DAY 3

Certified ISO/IEC 27001 Lead Implementer

Version 10.0

Document number: ISMSLID3V10.0

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

1. Select, design, and implement information security controls
2. Manage documented information and implement a documented information management system
3. Explain the latest trends and technologies, including big data, artificial intelligence, machine learning, cloud computing, and outsourced operations
4. Establish communication objectives and perform and evaluate communication activities
5. Design, plan, and provide an information security training program
6. Establish, measure, and review an incident management process and create an incident management policy

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

Selection and Design of Controls

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

PECB

Selection and Design of Controls

Operational planning and control

- The organization should plan, implement, maintain, and continually improve the processes and controls needed to meet information security requirements.
- The organization should select and implement information security controls based on the results of the risk assessment.
- Documented information should be regularly retained 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 identified and controlled.

PECB

2.1 Selection and Design of Controls

List of activities

2.1.1

Analyze the organization's security architecture

2.1.2

Design and describe the controls

2.1.3

Prepare for the implementation of controls

PECB

2.1.1 Analyze the Organization's Security Architecture

The organization should analyze its existing security architecture to understand its current security posture and take adequate actions for improvement.

The analysis of the existing security architecture enables organizations to determine the suitability, efficiency, and effectiveness of information security processes, procedures, and controls.

The organization should conduct an in-depth review to determine whether it is capable to meet the security requirements based on industry best practices.

The network architecture, traffic flow, and general technology processes should be involved in the review.

PECB

Security Architecture

Security architecture refers to the structured design and coordination of elements (policies, principles, procedures, controls, etc.) that protect the organization's information technology systems, data, and assets.

When establishing a new security architecture, the organization should make sure that it:

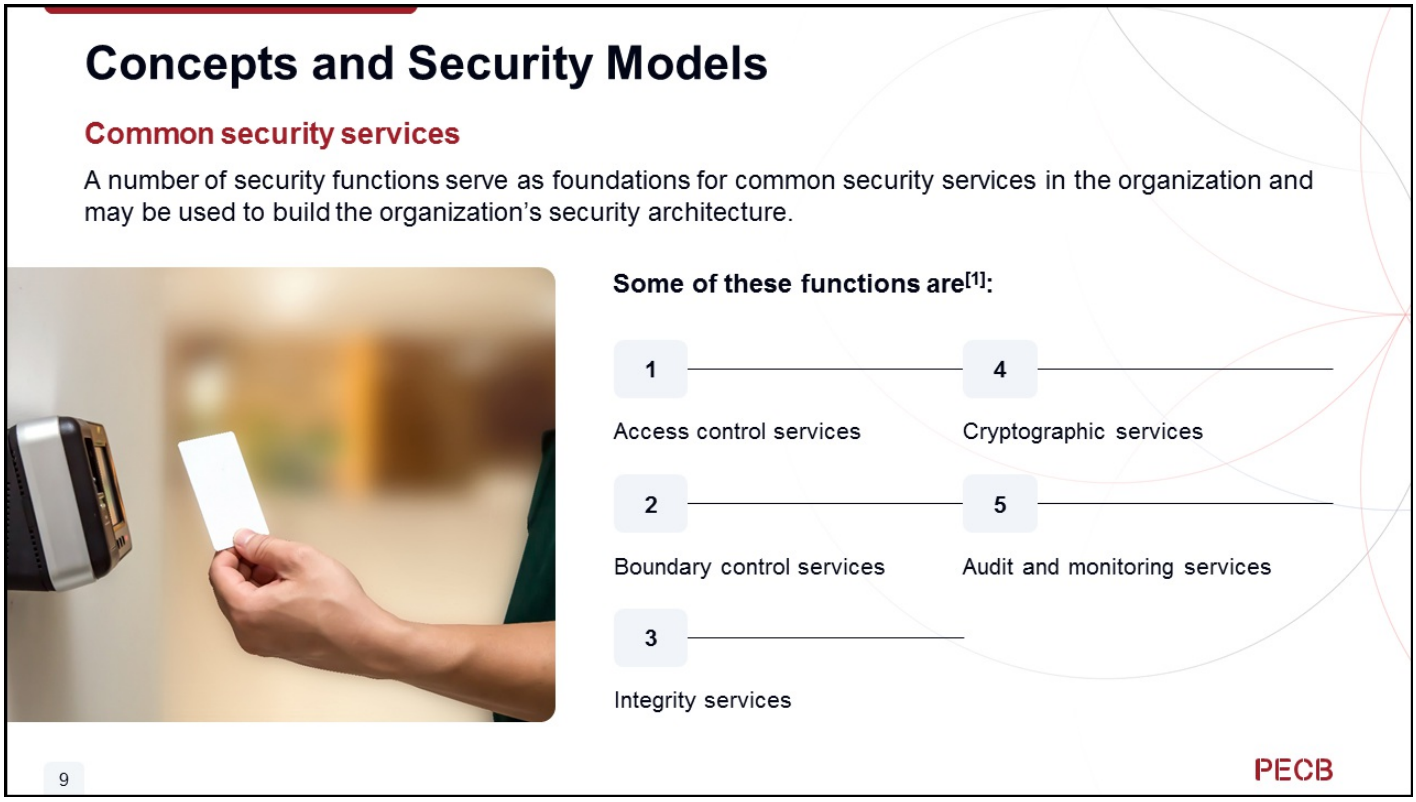
- Is concise and ensures a continuing view of security controls
- Consolidates the purpose of common security controls tied to business objectives
- Takes advantage of the existing technology investments and maximizes the benefits from the new ones
- Is able to effectively address current and future threats

8

PECB

A set of practices established to address security requirements at a system level is known as security architecture. A good security architecture consists of a set of security services that ensure the safety of multiple processes, systems, and applications.

