Some types of documents that can be used are policies, procedures, guidelines, security manuals, forms, data sheets, etc.
- A document life cycle should include the following steps: identification, creation of a draft, classification and security, review, approval, distribution, adequate use, archiving, and disposal.
- A master list of documents helps organize all documentation related to the ISMS in a single list.

This section provides information that will help the participants gain knowledge about the process of preparing for the implementation of controls.

2.2 Selection and Design of Controls



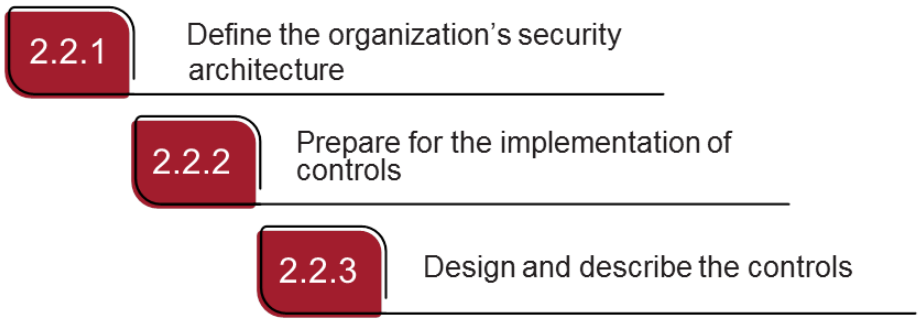
Selection and Design of Controls

Operational planning and control

- The organization should plan, implement, control, and continually improve the processes needed to meet information security requirements.
- The organization should, following the risk assessment process, select controls and implement them.
- Documented information should be regularly maintained in order to ensure that the processes have been carried out as planned.
- Planned and unplanned changes should be controlled in order to mitigate their consequences and adverse effects.
- The organization should also ensure that outsourced processes are properly determined and controlled.

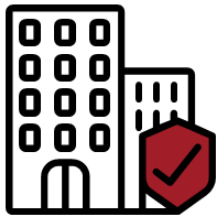
2.2 Selection and Design of Controls

List of activities



2.2.1 Define the Organization's Security Architecture

- The organization's security architecture represents a holistic approach to incorporate building blocks of security across the entire organization.
- It focuses on the following:
  - Representing a simple and long-term view of security controls
  - Providing a unified vision for common security controls tied to business objectives
  - Leveraging existing technology investments and maximizing benefits from new ones
  - Providing a flexible approach to current and future threats and also the needs of core functions
  - Providing efficiency: the right assets, at the right time, in the right places



PECB

34

Security architecture presents a set of disciplines used to design solutions to address security requirements at a system level. The organization's security architecture implements the building blocks of information security infrastructure across the entire organization. It focuses on a strategic design of a set of security services that can be leveraged by multiple applications, systems, or business processes, instead of focusing on individual functional and nonfunctional components in an application.

The organization's security architecture is focused on setting the long-term strategy for security services in the organization. Its primary purpose is to establish the priorities for the development security services and provide that input into the planning phase of the information security management system implementation. It focuses on the enforcement of security zones of controls and the design and implementation of common security services. These approaches are used to help ensure that the organization's security services are both effective and cost-sensitive.

Source: Gordon, Adam., ed. Official (ISC)2 Guide to the CISSP CBK. CRC Press, 2015.

Concepts and Security Models

Common security services

A number of security functions serve as foundations for common security services in the organization and may be used to build the organization's security architecture. Some of these functions are:

- Identity and access control services
- Boundary control services
- Integrity services
- Cryptographic services
- Audit and monitoring services

PECB

35

Identity and access control services

- These services aim at normalizing identification and promoting shared authentication across the organization.
- These services will promote reduced-sign-on (RSO) or single-sign-on (SSO), but they will also include RSO or SSO services themselves as common security services. It will also include a number of other services surrounding the creation, handling, and storage of credentials in the organization.
- On the authorization side, these services focus on what valid user entities are allowed and not allowed to do within the organization, given a set of rules enforced through automated systems. They will offer coarse-grained (system-level) authorization services that can be leveraged by other domains in the organization architecture.

Boundary control services

- These services control the transferring of information from a state or set of systems to another.
- Boundary control systems are intended to enforce security zones of control by isolating entry points from one zone to another (choke points).

Slide Notes Extension

PECB

36

Integrity services

- These services focus on the maintenance of high-integrity systems and data through automated checking in order to detect and correct corruption.
- Many are intended for systems that can be accessed directly by distrusted or less trusted user entities or systems.

Cryptographic services

- These services focus on common services that can be deployed and reused by a variety of systems.
- This may also include common hashing and encryption services, tools, and technologies.

Audit and monitoring services

- These services include log collection, collation, and analysis services through the deployment of security event information management (SEIM) solutions.
- Given the centralized infrastructure required, this is also the suitable place to consider centralized management systems.

Source: Gordon, Adam., ed. *Official (ISC)^2 Guide to the CISSP CBK*. CRC Press, 2015.

Concepts and Security Models

Common architecture frameworks

- Zachman framework provides a formal and structured way of understanding a complex architecture. It allows for the communication and collaboration of all entities in the development of the architecture (not specific to security architecture).
- Sherwood Applied Business Security Architecture (SABSA) is a holistic life cycle for developing security architecture beginning with assessing business requirements and creating a “chain of traceability” through the phases of strategy, concept, design, implementation, and metrics.
- The Open Group Architecture Framework (TOGAF) is an open framework for organizations wishing to design and build enterprise architecture.
- IT Infrastructure and Library (ITIL) is a collection of best practices for IT governance.

Sherwood Applied Business Security Architecture (SABSA)

The SABSA model for security architecture development

	Assets (What?)	Motivation (Why?)	Process (How?)	People (Who?)	Location (Where?)	Time (When?)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetime and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices, and procedures	Security mechanisms	Users, applications, and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions, and ACLs	Processes, nodes, addresses, and protocols	Security step timing and sequencing
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites and platforms	Security operations schedule

PECB

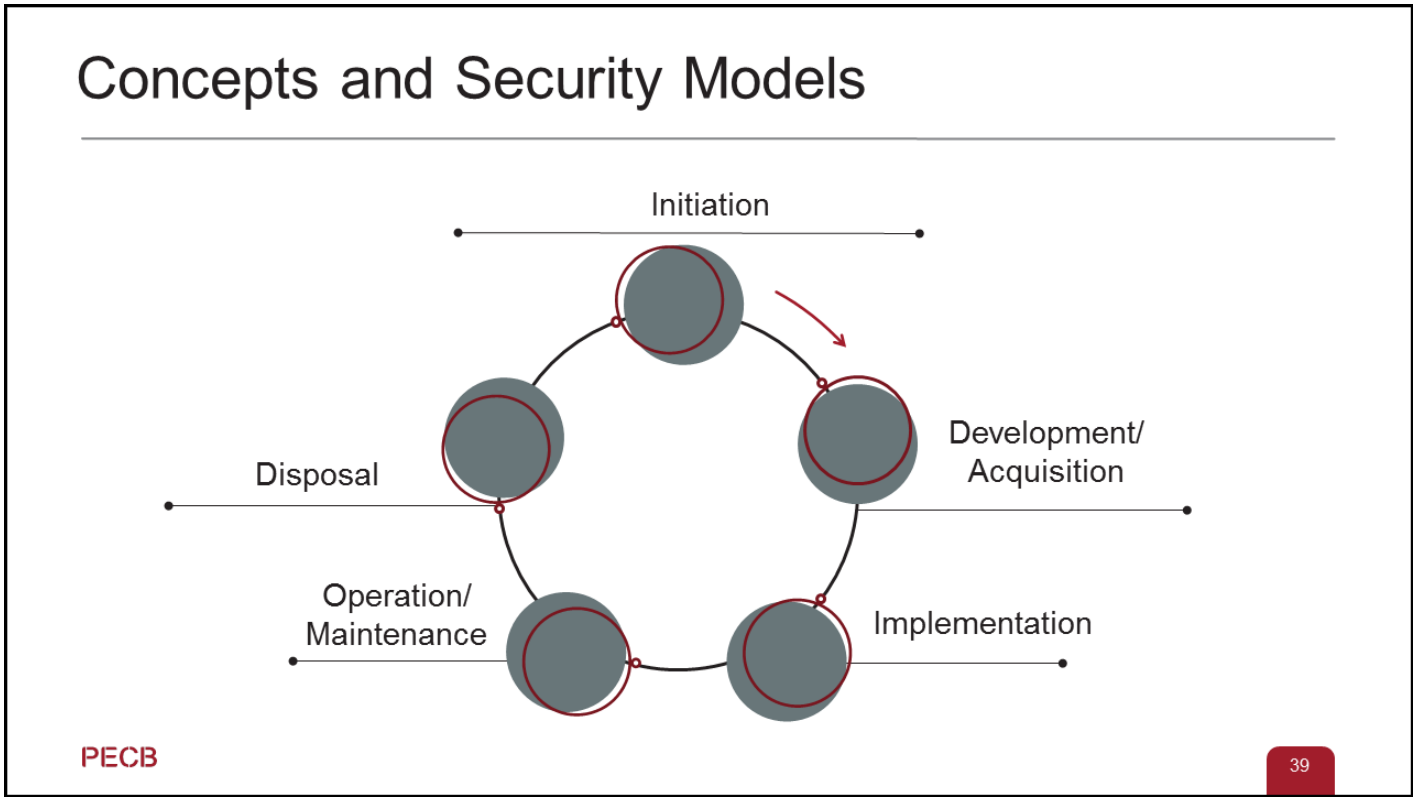
38

SABSA is an open standard available for use by anyone. It comprises frameworks, terminology, models, and processes. The SABSA matrix for security architecture development covers six cascading levels, also known as the "6 W's." These levels are assets (what), motivation (why), process (how), people (who), location (where), and time (when) which together with the layers of the security architecture form a 6X6 matrix known as the "SABSA® Matrix."

The SABSA model for security architecture at a high level uses the six layers of design to complete security architecture, by providing different levels of detail. These layers are:

- **Contextual** security architecture is focused on the business view.
- **Conceptual** security architecture is focused on the architect's view.
- **Logical** security architecture is focused on the designer's view by viewing the services in high level.
- **Physical** security architecture is focused on the builder's view by viewing in detail all services and their deployment against physical assets.
- **Component** security architecture is focused on the tradesman's view by viewing individual security services.
- **Operational** security architecture is focused on the facility manager's view.

Source: Gordon, Adam., ed. *Official (ISC)^2 Guide to the CISSP CBK*. CRC Press, 2015.



The steps involved in developing and deploying information systems should be made with clear architectural principles in mind as per the following:

- **Initiation —** During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Activities include conducting an impact assessment in accordance with FIPS-199.
- **Development/Acquisition** — During this phase, the system is designed, purchased, programed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle. Activities include determining security requirements, incorporating security requirements into specifications, and obtaining or developing the system.
- **Implementation** — During the implementation phase, the system is tested and installed or fielded. Activities include installing or turning on controls, security testing, certification, and accreditation.
- **Operation/Maintenance** — During this phase, the system performs its work. Typically, the system is also modified by the addition of hardware and software and by numerous other events. Activities include security operations and administration, operational assurance, and audits and monitoring.
- **Disposal —** The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software. Activities include moving, archiving, discarding, or destroying information and sanitizing the media.

Source: Gordon, Adam., ed. *Official (ISC)^2 Guide to the CISSP CBK*. CRC Press, 2015.

2.2.2 Prepare for the Implementation of Controls

- The organization's overall security architecture helps in identifying all the types of security controls to be implemented (information security controls, in particular).
- When preparing for the implementation of information security controls, the organization should:
  - Allocate the required resources and physical means to implement every control that is listed in the Statement of Applicability
  - Conduct a cost analysis
  - Assess the competence of the people involved in the process of implementing controls to perform the assigned tasks
  - Allocate the time, including the complete schedule for the implementation of each control
  - Prepare the required documented information
  - Prepare a detailed list of activities and tasks to be performed during the implementation process
  - Outline the intended results and outputs

Prepare for the Implementation of Controls

- As part of the preparation process, it is best practice to draft the information security procedures and policies before initiating the implementation of the selected information security controls.
- Employees in charge of operations should be involved in drafting, reviewing, and validating the content of such procedures and policies.
- When the employees are involved in the process of drafting information security procedures and policies, they are more likely to contribute towards the implementation of information security controls within the organization.
- The implementation of information security controls should not affect the organization's day-to-day operations, so that its efficiency remains intact.

2.2.3 Design and Describe the Controls

Practical tips

- The design and description of the security controls selected for the ISMS should be properly documented.
- ISO/IEC 27001 does not provide any specific documentation method to be used.
- Since the organization's security architecture divides security controls into groups, it is best practice to divide their respective documents into groups, as well. For example, all the information security controls should be included in a single document.
- Documentation must be concise and reader-friendly.

PECB

1. **What does an organization's security architecture represent?**
   A. A set of disciplines used to design solutions to address security requirements at a human level
   B. A set of disciplines used to design solutions to address security requirements at an operational level
   C. A set of disciplines used to design solutions to address security requirements at a system level
2. **Which services aim at normalizing user identification and promoting shared authentication across the organization?**
   A. Boundary control services
   B. Access control services
   C. Cryptographic services
3. **Boundary control services control the transfer of information from a state or set of systems to another.**
   A. True
   B. False
4. **The _____ matrix for security architecture development covers six cascading levels, also known as the "6 Ws."**
   A. IT Infrastructure and Library (ITIL)
   B. The Open Group Architecture Framework (OGAF)
   C. Sherwood Applied Business Security Architecture (SABSA)
5. **What are some of the steps to take when preparing for the implementation of information security controls?**
   A. Conduct a cost analysis and prepare the required documented information
   B. Conduct a cost analysis and avoid the intended results and outputs
   C. Conduct a cost analysis and prepare a general list of activities without providing details

6.Why is it important to involve employees in the draft, review, and validation processes?

A. Because it helps them gain experience and expertise for their personal intellect
B. Because it helps them implement the information security controls within the organization
C. Because it helps them automate procedures easily and work faster

7.ISO/IEC 27001 provides a specific documentation method to be used for designing and describing controls?

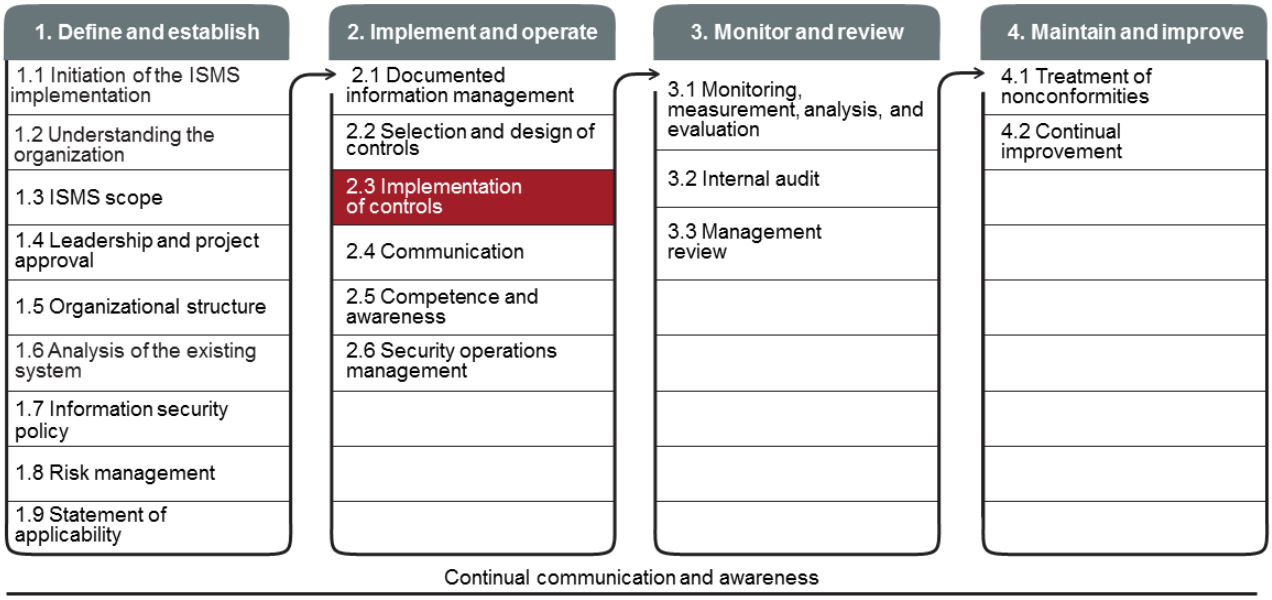
A. True
B. False

Section summary

- A set of disciplines used to design solutions which address security requirements at a system level is known as security architecture.
- Common security services such as access control services, boundary control services, integrity services, cryptographic services, and audit and monitoring services can be used to build the organization's security architecture.
- Zachman framework, SABSA, TOGAF, and ITIL are some of the most commonly used architecture frameworks.
- NIST 800-160 planning life cycle of developing and deploying information systems includes the initiation, development and acquisition, implementation, and operation and maintenance phase.
- Design and description of security controls selected to be implemented in the ISMS should be documented.
- ISO/IEC 27001 does not explicitly provide any documentation method to be used.

This section provides information that will help the participants gain knowledge about the implementation of security processes and controls and the controls of Annex A.

2.3 Implementation of Controls



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 8.1

- *The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.*
- *The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.*
- *The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.*
- *The organization shall ensure that outsourced processes are determined and controlled.*

PECB

48

An organization wishing to comply with the requirements of ISO/IEC 27001 shall, at least, implement security controls detailed in the risk treatment plan and those that have been declared applicable in the Statement of Applicability.

ISO/IEC 27003, clause 8.1 Operational planning and control

Processes to meet information security requirements include:

a. *ISMS processes (e.g. management review, internal audit); and*
b. *processes required for implementing the information security risk treatment plan.*

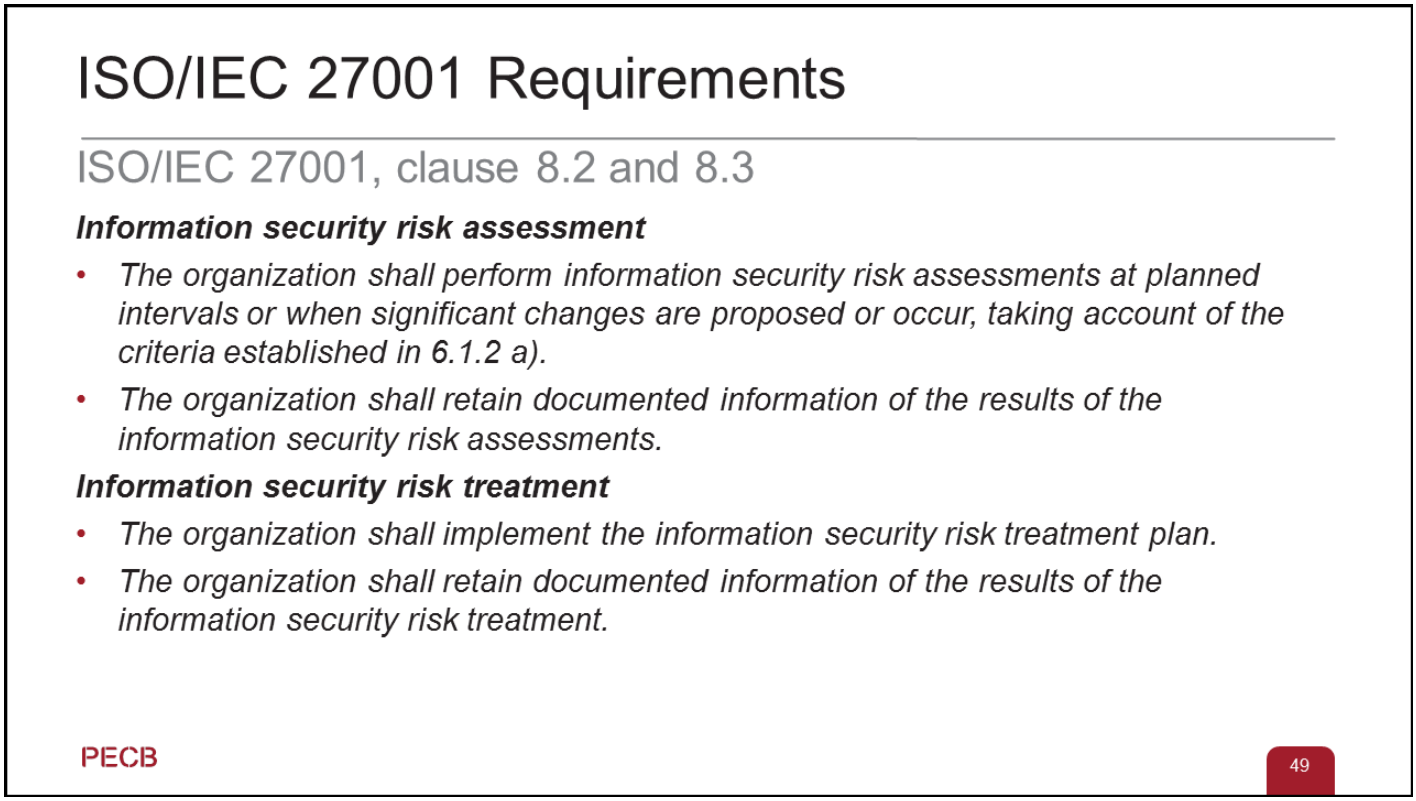
Implementation of plans results in operated and controlled processes.

The organization ultimately remains responsible for planning and controlling any outsourced processes in order to achieve its information security objectives. Thus the organization needs to:

a. *determine outsourced processes considering the information security risks related to the outsourcing; and*
b. *ensure that outsourced processes are controlled (i.e. planned, monitored and reviewed) in a manner that provides assurance that they operate as intended (also considering information security objectives and the information security risk treatment plan).*

If part of the organization's functions or processes are outsourced to suppliers, the organization should:

q.*determine all outsourcing relationships;*
r.*establish appropriate interfaces to the suppliers;*
s.*address information security related issues in the supplier agreements;*
t.*monitor and review the supplier services to ensure that they are operated as intended and associated information security risks meet the risk acceptance criteria of the organization; and*
u.*manage changes to the supplier services as necessary.*



ISO/IEC 27003, clause 8.2 Information security risk assessment

Guidance

Organizations should have a plan for conducting scheduled information security risk assessments.

When any significant changes of the ISMS (or its context) or information security incidents have occurred, the organization should determine:

a. *which of these changes or incidents require an additional information security risk assessment; and*
b. *how these assessments are triggered.*

The level of detail of the risk identification should be refined step by step in further iterations of the information security risk assessment in the context of the continual improvement of the ISMS. A broad information security risk assessment should be performed at least once a year.

ISO/IEC 27003, clause 8.3 Information security risk treatment

Explanation

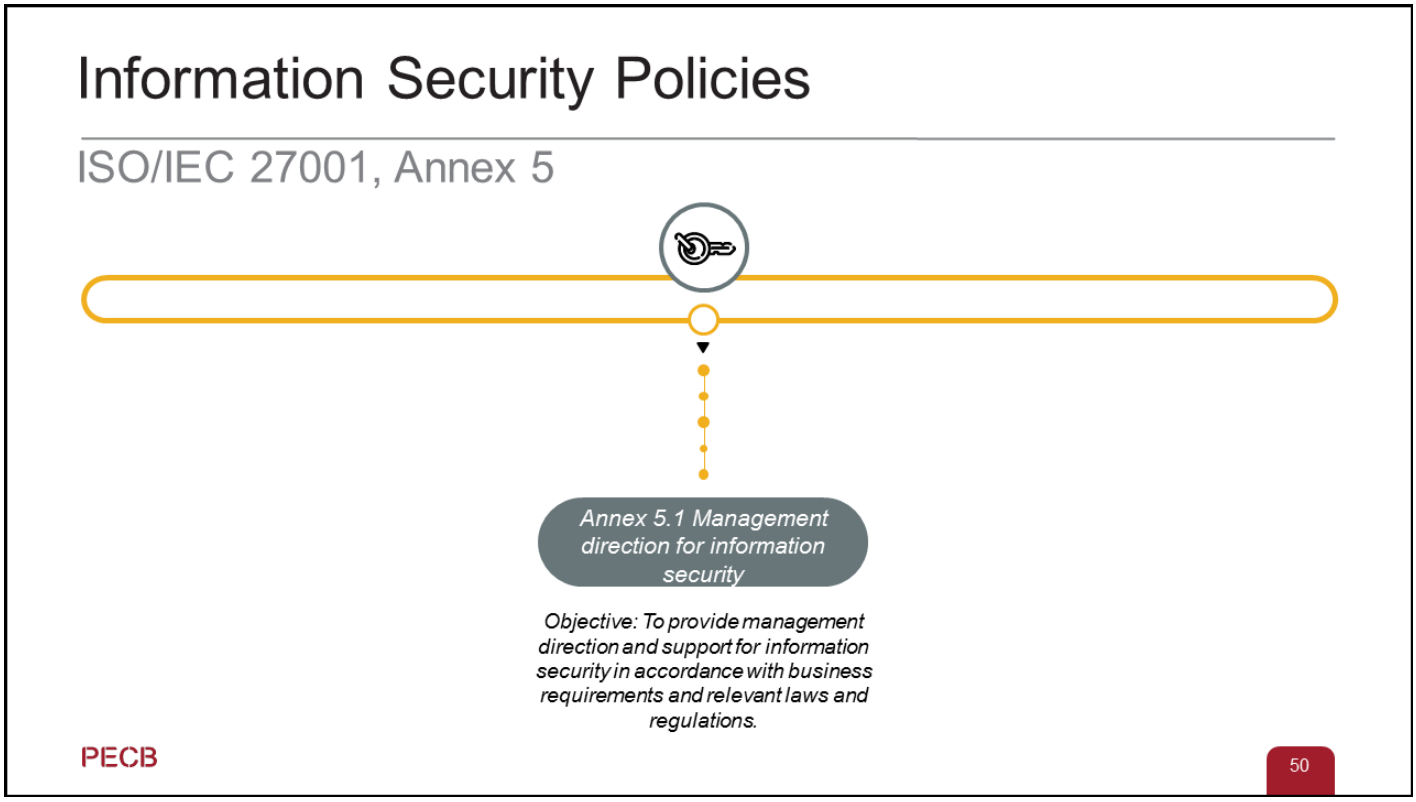
In order to treat information security risks, the organization needs to carry out the information security risk treatment process defined in 6.1.3. During operation of the ISMS, whenever the risk assessment is updated according to 8.2, the organization then applies the risk treatment according to 6.1.3 and updates the risk treatment plan. The updated risk treatment plan is again implemented.

The results of the information security risk treatment are retained in documented information as evidence that the process in 6.1.3 has been performed as defined.

Guidance

The information security risk treatment process should be performed after each iteration of the information security assessment process in 8.2 or when the implementation of the risk treatment plan or parts of it fails.

The progress of implementation of the information security risk treatment plan should be driven and monitored by this activity.



ISO/IEC 27001, Annex 5.1.1 Policies for information security

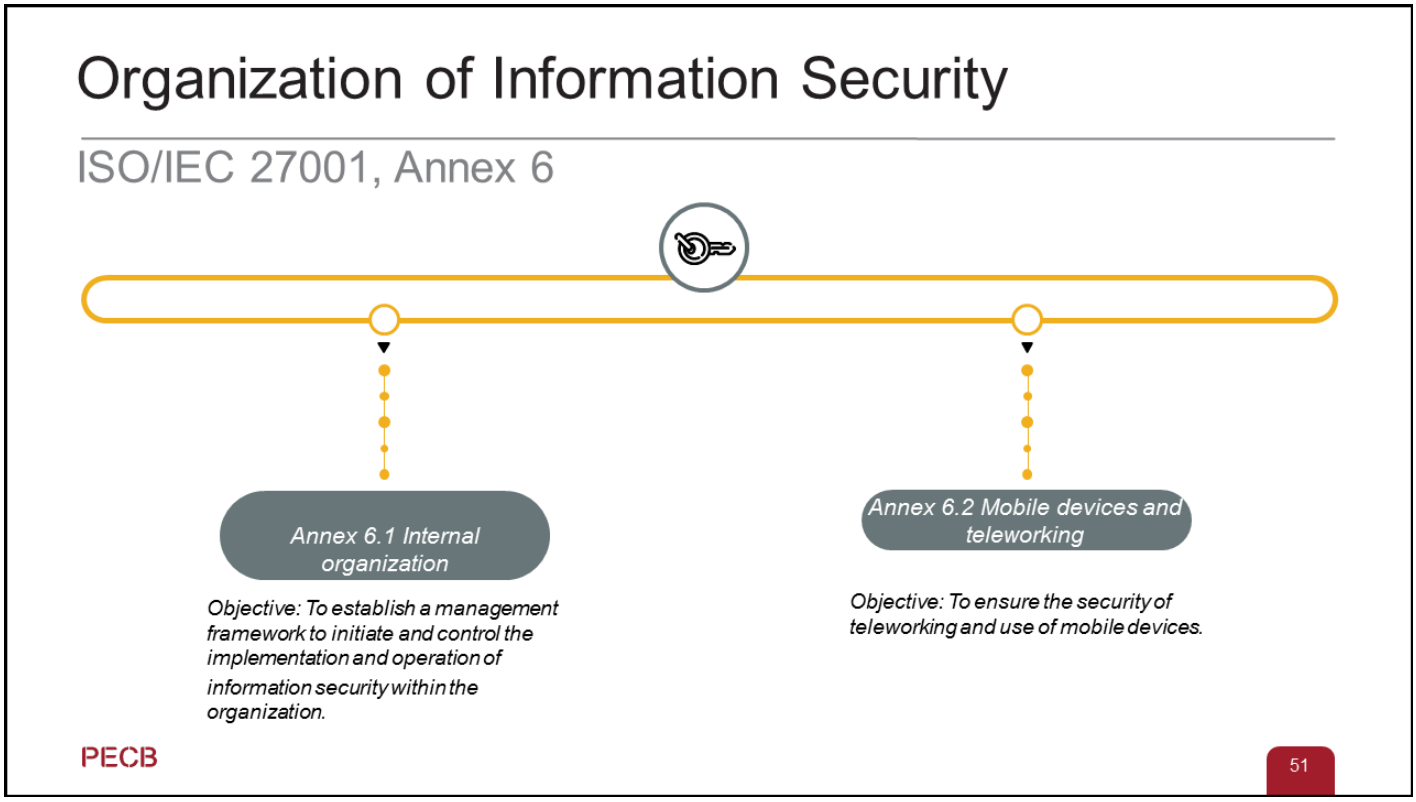
Control

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

ISO/IEC 27001, Annex 5.1.2 Review of the policies for information security

Control

The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.



ISO/IEC 27001, Annex 6.1.1 Information security roles and responsibilities

Control

All information security responsibilities shall be defined and allocated.

ISO/IEC 27001, Annex 6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

ISO/IEC 27001, Annex 6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities shall be maintained.

ISO/IEC 27001, Annex 6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

ISO/IEC 27001, Annex 6.1.5 Information security in project management

Control

Information security shall be addressed in project management, regardless of the type of the project.