Organizations should establish a security architecture which can be effective on a long term. Initially, the security architecture should set the priorities for the development of security services. Then, this information should be used when planning the security program. This approach enables organizations to establish effective security services at a low cost. [1]



Access control services

- The purpose of these services is to facilitate identification and support shared authentication across the organization.
- They include a number of other services related to the creation, handling, and storage of credentials in the organization.

Boundary control services

- These services control the transferring of information from a set of systems to another.
- Their purpose is to impose security zones of control by isolating entry points from one zone to another (choke points).

Integrity services

- The purpose of these services is to ensure the integrity of systems and data by establishing automated checking systems which detect and correct corruption.
- These services can be used at different levels of the organization, however, they are mainly intended for distrusted or less trusted systems.

Cryptographic services

- These services are intended for common services that can be used and reused by different systems.
- Cryptographic services include common hashing and encryption tools, technologies, and services.

Audit and monitoring services

- The purpose of these services is to ensure the secure collection, storage, and analysis of audited events. This can be done through centralized logging or intrusion detection systems (IDSs).

Common Security Architecture Frameworks

A security architecture framework plays a crucial role in aligning business and technology resources to accomplish strategic objectives. The following are some common security architecture frameworks that organizations can adopt[1]:

- The Zachman Framework
- The Sherwood Applied Business Security Architecture (SABSA)
- The Open Group Architecture Framework (TOGAF)
- Open Security Architecture (OSA)

PECB

Zachman Framework

- Regarded as an "ontology" or "schema," the Zachman Framework helps to organize enterprise architecture artifacts, including documents, specifications, and models. It also considers the impact of these artifacts on various stakeholders and evaluates their relevance in relation to the concern at hand. [2]

- Zachman Framework differs from typical IT management frameworks as it is not a traditional methodology that provides explicit procedures for managing data.

- This framework continues to be significant for contemporary businesses due to the escalating complexity of technology landscapes.