ISO/IEC 27001, Annex 6.2.1 Mobile device policy

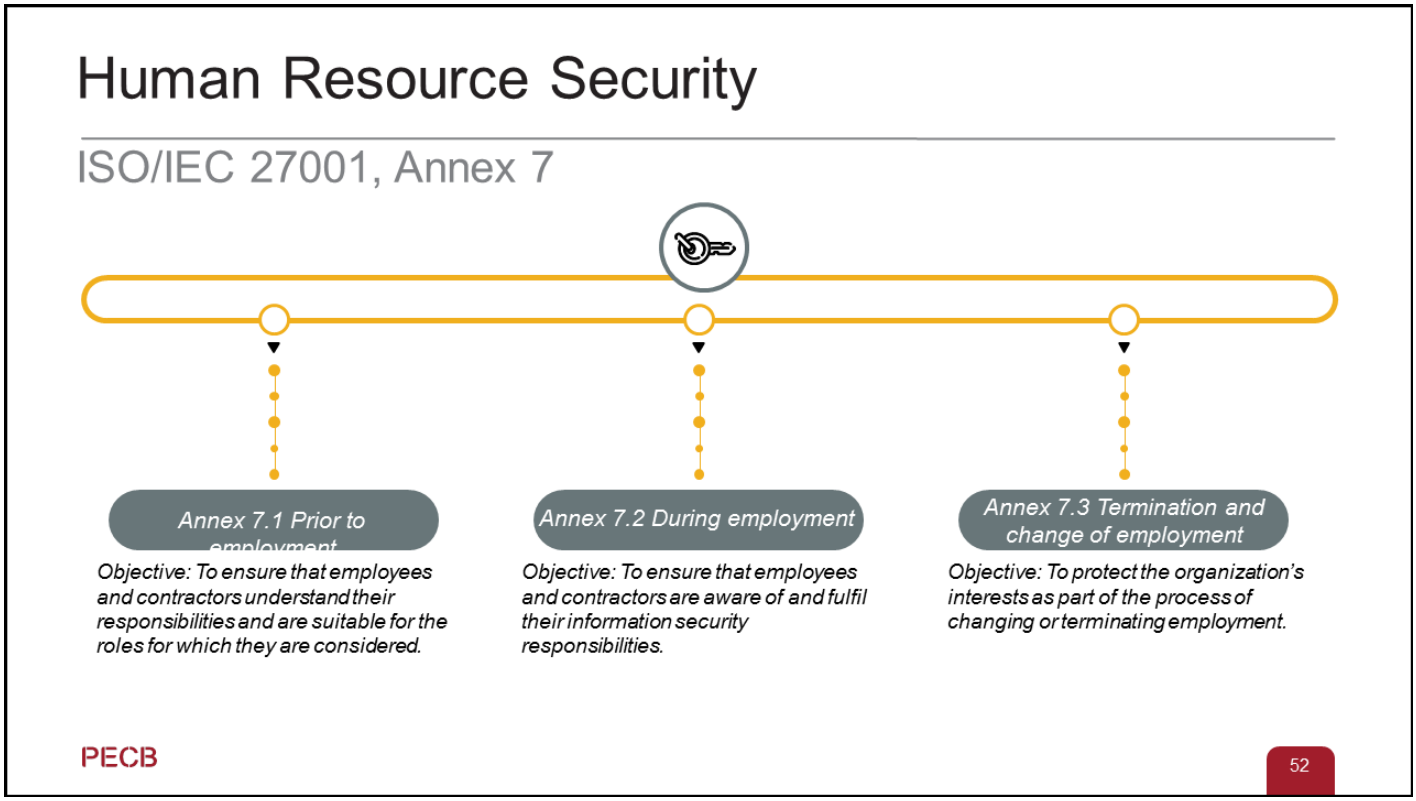
Control

A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

ISO/IEC 27001, Annex 6.2.2 Teleworking

Control

A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.



ISO/IEC 27001, Annex 7.1.1 Screening

Control

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

ISO/IEC 27001, Annex 7.1.2 Terms and conditions of employment

Control

The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

ISO/IEC 27001, Annex 7.2.1 Management responsibilities

Control

Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

ISO/IEC 27001, Annex 7.2.2 Information security awareness, education and training

Control

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

ISO/IEC 27001, Annex 7.2.3 Disciplinary process

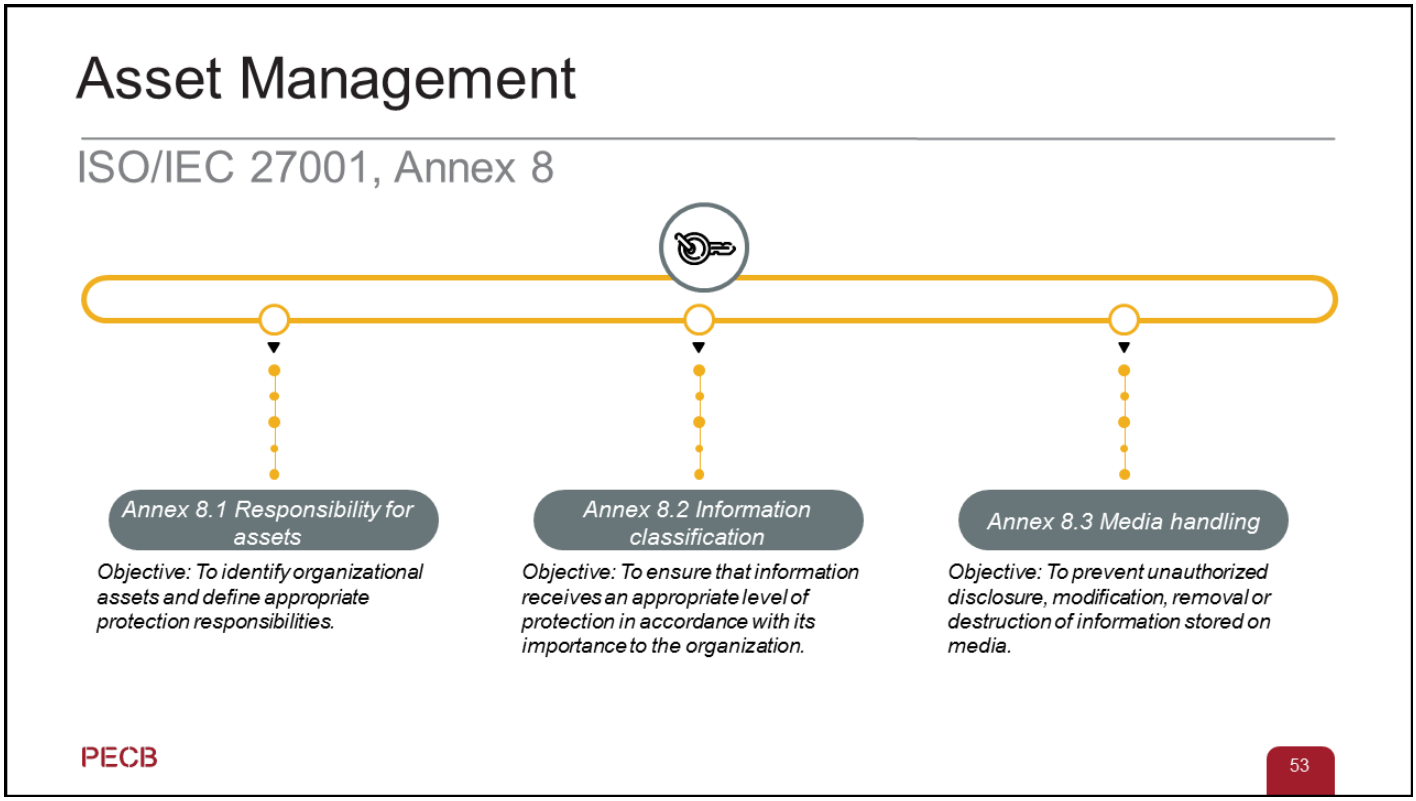
Control

There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

ISO/IEC 27001, Annex 7.3.1 Termination or change of employment responsibilities

Control

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.



ISO/IEC 27001, Annex 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 8.1.2 Ownership of assets

Control

Assets maintained in the inventory shall be owned.

ISO/IEC 27001, Annex 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 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.

Slide Notes Extension

PECB

54

ISO/IEC 27001, Annex 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 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 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.

ISO/IEC 27001, Annex 8.3.1 Management of removable media

Control

Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

ISO/IEC 27001, Annex 8.3.2 Disposal of media

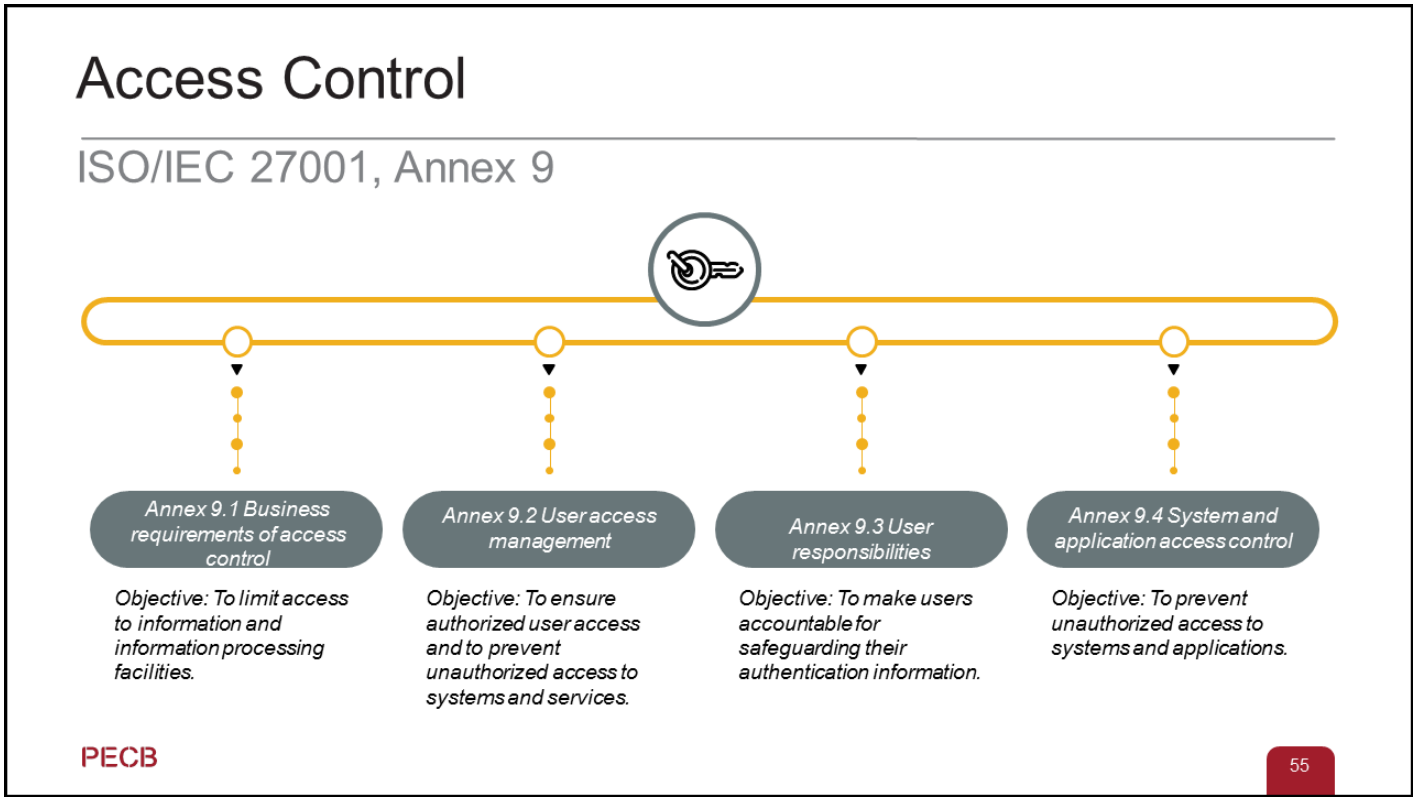
Control

Media shall be disposed of securely when no longer required, using formal procedures.

ISO/IEC 27001, Annex 8.3.3 Physical media transfer

Control

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.



ISO/IEC 27001, Annex 9.1.1 Access control policy

Control

An access control policy shall be established, documented and reviewed based on business and information security requirements.

ISO/IEC 27001, Annex 9.1.2 Access to networks and network services

Control

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

ISO/IEC 27001, Annex 9.2.1 User registration and de-registration

Control

A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

ISO/IEC 27001, Annex 9.2.2 User access provisioning

Control

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

ISO/IEC 27001, Annex 9.2.3 Management of privileged access rights

Control

The allocation and use of privileged access rights shall be restricted and controlled.

ISO/IEC 27001, Annex 9.2.4 Management of secret authentication information of users

Control

The allocation of secret authentication information shall be controlled through a formal management process.

Slide Notes Extension

PECB

56

ISO/IEC 27001, Annex 9.2.5 Review of user access rights

Control

Asset owners shall review users' access rights at regular intervals.

ISO/IEC 27001, Annex 9.2.6 Removal or adjustment of access rights

Control

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

ISO/IEC 27001, Annex 9.3.1 Use of secret authentication information

Control

Users shall be required to follow the organization's practices in the use of secret authentication information.

ISO/IEC 27001, Annex 9.4.1 Information access restriction

Control

Access to information and application system functions shall be restricted in accordance with the access control policy.

ISO/IEC 27001, Annex 9.4.2 Secure log-on procedures

Control

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

ISO/IEC 27001, Annex 9.4.3 Password management system

Control

Password management systems shall be interactive and shall ensure quality passwords.

ISO/IEC 27001, Annex 9.4.4 Use of privileged utility programs

Control

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

ISO/IEC 27001, Annex 9.4.5 Access control to program source code

Control

Access to program source code shall be restricted.

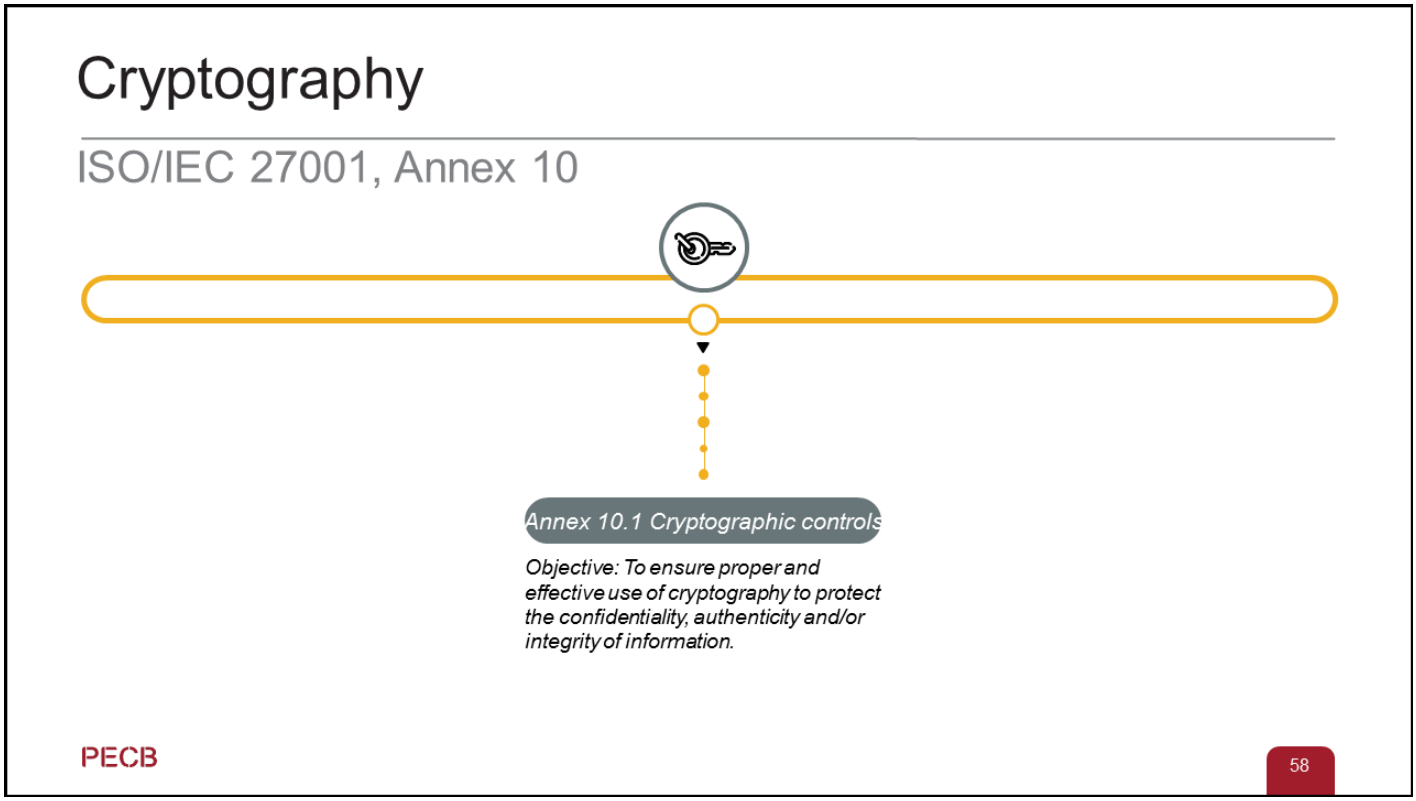
Exercise 11: Access control

Following the conduct of an internal audit of the information security controls in e-Scooter, it was found that there are no records of the Software Development Department employees that worked remotely and had access to their customers' personally identifiable information stored in the cloud blockchain database.

Determine and explain the control that has not been applied in the company.

Duration of the exercise: 20 minutes

Comments: 15 minutes



ISO/IEC 27001, Annex 10.1.1 Policy on the use of cryptographic controls

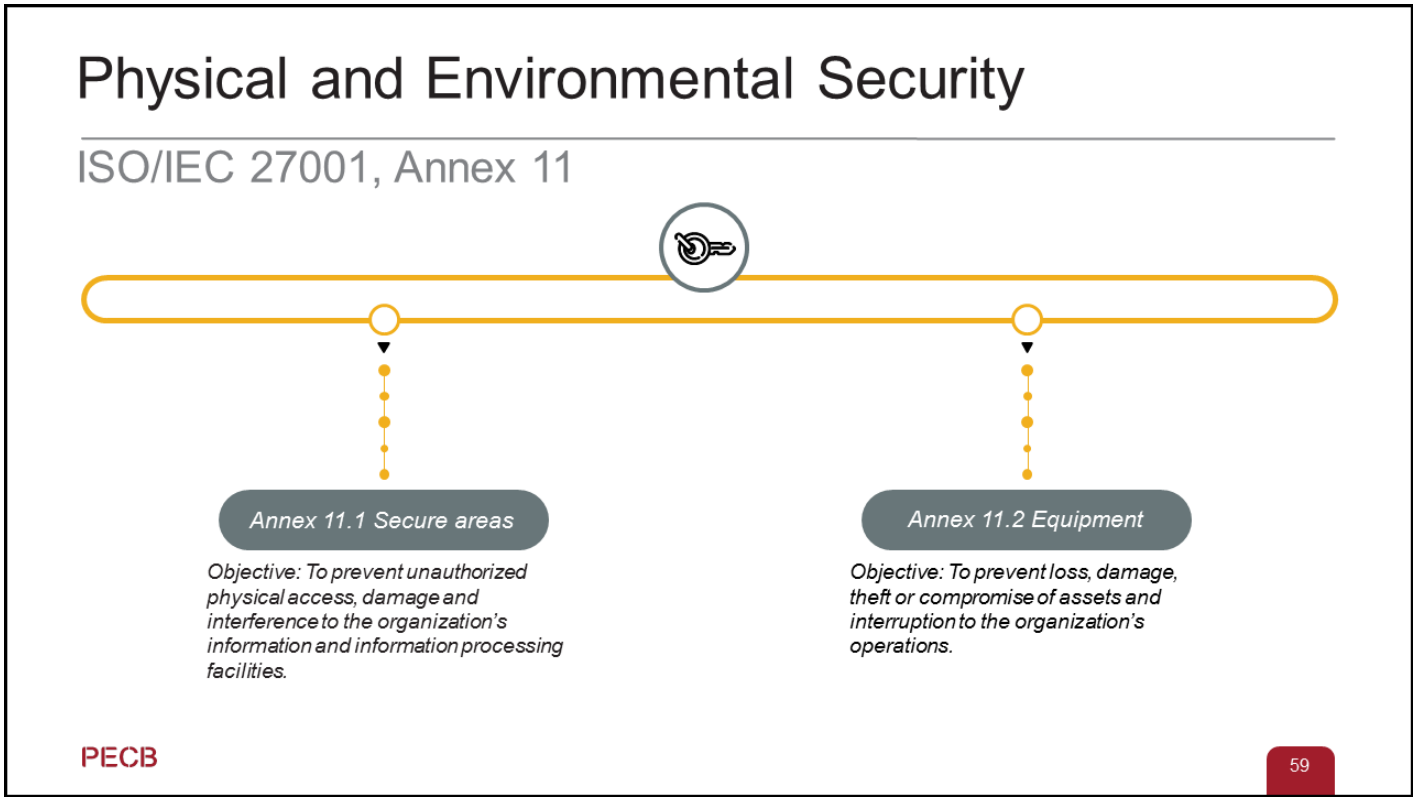
Control

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

ISO/IEC 27001, Annex 10.1.2 Key management

Control

A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole life cycle.



ISO/IEC 27001, Annex 11.1.1 Physical security perimeter

Control

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

ISO/IEC 27001, Annex 11.1.2 Physical entry controls

Control

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

ISO/IEC 27001, Annex 11.1.3 Securing offices, rooms and facilities

Control

Physical security for offices, rooms and facilities shall be designed and applied.

ISO/IEC 27001, Annex 11.1.4 Protecting against external and environmental threats

Control

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

ISO/IEC 27001, Annex 11.1.5 Working in secure areas

Control

Procedures for working in secure areas shall be designed and applied.

ISO/IEC 27001, Annex 11.1.6 Delivery and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Slide Notes Extension

PECB

60

ISO/IEC 27001, Annex 11.2.1 Equipment siting and protection

Control

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

ISO/IEC 27001, Annex 11.2.2 Supporting utilities

Control

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

ISO/IEC 27001, Annex 11.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

ISO/IEC 27001, Annex 11.2.4 Equipment maintenance

Control

Equipment shall be correctly maintained to ensure its continued availability and integrity.

ISO/IEC 27001, Annex 11.2.5 Removal of assets

Control

Equipment, information or software shall not be taken off-site without prior authorization.

ISO/IEC 27001, Annex 11.2.6 Security of equipment and assets off-premises

Control

Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

ISO/IEC 27001, Annex 11.2.7 Secure disposal or reuse of equipment

Control

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

ISO/IEC 27001, Annex 11.2.8 Unattended user equipment

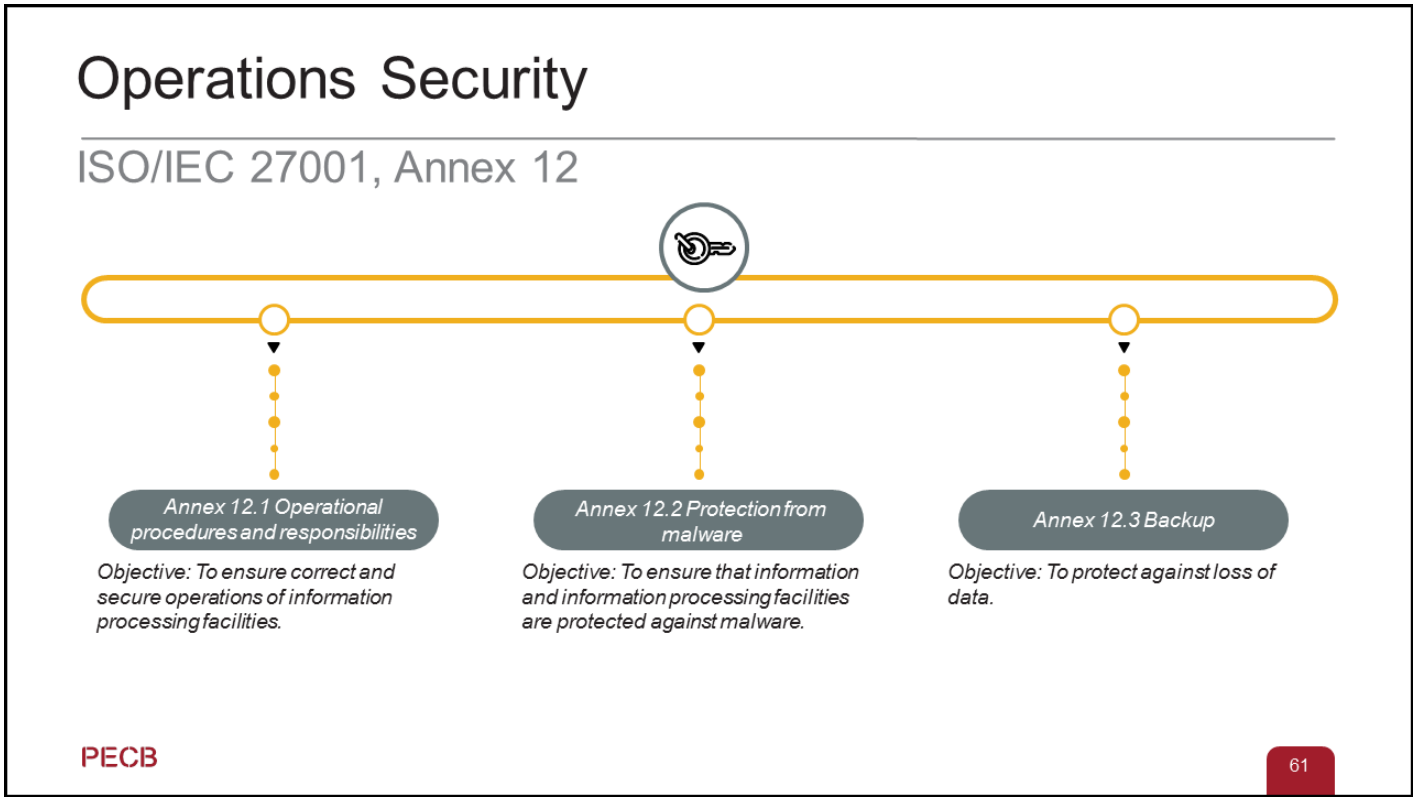
Control

Users shall ensure that unattended equipment has appropriate protection.

ISO/IEC 27001, Annex 11.2.9 Clear desk and clear screen policy

Control

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.



ISO/IEC 27001, Annex 12.1.1 Documented operating procedures

Control

Operating procedures shall be documented and made available to all users who need them.

ISO/IEC 27001, Annex 12.1.2 Change management

Control

Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

ISO/IEC 27001, Annex 12.1.3 Capacity management

Control

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

ISO/IEC 27001, Annex 12.1.4 Separation of development, testing and operational environments

Control

Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

ISO/IEC 27001, Annex 12.2.1 Controls against malware

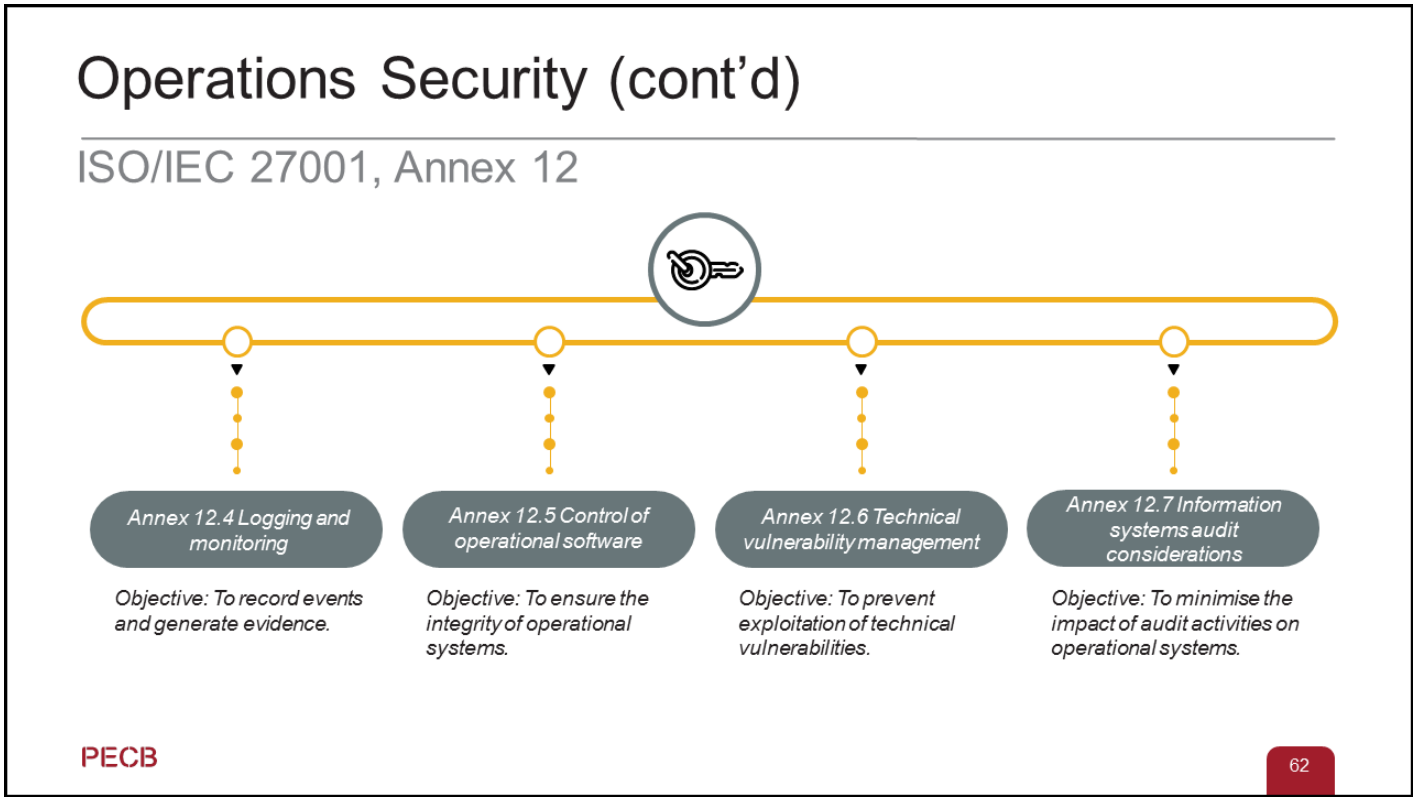
Control

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

ISO/IEC 27001, Annex 12.3.1 Information backup

Control

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.



ISO/IEC 27001, Annex 12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

ISO/IEC 27001, Annex 12.4.2 Protection of log information

Control

Logging facilities and log information shall be protected against tampering and unauthorized access.

ISO/IEC 27001, Annex 12.4.3 Administrator and operator logs

Control

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

ISO/IEC 27001, Annex 12.4.4 Clock synchronization

Control

The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.

ISO/IEC 27001, Annex 12.5.1 Installation of software on operational systems

Control

Procedures shall be implemented to control the installation of software on operational systems.

ISO/IEC 27001, Annex 12.6.1 Management of technical vulnerabilities

Control

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

ISO/IEC 27001, Annex 12.6.2 Restrictions on software installation

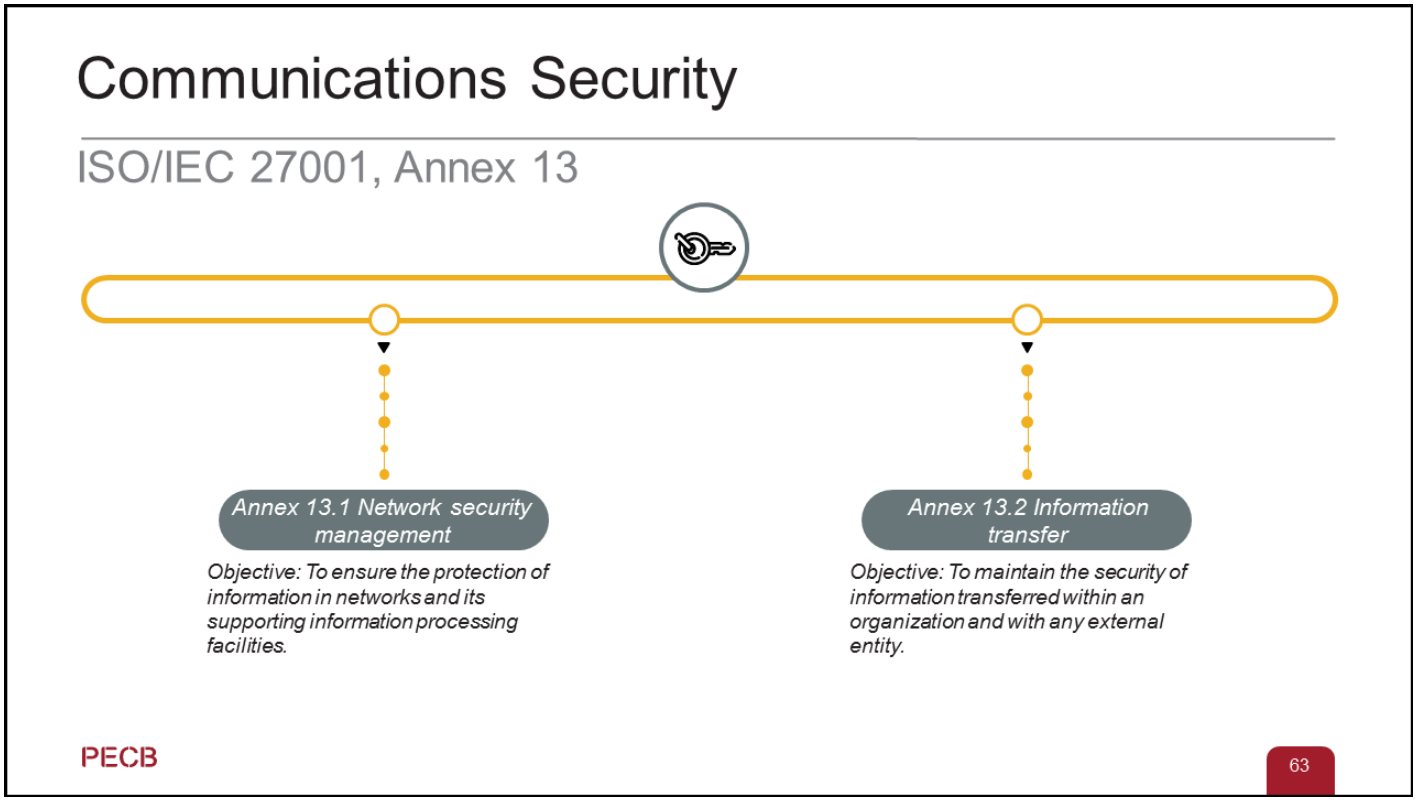
Control

Rules governing the installation of software by users shall be established and implemented.

ISO/IEC 27001, Annex 12.7.1 Information systems audit controls

Control

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.



ISO/IEC 27001, Annex 13.1.1 Network controls

Control

Networks shall be managed and controlled to protect information in systems and applications.

ISO/IEC 27001, Annex 13.1.2 Security of network services

Control

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

ISO/IEC 27001, Annex 13.1.3 Segregation in networks

Control

Groups of information services, users and information systems shall be segregated on networks.

ISO/IEC 27001, Annex 13.2.1 Information transfer policies and procedures

Control

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

ISO/IEC 27001, Annex 13.2.2 Agreements on information transfer

Control

Agreements shall address the secure transfer of business information between the organization and external parties.

ISO/IEC 27001, Annex 13.2.3 Electronic messaging

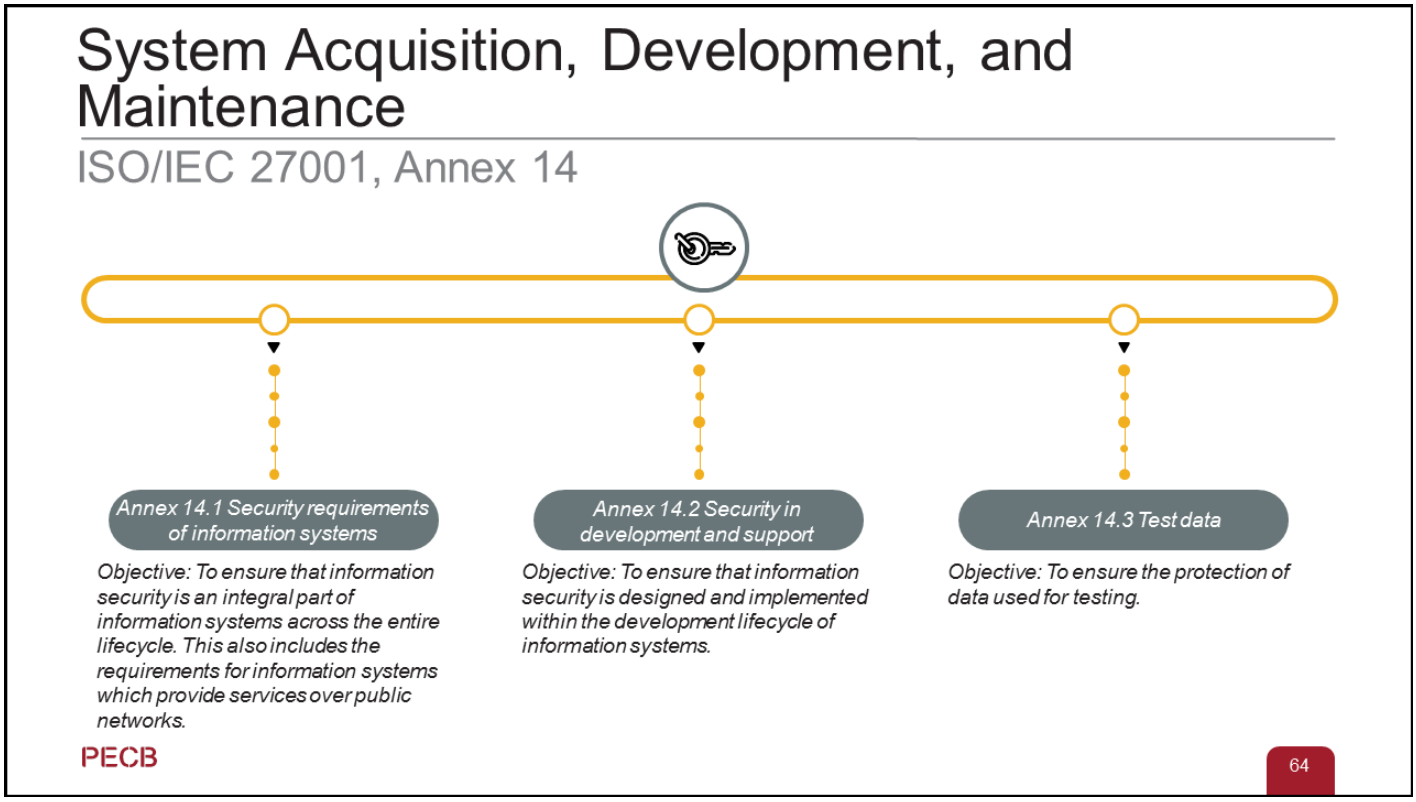
Control

Information involved in electronic messaging shall be appropriately protected.

ISO/IEC 27001, Annex 13.2.4 Confidentiality or nondisclosure agreements

Control

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.



ISO/IEC 27001, Annex14.1.1 Information security requirements analysis and specification

Control

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

ISO/IEC 27001, Annex14.1.2 Securing application services on public networks

Control

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

ISO/IEC 27001, Annex14.1.3 Protecting application services transactions

Control

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

ISO/IEC 27001, Annex14.2.1 Secure development policy

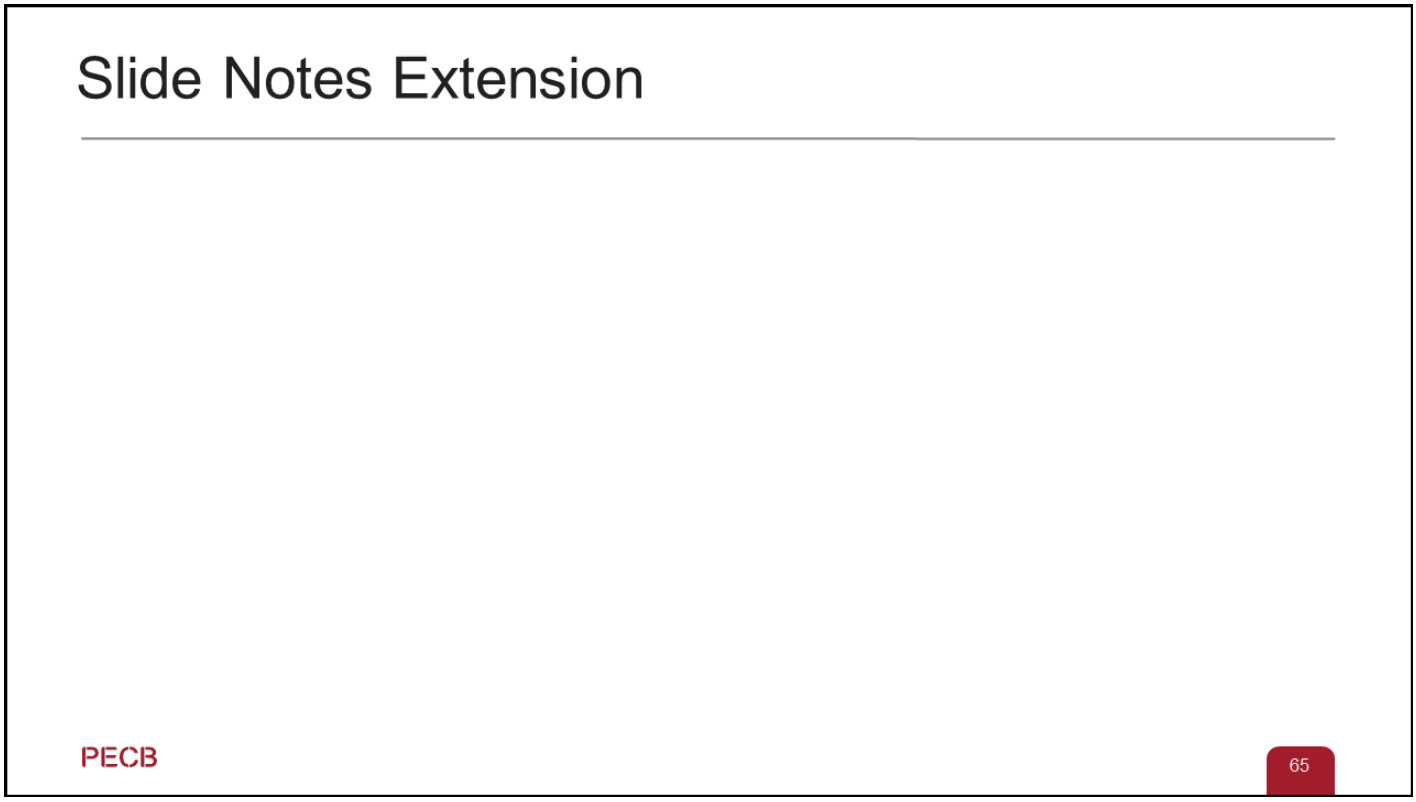
Control

Rules for the development of software and systems shall be established and applied to developments within the organization.

ISO/IEC 27001, Annex14.2.2 System change control procedures

Control

Changes to systems within the development life cycle shall be controlled by the use of formal change control procedures.



ISO/IEC 27001, Annex14.2.3 Technical review of applications after operating platform changes

Control

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

ISO/IEC 27001, Annex14.2.4 Restrictions on changes to software packages

Control

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

ISO/IEC 27001, Annex 14.2.5 Secure system engineering principles

Control

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

ISO/IEC 27001, Annex 14.2.6 Secure development environment

Control

Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

ISO/IEC 27001, Annex 14.2.7 Outsourced development

Control

The organization shall supervise and monitor the activity of outsourced system development.

ISO/IEC 27001, Annex 14.2.8 System security testing

Control

Testing of security functionality shall be carried out during development.

ISO/IEC 27001, Annex 14.2.9 System acceptance testing

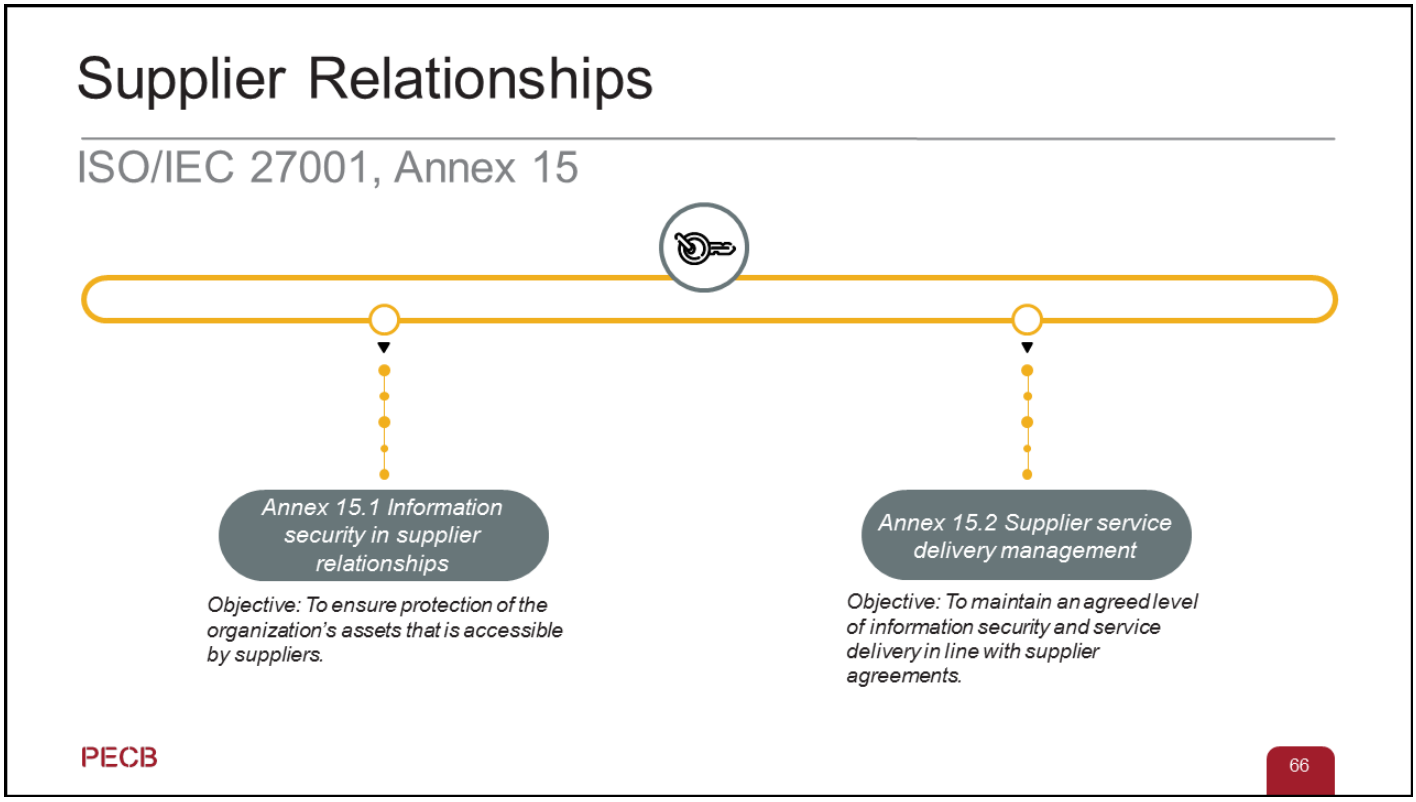
Control

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

ISO/IEC 27001, Annex 14.3.1 Protection of test data

Control

Test data shall be selected carefully, protected and controlled.



ISO/IEC 27001, Annex 15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

ISO/IEC 27001, Annex 15.1.2 Addressing security within supplier agreements

Control

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

ISO/IEC 27001, Annex 15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

ISO/IEC 27001, Annex 15.2.1 Monitoring and review of supplier services

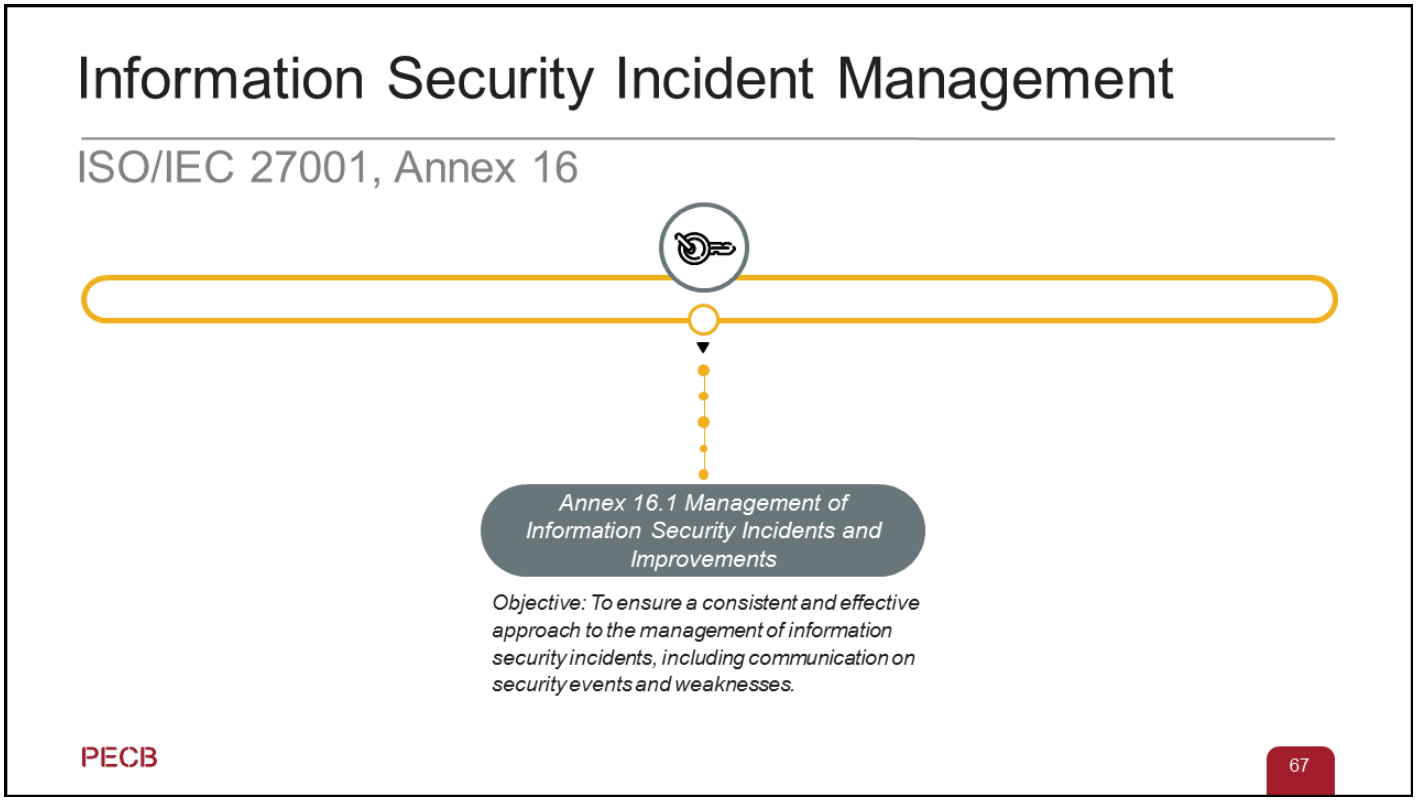
Control

Organizations shall regularly monitor, review and audit supplier service delivery.

ISO/IEC 27001, Annex 15.2.2 Managing changes to supplier services

Control

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.



ISO/IEC 27001, Annex 16.1.1 Responsibilities and procedures

Control

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

ISO/IEC 27001, Annex 16.1.2 Reporting information security events

Control

Information security events shall be reported through appropriate management channels as quickly as possible.

ISO/IEC 27001, Annex 16.1.3 Reporting information security weaknesses

Control

Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

ISO/IEC 27001, Annex 16.1.4 Assessment of and decision on information security events

Control

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

ISO/IEC 27001, Annex 16.1.5 Response to information security incidents

Control

Information security incidents shall be responded to in accordance with the documented procedures.

ISO/IEC 27001, Annex 16.1.6 Learning from information security incidents

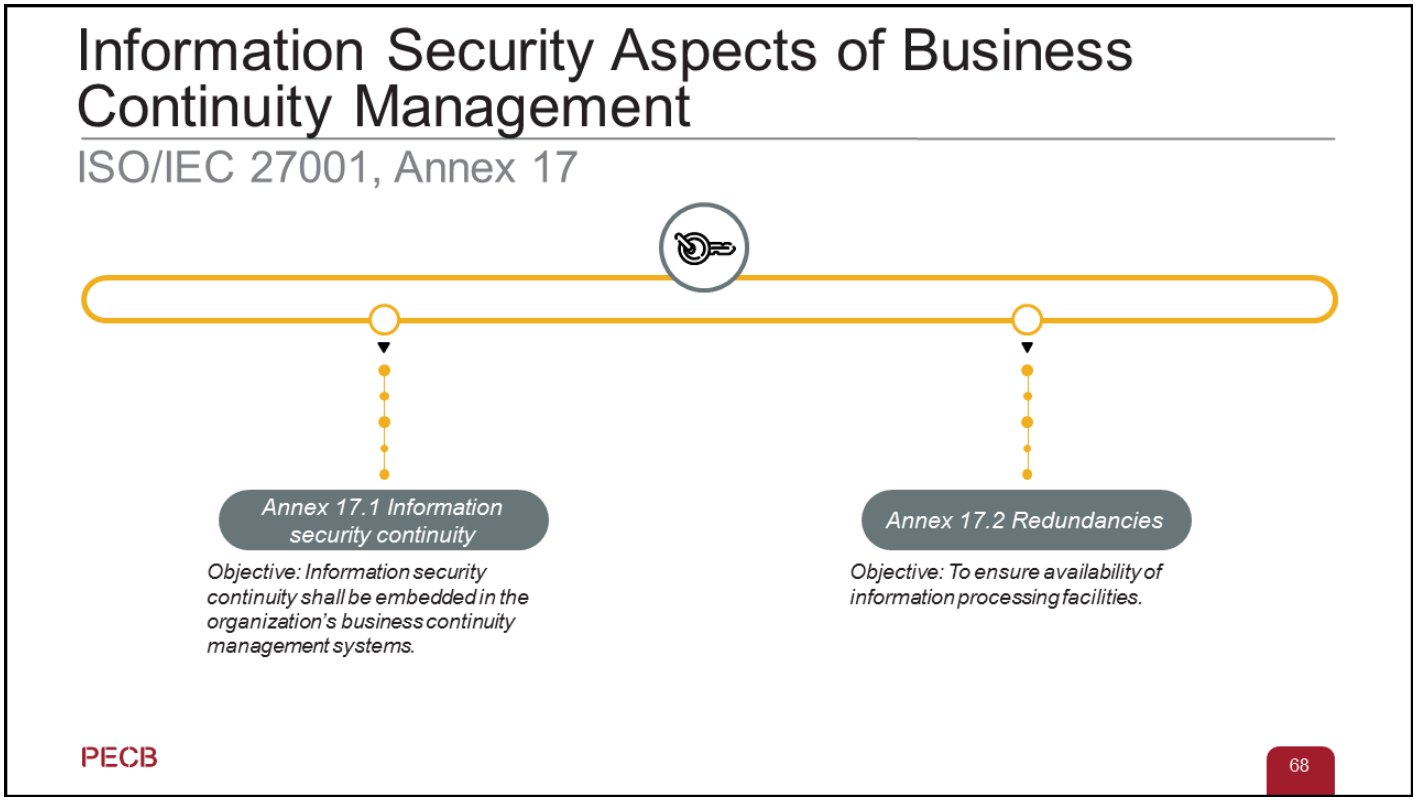
Control

Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

ISO/IEC 27001, Annex 16.1.7 Collection of evidence

Control

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.



ISO/IEC 27001, Annex 17.1.1 Planning information security continuity

Control

The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

ISO/IEC 27001, Annex 17.1.2 Implementing information security continuity

Control

The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

ISO/IEC 27001, Annex 17.1.3 Verify, review and evaluate information security continuity

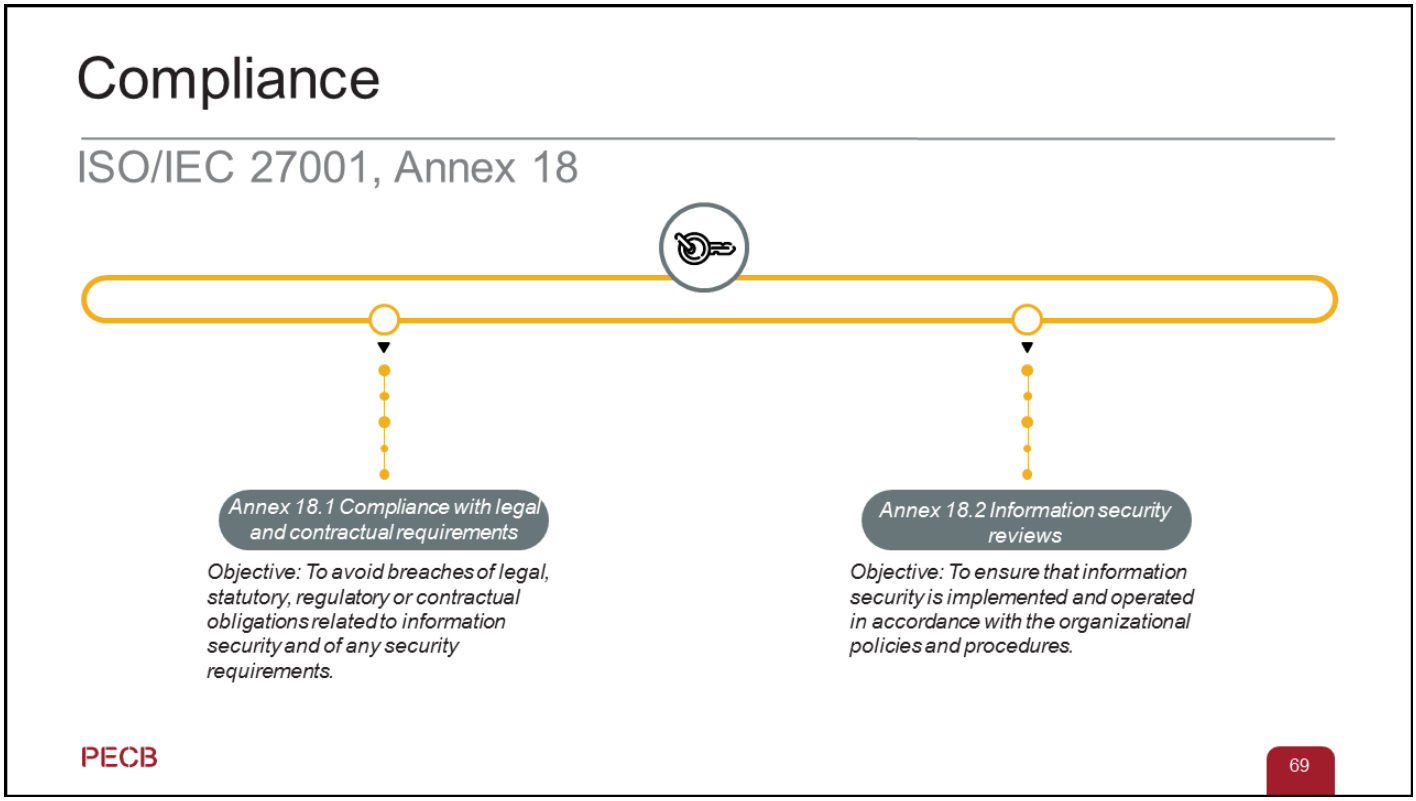
Control

The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

ISO/IEC 27001, Annex 17.2.1 Availability of information processing facilities

Control

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.



ISO/IEC 27001, Annex 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 shall be explicitly identified, documented and kept up to date for each information system and the organization.

ISO/IEC 27001, Annex 18.1.2 Intellectual property rights

Control

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

ISO/IEC 27001, Annex 18.1.3 Protection of records

Control

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with the legislatory, regulatory, contractual and business requirements.

ISO/IEC 27001, Annex 18.1.4 Privacy and protection of personally identifiable information

Control

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

ISO/IEC 27001, Annex 18.1.5 Regulation of cryptographic controls

Control

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

Slide Notes Extension

PECB

70

ISO/IEC 27001, Annex 18.2.1 Independent review of information security

Control

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

ISO/IEC 27001, Annex 18.2.2 Compliance with security policies and standards

Control

Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

ISO/IEC 27001, Annex 18.2.3 Technical compliance review

Control

Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Exercise 12: Security controls

Provide an action plan constituting at least two actions to be taken to ensure conformity to the following clauses and controls of ISO/IEC 27001.