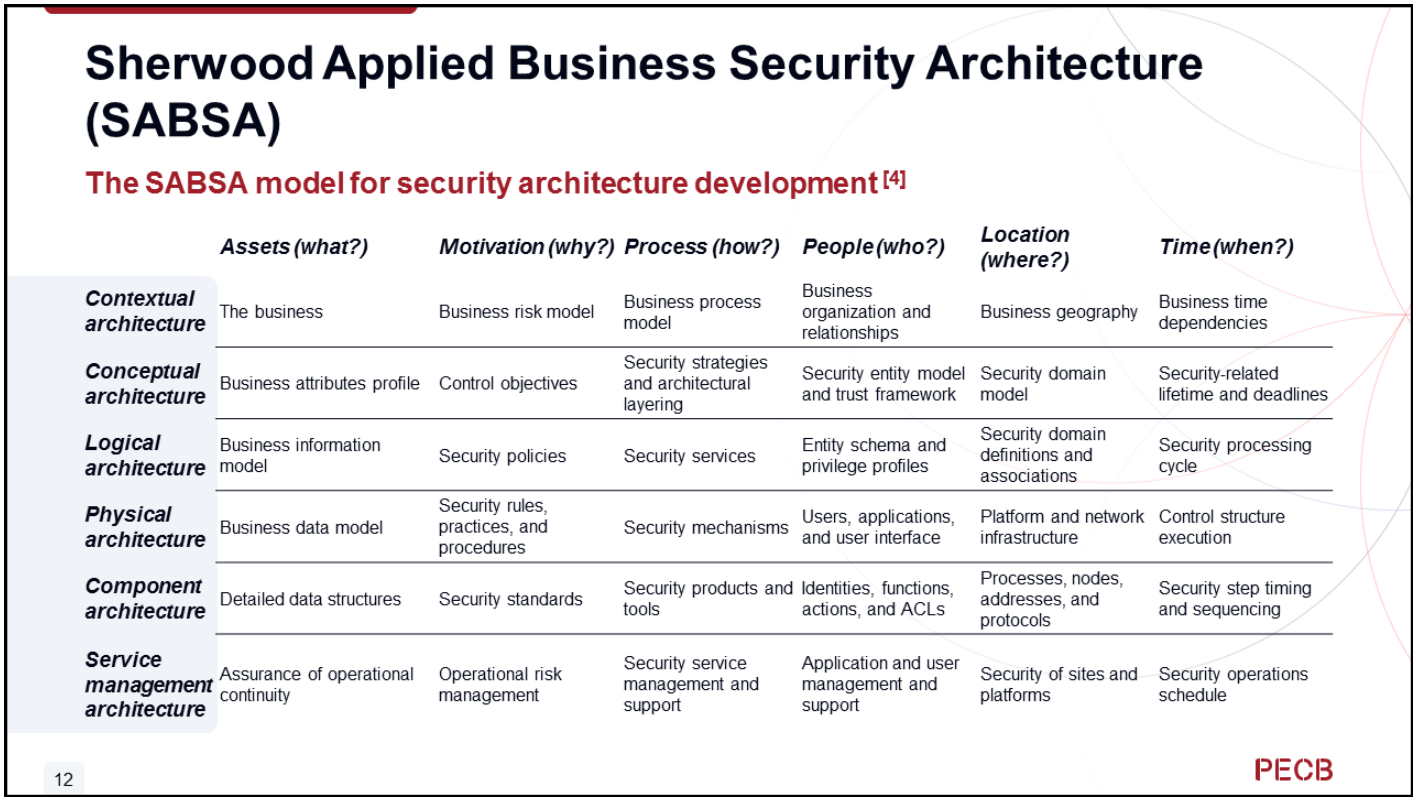
11

PECB

John Zachman initially created the Zachman Framework at IBM in 1987, and it has undergone multiple updates since then. The framework's purpose is to structure and evaluate data, address problems, facilitate future planning, oversee enterprise architecture, and generate analytical models. It employs 36 distinct categories that encompass a wide range of elements, including products, services, hardware, and software. These categories are structured in a two-dimensional matrix consisting of six rows and six columns, resulting in a total of 36 cells. This matrix serves as a visual representation to aid in comprehending and visualizing various problems. [3]

The framework describes models that are applicable to illustrate an enterprise:

- Every cell needs to be coordinated with the cells directly above and below it.
- Within each row, all cells must also align with one another.
- Each cell possesses its own distinct characteristics and purpose.
- The combination of cells within a single row forms a comprehensive depiction of the enterprise from that specific viewpoint.



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[1]:

- **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.
- **Service** management security architecture is focused on the facility manager's view.

The Open Group Architecture Framework (TOGAF)

TOGAF assists organizations in determining the objectives of developing their security architecture. [5]

It focuses on the initial stages of security architecture, defining the scope and objectives of an organization and outlining the specific problems it aims to solve through this approach, but it does not provide explicit instructions on resolving security issues.

Some of TOGAF examples include:

- Selecting business principles, objectives, and goals
- Establishing roadmaps for security architecture
- Establishing security architecture components
- Selecting specific requirements for security architecture

PECB

Open Security Architecture (OSA)

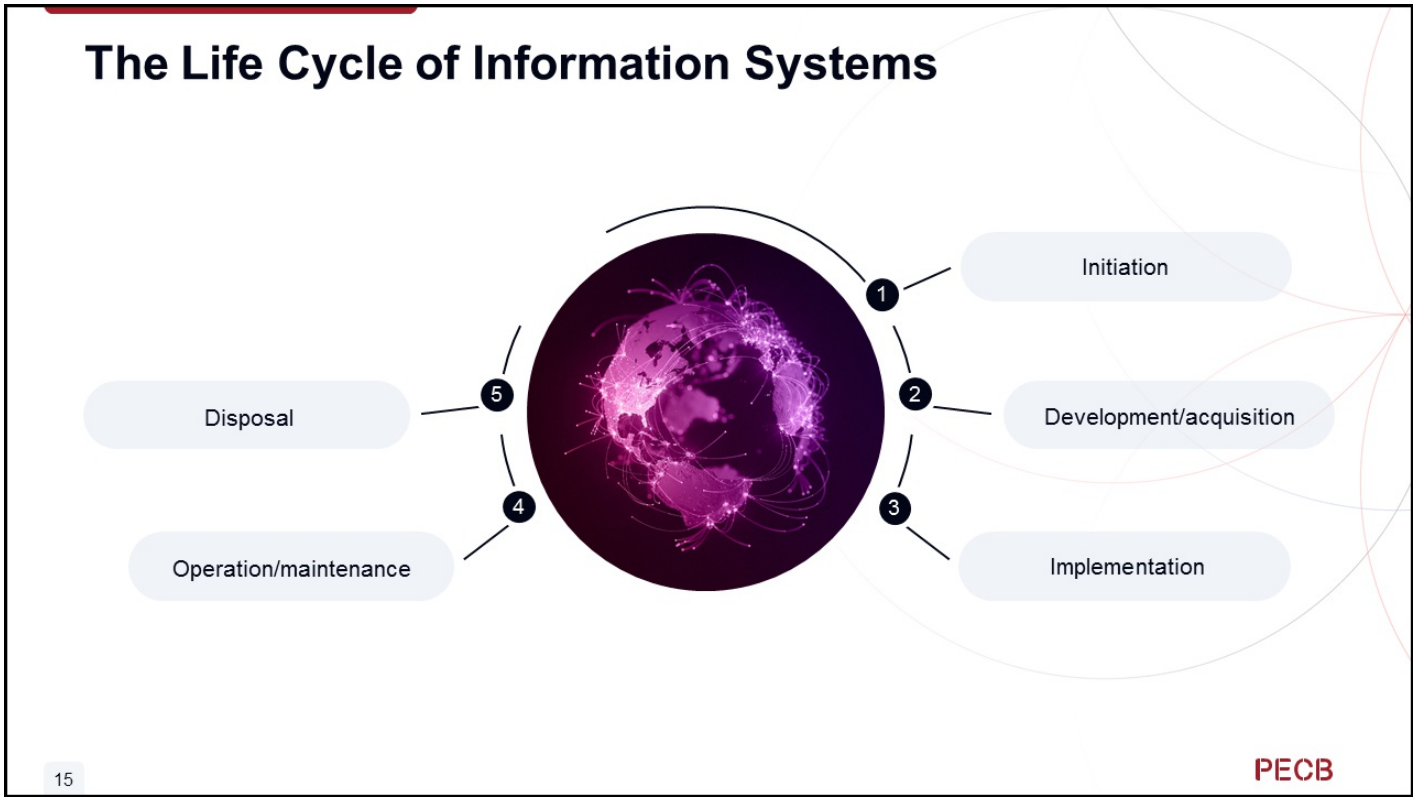
OSA provides a framework that explains the functionality and technical controls of security. It aims to present a holistic view of crucial security concerns, regulations, and concepts that form the fundamental architectural decisions when developing effective security architecture.[5]