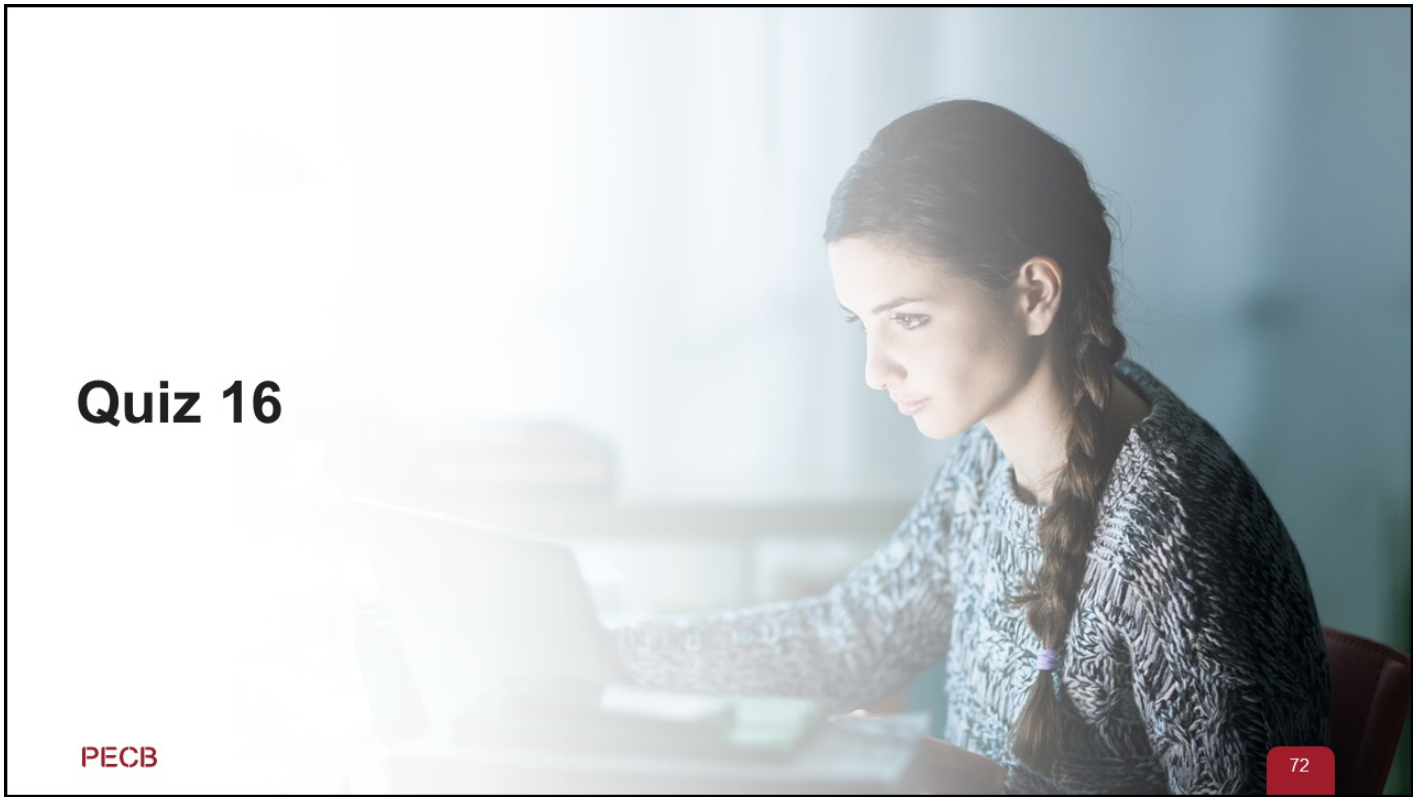
Example: Annex 11.2.3 Cabling security

- *Use shielded network cabling conduit to isolate and protect power and telecommunications cabling from interception*
- *Document the authorized cabling material to avoid the usage of low quality material*

1. Clause 7.2 a) Determine the necessary competence of person(s) doing work under its control that affects its information security performance
2. Clause 10.1 a) React to the nonconformity
3. Annex 12.1.3 Capacity management
4. Annex 12.2.1 Controls against malware
5. Annex 13.2.3 Electronic messaging

Duration of the exercise: 30 minutes

Comments: 15 minutes



1. **Why should organizations review the information security policies after the occurrence of significant changes?**
   A. To ensure continuing suitability, adequacy, and effectiveness of the information security policy
   B. To ensure continuing reliability of the information security policy
   C. To ensure continuing efficiency, performance, and correctness of the information security policy
2. **Which is the main objective of the prior-to-employment control?**
   A. To ensure that employees and contractors understand their responsibilities
   B. To ensure that employees and contractors are aware of and fulfill their information security responsibilities
   C. To protect the organization's interests as part of the process of any changes in employment
3. **Who shall have access to documented operating procedures?**
   A. Only the top management
   B. The person responsible for operating procedures
   C. Any user that needs them
4. **What is the main objective of the control regarding security in development and support?**
   A. To ensure that information security is an integral part of information systems across the entire life cycle
   B. To ensure that information security is designed and implemented within the development life cycle of information systems
   C. To ensure the protection of data used for testing
5. **Why should the organization implement a user registration and de-registration process?**
   A. To enable assignment of access rights
   B. To protect and review administrator logs
   C. To control the installation of software on operational systems

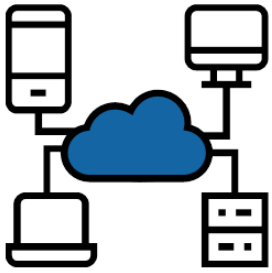
Section summary

- In order to comply with information security requirements, the organization shall implement security controls that meet its purpose and affect its ISMS.
- In order to comply with the requirements of ISO/IEC 27001, organizations shall, in all cases, implement security controls in the risk treatment plan and those in the Statement of Applicability.
- Annex A lists the control objectives and controls that can be used in context with clause 6.1.3 Information security risk treatment.

This section provides information that will help the participants gain knowledge on the today's world trends and technologies, including big data, artificial intelligence, machine learning, cloud computing, and outsourced operations.

Big Data

- The dictionary of Merriam-Webster defines big data as "an accumulation of data that is too large and complex for processing by traditional database management tools."
- Big data includes a large number of structured and unstructured data.
- Structured data are organized and easily reachable.
- Unstructured data cannot be organized in relational databases and are not easily reachable.



PECB

75

The difference between structured and unstructured data

- Structured data have a defined data model and are based on relational databases. Examples of structured data include SQL (Structured Query Language) databases and Microsoft Excel files which have structured tables, rows, and columns.
- Unstructured data do not have a predefined data model and are based on binary data. Examples of unstructured data are MongoDB and Apache Giraph.

The Three V's of Big Data

1. **Volume of data** refers to the amount of data generated through websites, online applications, transactions, data saved in records, tables, files, etc.

2. **Variety** refers to the different types of data, including structured and unstructured data, online images and videos, human-generated texts, machine-generated readings, etc.

3. **Velocity** refers to the speed of data processing generated in real time, online and offline, in streams, batches, or bits.

Artificial Intelligence (AI)

- The Oxford English Dictionary defines Artificial Intelligence (AI) as “the theory and development of computer systems able to perform tasks usually requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.”
- The interconnectivity and fast data transfers that are made possible through the usage of 5G will allow for AI applications to become integral parts of our lives.
- Common application of AI are:
  - AI in banking
  - AI in marketing
  - AI in healthcare
  - AI in autonomous vehicles

PECB

77

Artificial Intelligence (AI) (Cont'd)

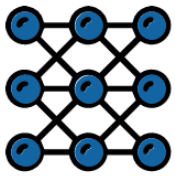
Weak and strong AI

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

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

Machine Learning (ML)

- Machine learning and artificial intelligence are sometimes mistakenly used interchangeably, but they do not represent the same thing.
- As previously mentioned, AI encompasses a broader concept of machines that have the capacity to mimic a human being, whereas the main purpose of ML is to enable computers to learn automatically.
- In machine learning, the processor is given the entry data and the machine solves the problems by applying various methodologies.
- Some of the essential algorithms that are utilized by machine learning are:
  - Linear regression
  - Logistic regression
  - Decision tree



PECB

79

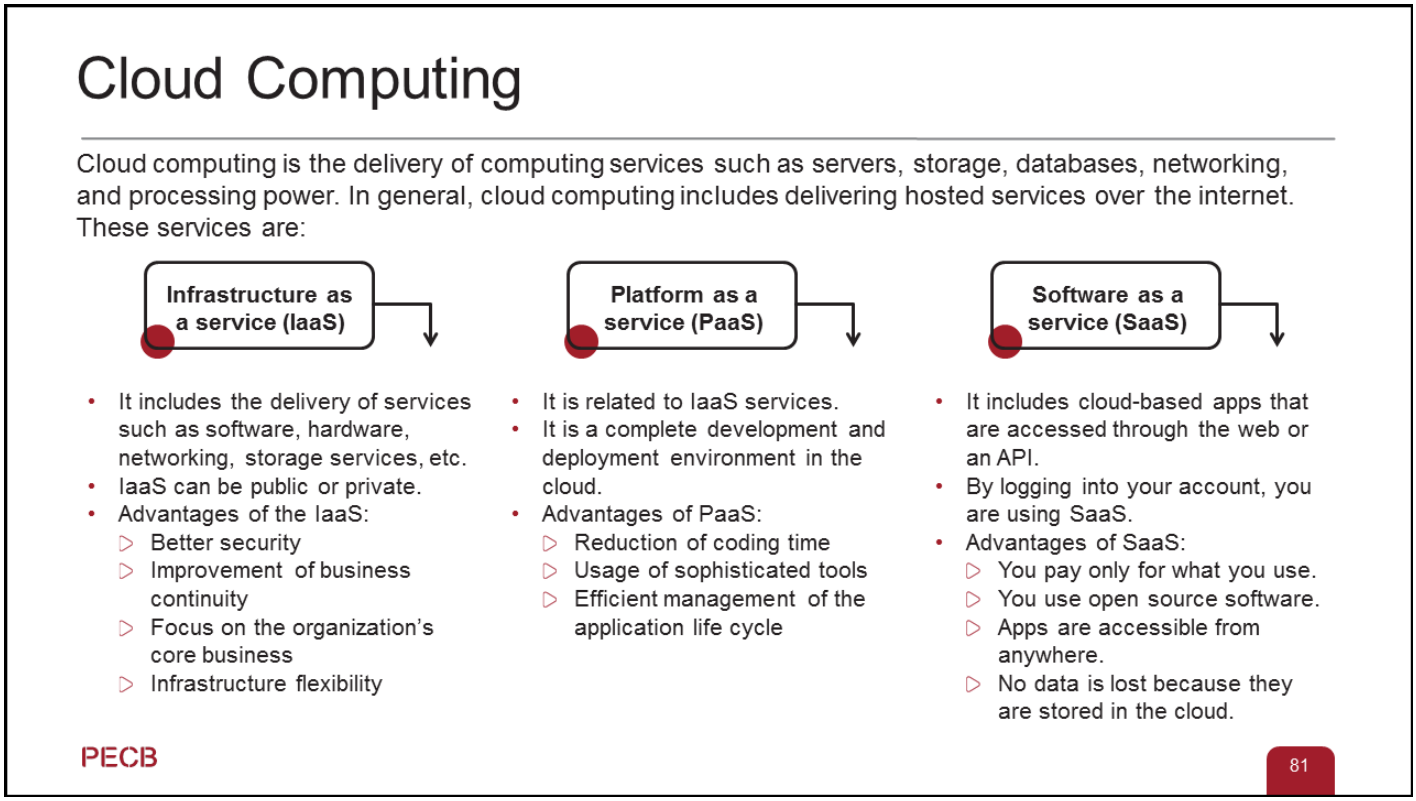
There are two main types of machine learning:

- **Supervised machine learning**, which is used in the context of classification and regression. Algorithms used in supervised machine learning include logistic regression, support vector machines, etc. The aim of both classification and regression is to find the structure of the input, data so that it can produce accurate output data.
- **Unsupervised machine learning** includes clustering, representation learning, and density estimation. It groups data based only on outputs. Algorithms used in unsupervised machine learning include autoencoders, principal component analysis, and clustering. Cluster analysis is the most common method.

Machine Learning — Example

Google photos machine learning algorithm

- The Google Photos application has recently provided a new search feature that recognizes things and items within photos. It allows its users to search by generic terms such as dog, beach, sunset, etc.
- This feature is powered by Google's machine learning algorithms and operators due to the large amount of photos that are uploaded in Google Photos by users.
- The algorithm processes all of the photos and then tags what it can recognize in that photo. These tags can then be used as search inputs.
- Firstly, the algorithm attaches a score to each of the tags, then the photo that contains the tag with the highest score is displayed first when searched, and so on.



NIST SP 500-291, Chapter 3

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

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

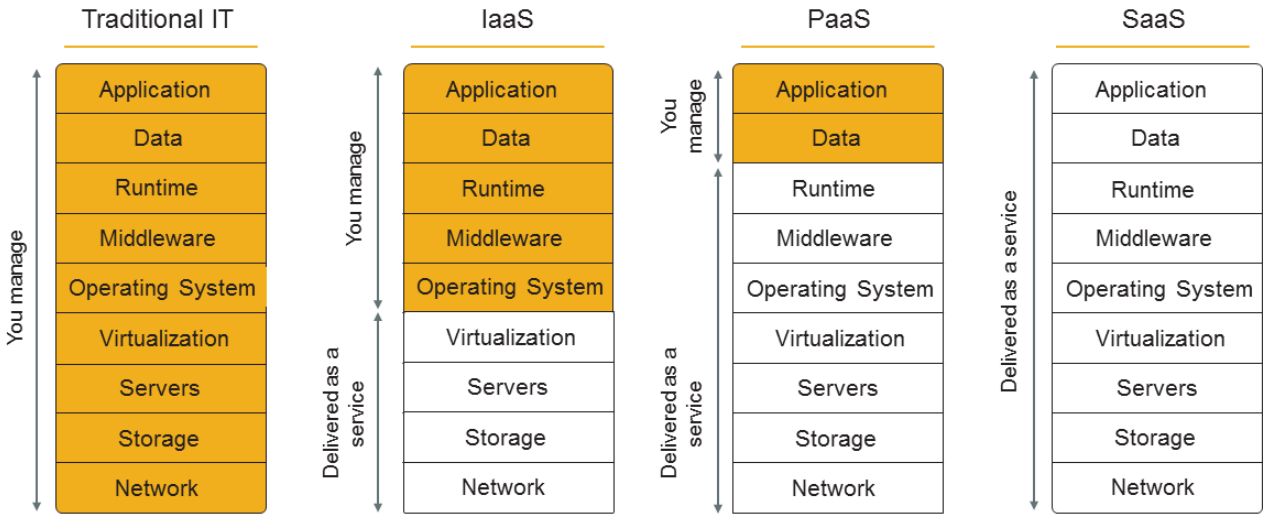
The benefits of cloud computing include:

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

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

Cloud Computing (Cont'd)

Levels of integration



PECB

82

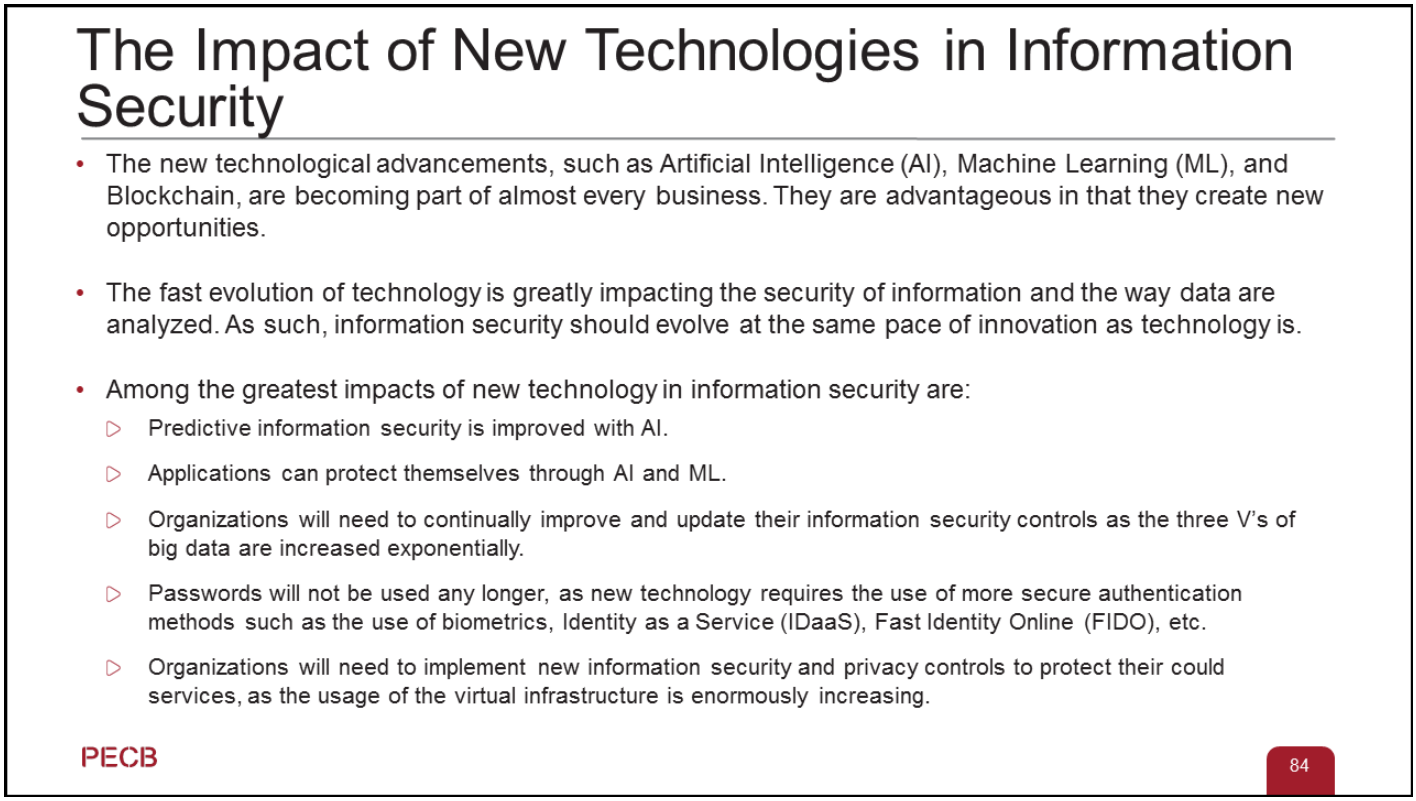
Note: The slide provides a visual representation of the services that you manage (yellow background) and the services that are delivered as a service by the cloud provider (white background).

Some examples of companies that use cloud services:

- **IaaS** is used by AWS EC2, Google Compute Engine (GCE), and Digital Ocean.
- **PaaS** is used by AWS Elastic Beanstalk, Heroku, Force.com, Apache, and Commerce Cloud.
- **SaaS** is used by BigCommerce, Google Apps, Salesforce, Dropbox, DocuSign, and Slack.

Outsourced Operations

- Outsourcing is the practice of hiring a third party (an organization or a person) to perform activities, tasks, or provide services. Organizations practice this with the purpose of focusing more on their crucial activities.
- Nowadays, organizations can outsource different kinds of services such as payroll, technical support, human resource activities, and so forth.
- Organizations outsource in order to reduce their costs, become more efficient, and focus on key business operations.



Predictive information security is an approach that uses predictive, strategic, and intelligent analytics through AI to anticipate and diagnose information security in real time. For instance, as the issues of fraud and money laundering constantly arise, machine learning models are able to automatically detect fraudulent activity with the ability to understand patterns in real time so as to stop fraud.

AI and ML play a significant role in the self-protection of applications. As humans are more likely to unintentionally leave gaps on the system, automation, in combination with AI, is the newest and most important movement of the recent years. Runtime application self-protection (RASP) will provide an extra layer of security to identify, diagnose, and protect the system at the application level, without human intervention.

The increase of the data volume, variety and velocity has caused the need to reevaluate the information security governance, taking into account big data governance and cloud computing, in order to improve the overall security of the organizations' information.

In the digital world, passwords are considered as poor tools to guarantee proper information security. As such, organizations need to implement more secure authentication methods such as IDaaS, FIDO, blockchain, etc.

1. **Which of the options below is NOT part of the three V's of big data?**
   A. Volume
   B. Velocity
   C. Voltage
2. **Structured data are based on binary data and do not have a data model.**
   A. True
   B. False
3. **Which of the following is an example of unstructured data?**
   A. MongoDB
   B. SQL (Structured Query Language)
   C. Microsoft Excel files
4. **Which of the following is a benefit of weak artificial intelligence?**
   A. Automated tasks
   B. Problem-solving
   C. Critical thinking improvement
5. **Linear regression and logistic regression are algorithms utilized by:**
   A. Machine learning
   B. Outsources operations
   C. Cloud computing

6.Which cloud computing service ensures an efficient management of the application life cycle?

A. Infrastructure as a service (IaaS)
B. Platform as a service (PaaS)
C. Software as a service (SaaS)

7.Which of the statements below regarding cloud computing is NOT true?

A. Cloud computing reduces the costs needed to manage and maintain the network system
B. Cloud computing promotes security of information because data can be accessed no matter what happens to the machine
C. Cloud computing requires too many tasks, such as software patching, hardware setup, and “racking and stacking”

8.Which services are delivered by the cloud provider when using Infrastructure as a Service (IaaS)?

A. Virtualization, servers, storage, network
B. Virtualization, servers, application, data, network
C. Application, data, runtime, middleware, operating system

9.New technologies do not require the use of more secure authentication methods since passwords are good enough to guarantee information security.

A. True
B. False

10.Which of the statements below is correct?

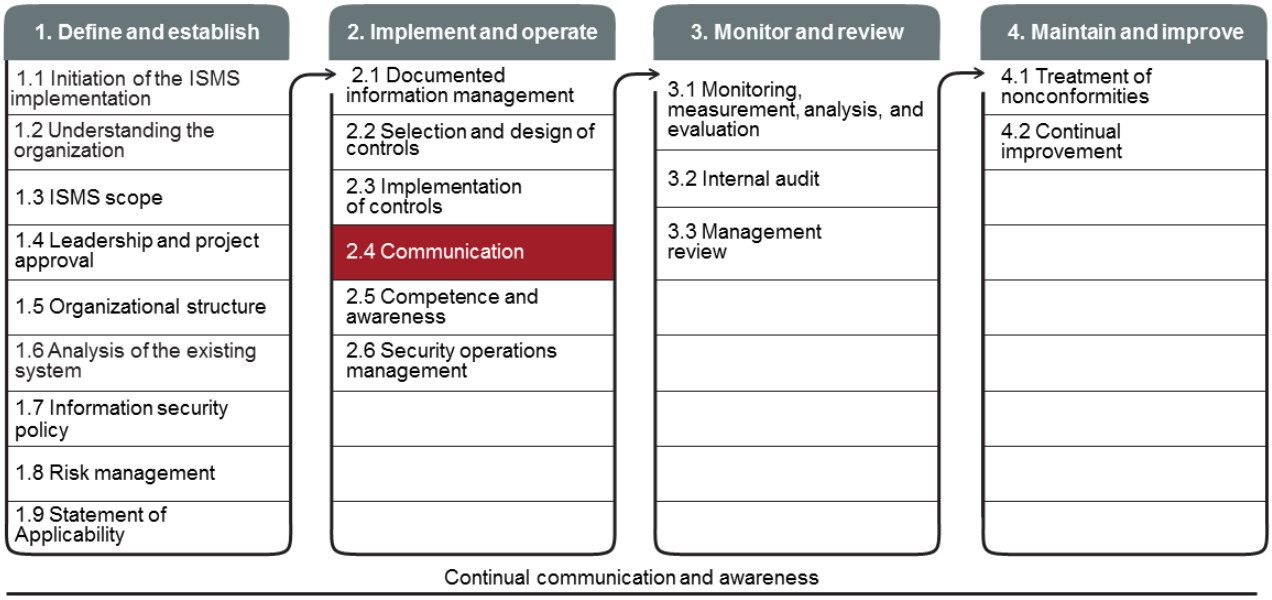
A. Machine learning is synonymous to artificial intelligence and the terms can be used interchangeably
B. Machine learning includes the delivery of hosted services over the internet
C. There are two types of machine learning: supervised machine learning and unsupervised machine learning

Section summary

- Big data, artificial intelligence, machine learning, and cloud computing are among the most well-known trends and technologies of today's data-driven world.
- Big data includes a large volume of structured and unstructured data.
- The three V's of big data represent the volume, variety, and velocity of data.
- Artificial intelligence is defined as the ability of a machine to emulate human behavior.
- Machine learning is related to AI but they are not interchangeable. The goal of ML is to let computers learn automatically.
- Cloud computing includes the delivery of hosted services over the internet. Software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) are known as cloud services.
- Despite having a great impact on the way business is conducted, the new technology has an enormous influence on information security as well. It has brought information security into another level of development and evolution.

This section provides information that will help the participants gain knowledge about the communication plan, including the principles of an efficient communication strategy, how to establish communication objectives and identify interested parties, and how to perform and evaluate a communication activity.

2.4 Communication



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.4

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the processes by which communication shall be effected.

PECB

90

An organization wishing to conform to the requirements of ISO/IEC 27001 should:

1. Identify the skills that employees need to ensure the proper functioning of the ISMS
2. Provide a training program for the employees that are involved directly or indirectly in the ISMS implementation
3. Provide an awareness program on information security appropriate to different interested parties
4. Provide a communication program to inform all interested parties about the ISMS and the changes that may affect them
5. Evaluate the effectiveness of actions taken and keep records

Slide Notes Extension

PECB

91

ISO/IEC 27003, clause 7.4 Communication

Guidance

Communication relies on processes, channels and protocols. These should be chosen to ensure the communicated message is integrally received, correctly understood and, when relevant, acted upon appropriately.

Organizations should determine which content needs to be communicated, such as:

a. *plans and results of risk management to interested parties as needed and appropriate, in the identification, analysis, evaluation, and treatment of the risks;*
b. *information security objectives;*
c. *achieved information security objectives including those that can support their position in the market (e.g. ISO/IEC 27001 certificate granted; claiming conformance with personal data protection laws);*
d. *incidents or crises, where transparency is often key to preserve and increase trust and confidence in the organization's capability to manage its information security and deal with unexpected situations;*
e. *roles, responsibilities and authority;*
f. *information exchanged between functions and roles as required by the ISMS's processes;*
g. *changes to the ISMS;*
h. *other matters identified by reviewing the controls and processes within the scope of the ISMS;*
i. *matters (e.g. incident or crisis notification) that require communication to regulatory bodies or other interested parties; and*
j. *requests or other communications from external parties such as customers, potential customers, users of services and authorities.*

The organization should identify the requirements for communication on relevant issues:

k.*who is allowed to communicate externally and internally (e.g. in special cases such as a data breach), allocating to specific roles with the appropriate authority. For example, official communication officers can be defined with the appropriate authority. They could be a public relations officer for external communication and a security officer for internal communication;*
l.*the triggers or frequency of communication (e.g. for communication of an event, the trigger is the identification of the event);*
m.*the contents of messages for key interested parties (e.g. customers, regulators, general public, important*

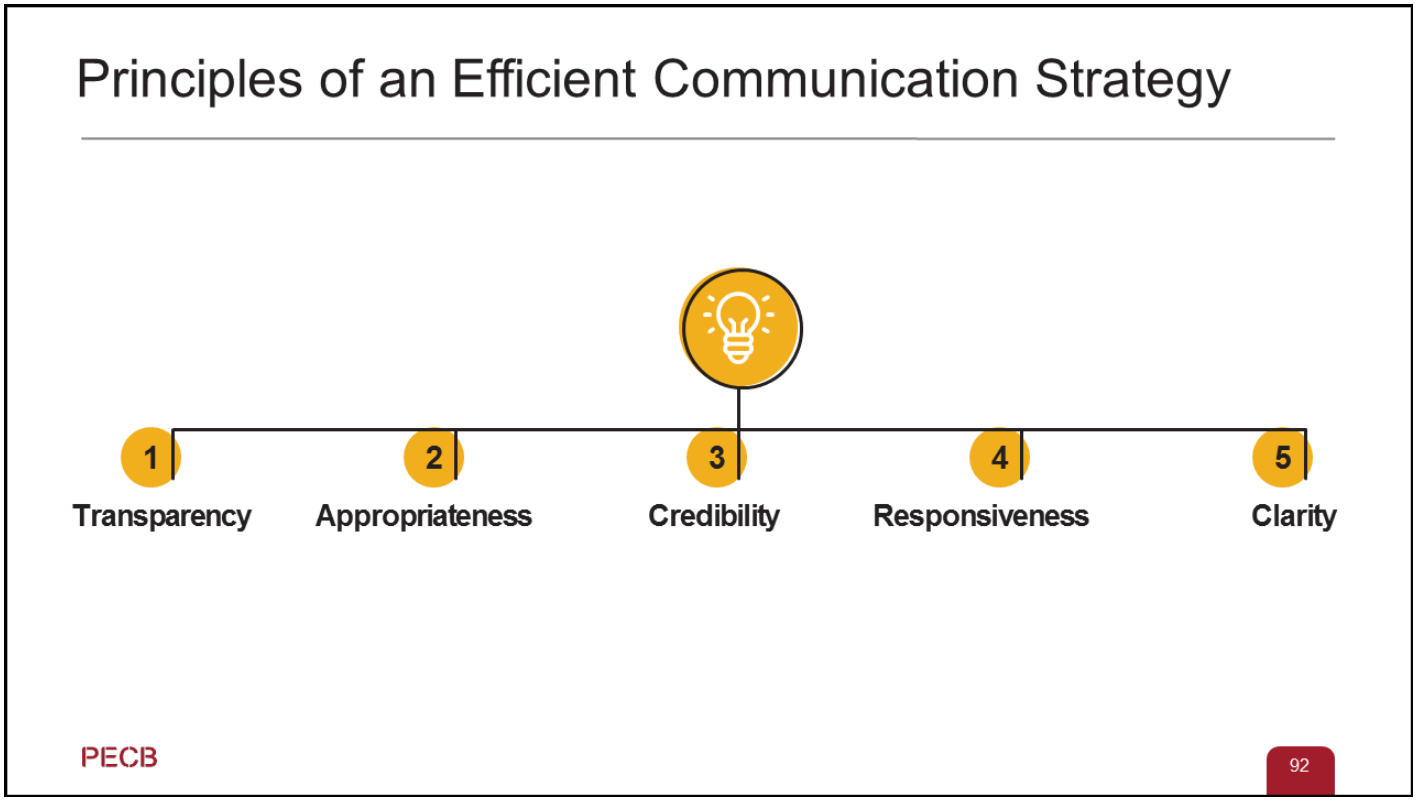
internal users) based on high level impact scenarios. Communication can be more effective if based on messages prepared and pre-approved by an appropriate level of management as part of a communication plan, the incident response plan or the business continuity plan;

n.*the intended recipients of the communication; in some cases, a list should be maintained (e.g. for communicating changes to services or crisis);*

o.*the communication means and channels. Communication should use dedicated means and channels, to make sure that the message is official and bears the appropriate authority. Communication channels should address any needs for the protection of the confidentiality and integrity of the information transmitted; and*

p.*the designed process and the method to ensure messages are sent and have been correctly received and understood.*

Communication should be classified and handled according to the organization's requirements.