It usually applies only after the security architecture has been designed.

Some of OSA examples include:

- Functionality and technical controls related to security
- Classification of techniques that provide protection for software integrity

PECB



NIST SP 800-27 Rev A outlines the five stages of developing and deploying information systems as follows[1]:

1. **Initiation:** In this stage, the need for a system is addressed and the objectives of the system are retained as documented information. An important activity in this stage is performing an effective risk assessment process.
2. **Development/acquisition:** In this stage, the system is developed. The identification and integration of security requirements are some of the activities conducted in this stage.
3. **Implementation:** During this stage, the system is assessed and implemented. Some of the activities conducted in this stage are implementing controls, assessing security, and acquiring certification and accreditation.
4. **Operation/maintenance:** In this stage, the system does its work. Usually, the system is adjusted by adding hardware and software and by various other events. Activities conducted in this stage are mainly related to the monitoring and assessment of the system.
5. **Disposal:** In this stage, information, hardware, and software are disposed. The information is transferred, stored, removed, or destroyed, and the media is sanitized.

2.1.2 Prepare for the Implementation of Controls

- The organization's security architecture determines the types of information security controls to be implemented.
- To effectively implement information security controls, the organization should:
  - Allocate the necessary resources to implement the applicable information security controls 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
  - Establish a 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
  - Determine the intended results

PECB

Prepare for the Implementation of Controls

- Prior to initiating the implementation of the selected information security controls, it is a good practice to establish the information security policies and procedures.
- Employees holding important information security responsibilities should be involved in drafting, reviewing, and validating the content of such procedures and policies.
- By involving employees in the process of drafting information security procedures and policies, organizations can motivate them to contribute in 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.

PECB

2.1.3 Design and Describe the Controls

- The design and description of the security controls selected for the ISMS should be properly documented.
- ISO/IEC 27001 does not provide any specific requirements regarding the documentation methods that the organization can use.
- 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

Section 14 Summary:

- The organization's security architecture represents a comprehensive approach which establishes information security infrastructure across the entire organization.
- 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.
- The Zachman Framework, SABSA, TOGAF, and OSA are some of the most commonly used architecture frameworks.
- According to NIST SP 800-27 Rev A , the life cycle of developing and deploying information systems consist of five main stages: initiation, development/acquisition, implementation, and operation/maintenance and disposal.
- Design and description of security controls selected to be implemented in the ISMS should be documented. ISO/IEC 27001 does not provide any specific requirements for documentation methods that organizations can use.

Questions?

Quiz 14

Note:To complete Quiz 14, please go to the Quizzes Worksheet.

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

Implementation of Controls

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

PECB

ISO/IEC 27001's Requirements for Operational Planning and Control

ISO/IEC 27001, clause 8.1

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Cause 6, by:

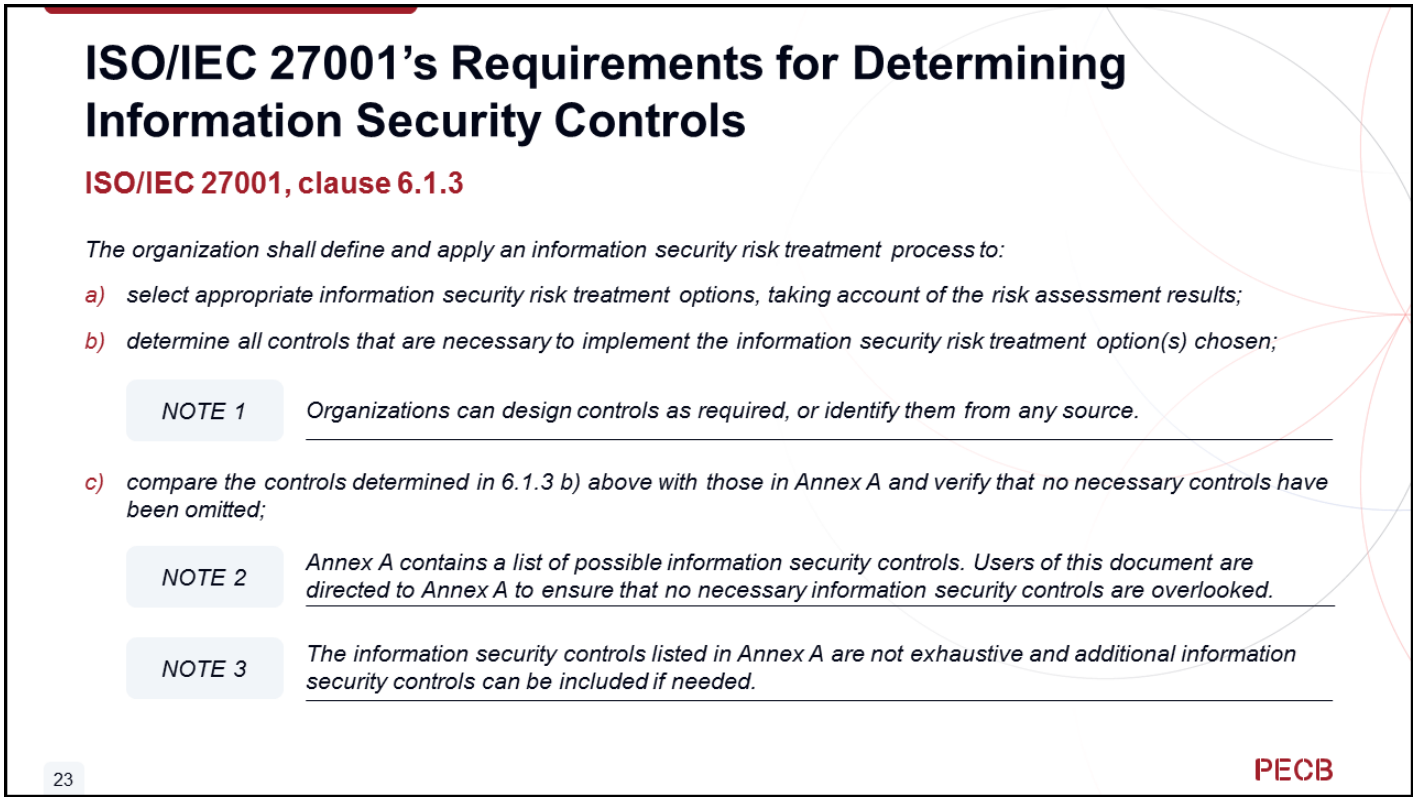
- *establishing criteria for the processes;*
- *implementing control of the processes in accordance with the criteria.*

Documented information shall be available 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 externally provided processes, products or services that are relevant to the information security management system are controlled.

PECB



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 6.1.3 Information security risk treatment

Guidance on determining necessary controls (6.1.3 b))

Special attention should be given to the determination of the necessary information security controls. Any control should be determined based on information security risks previously assessed. If an organization has a poor information security risk assessment, it has a poor foundation for its choice of information security controls.

Appropriate control determination ensures:

f.*all necessary controls are included, and no unnecessary controls are chosen; and*

g.*the design of necessary controls satisfies an appropriate breadth and depth.*

As a consequence of a poor choice of controls, the proposed information security risk treatment can be:

h.*ineffective; or*

i.*inefficient and therefore inappropriately expensive.*

To ensure that information security risk treatment is effective and efficient, it is therefore important to be able to demonstrate the relationship from the necessary controls back to the results of the risk assessment and risk treatment processes.

It can be necessary to use multiple controls to achieve the required treatment of the information security risk. For example, if the option to change the consequences of a particular event is chosen, it may require controls to effect prompt detection of the event as well as controls to respond to and recover from the event.

Slide Notes Extension

ISO/IEC 27003, clause 6.1.3 Information security risk treatment (cont'd)

When determining controls, the organization should also take into account controls needed for services from outside suppliers of e.g. applications, processes and functions. Typically, these controls are mandated by entering information security requirements in the agreements with these suppliers, including ways to get information about to which extent these requirements are met (e.g. right of audit). There may be situations where the organization wishes to determine and describe detailed controls as being part of its own ISMS even though the controls are carried out by outside suppliers. Independently of the approach taken, the organization always should consider controls needed at their suppliers when determining controls for its ISMS.

Guidance on comparing controls with those in ISO/IEC 27001, Annex A (6.1.3 c))

ISO/IEC 27001, Annex A contains a comprehensive list of control objectives and controls. Users of this document are directed to the generic representation of controls in ISO/IEC 27001, Annex A to ensure that no necessary controls are overlooked. Comparison with ISO/IEC 27001, Annex A can also identify alternative controls to those determined in 6.1.3 b) which can be more effective at modifying information security risk.

Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in ISO/IEC 27001, Annex A are not exhaustive and additional control objectives and controls should be added as needed.

Not every control within ISO/IEC 27001, Annex A needs to be included. Any control within ISO/IEC 27001, Annex A that does not contribute to modifying risk should be excluded and justification for the exclusion should be given.

Introduction of Annex A Controls

- Annex A of ISO/IEC 27001 contains a list of possible information security controls. The controls of Annex A are derived from ISO/IEC 27002 controls.
- Annex A includes 93 information security controls that are grouped into four categories.