Principles of an efficient communication strategy:

Transparency: Properly communicate the processes, procedures, methods, data sources, and assumptions used to all interested parties, taking into account the confidentiality of information

Appropriateness: Provide relevant information to interested parties, using formats, language, and media that meet their interests and needs, enabling them to participate fully

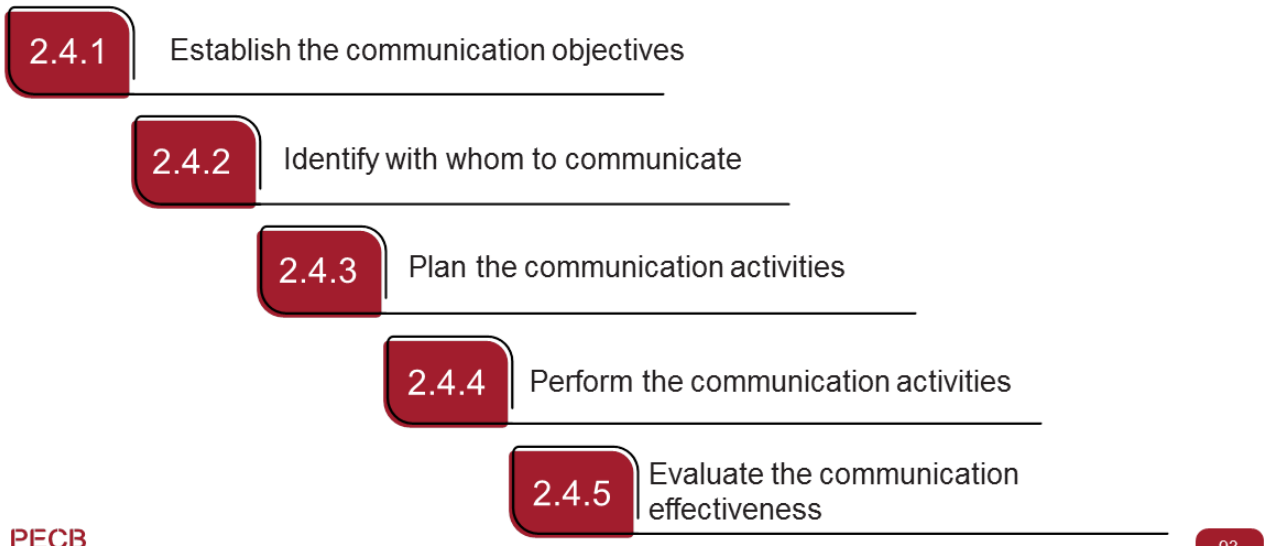
Credibility: Conduct communication in an honest and fair manner, and provide information that is truthful, accurate, and substantive; develop information and data using recognized and reproducible methods and indicators

Responsiveness: Respond to the queries and concerns of interested parties in a full and timely manner; make interested parties aware of how their queries and concerns have been addressed

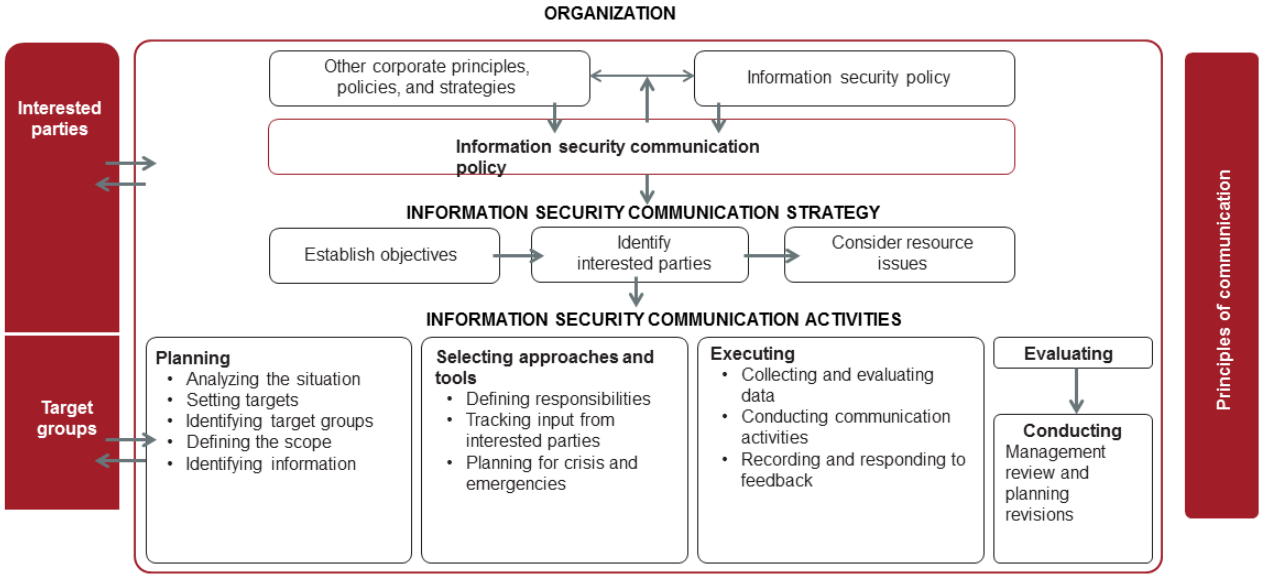
Clarity: Ensure that communication approaches and language are understandable to interested parties in order to avoid ambiguity

2.4 Communication

List of activities



Information Security Communication Process



PECB

2.4.1 Establish the Communication Objectives

Examples

- Improving the organization's credibility and reputation
- Establishing ongoing dialogue on information security matters with interested parties
- Complying with applicable legal requirements and with other requirements to which the organization subscribes
- Influencing public policy on information security issues
- Providing information and encouraging the understanding of information security activities by interested parties
- Meeting the expectations of interested parties in terms of information security

Communication is crucial in achieving the ISMS objectives.

PECB

95

An organization should set information security objectives that can provide the basis for an effective communication strategy. When setting its information security communication objectives, the organization should ensure that they are aligned with its information security policy, have taken into account the views of internal and external interested parties, and are consistent with the communication principles. Upon setting objectives for its communication activities, the organization should consider its priorities and desired results, making sure that the objectives defined are expressed in such a way that no further explanations are necessary.

The organization's top management should develop a strategy to implement the communication plan. The strategy should include communication objectives, identification of interested parties, an indication of when and what it plans to communicate, and the top management's commitment to allocate adequate resources. The organization should clarify what is possible, taking into account its resources, so that it can most realistically meet the expectations of interested parties.

Consideration should be given to the fact that information security communication is part of the organization's activities in general, and should be aligned with other elements of the management system, policies, strategies, or relevant activities.

Slide Notes Extension

PECB

96

The following questions can serve as guide when developing the communication strategy:

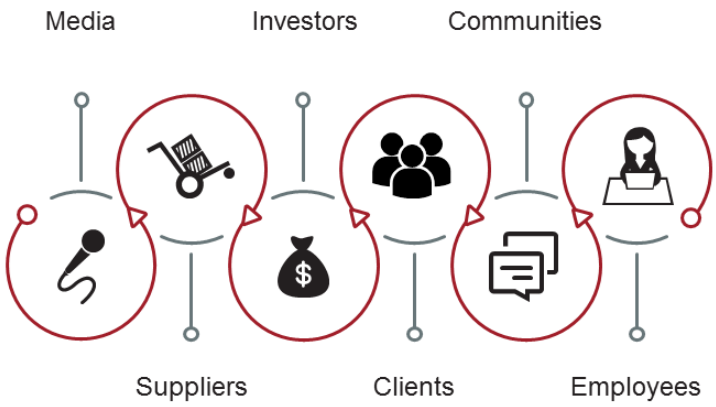
1. Why is the organization engaging in information security communication?
2. Who is the target audience?
3. What are the organization's key information security issues and impacts?
4. What are the main issues to be covered, messages to be conveyed, and communication techniques, approaches, tools, and channels to be used?
5. How much time is needed to implement the strategy?
6. How will the strategy involve and coordinate the information security managers, interested parties, individuals responsible for information security issues and individuals who are responsible for the organization's internal and external communication?
7. What are the local, regional, national, and international boundaries for the strategy?

Once defined, the strategy should be approved by top management and used as the basis for the organization's information security communications activities.

An organization's information security communication activities are dependent on the available resources. The information security communication strategy should include an allocation of human, technical, and financial resources, as well as designated responsibilities and authority and defined actions. Employees' experience and training needs should also be considered.

2.4.2 Identify with Whom to Communicate

Adaptation of the communication plan



PECB

97

Engagement with interested parties provides an opportunity for the organization to understand its issues and concerns; it can lead to enhanced knowledge gained by both sides, and can influence opinions and perceptions. When done properly, any particular approach can be successful and satisfy the needs of the organization and interested parties.

In some cases, understanding the communication pattern and the behavior of each interested party (or target group) is also important in communication. The most effective communication processes involve ongoing contact by the organization with internal and external interested parties as part of the organization's overall communication strategy.

When developing the information security communication strategy and setting objectives, the organization should identify internal and external interested parties who have expressed interest in its activities, products, and services. It should also identify other potential interested parties with whom it wishes to communicate, in order to achieve the overall objectives of its information security communication strategy.

2.4.3 Plan the Communication Activities

Key for success

- An organization should decide its goals and intentions by means of information security communication activities.
- The established targets should be specific, measurable, achievable, realistic, time-bound, and consistent with the information security communication objectives.
- The organization should anticipate information security issues of concern and communicate them with the interested parties.

This will allow the organization to evaluate the information security communication activity and determine whether the targets have been met or not.

PECB

98

Organizations will typically undertake a range of information security communication activities in implementing their information security communication plan. In advancing the information security communication strategy and objectives, specific information security communication activities should be developed, taking into account the information security issue, geographic boundaries, and the interested parties.

The development or improvement of an information security communication activity begins with an understanding of the context for the communication.

In the situational analysis, the organization should consider the following issues:

- Identification and understanding of issues of concern to interested parties
- Expectations and perceptions of the interested parties about the organization
- Information security awareness of interested parties (e.g., local communities)
- Communication media and activities that have proven to be the most effective in communicating with interested parties in similar situations
- Identification of the leaders' opinion and their influence on issues related to information security communication
- Public (or even internal) image of the organization
- Latest developments and trends on information security issues related to the organization's specific context

When evaluating the context for an information security communication activity, it is also important to consider the potential costs and consequences of not communicating. Such consequences can be material; they can cost more than information security communication in the long run, and also impose other costs on an organization, e.g., damage to reputation.

In planning an information security communication activity, the organization should identify the target groups among its interested parties. Good communication involves a range of possible target groups.

Slide Notes Extension

PECB

99

It is common to identify conflicting interests among different target groups. As a result, the information security communication activities need to address and respond to different and often conflicting demands from target groups, in particular those that are the most influential, and who may negatively impact the outcomes of an information security communication activity.

The organization should anticipate information security issues of concern to interested parties. This will help collecting information security impacts and performances of its products, services, processes, and activities. Based on the targets set for an information security communication activity, appropriate quantitative and qualitative data and information can be selected or generated. Such information should be aligned to current standards and guidelines on information security performance and performance indicators.

2.4.4 Perform the Communication Activities

Communication approaches and tools

Communication can be carried out using the following approaches and tools:

- Websites
- Reports
- Brochures and newsletters
- Posters
- Emails
- Newspaper articles
- Press releases
- Advertisements

- Public meetings
- Focus groups
- Surveys
- Workshops and conferences
- Media interviews
- Presentation to groups

PECB

100

The organization's approach to information security communication will be influenced by whether it wants to consult, understand, inform, persuade, or involve target groups.

It is important to note that information security communication is a dynamic process, and that there is an ongoing change among target groups, as well as within organizations.

In choosing the approaches to communication, it is important to consider the needs and the degree of interest of the target groups involved in the communication activity have in regard to the issues covered. In addition, it is equally important to consider how active the organization wishes to be in its communication. There are different approaches to communication, depending on the activity or passivity of the organization and its target groups, the resources available, and on the organizational resilience communication objectives of the organization and its target groups.

The organization should tailor the information it provides, consistent with initial planning, for target groups. The information should:

a. Consider behavioral aspects, as well as the social, cultural, educational, economic, and political interests of target groups
b. Use appropriate language
c. Make use of visual images or electronic media, where appropriate
d. Be consistent with the selected approach and, where relevant, with other information on information security issues previously communicated by the organization

The organization may wish to test its means of information provision prior to making any public communication. Opinion research that focuses on testing of information provision can help identify areas that need more explanation or clarification, key issues, questions that need to be addressed, etc.

2.4.5 Evaluate the Communication Effectiveness

- The organization should allow the necessary time for the information security communication to be effective.
- The time needed depends on the nature of the communication, the number of interested parties and their concerns, and the type of media used.
- The organization should review and assess the effectiveness of its information security communication.

PECB

101

When evaluating the effectiveness of the communication, the organization should consider the following:

- Its information security policy
- How the principles of communication are applied
- Whether its objectives and targets have been achieved
- The quality and appropriateness of the information provided to target groups
- The way in which the information security communication is conducted
- The responses of the interested parties
- Whether the communication program has fostered effective and meaningful dialogue with target groups
- Whether the procedures and approaches were transparent
- Whether information security communication addresses the needs of the target groups
- Whether target groups know that they were heard and were made aware of how their input was to be used
- Whether target groups understood the purpose and content of the information security communication
- Whether appropriate follow-up was provided for the issues raised by target groups

Communication and Reporting

Example of form

Project name		Project number	
Individual responsible	<Name>	Date	18.10.2019

Communication	Stakeholder 1	Stakeholder 2	Stakeholder 3
Approach to communication*			
Main interest and subjects			
Current status (Supporter/Neutral/Opponent)			
Required support (High/Medium/Low)			
Proposed project role (if existing)			
Proposed actions			
Required notices			
Actions and further communication channels			

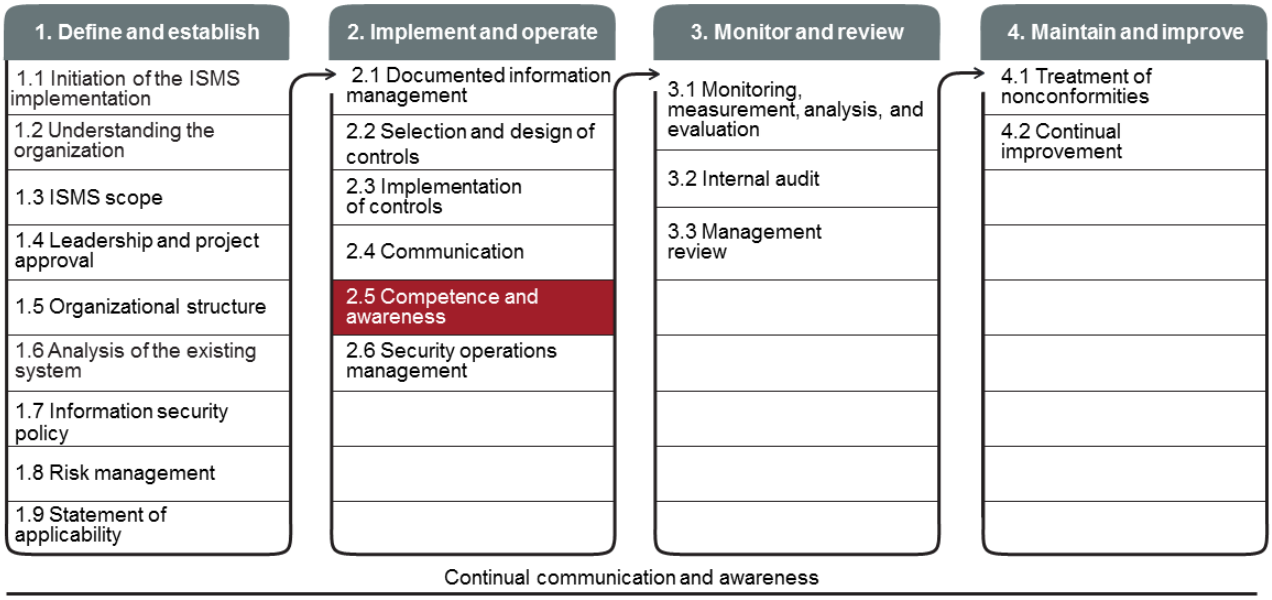
1. **What information aspect can transparency compromise in an efficient communication strategy, if not done properly?**
   A. Ambiguity
   B. Confidentiality
   C. Accuracy
2. **What do communication objectives reflect?**
   A. The information security objectives
   B. The organizational structure objectives
   C. The ISMS scope objectives
3. **The information security communication approach is impacted by whether it wants to consult, understand, inform, or involve target groups.**
   A. True
   B. False
4. **Why should an organization provide a communication program?**
   A. To integrate the ISMS into existing processes
   B. To obtain management support for the ISMS
   C. To inform all interested parties about the ISMS and the changes that may affect them
5. **Which of the following is NOT an information security communication objective?**
   A. Improving the credibility and reputation of the organization
   B. Enhancing information security risks
   C. Influencing public policy on information security issues

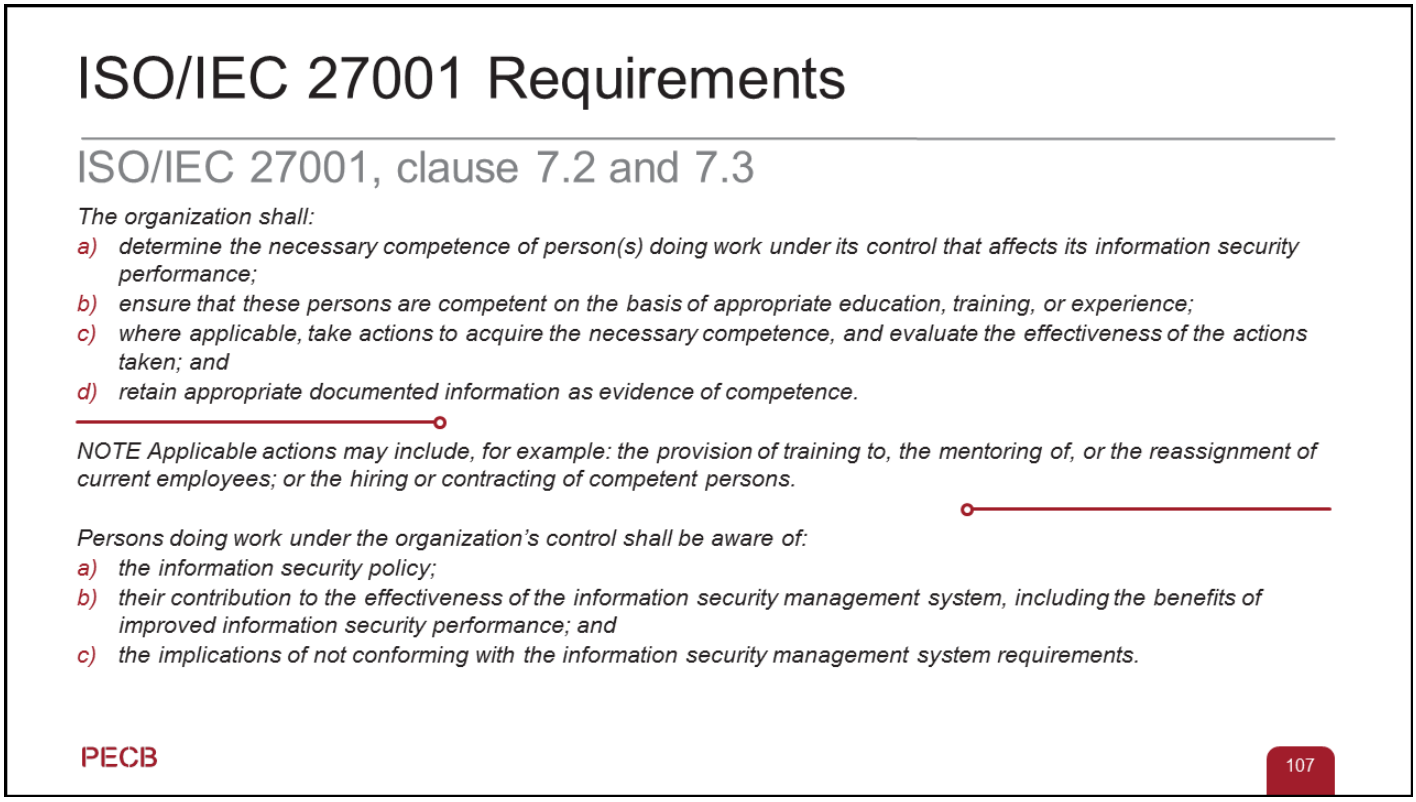
Section summary

- The organization shall determine what, when, and with whom to communicate regarding the ISMS.
- A communication program should provide a transparent, credible, clear, and appropriate communication.
- To implement a communication plan, the organization should establish the communication objectives, identify the interested parties, plan and perform communication activities, and evaluate the effectiveness of the communication.

This section will help the participants to gain knowledge on the competence development activities such as training and awareness plans, their development, implementation, and evaluation.

2.5 Competence and Awareness





An organization wishing to conform to the requirements of ISO/IEC 27001 should:

1. Identify the skills that its employees need to ensure the proper functioning of the ISMS
2. Provide a training program for the employees that are directly or indirectly involved in the implementation of the ISMS
3. Provide an awareness program on information security appropriate to the different interested parties
4. Provide a communication program to inform all interested parties about the ISMS and the changes that may affect them
5. Evaluate the effectiveness of the actions taken and keep records

ISO/IEC 27003, clause 7.2 Competence

Guidance

The organization should:

a. *determine the expected competence for each role within the ISMS and decide if it needs to be documented (e.g. in a job description);*
b. *assign the roles within the ISMS to persons with the required competence either by:*
    1. *identifying persons within the organization who have the competence (based e.g. on their education, experience, or certifications);*
    2. *planning and implementing actions to have persons within the organization obtain the competence (e.g. through provision of training, mentoring, reassignment of current employees); or*
    3. *engaging new persons who have the competence (e.g. through hiring or contracting);*
c. *evaluate the effectiveness of actions in b) above;*
d. *verify that the persons are competent for their roles; and*
e. *ensure that the competence evolves over time as necessary and that it meets expectations.*

Slide Notes Extension

PECB

108

ISO/IEC 27003, clause 7.3 Awareness

Guidance

The organization should:

c.*prepare a programme with the specific messages focused on each audience (e.g. internal and external persons);*
d.*include information security needs and expectations within awareness and training materials on other topics to place information security needs into relevant operational contexts;*
e.*prepare a plan to communicate messages at planned intervals;*
f.*verify the knowledge and understanding of messages both at the end of an awareness session and at random between sessions; and*
g.*verify whether persons act according to the communicated messages and use examples of 'good' and 'bad' behaviour to reinforce the message.*

Competence and People Development

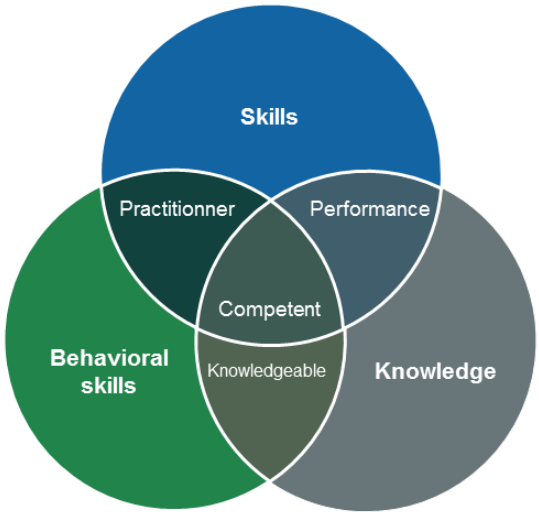
ISO 9000, clause 3.10.4 and ISO 10015, clause 3.2

Competence

Ability to apply knowledge and skills to achieve intended results

People development

Encouragement of employees to acquire new or advanced competence by creating learning and training opportunities with circumstances to deploy the outcomes that have been acquired



PECB

109

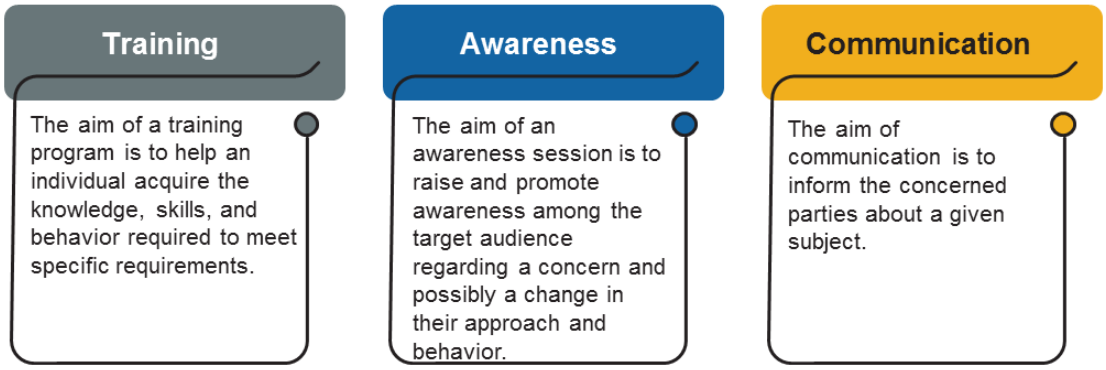
A systematic and planned training program can help the organization increase its capability and conform to its information security objectives.

ISO 10015, clause 5.4.1

Teams, groups and individuals should be encouraged to engage in competence management and people development planning activities to increase engagement and ownership.

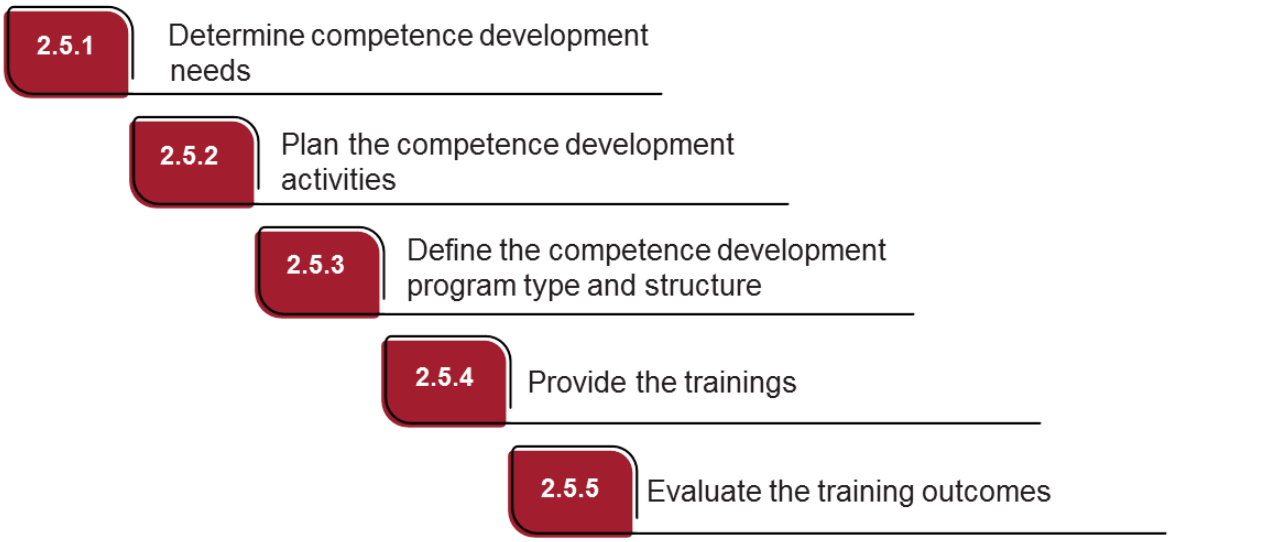
Training, Awareness, and Communication

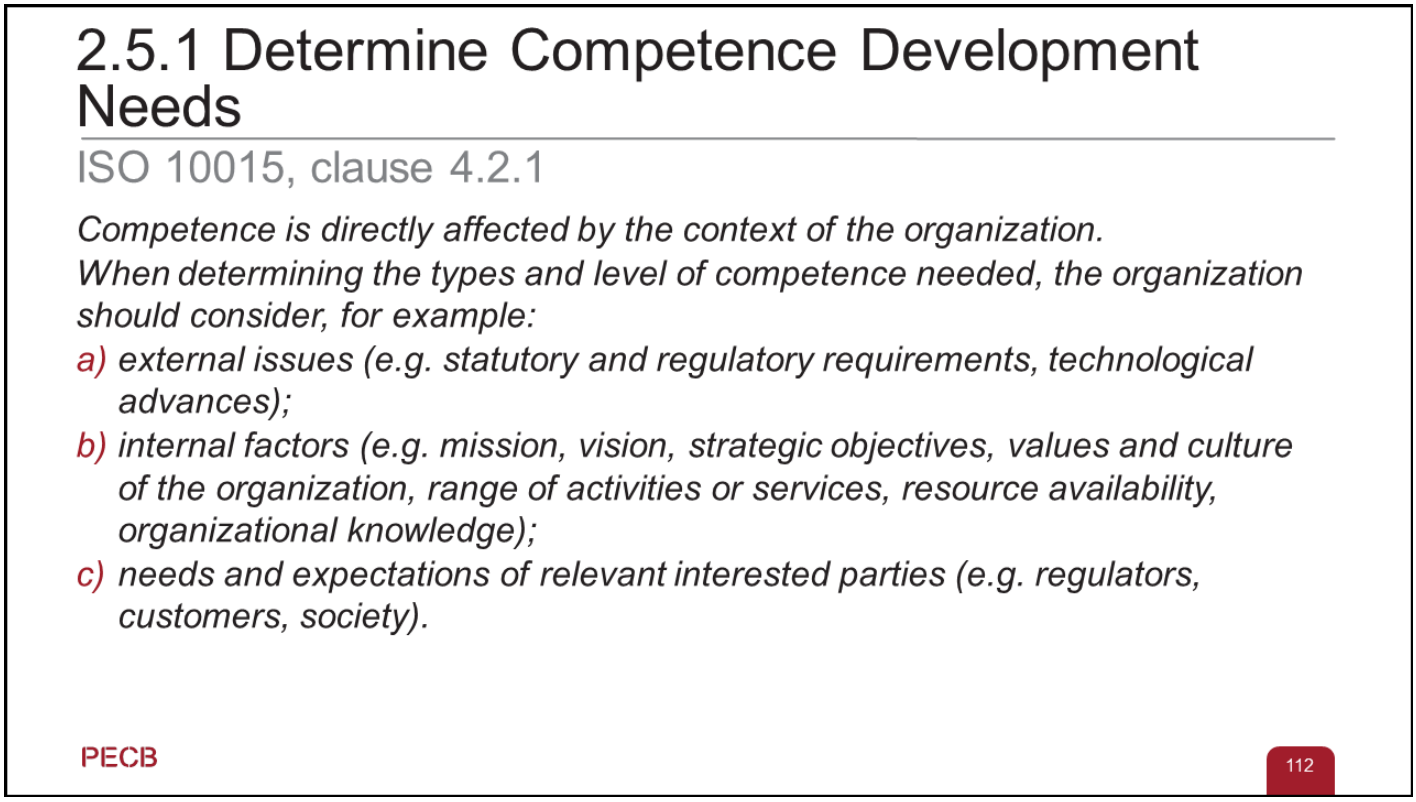
Differences



2.5 Competence and Awareness

List of activities





ISO 10015, clause 4.2.1 Organizational competence (cont'd)

Documented information should be maintained and/or retained as appropriate to support and demonstrate:

- *competence needs:*
  - *organizational related to the organization;*
  - *team (established team or more informal group training achievements);*
  - *individual (qualifications, performance/appraisal outcomes);*
- *development programmes and other initiatives;*
- *evaluation of the impact of competence development and associated actions.*

ISO 10015, clause 4.2.2 Team or group competence

Within the organization, different teams or groups will need different competences according to the activities they perform and the intended results.

When determining differing team or group needs, the organization should consider:

a. *leadership;*
b. *team or group objectives and intended results;*
c. *activities, processes and systems;*
d. *structure of the team or group: hierarchy, number of people, and roles and responsibilities;*
e. *team or group culture and the ability to co-operate, collaborate and cultivate respect.*

ISO 10015, clause 4.2.3 Individual competence

Individual competence requirements should be determined at all levels of the organization to ensure each different role or function is effective.

To determine individual competence, the organization should consider:

a. *external competence requirements;*
b. *roles and responsibilities;*
c. *activities related to roles or function;*
d. *behaviours (e.g. emotional intelligence, ability to remain calm in a crisis, ability to maintain concentration*

during monotonous work, ability to work co-operatively within a direct team and across the organization or with customers).

Assess Current Competence and Development Needs

ISO 10015, clause 4.3

The organization should review its current competence levels against required competence needs as determined in 4.2 at the organizational, team, group and individual level to establish if or where action needs to be taken to meet competence needs.

The organization should:

a) consider existing competence levels;

b) compare these with required competence levels;

c) use risk-based thinking to prioritize actions to address competence gaps.