5

Organizational controls

5.1-5.37

6

People controls

6.1-6.8

7

Physical controls

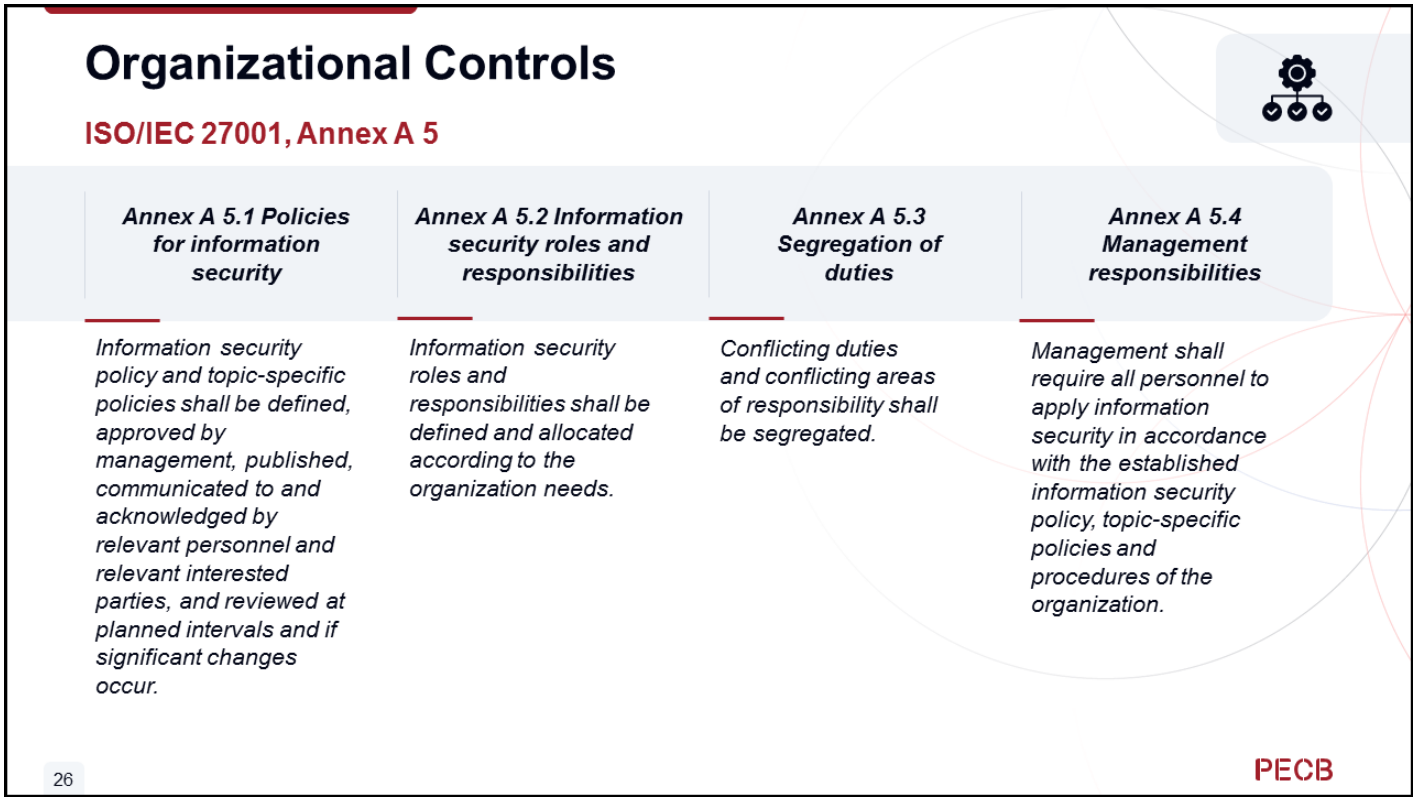
7.1-7.14

8

Technological controls

8.1-8.34

PECB



ISO/IEC 27002, clause 5.1 Policies for information security

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

ISO/IEC 27002, clause 5.2 Information security roles and responsibilities

Purpose

To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.

ISO/IEC 27002, clause 5.3 Segregation of duties

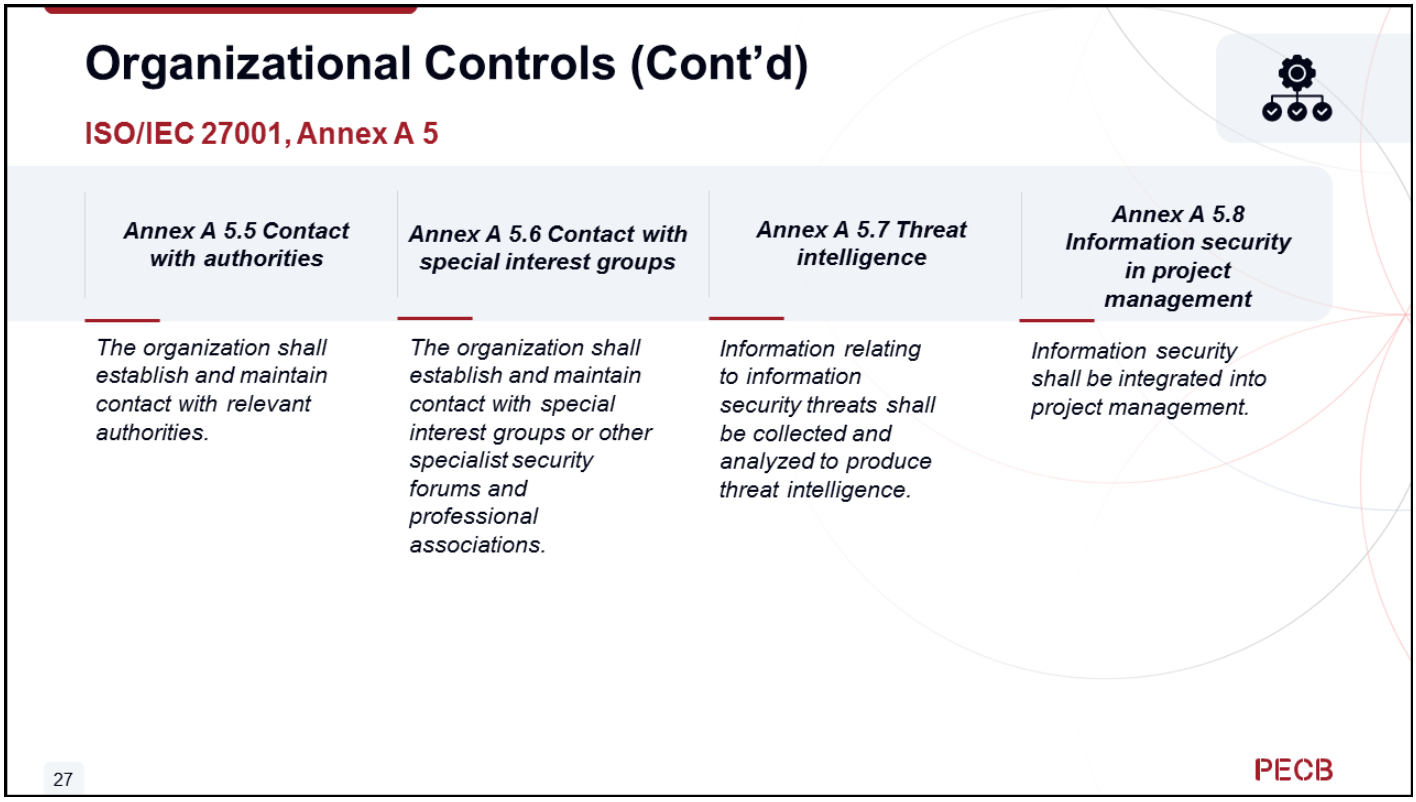
Purpose

To reduce the risk of fraud, error and bypassing of information security controls.

ISO/IEC 27002, clause 5.4 Management responsibilities

Purpose

To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.



ISO/IEC 27002, clause 5.5 Contact with authorities

Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

ISO/IEC 27002, clause 5.6 Contact with special interest groups

Purpose

To ensure appropriate flow of information takes place with respect to information security.

ISO/IEC 27002, clause 5.7 Threat intelligence

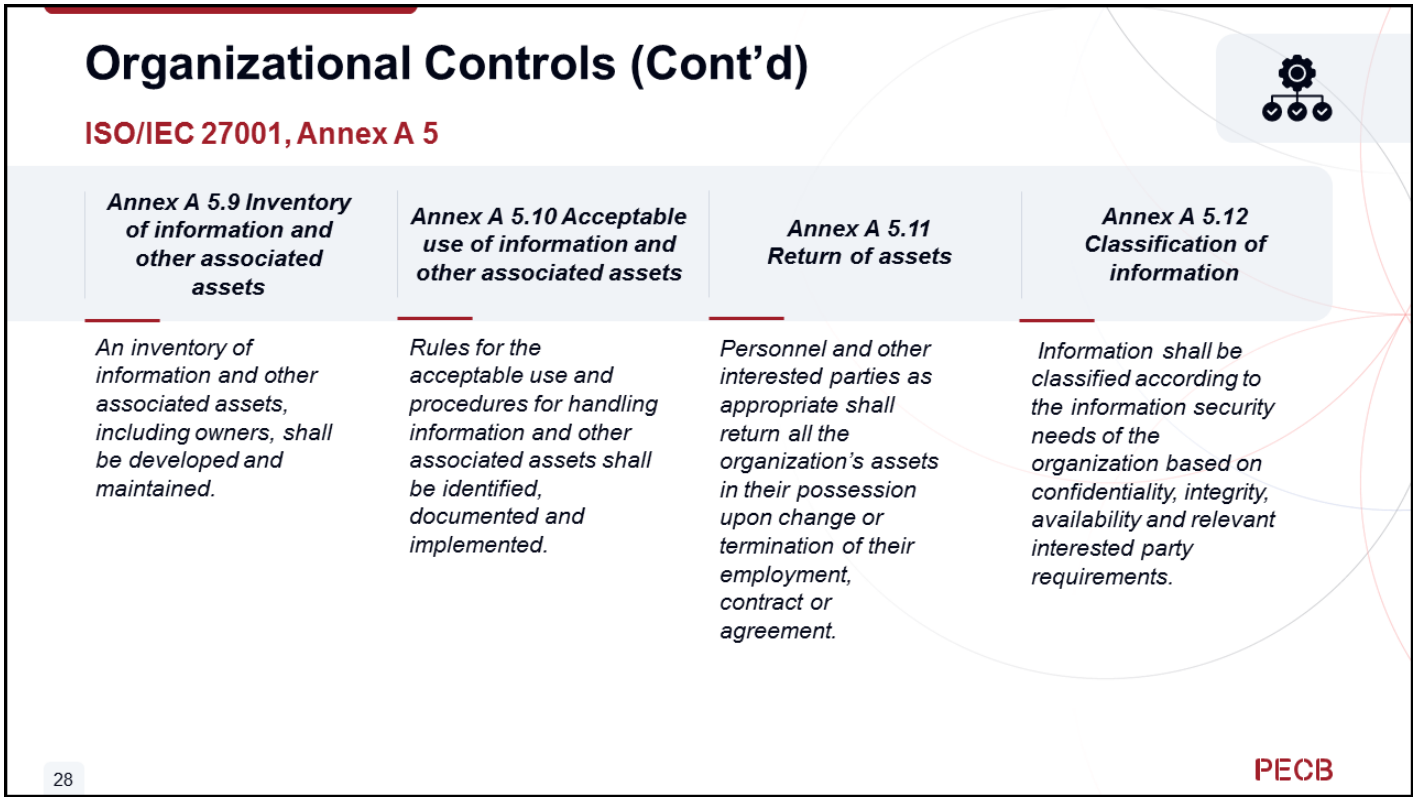
Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