2.5.2 Plan the Competence Development Activities

ISO 10015, clause 5.2

When planning competence development activities, the organization should:

a) *determine specific development objectives (to address a competence gap or personal development need);*
b) *consider relevant development activities;*
c) *determine criteria to monitor and evaluate the development outputs;*
d) *consider risks and opportunities that can affect effective delivery of the development activities;*
e) *consider statutory and regulatory requirements;*
f) *determine organizational resources, including financial considerations;*
g) *determine organizational policies;*
h) *determine contractual arrangements with external providers;*
i) *determine planning and scheduling requirements;*
j) *determine an appropriate provider;*
k) *determine individual (or team/group) availability, motivation and ability.*

PECB

114

ISO 10015, clause 5.1 General

Organizational competence needs can be met by developing the competence of teams, groups and individuals. Competence needs that have been identified should be related to the development of people. Gaps such as foreseeable future competence requirements should be identified and planned for.

People development should be related to:

a. *the competence needs determined in order to achieve competence in the organization at every level;*
b. *the competence needs determined by individuals as part of their personal development goals.*

2.5.3 Define the Competence Development Program Type and Structure

Depending on the results of the assessment of employee competencies, the organization must select the type of activities needed to address those competence gaps, including:

- Training programs
- Awareness programs
- Conferences, professional forums, and other networking events
- Workshops
- Self-studies

The competence development program structure should focus on the following key points:

- The target audience
- The objective of the competence development program
- The program details (place, time, etc.)
- Closing program activities (tests, awards, certifications)

PECB

115

ISO 10015, clause 5.4.2

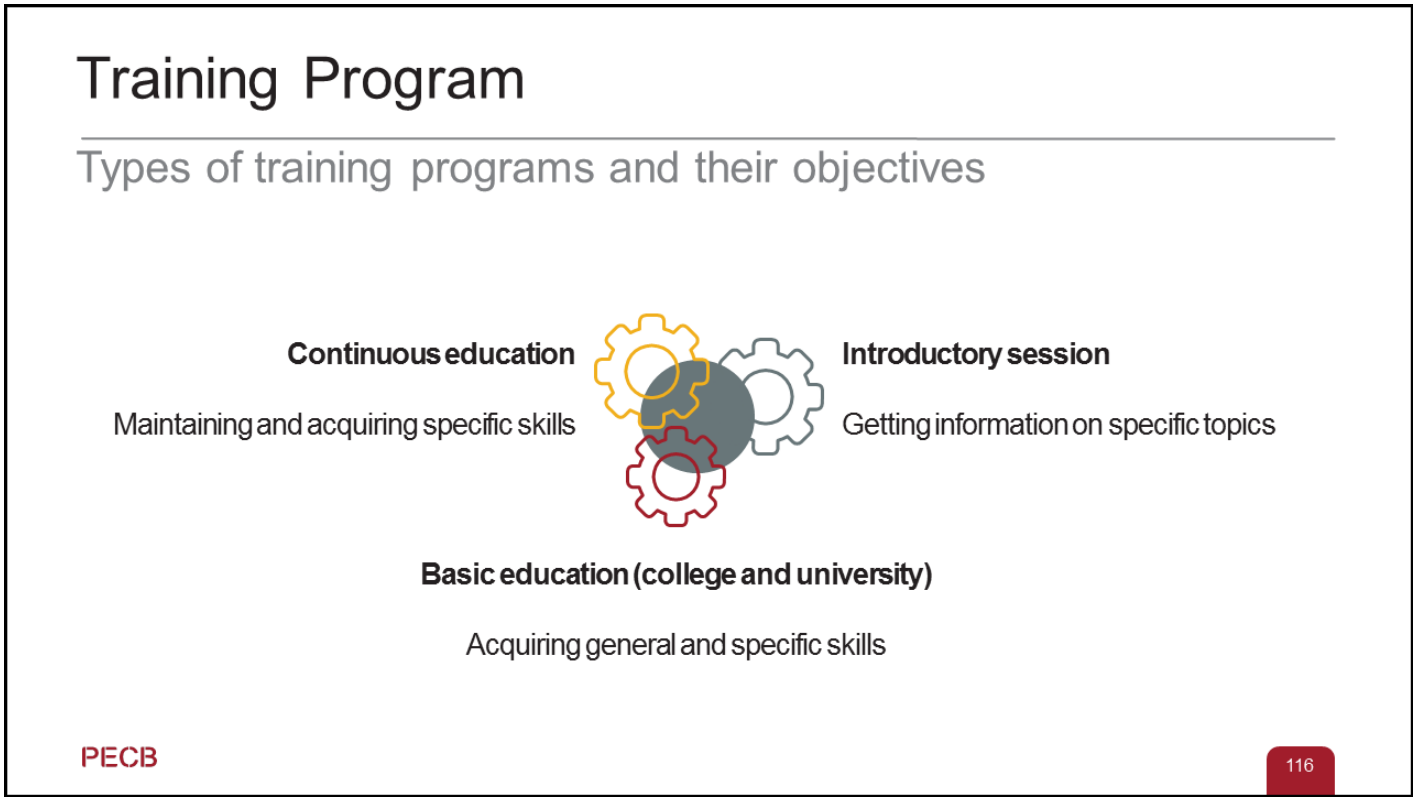
Competence management and people development activities at the team or group level should address:

a. *establishing and delivering team or group training programmes;*
b. *developing and providing a range of targeted communications (e.g. newsletters, websites, e-learning);*
c. *attending external conferences, professional forums and networking events;*
d. *liaising with relevant professional or trade bodies;*
e. *providing support structures to share knowledge and skills;*
f. *recruiting to address specific gaps;*
g. *restructuring to utilize competence within the organization in a more effective and focused way.*

ISO 10015, clause 5.3 Programme structure

The competence management and people development programme structure should include:

a. *who the target audience is;*
b. *when development objectives should be achieved (e.g. within six months or by a set date);*
c. *how specific activities are to be delivered;*
d. *where specific activities will take place;*
e. *when specific activities will take place and how long they will last;*
f. *how development will be evaluated;*
g. *how the achievement of objectives will be recognized (e.g. awards, certification).*



- The basic objective of education is to enable individuals to acquire general and specific skills. Educational programs are usually provided by colleges and universities.
- Continuous education includes all the formal and informal training activities that help maintain and acquire specific skills.
- An introductory session is a short training session that provides general information on a specific topic. The duration of this activity is usually one hour to a few days, depending on the subject and scope to which it is addressed.

A course that lasts longer helps develop a broader expertise in information security. In the recent years, many universities and colleges offer complete specialized courses in information security.

Long-term courses can provide expertise and additional specialization to certain employees who are responsible for information security on specific areas.

Basic courses provide an upgrade of basic skills in information security for all employees and other interested parties, regardless of their field of specialization or level of responsibility.

Companies such as Microsoft, CheckPoint, or Cisco have popularized the so-called professional certifications, which are usually obtained after attending a course followed by an examination. In the recent years, professional certifications in information security have been developed, independent of any publisher. These certifications can help enhance personal development and receive market recognition.

The main independent certifications in information security are:

1. For ISO/IEC 27001 professionals: ISO/IEC 27001 Lead Auditor, ISO/IEC 27001 Lead Implementer, and ISO/IEC 27005 Certified Risk Manager
2. For professional experience in information security: CISSP, CISA, and CISM
3. For new graduates: Security+, SSCP, ISMS Foundation, and COBIT Foundation

Awareness Program

An awareness program allows the organization to:

- Raise awareness regarding information security threats and how to protect from potential risks
- Ensure consistency in information security practices
- Contribute to the dissemination and implementation of its policies, guidelines, and procedures

An employee who is neither aware nor trained represents a potential risk.

PECB

117

The technological factor is one of the key parameters in the process of providing a functional management system. However, the “human” factor is equally important in ensuring its effectiveness. Humans can be as big a weakness as they are a strength. Thus, they require considerable attention. The staff should know and understand what their responsibilities are, how they can contribute to the effectiveness of the information security management system, and how they can positively affect the business.

Regarding the awareness of interested parties, the main objective of an awareness program is to reinforce or modify their behavior and attitudes and encourage them to adhere to the values of the organization.

Awareness Program

Main areas that should be addressed

- Information security policy
- Use of passwords
- Protection against viruses
- Proper use of the internet
- Risks associated with emails (spam, phishing, malicious code)
- Backup and data storage
- Social engineering
- Security incidents
- Use of encryption
- Security of laptops and smartphones
- Use of private files or systems at work
- Respect for intellectual property
- Problems related to access control
- Individual roles and responsibilities

PECB

2.5.4 Provide the Trainings

- The training provider is responsible to fulfill the requirements specified in the training plan.
- However, the organization has an important role too — that is to provide the necessary resources for the successful delivery of the training, to support both the trainer and the trainee, as well as to ensure that the training is qualitative and achieves its intended results.

PECB

119

Before the training: In this phase, the organization is responsible for providing the necessary information to the training provider such as the nature of the training and the competence gaps that have been identified during the training needs assessment.

During the training: In this phase, the organization is responsible for providing the resources needed to successfully deliver the training, such as the relevant tools, the documentation, and the required equipment.

After the training: In this phase, the organization receives feedback from the trainee and the training provider regarding the training. In addition, after the training, the person responsible within the organization should provide feedback to the managers and employees involved in the training

2.5.5 Evaluate the Training Outcomes

- The purpose of evaluating a training program is to acquire knowledge on whether its objectives have been accomplished or not.
- The evaluation of the training includes getting feedback from the trainer, trainee, and other people involved to improve the quality of the training and ensure that the training objectives have been met.

PECB

120

Kirkpatrick's four-level training evaluation model is an effective method to understand whether the training was effective and, in particular, find out what the trainees have learned from the training.

Level 1: Reaction

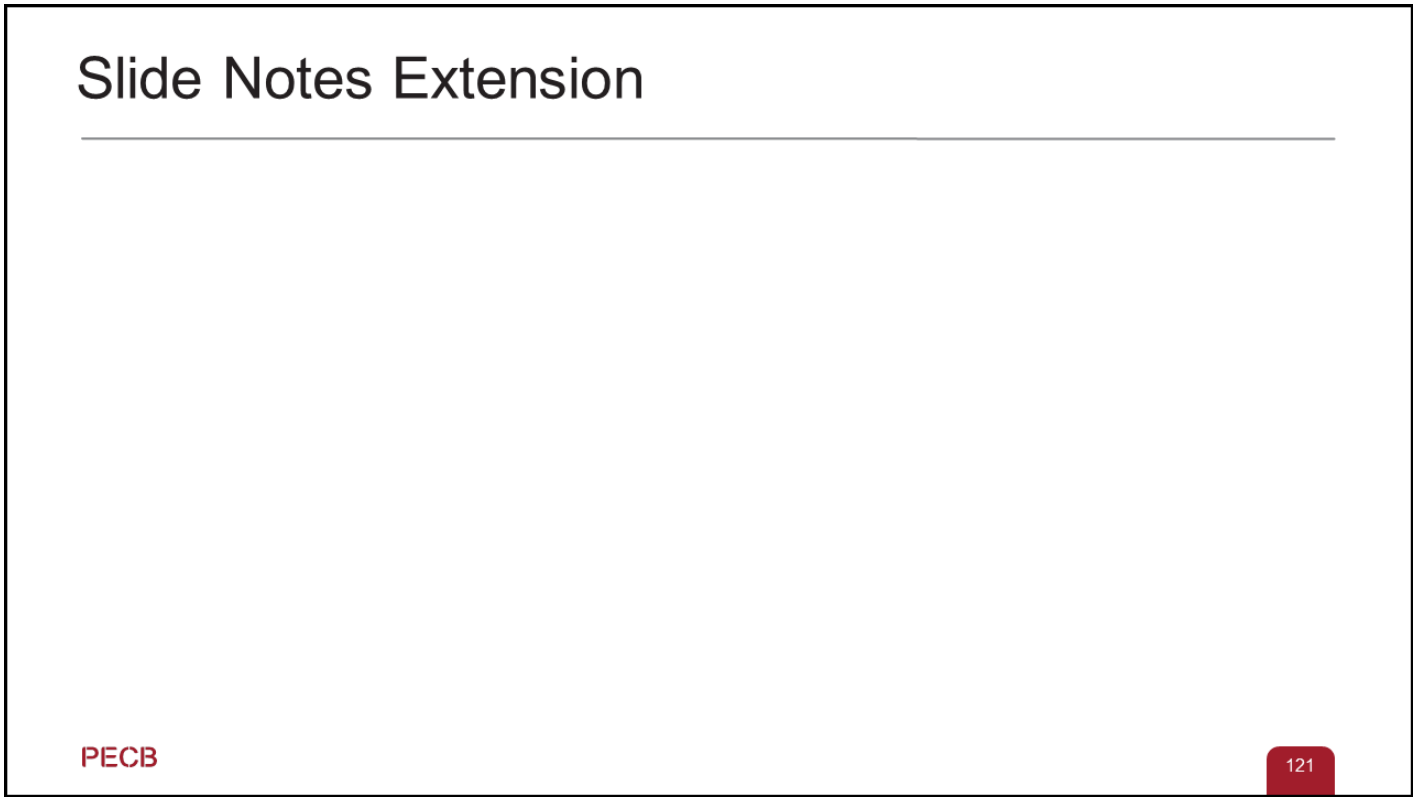
During this level, the organization measures the trainees' involvement in the training, whether they were active or not, and what their impressions of the training in general were. This will, in turn, help the organization to improve the training in the future by identifying any gaps in the training.

The organization can ask their employees that participated in the training the following questions:

1. Were you content with the training?
2. Do you think that the training was effective?
3. What were the main strengths of the training?
4. What were the main weaknesses of the training?
5. Did the training activities allow for interaction?
6. Are there any things that you learned from the training? If so, what are the most important ones?
7. Will the training help you do your work more efficiently and effectively?

Level 2: Learning

During this level, the organization evaluates the learning outcomes of the training by analyzing the trainees and what they learned from the training. The organization also evaluates whether the trainees think and act differently regarding their work after the training. If this is the case, the organization will be content with the training since it shows that it has developed the trainees' skills, behavior, and knowledge. However, it is recommended that organizations evaluate trainees in terms of their skills and knowledge before and after the training, so that the results of the training can be tangible.



Level 3: Behavior

During this level, the organization evaluates the behavior of trainees after the training. In this way, the organization determines how trainees apply the knowledge acquired in the training to their everyday work. In addition, the organization also determines where and when trainees need support. This level is important since the training's effectiveness may be seen directly by the organization.

Evaluating trainee behavior takes commitment and is an ongoing process that lasts for weeks or even months. Organizations can ask trainees the following questions in order to get some understanding on the training's effectiveness:

1. Did the trainees apply the knowledge they acquired during the training to the work?
2. Can trainees who have developed their skills, knowledge, and behavior help others?
3. Can trainees notice that their behavior has changed after the training?

The organization can both observe and interview the trainees to evaluate the training's effectiveness.

Level 4: Results

During this level, the organization evaluates the results of the training. The organization understands whether the training objectives are met and whether the trainees demonstrate that through their behavior after the training. This level is in particular difficult for the organization to identify which training objectives have been met, which benefits have been gained, and which results are linked to the training.

The organization can measure the results of the training by considering the following:

- Customer satisfaction has increased.
- Customer retention has increased.
- The production of the organization has increased.
- The employee morale has increased.
- The percentage of sales has increased.
- The quality of the products has increased.
- The number of customer complaints has decreased.

Exercise 13: Awareness and training program

e-Scooter has not conducted a training and awareness program related to information security within their company. As a result, employees were unsuccessful in preventing and responding to information security breaches.

Explain the importance of conducting training and awareness programs in an company, and propose actions that should be taken in order for the training and awareness programs to be successful and efficient.

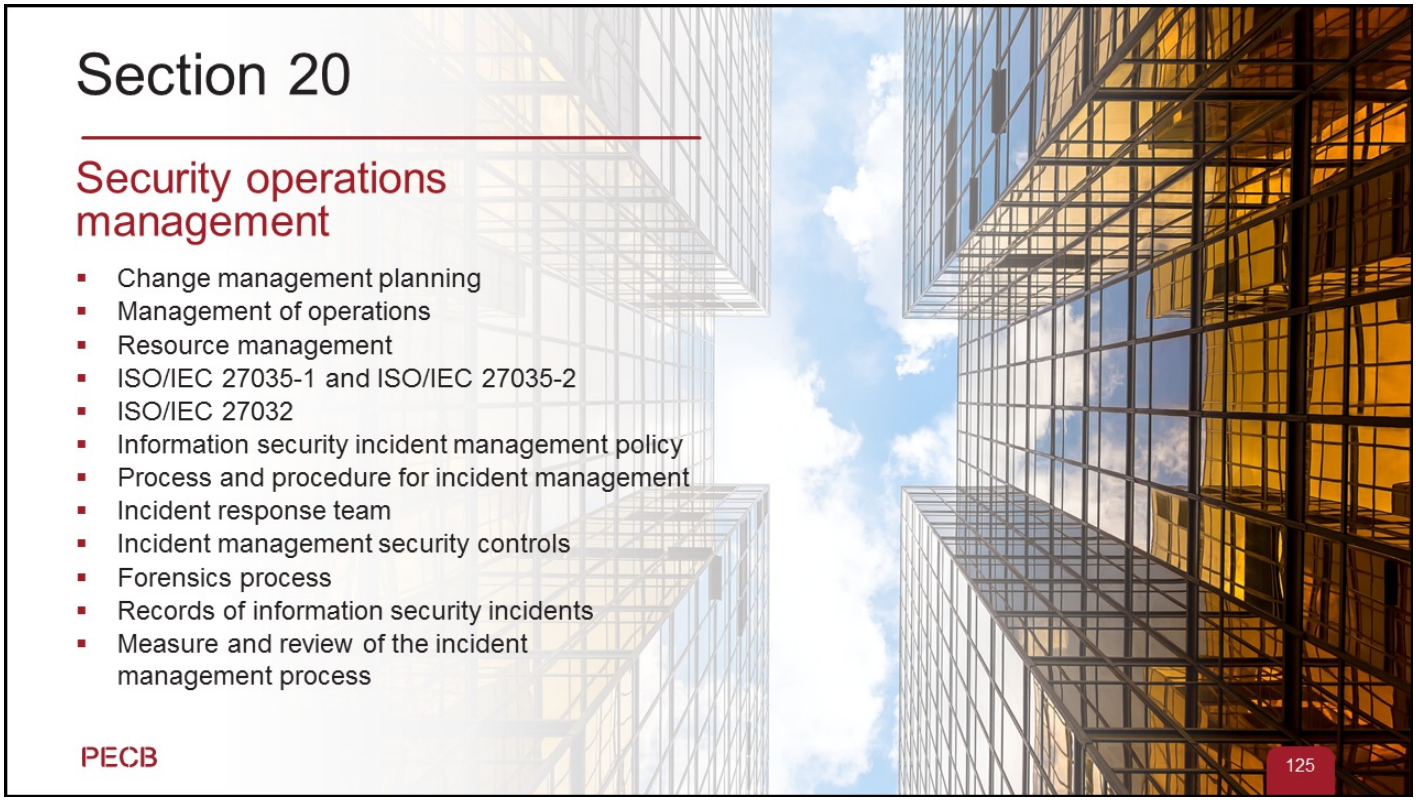
Duration of the exercise: 30 minutes

Comments: 15 minutes

1. **How can an organization ensure employee competence for the proper functioning of the ISMS?**
   A. Through appropriate education, training, or experience
   B. Through understanding the information security policy
   C. Through personal behavior
2. **What is the main objective of an ISMS training program?**
   A. To inform the interested parties about information security
   B. To promote the importance of information security within an organization
   C. To enable individuals to acquire general and specific skills related to the implementation of an ISMS.
3. **How can competence gap be identified?**
   A. Based on statutory and regulatory requirements
   B. By comparing current and required competence levels
   C. Based on the training and awareness programs output
4. **Which of the options below should be included in an awareness program?**
   A. The implementation of antivirus software
   B. Documented information required by the ISMS
   C. The use of passwords
5. **An employee has received an email with a link that, when clicked, redirects to a malicious website. The IT manager identifies the issue and immediately blocks the email forward system. What action should the organization take to prevent similar situations from recurring?**
   A. Conduct an awareness program to address social engineering and risks associated with emails
   B. Conduct a training program to inform the employees about the risks associated with phishing and spams
   C. Conduct an awareness program to address problems related to access control

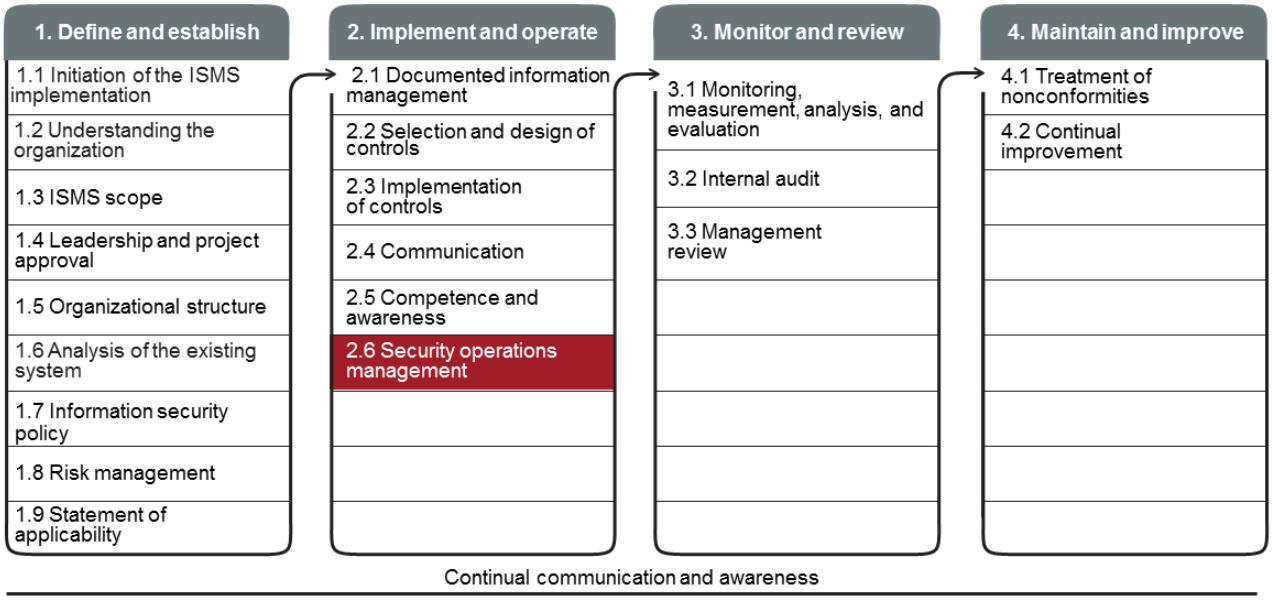
Section summary

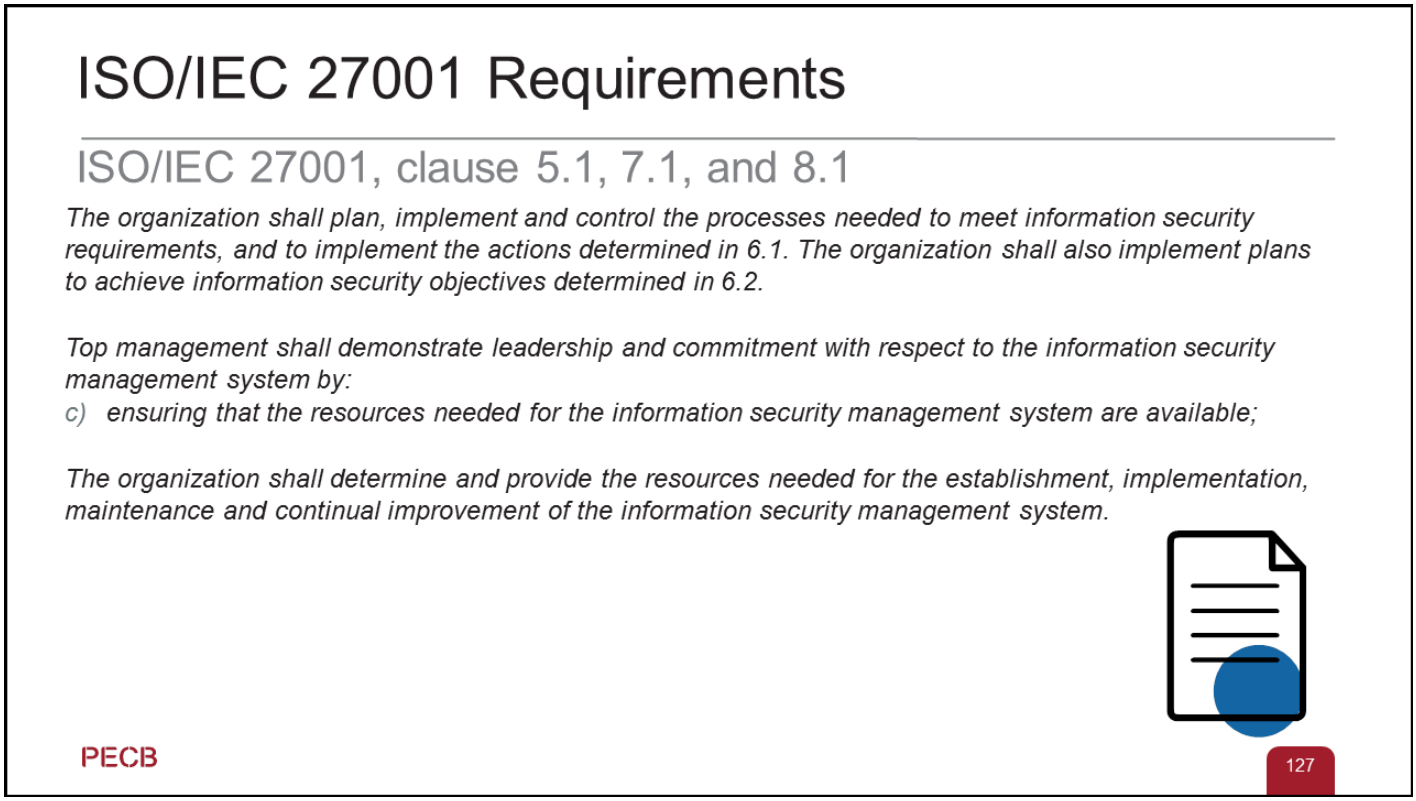
- The organization shall conduct competence development activities such as training and awareness programs for employees whose work affects the ISMS. Such regular activities help organizations conform to the information security objectives.
- Some of the steps that organizations should follow in order to comply with this requirement are:
  - Determine competence and development needs
  - Assess current competence and development needs
  - Plan competence development activities
  - Define the type and structure of the activities
  - Provide the training and awareness sessions
  - Evaluate their outcomes
- Training programs are focused on the skills needed to be acquired, while the awareness programs are focused on changing habits.
- Awareness programs ensure consistency in information security practices. Some of the areas that an awareness program should address include information security polices, the use of passwords, the risk associated with emails, the security of laptops and smartphones, etc.



This section provides information that will help the participants gain knowledge about the security operations management, including change management planning and resource management necessary to maintain the ISMS, information security incident management policy, and the incident response team.

2.6 Security Operations Management





An organization wishing to conform to the requirements of ISO/IEC 27001 should:

1. Ensure the effective management of operations related to the ISMS
2. Ensure the provision of adequate resources for the effective operation of the ISMS

ISO/IEC 27003, clause 8.1 Operational planning and control

Explanation

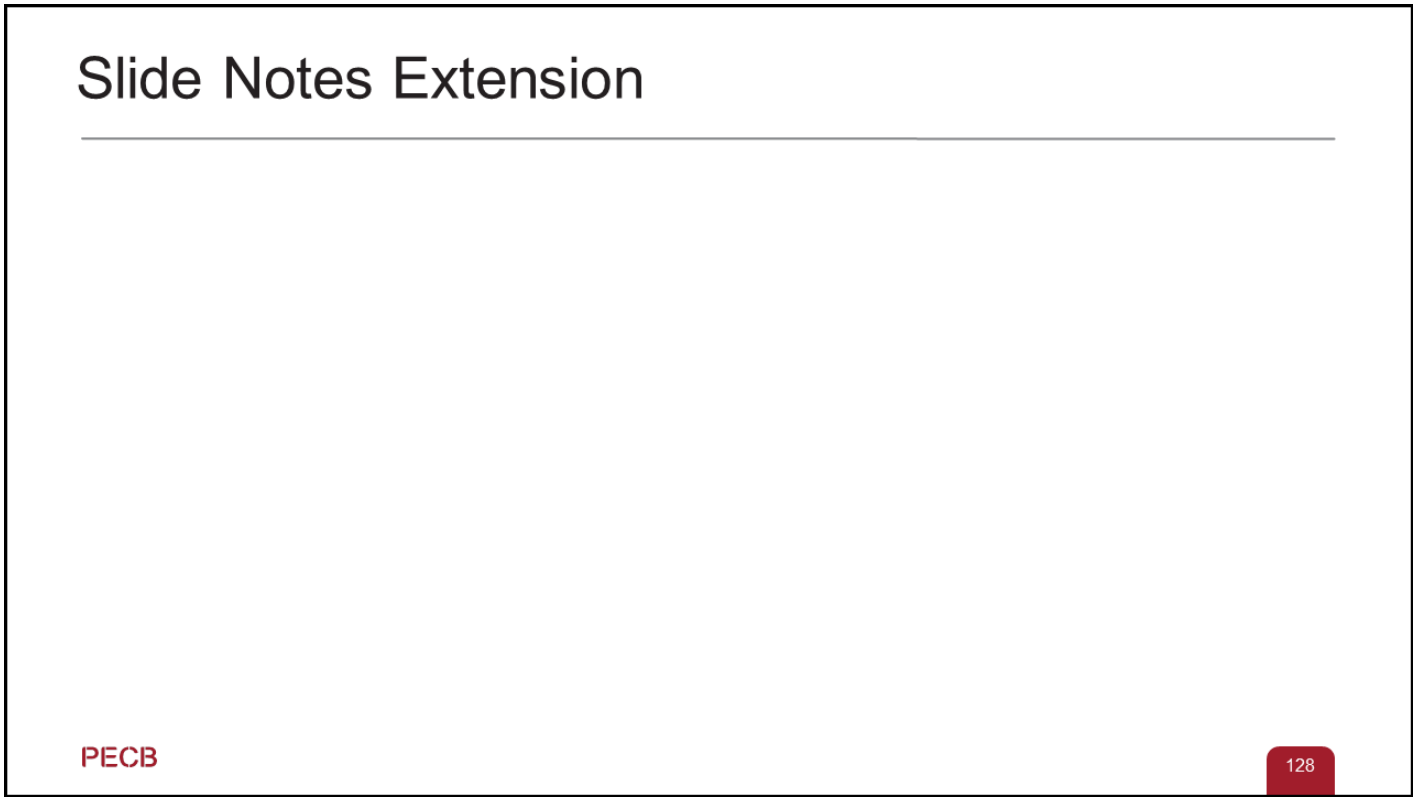
Processes to meet information security requirements include:

a. *ISMS processes (e.g. management review, internal audit); and*
b. *processes required for implementing the information security risk treatment plan.*

Implementation of plans results in operated and controlled processes.

The organization ultimately remains responsible for planning and controlling any outsourced processes in order to achieve its information security objectives. Thus the organization needs to:

> *c.determine outsourced processes considering the information security risks related to the outsourcing; and*
> *d.ensure that outsourced processes are controlled (i.e. planned, monitored and reviewed) in a manner that provides assurance that they operate as intended (also considering information security objectives and the information security risk treatment plan).*



ISO/IEC 27003, clause 5.1 Leadership and commitment

Guidance

Top management should provide leadership and show commitment through the following:

a. *top management should ensure that the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;*
b. *top management should ensure that ISMS requirements and controls are integrated into the organization's processes. How this is achieved should be tailored to the specific context of the organization. For example, an organization that has designated process owners can delegate the responsibility to implement applicable requirements to these persons or group of people. Top management support can also be needed to overcome organizational resistance to changes in processes and controls;*
c. *top management should ensure the availability of resources for an effective ISMS. The resources are needed for the establishment of the ISMS, its implementation, maintenance and improvement, as well as for implementing information security controls. Resources needed for the ISMS include:*
    1. *financial resources;*
    2. *personnel;*
    3. *facilities; and*
    4. *technical infrastructure.*
        - *The needed resources depend on the organization's context, such as the size, the complexity, and internal and external requirements. The management review should provide information that indicates whether the resources are adequate for the organization;*
d. *top management should communicate the need for information security management in the organization and the need to conform to ISMS requirements. This can be done by giving practical examples that illustrate what the actual need is in the context of the organization and by communicating information security requirements;*

ISO/IEC 27003, clause 7.1 Resources

Explanation

Resources are fundamental to perform any kind of activity. Categories of resources can include:

a. *persons to drive and operate the activities;*
b. *time to perform activities and time to allow results to settle down before making a new step;*
c. *financial resources to acquire, develop and implement what is needed;*
d. *information to support decisions, measure performance of actions, and improve knowledge; and*
e. *infrastructure and other means that can be acquired or built, such as technology, tools and materials, regardless of whether they are products of information technology or not.*

Guidance

The organization should:

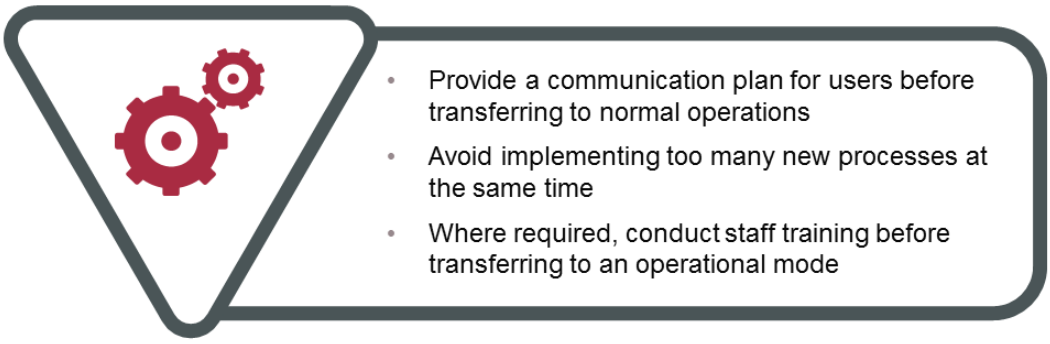
f.*estimate the resources needed for all the activities related to the ISMS in terms of quantity and quality (capacities and capabilities);*
g.*acquire the resources as needed;*
h.*provide the resources;*
i.*maintain the resources across the whole ISMS processes and specific activities; and*
j.*review the provided resources against the needs of the ISMS, and adjust them as required.*

2.6 Security Operations Management

List of activities

- 2.6.1 Plan the change management
- 2.6.2 Manage the operations
- 2.6.3 Ensure resource management
- 2.6.4 Create an information security incident management policy
- 2.6.5 Define the processes and draft the procedures
- 2.6.6 Create an incident response team
- 2.6.7 Define a forensics process
- 2.6.8 Record the information related to security incidents
- 2.6.9 Measure and review the incident management process

2.6.1 Plan the Change Management

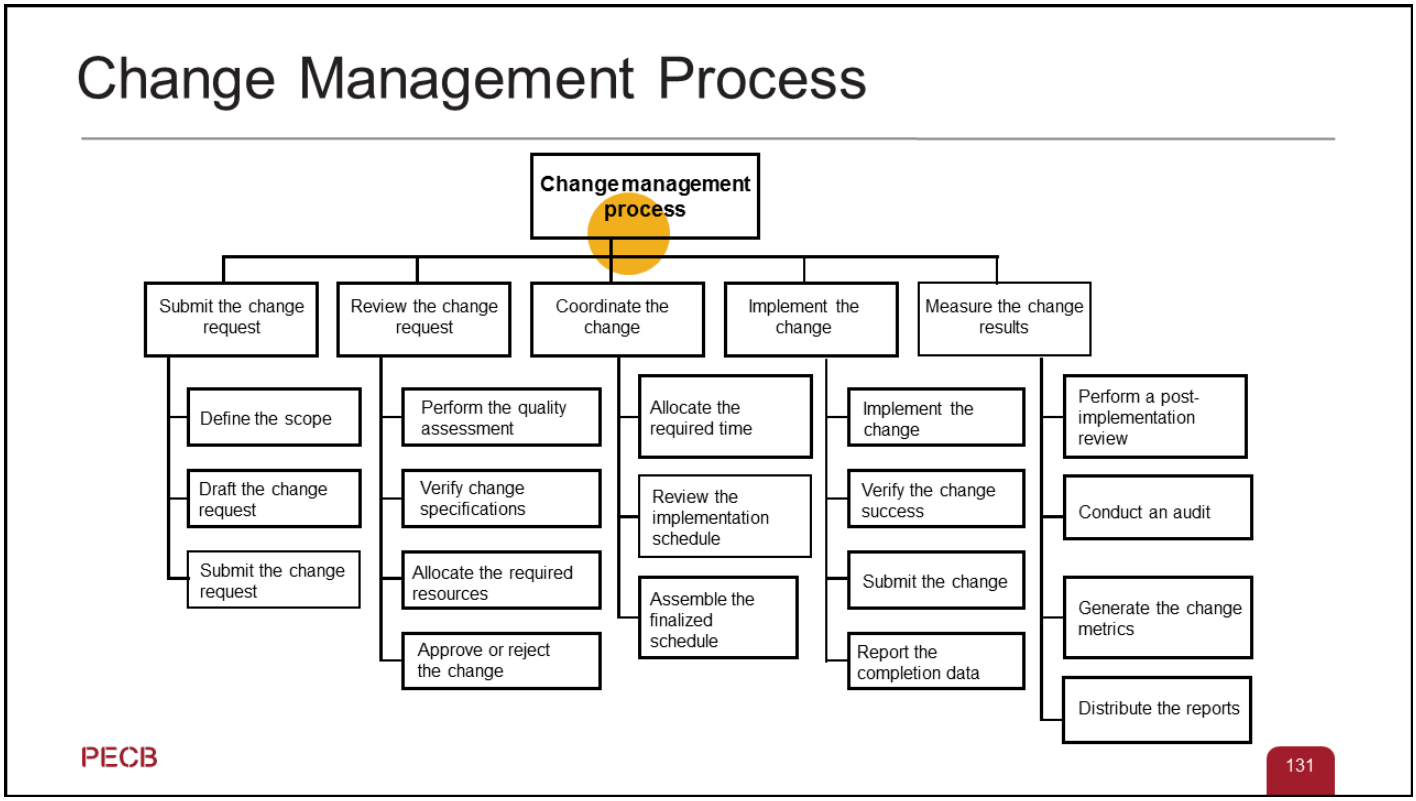


PECB

130

The steps described above are applicable to a change that has significant effect in terms of new or changed elements of the ISMS, based on materiality. However, the scale of a change may require minimal communication or training. Each change should, therefore, be judged on its own merits.

For example, when the implementation plan of an ISMS is successfully completed, the ISMS will be formally transferred into an operational mode. The materiality of this change should be decided by the organization's top management.



Submit the change request: Before preparing and submitting a change request, the requester and the personnel affected by the change should coordinate all change aspects. The changes included in the change request should be tested.

Review the change request: Having been submitted, the change request should, then, be reviewed.

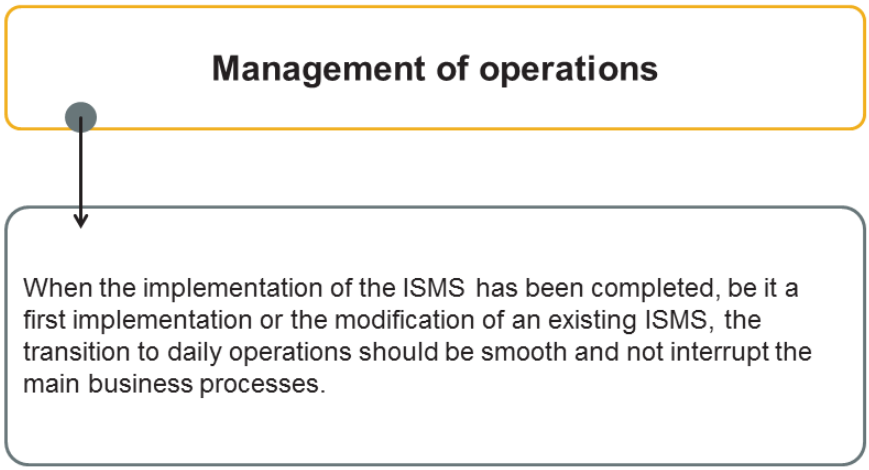
Coordinate the change: The group responsible for the implementation of a change is also responsible for refining the final change schedule.

Implement the change: An appointed person is responsible for the implementation of the change. However, there may be another level of authority for approving and incorporating the change in the organization's operational activities (e.g., the ISMS Coordinator). The scale and nature of the change (and perhaps of the organization) should determine who and at what level authorizes a completed change.

Measure the change results: This phase involves the review of:

- Change request documentation
- Final implementation status
- Metrics

2.6.2 Manage the Operations



PECB

132

In practice, although there may be an official launch of the ISMS (e.g., it formally passes into an operational mode), it is more likely that a transfer to operations is going to be a gradual event. As elements of the ISMS are completed and approved, they should be put into an operational mode. Processes and controls intended to reduce organizational risk will not do their job until they are put into operation. Thus, the transfer to operations should be continual and properly managed.

2.6.3 Ensure Resource Management

To ensure the maintenance and continual improvement of the information security management system, the organization must allocate sufficient resources for its operation.

Budget | Qualified personnel | Required tools

PECB

133

Note: The allocation of resources for the operation of the ISMS depends on the business case.

ISO/IEC 27021, clause 5.9 Competence: Resource management

Intended outcome

Ensuring that appropriate resources are determined and provided in time for the establishment, implementation, maintenance and continual improvement of the ISMS

Knowledge required

- *Financial reporting and measurement*
- *Budget creation and management techniques*
- *Cost management and reduction techniques*
- *Time and materials management techniques*
- *Management review and corrective action processes*

Skills required

- *Determine the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS*
- *Budget business elements including cost of implementation and operation of the ISMS*
- *Understand financial reporting, including cashflow and profit and loss*
- *Create business and investment cases*
- *State ROI (return on investment), ROSI (return on security investment) and other financial benefits*
- *Apply cost control and budget management techniques*
- *Provide appropriate resources in time in the right place*

Slide Notes Extension

PECB

134

Definitions related to information security incidents

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 27035-1, clause 3.3 Information security event

Occurrence indicating a possible breach of information security or failure of controls

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 27035-1, clause 3.4 Information security incident

One or multiple related and identified information security events that can harm an organization's assets or compromise its operations

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 27035-1, clause 3.5 Information security incident management

Exercise of a consistent and effective approach to the handling of information security incidents

ISO/IEC 27035-1, clause 3.1 Information security investigation

Application of examinations, analysis and interpretation to aid understanding of an information security incident

ISO/IEC 27035-1, clause 3.2 Incident response team

IRT

Team of appropriately skilled and trusted members of the organization that handles incidents during their life cycle

Notes on terminology:

1. ISO/IEC 27035 distinguishes an incident from a security event. According to the standard, an incident is a high probability of compromising operations, while an event only indicates a possible breach. A security incident is the realization of a risk that threatens the confidentiality, integrity, or availability of informational resources and threatens, depending on its severity, the conduct of activities of the organization.
2. ISO/IEC 27005 defines an incident scenario as a threat exploiting a vulnerability or group of vulnerabilities during an information security incident.
3. ISO/IEC 27001 describes the occurrence of incident scenarios as “security breaches.”
4. Do not confuse the definition of security incidents with the definition of “fault,” as defined in ITIL: “Any event that is not part of standard operating of a service and that causes or may cause, an interruption or diminution of the quality of this service.”

ISO/IEC 27035-1

- The standard presents basic concepts and phases for managing information security incidents.
- It also provides combined concepts with principles in a structured approach.
- It is a document to be used as a reference to ISO/IEC 27001 and ISO/IEC 27002.
- Organizations cannot get certified against this standard.

PECB

135

ISO/IEC 27035-1 provides guidance to plan, implement, manage, and improve a process for incident management for an organization in the context of the implementation of an ISMS. This standard provides additional information on security controls described in ISO/IEC 27001 and ISO/IEC 27002. It should be noted that an organization has no obligation to follow these recommendations when preparing for an ISO/IEC 27001 certification.

ISO/IEC 27035-1, clause 1 Scope

This part of ISO/IEC 27035 is the foundation of this multipart International Standard. It presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.

The principles given in this part of ISO/IEC 27035 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation. This part of ISO/IEC 27035 is also applicable to external organizations providing information security incident management services.

ISO/IEC 27035-2

- The standard provides guidelines to plan and prepare for incident response.
- It is a document to be used as a reference to ISO/IEC 27001 and ISO/IEC 27002.
- The guidelines are based on a new model: "Plan and prepare," "Lessons learned," and "Information security incident management phases."
- Organizations cannot get certified against this standard.

PECB

136

ISO/IEC 27035-2 provides guidance for organizations to plan, implement, manage, and improve a process for incident management in the context of the implementation of an information security management system (ISMS). It also provides additional information on security controls described in ISO/IEC 27001 and ISO/IEC 27002. It should be noted that an organization has no obligation to follow these recommendations when preparing for an ISO/IEC 27001 certification.

ISO/IEC 27035-2, clause 1 Scope

This part of ISO/IEC 27035 provides the guidelines to plan and prepare for incident response. The guidelines are based on the "Plan and Prepare" phase and the "Lessons Learned" phase of the "Information security incident management phases" model presented in ISO/IEC 27035-1.

The major points within the "Plan and Prepare" phase include the following:

- *information security incident management policy and commitment of top management;*
- *information security policies, including those relating to risk management, updated at both corporate level and system, service and network levels;*
- *information security incident management plan;*
- *incident response team (IRT) establishment;*
- *establish relationships and connections with internal and external organizations;*
- *technical and other support (including organizational and operational support);*
- *information security incident management awareness briefings and training;*
- *information security incident management plan testing.*

The principles given in this part of ISO/IEC 27035 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation. This part of ISO/IEC 27035 is also applicable to external organizations providing information security incident management services.

ISO/IEC 27032

- The standard provides guidelines for security practices for stakeholders in the cyberspace.
- It provides an explanation of the relationship between cybersecurity and other types of security.
- It is a framework to enable stakeholders to collaborate on resolving cybersecurity issues.
- Organizations cannot obtain certification against this standard.

PECB

137

ISO/IEC 27032, clause 1 Scope

This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- *information security,*
- *network security,*
- *internet security, and*
- *critical information infrastructure protection (CIIP).*

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- *an overview of Cybersecurity,*
- *an explanation of the relationship between Cybersecurity and other types of security,*
- *a definition of stakeholders and a description of their roles in Cybersecurity,*
- *guidance for addressing common Cybersecurity issues, and*
- *a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.*

ISO/IEC 27032, clause 2.1 Audience

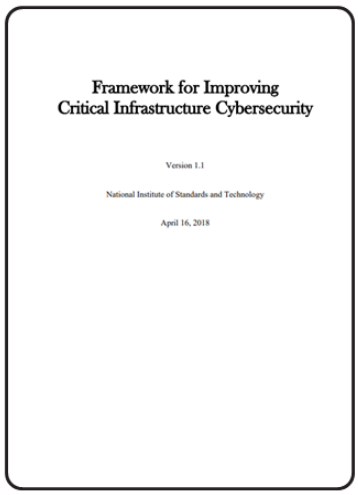
This International Standard is applicable to providers of services in the Cyberspace. The audience, however, includes the consumers that use these services. Where organizations provide services in the Cyberspace to people for use at home or other organizations, they may need to prepare guidance based on this International Standard that contains additional explanations or examples sufficient to allow the reader to understand and act on it.

ISO/IEC 27032, clause 11.3 Guidelines for consumers

This International Standard is not directed at individuals of the Cyberspace specifically, but focuses on organizations providing services to consumers, and organizations that require their employees or end-users to practice secure use of the Cyberspace to manage the Cybersecurity risk effectively. The guidance on the roles and security of users in the Cyberspace and how they could positively influence the state of Cybersecurity aims to serve as a guide for the design and development contents by these organizations, in the context of their service provisioning and awareness and training programs for delivery to their end-users.

NIST Cybersecurity Framework

- It is a framework created by NIST.
- It is designed for the US Federal Government, but can be used by any organization worldwide.
- It follows a phased modeling approach.
- Organizations cannot obtain certification against this standard.



PECB

138

Founded in 1901, NIST is a non-regulatory federal agency of the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life. One area NIST is focused on is cybersecurity.

The framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the framework as a reference to establish one.

Just as the framework is not industry-specific, the common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the framework to strengthen their own cybersecurity efforts. The framework can also contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

Security Operations Center (SOC)

- The Security Operations Center is the facility of the information security team responsible for detecting, analyzing, responding, reporting, monitoring, and preventing organizations from cybersecurity incidents.
- The SOC team is a group of expert individuals, security analysts, engineers, and managers who supervise security operations. This team works closely with other teams and departments of the organization to ensure that security issues are addressed prior to discovery.
- The primary benefit of correctly implementing the SOC is the improvement of security incident detection through continual monitoring and analysis of the organization's activities.

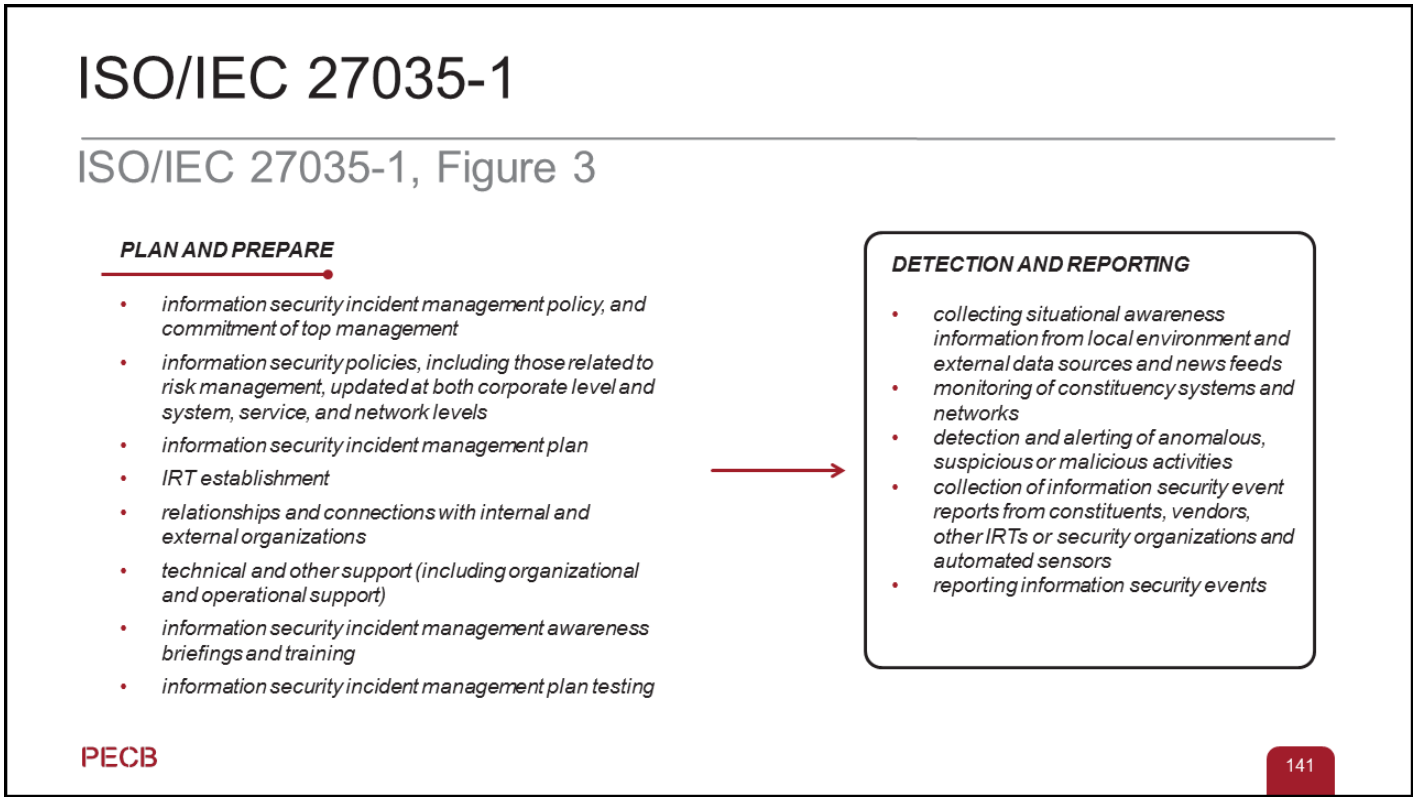
PECB

139

Most used technologies in security operations center include firewalls, probes, security information, and event management systems. The SOC team uninterruptedly manages known and existing threats by establishing rules, identifying exceptions, and identifying emerging risks.

Security operations centers are most popular among strategy-focused organizations that trust the assessment and mitigations of threats to humans more than a script. Thus, SOC relies severely on the knowledge of the SOC team members.

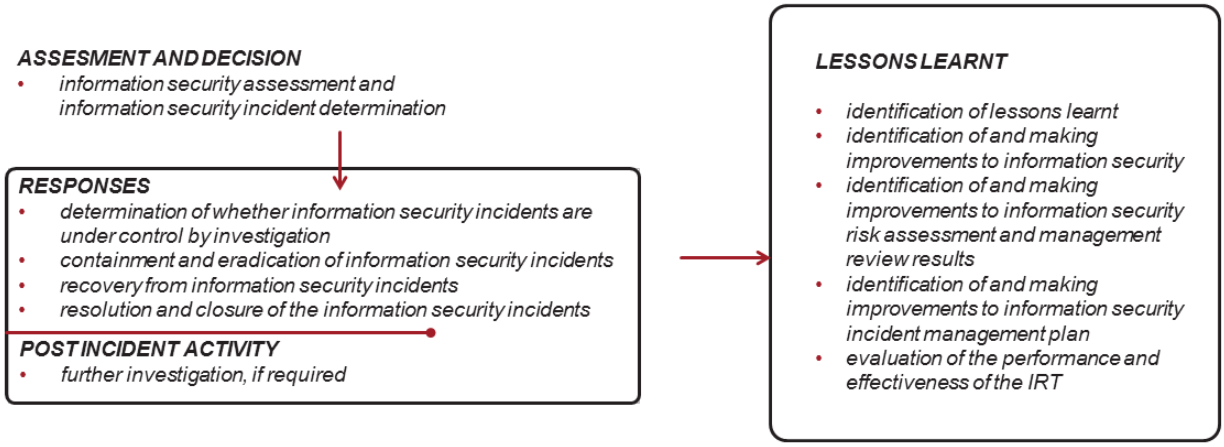
1. **What does the measurement of change results include?**
   A. Generating the change metrics
   B. Verifying the change success
   C. Approving or rejecting the change
2. **Which of the statements below is NOT true?**
   A. Organizations cannot get certified against ISO/IEC 27032
   B. Organizations cannot get certified against ISO/IEC 27035-2
   C. Organizations can get certified against ISO/IEC 27035-1
3. **Which standard provides guidelines for security practices in the Cyberspace?**
   A. ISO/IEC 27032
   B. ISO/IEC 27035-1
   C. ISO/IEC 27035-2
4. **What is a Security Operations Center (SOC) team?**
   A. A group of information security program coordinators
   B. A group of expert individuals, security analysts, engineers, and managers who supervise security operations
   C. A group of internal auditors who uninterruptedly manage operational activities of the organization
5. **The top management must ensure that all members within the ISMS scope understand the value and importance of an effective information security incident management policy.**
   A. True
   B. False

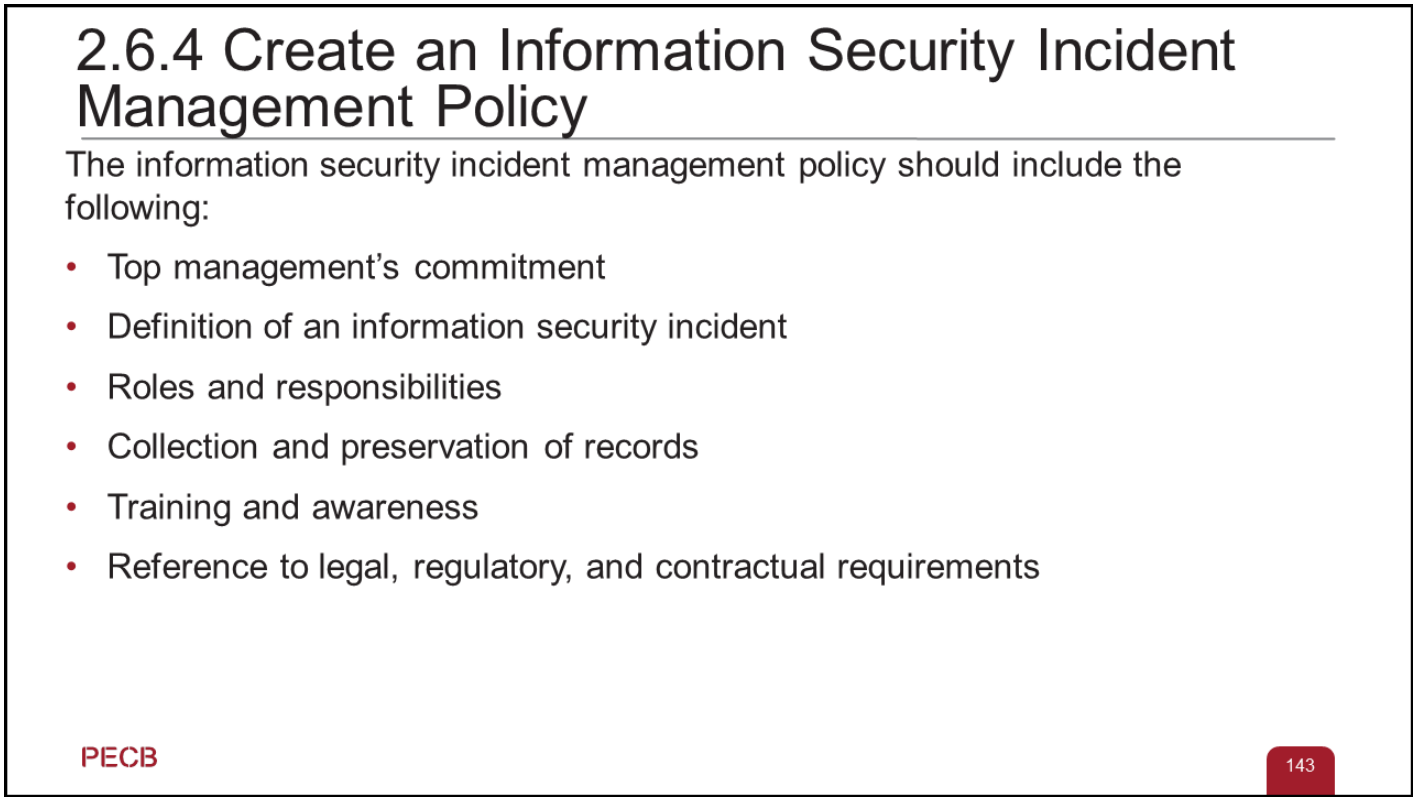


Note: IT incident and information security incident are different terms, and cannot be used interchangeably. An information security incident is any event that has the potential to affect the preservation of confidentiality, integrity, and availability of information. Examples of information security incidents include unauthorized access, use, disclosure, modification, or destruction of information, denial of service attacks, computer system intrusions, etc. An IT incident is any unexpected event that disrupts the normal operation of an IT service. Examples of IT incidents include hardware, software, and security failings.

ISO/IEC 27035-1

ISO/IEC 27035-1, Figure 3 (cont'd)

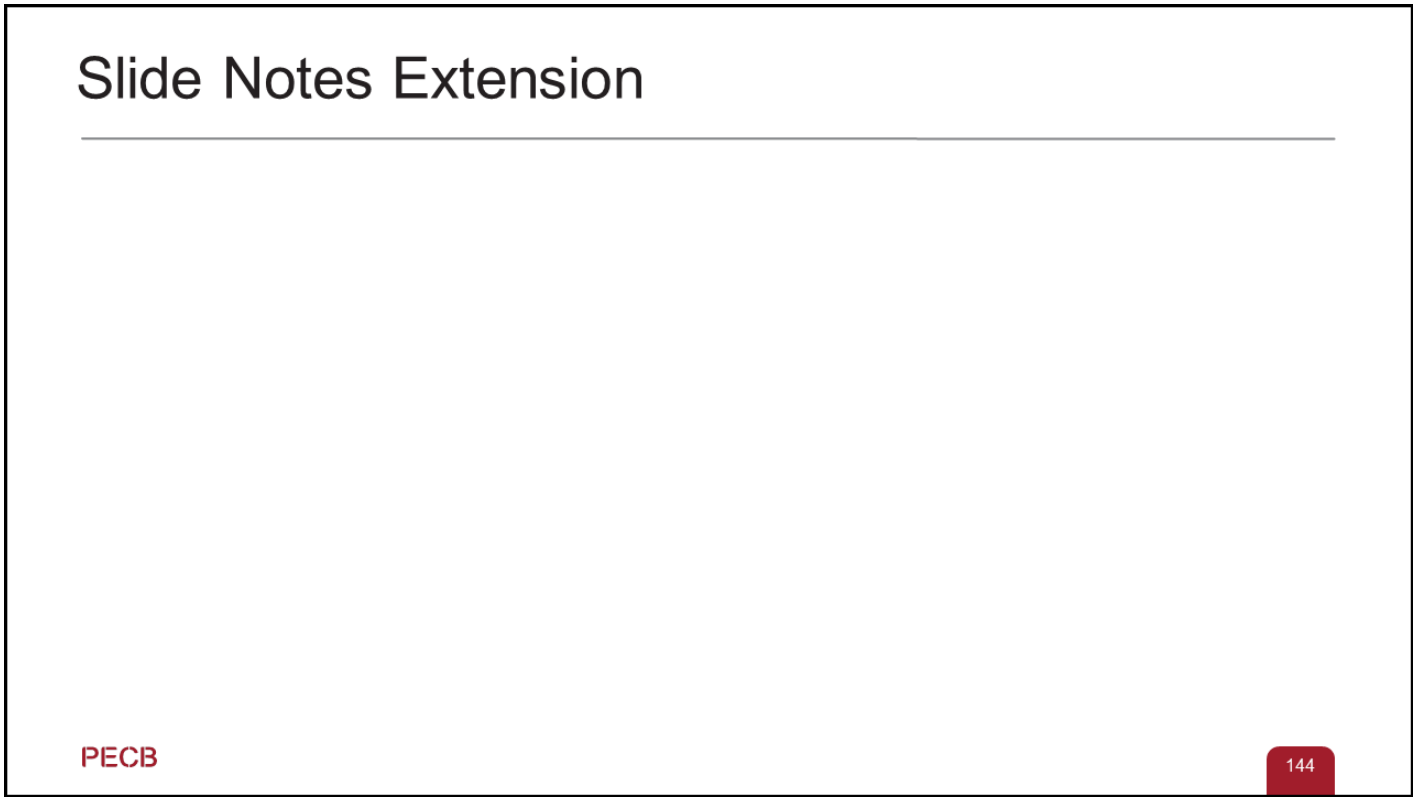




ISO/IEC 27035-2, clause 4.3 highlights the importance of a clear and effective policy regarding information security incident management.

The information security incident management policy should consider:

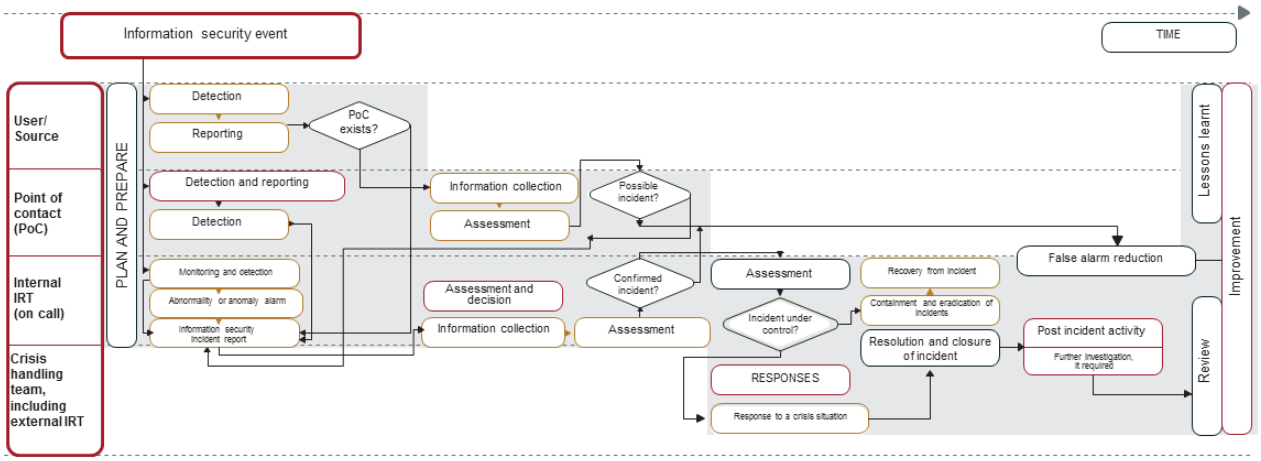
- **Top management's commitment:** Top management must support the initiatives stated in the policy and ensure that all members within scope of the ISMS understand the value and importance of an effective policy and processes associated in this area. When an incident occurs, no one should be in any doubt about the importance of the policy and should be working in line with the clearly stated requirements.
- **Definition of an information security incident:** This definition should be clear and unambiguous. Any person in the organization should be able to identify whether an event or set of events constitutes an incident. Having such clarity is vital for both accurate reporting and effective response.
- **Roles and responsibilities:** All those involved in the organization should clearly understand their roles and responsibilities when it comes to identifying, reporting, and responding to incidents.
- **Collection and preservation of records:** During the reporting, response to, and analysis of an incident, various records will be generated. It must be clear to anyone involved what records should be created, where those records should be kept, and what format and content they should have.
- **Training and awareness:** In general, information security awareness is critical to the overall security posture of the organization. A key part of the awareness-raising process needs to include a clear description of what an incident is, the importance of reporting the incident, and the reporting channel.



- **Reference to legal, regulatory, and contractual requirements:** Making sure that the individuals involved in incident management understand the relevant laws and regulations is critical to having an effective information security incident management process. Some laws and regulations require incidents to be addressed and reported within a set timeframe. From a contractual point of view, organizations may have requirements to report or handle incidents in certain timeframes dictated by customers.

This policy may be drafted as a separate document or be integrated into the overall information security policy or in an overall incident management policy integrating various aspects, such as environmental, health, and safety incidents.

2.6.5 Define the Processes and Draft the Procedures



PECB

Important note:

Please note that the figure in the slide is displayed and explained in the following notes pages.

Slide Notes Extension

PECB

146

1.Detection and reporting

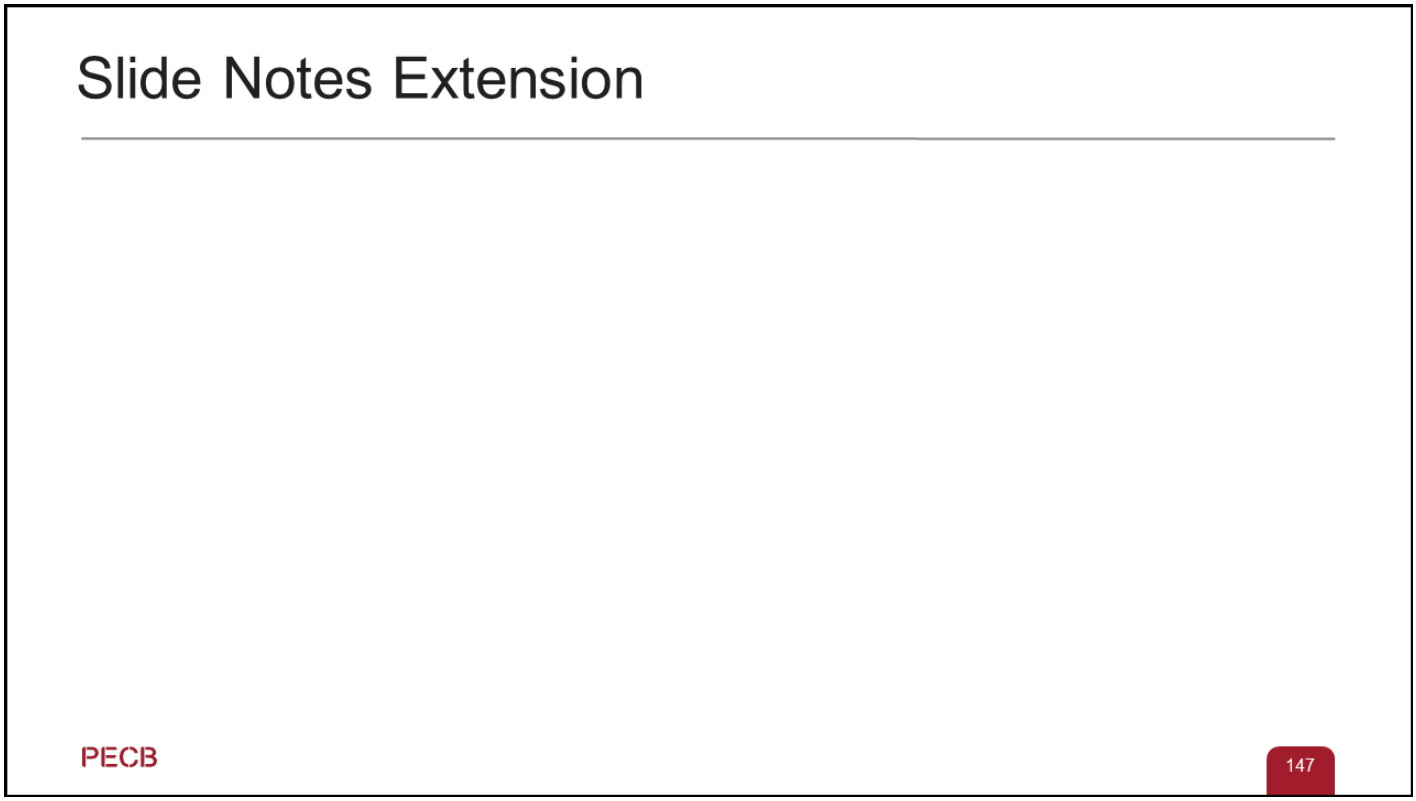
- When an information security event is detected, the person responsible initiates the detection and reporting process. This person should follow the procedures and use the report form for the event type as indicated in the appropriate procedure, so as to bring the event to the attention of the operational support group. All personnel should be aware of and have access to procedures for reporting information security events.

2.Initial assessment and decision

- Upon receiving an event report, the operations support group should complete the information security event ticket, analyze (triage) it, and assign a priority. If necessary, the person handling the report should seek clarification from the person who produced it and collect any additional information, potentially seeking input from other sources.
- After the initial receipt of the event, an evaluation should be conducted to determine if the event report needs further analysis. Essentially, the evaluation is conducted to determine whether the event should be classified as a real information security incident or a false alarm.
- If it is determined that the information security event may be an information security incident and if the group's operational support has the appropriate level of competence, further evaluation may be conducted. This can result in corrective actions, for example, emergency protection controls are identified and returned to the competent people so that actions can be taken.

3.Second evaluation and confirmation of an incident

- The second evaluation and confirmation of the decision to close the incident event in the category of information security or not, should be the responsibility of the computer security incident response team (CSIRT), If a CSIRT has been implemented. If it is determined that the information security incident is real, then a member of the CSIRT, involving colleagues if necessary, should do a more thorough evaluation. The aim is to confirm the nature of the information security incident, how it was done—and what or whom it might affect, the impact or potential impact of the security incident on the business of the organization, an indication of whether the information security incident is deemed significant or not (using the predetermined security matrix of the organization).



4.Response

- In most cases, the next activity of the CSIRT member will be to identify the immediate response actions to address the information security incident: recording the details on the information security incident form and informing the appropriate persons or groups about the incident and any required actions. This may result in emergency protection measures (e.g., isolating or halting an information system, service, or affected network with prior approval from the respective managers) or identification of protective controls, as well as constant additional reporting to the appropriate person or group for action.
- If not already done so, the seriousness of the security incident information should be determined using the predetermined scale of severity of the organization, and, if needed, members of the top management should be notified directly. While it is clear that a crisis situation should be declared, for example, the director of business continuity should be notified for the possible activation of the business continuity plan. In addition, the CSIRT director and top management should also be informed.
- Once the CSIRT member has initiated the immediate responses and the activities of forensic analysis and communications are completed, a quick determination must be made on whether the information security incident is under control. If necessary, the member may consult with colleagues, the CSIRT director, or other individuals or groups.
- If the incident is determined to be under control, the CSIRT member should provide all the answers, forensic analysis, and subsequent communications required to close the information security incident and restore normal operations of the affected information system.
- If determined that an information security incident is under control and should not be subjected to any “crisis” activities, the member of the CSIRT should identify what, if any, additional responses are required to address the information security problem. This could include the restoring of affected information system(s), service(s), or network(s) to resume their normal operations. The CSIRT member should, then, record the details related to the information security incident on the information security incident report form and in the database of events or incidents of information security and notify those responsible to complete the related actions. Once these actions have been successfully completed, the details should be recorded on the information security incident report form and in the database of events or incidents of information security. Then, the information security incident should be closed, and the appropriate personnel should be notified.

2.6.6 Create an Incident Response Team

ISO/IEC 27035-2, clause 7.1

- *The aim of establishing the IRT is to provide the organization with appropriate capability for assessing, responding to and learning from information security incidents, and providing the necessary coordination, management, feedback and communication.*
- *An IRT contributes to the reduction in physical and monetary damage, as well as the reduction of the damage to the organization's reputation that is sometimes associated with information security incidents.*
- *IRTs can be structured differently depending on the organization size, its staff members and industry type.*

PECB

148

Throughout the course, the term IRT is going to be used for Incident Response Team. However, there can be other terms, as seen in quotes below.

There is a difference between "Security teams," "Internal CSIRT," and "Coordinating CSIRT":

- In a **security team**, the formal responsibility of processing incident activities is assigned to any group or section of the organization. No CSIRT (Computer Security Incident Response Team) is established; instead of a CSIRT, available staff (typically system, network, or security administrators) or a local subsidiary handles security events ad hoc and, in case of an isolated incident, as part of their general responsibilities or work assignments.
- In an **internal CSIRT**, the responsibility for dealing with incidents is typically assigned to a specifically qualified group of individuals.
- In the **coordinating CSIRT** model, the CSIRT coordinates and facilitates the handling of incidents, vulnerabilities, and information in a variety of internal and external organizations that may also include other CSIRTs, provider organizations, security experts, and even law enforcement agencies.

Source: Brown, Moira West., Stikvoort, Don., Kossakowski, Klaus-Peter., Killcrece, Georgia., Ruefle, Robin., and Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs).* Software Engineering Institute, Pittsburgh: 2003.

- The scale of the organization as a whole, and of the organization in terms of the ISMS may dictate that establishing a CSIRT constantly is not a realistic proposition. In such a case specific personnel could be defined as being the first line of information security event defense. This core IRT should have access to other personnel and disciplines (IT, Legal, HR, Operations, Public relations, etc.) as required.
- The IRT also needs to have delegated authority from the top management to be able to promptly execute its responsibilities in the event of an event being a serious information security incident.

Slide Notes Extension

PECB

149

Note on terminology:

ISO/IEC 27035-1, clause 3.2 Incident response team

IRT

Team of appropriately skilled and trusted members of the organization that handles incidents during their life cycle

Note 1 to entry: CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) are commonly used terms for IRT.

The IRT may choose to offer multiple services. The services offered by each IRT should be based on the mission, purpose, and composition of the team. IRT services can be grouped into three categories:

1. **Reactive services:** These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of IRT work.
2. **Proactive services:** These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. The performance of these services will directly reduce the number of incidents in the future.
3. **Security quality management services:** These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization, such as the IT, audit, or training departments. If the IRT performs or assists with these services, their point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reduce the number of incidents.

Source: Brown, Moira West., Stikvoort, Don., Kossakowski, Klaus-Peter., Killcrece, Georgia., Ruefle, Robin., and Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs).* Software Engineering Institute, Pittsburgh: 2003.

Implement Incident Management Security Controls

Examples of preventive controls

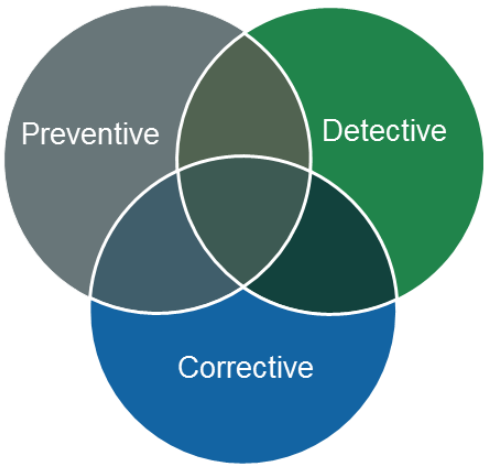
- Training sessions, user awareness, demilitarized zone (DMZ), virtual private network (VPN), personnel selection, etc.

Examples of detective controls

- Intrusion detection system (IDS), security guard, security alerts, etc.

Examples of corrective controls

- Incident response group, incidents handling process, forensics process, etc.



PECB

150

ISO/IEC 27001 emphasizes the need to implement controls to detect and respond (e.g., correction) to security incidents. It is also requires to establish a number of preventive measures, such as training of key stakeholders and user awareness.

Here are the main security controls related to incident management:

Examples of preventive controls

- Proper training of staff
- Controlling of physical access to the equipment
- Well-designed documents
- Authentication and authorization (password)
- Cryptography

Examples of detective controls

- Telecommunications equipment with built-in alarm systems
- Intrusion detection systems (IDS)
- Alarms for the detection of heat, smoke, fire, or risk to water
- Checking of duplicate calculations
- Video cameras

Examples of corrective controls

- Establishment of emergency plans with all the necessary training, awareness, test, and maintenance activities
- Creation of an incident response team
- Incidents investigation process

2.6.7 Define a Forensics Process

ISO/IEC 27002, clause 16.1.7

- *Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.*
- *In general, these procedures for evidence should provide processes of identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off.*

Competent personnel | Defined processes | Specialized tools

PECB

151

The concept of “computer forensics” is built on the older model of forensic (medical) science.

Forensics is about the application of techniques and protocols of the investigative and legal procedures designed to capture and preserve digital evidence, such that it can be admissible in court. It can also be defined as the body of knowledge and methods to collect, preserve, and analyze evidence from electronic media to present them as part of a lawsuit.

There are four main steps in a forensic analysis:

1. Preparation (Investigators must have the skills necessary for this type of survey.)
2. Collection and archiving of data (in accordance with the required procedures)
3. Review and analysis (interpretation of information for research purposes)
4. Report (including conclusions and comments)

A forensic investigation also requires:

- Technical tools (tools for audit, analysis equipment, etc.)
- Procedures
- Skilled personnel

Important note: An organization that wants to conform to control A.16.1.3 of ISO/IEC 27001 can either develop the skills of forensic investigation internally or use external consultants.

2.6.8 Record the Information Related to Security Incidents

All relevant information related to the incident should be recorded, including:

- Unique record identifier
- Category and priority
- Date and time of the recording
- Identification of the person who reported the incident
- Identification of the person who created the incident record
- Description of the symptoms
- Incident status (active, pending, closed)
- Assets affected
- Closing information (resolution, date, and time of the closure)
- Groups or individuals affected by the incident
- Activities undertaken to resolve the incident and their results
- Approvals of actions taken and incident closure

PECB

152

It is important to document and record any incident to ensure that the personnel responsible for handling the incident can have all the information needed to solve it in the most effective way.

This information will serve as input for corrective actions and evidence demonstrating to auditors (internal and external) that the ISMS is being maintained. This, in turn, can feed back into measurements and metrics.

2.6.9 Measure and Review the Incident Management Process

The performance of the incident management process should be regularly:

- **Measured** using performance indicators
- **Re-evaluated** to identify corrective and preventive actions

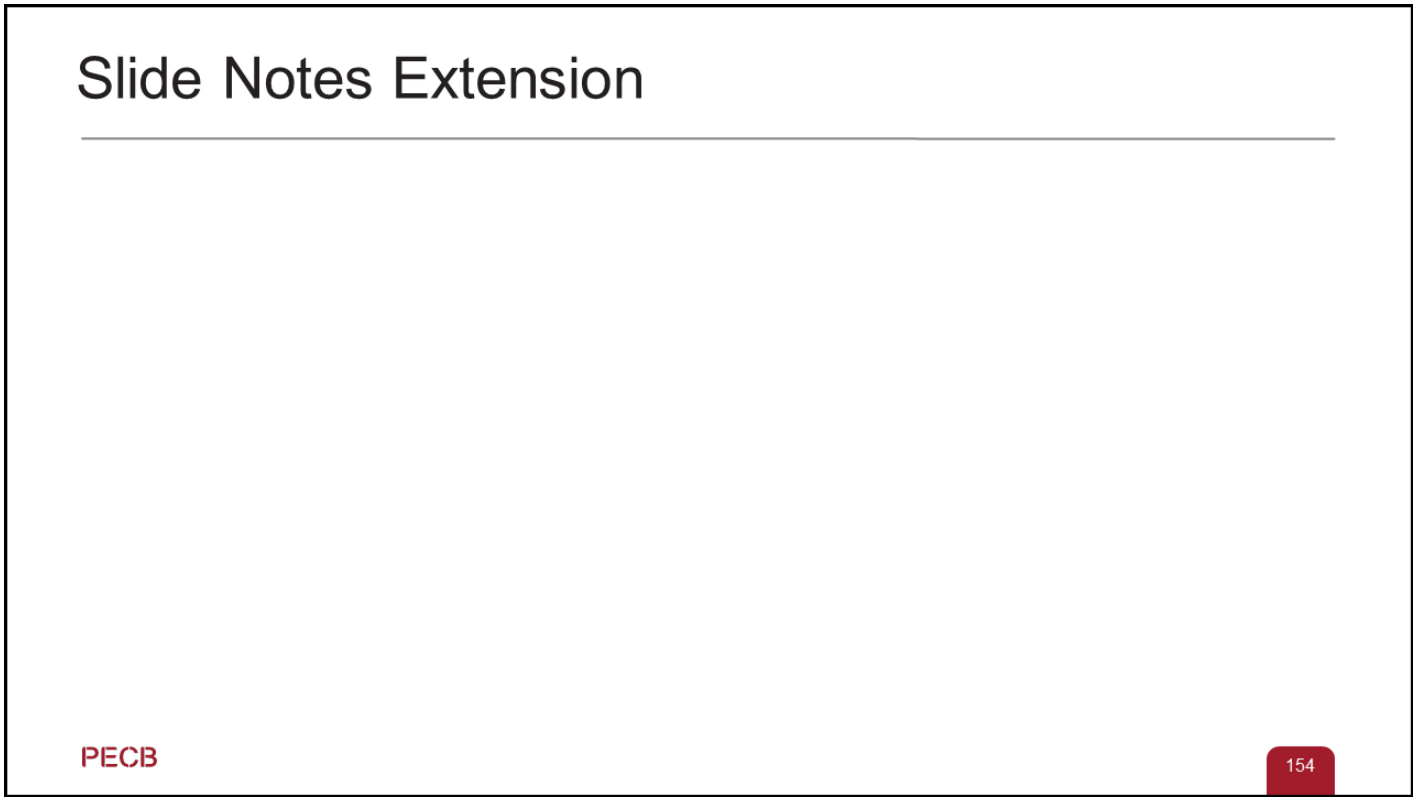
PECB

153

Once an information security incident is closed, it is important that the lessons learned related to the processing of the information security incident are promptly identified and employed to avoid similar incidents from recurring. These lessons may include:

1. New or modified requirements for the safeguarding of information security—These safeguards can be technical or nontechnical (including physical). Based on the lessons learned, these controls could include the need for urgent updating of material to raise awareness on information security (for users and other staff), and the revision and instant release of guidelines or security standards.
2. Changes to processes and procedures for managing incidents of information security, report forms, and database of events or incidents of information security

Later in this activity, it is necessary to look beyond a single information security incident and check for trends that might help identify the need for changes in protection measures.



Identification of security improvements

During the review of closing an incident, new security controls and amendments to existing ones can be identified as required.

Recommendations and requirements for protective measures may not be financially feasible to be implemented immediately. As such, they should be identified as long-term goals of the organization.

For example, firewall migration services and a more robust security may not be financially feasible in the short term; however, these should be recognized as information security long-term goals of the organization.

Any such changes should be captured in the risk assessment, risk treatment plans, and SoA.

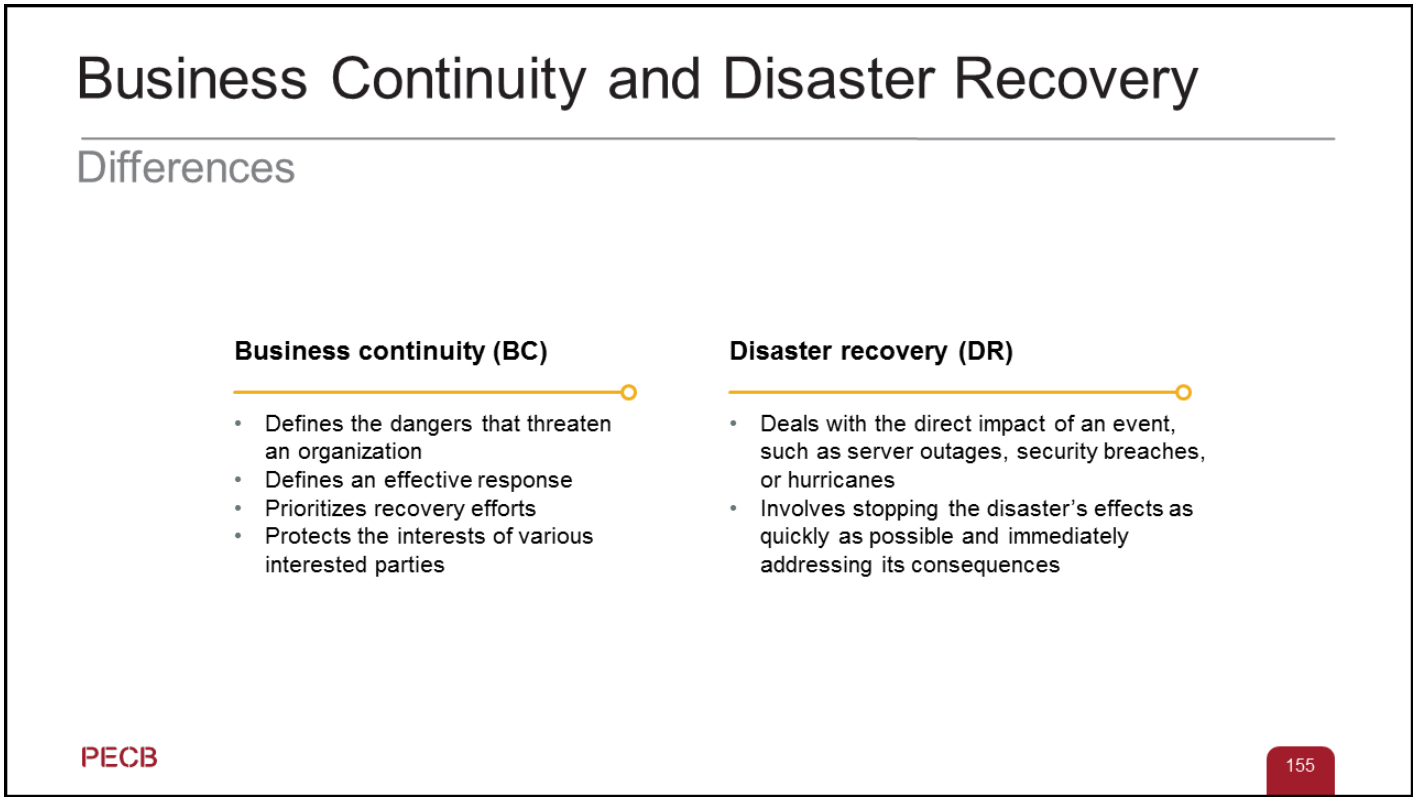
Identification of scheme improvements

After the incident has been resolved, the head of the CSIRT team, or a nominee, has to investigate what happened to evaluate and, therefore, "quantify" the effectiveness of the overall response to information security incidents. Such analysis determines the parts of the information security incident management scheme that have worked well and identifies the places where improvements are required.

An important aspect of the "post-response" analysis is the reintroduction of the information and knowledge in the information security incident management scheme. If the incident is of high severity, it is important to plan a meeting with all parties concerned, while the information is still fresh in memory. Some factors to consider in this type of meeting include:

- Do the procedures set out in the information security incidents scheme work as expected?
- Could the existing methods or procedures help detect the incident?
- Have the procedures and tools that could help the response process been identified?
- Are there procedures that could help restore information systems following an incident identified?
- Has communication of the incident to all interested parties been effective throughout the process of detecting, reporting, and response?

The results of the meeting should be documented and any action agreed should be implemented appropriately.



At some time during the disaster recovery, business continuity activities begin to overlap. The three following questions, with a primarily focus on continuing businesses operations, are related to business continuity and disaster recovery maintenance cycle (BC/DR):

- Where to set up temporary systems?
- How to acquire replacement systems or parts?
- How to secure the new location?

Example: Failover resilience

An organization decides to invest in a "failover" system, meaning that if the server that provides the organization with the data and applications that are used on a daily basis gets damaged and fails, another server will automatically replace the damaged server. Thus, the employees will be capable of immediately continuing their duties. This is considered as a resilience of the IT data, but is provided by a disaster recovery device. Even though disaster recovery is capable of existing on its own, it is an essential component in business continuity management, given that it offers the required resources that facilitate normal business operations.

1. **Upon receiving an event report, the operations support group should complete the information security event ticket, analyze it (triage), and assign a priority. What process is this?**
   A. Initial assessment and decision
   B. Detection and reporting
   C. Response
2. **A team where the responsibility for dealing with incidents is typically assigned to a specifically qualified group of individuals is known as:**
   A. Security team
   B. Internal computer security incident response team (Internal CSIRT)
   C. Management team
3. **What type of control is cryptography?**
   A. Preventive control
   B. Detective control
   C. Corrective control
4. **What are the steps of a forensic analysis?**
   A. Prepare, review, and analyze
   B. Prepare, collect, archive, and report
   C. Prepare, collect and archive, review and analyze, and report
5. **The performance of the incident management process should be regularly _____.**
   A. Measured using imperial units
   B. Evaluated to identify corrective actions
   C. Re-evaluated to identify corrective and preventive actions
6. **Disaster recovery (DR) defines the dangers that threaten an organization and protects the interests of various interested parties.**
   A. True
   B. False

Section summary

- Organizations can use ISO/IEC 27035-1 and ISO/IEC 27035-2 in addition to ISO/IEC 27001 and ISO/IEC 27002 when planning, implementing, managing, and improving incident management processes.
- To manage information security incidents, the organization is required to create an incident management policy and an incident response team to define processes and write procedures and define forensics processes, to implement security controls, to record the information related to security incidents, and to measure and review incident management processes.
- An incident management policy should include the management commitment, roles and responsibilities of employees involved in identifying, reporting, and responding to incidents, the definition of an information security incident (clearly and explicitly), collection and preservation of records, etc.
- The incident response team (IRT) is responsible to provide the coordination, management, feedback, and communication in regards to information security incidents.
- Information related to security incidents may include the records identifier, date and time of the recording, its category and priority, incident status, assets affected, activities undertaken to resolve the incident, the approval of actions taken, and incident disclosure.
- Incident management processes should be measured and re-evaluated on a regular basis to identify corrective and preventive actions.

Pharm is a pharmaceutical company that develops and distributes medication products. This company has been victim to several information security attacks in the last month due to the high amount of important data they had to collect for their development researches.

They, therefore, decided to restrict user access to information and application system functions only to specific persons by designing specific access controls. *Pharm* decided that all types of information, regardless of their importance or impact, will get the same level of protection so that the number of attacks can be reduced. A team of five competent persons was established to evaluate the information security attacks and confirm their nature, the way they are done, what or who they might affect, and what their potential impact in the company can be.

After completing the implementation of the new security controls and ensuring their successful operation, *Pharm* decided to provide a communication plan for the users and concluded that a training session for the staff was not necessary.

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

1.What controls should *Pharm* implement to preserve the integrity and confidentiality of information?

A. Event logging controls
B. Cryptographic controls
C. Secure areas controls

2.*Pharm* provided the same level of protection for all information, regardless of importance or impact, to reduce the number of attacks. Does this comply with ISO/IEC 27001?

A. Yes, because the same level of protection for all types of information is required by the standard
B. No, because information should be protected according to its importance
C. No, because information protection cannot reduce the number of attacks

3.What type of security control did *Pharm* implement by establishing a team to evaluate the information security attacks?

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

4.The team of five competent persons established by *Pharm* is an:

A. Implementation security team
B. Internal management team
C. Incident response team

5.Based on the scenario, *Pharm* will provide a communication plan after concluding that a training session for the staff is not necessary. How do you consider this situation?

A. Acceptable; the communication plan regarding the implementation of the new security controls provided to the users is sufficient
B. Unacceptable; Pharm should conduct a training session because the implementation of access controls requires skills
C. Unacceptable; the communication plan should not be provided to the users

Slide Notes Extension

PECB

160

Summary of Day 3

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

- The definition of the document management process
- The implementation of a document management system
- The design of security controls and drafting of specific policies and procedures
- The implementation of security processes and controls
- Introduction of Annex A controls
- Principles of an efficient communication strategy
- Planning of communication activities
- The difference between training, awareness, and communication
- Designing and planning of training programs
- Security operations management
- Resource management necessary to maintain the ISMS
- Information security incident management policy
- Security controls related to incident management

Blank Page for Note Taking

Blank Page for Note Taking