ISO/IEC 27002, clause 5.8 Information security in project management

Purpose

To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.



ISO/IEC 27002, clause 5.9 Inventory of information and other associated assets

Purpose

To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.

ISO/IEC 27002, clause 5.10 Acceptable use of information and other associated assets

Purpose

To ensure information and other associated assets are appropriately protected, used and handled.

ISO/IEC 27002, clause 5.11 Return of assets

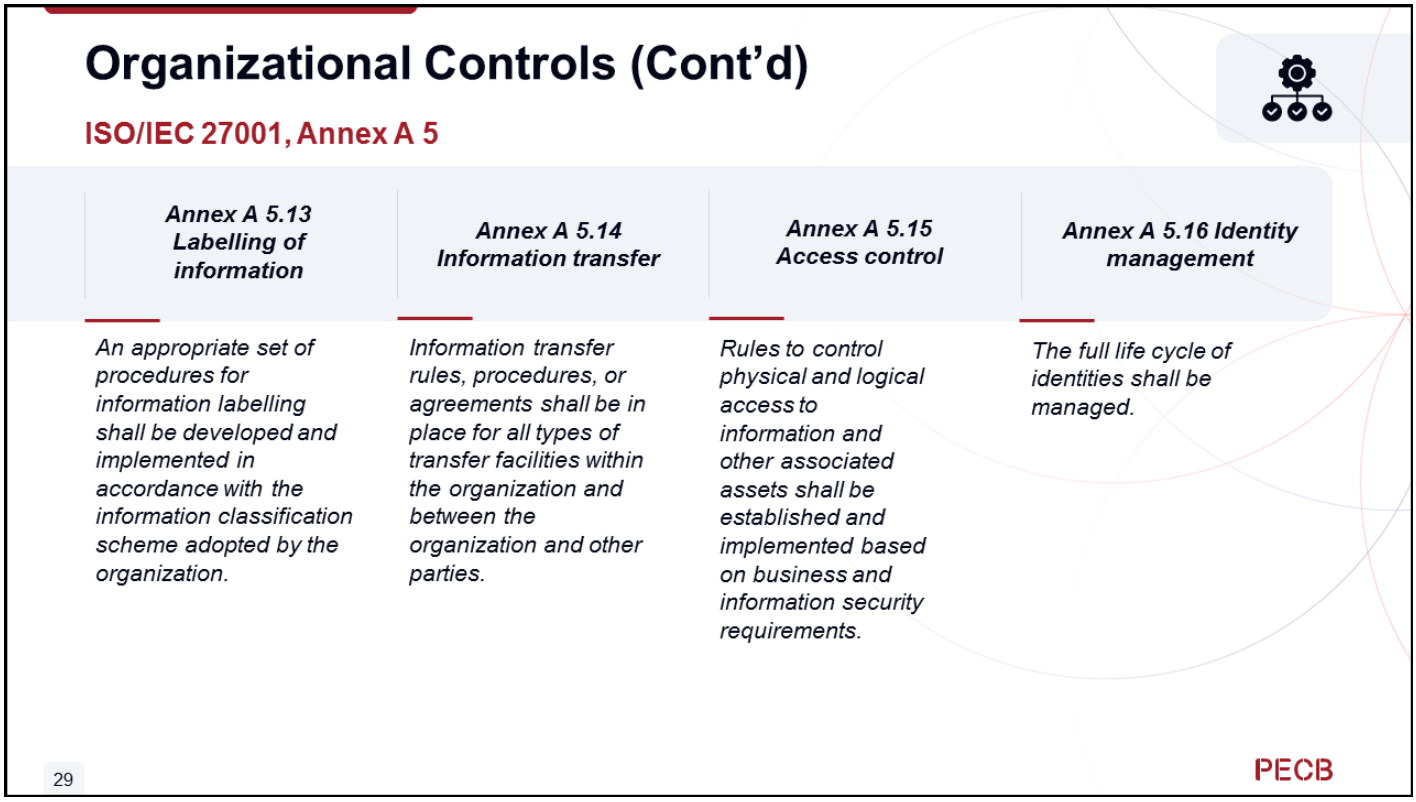
Purpose

To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.

ISO/IEC 27002, clause 5.12 Classification of information

Purpose

To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.



ISO/IEC 27002, clause 5.13 Labelling of information

Purpose

To facilitate the communication of classification of information and support automation of information processing and management.

ISO/IEC 27002, clause 5.14 Information transfer

Purpose

To maintain the security of information transferred within an organization and with any external interested party.

ISO/IEC 27002, clause 5.15 Access control

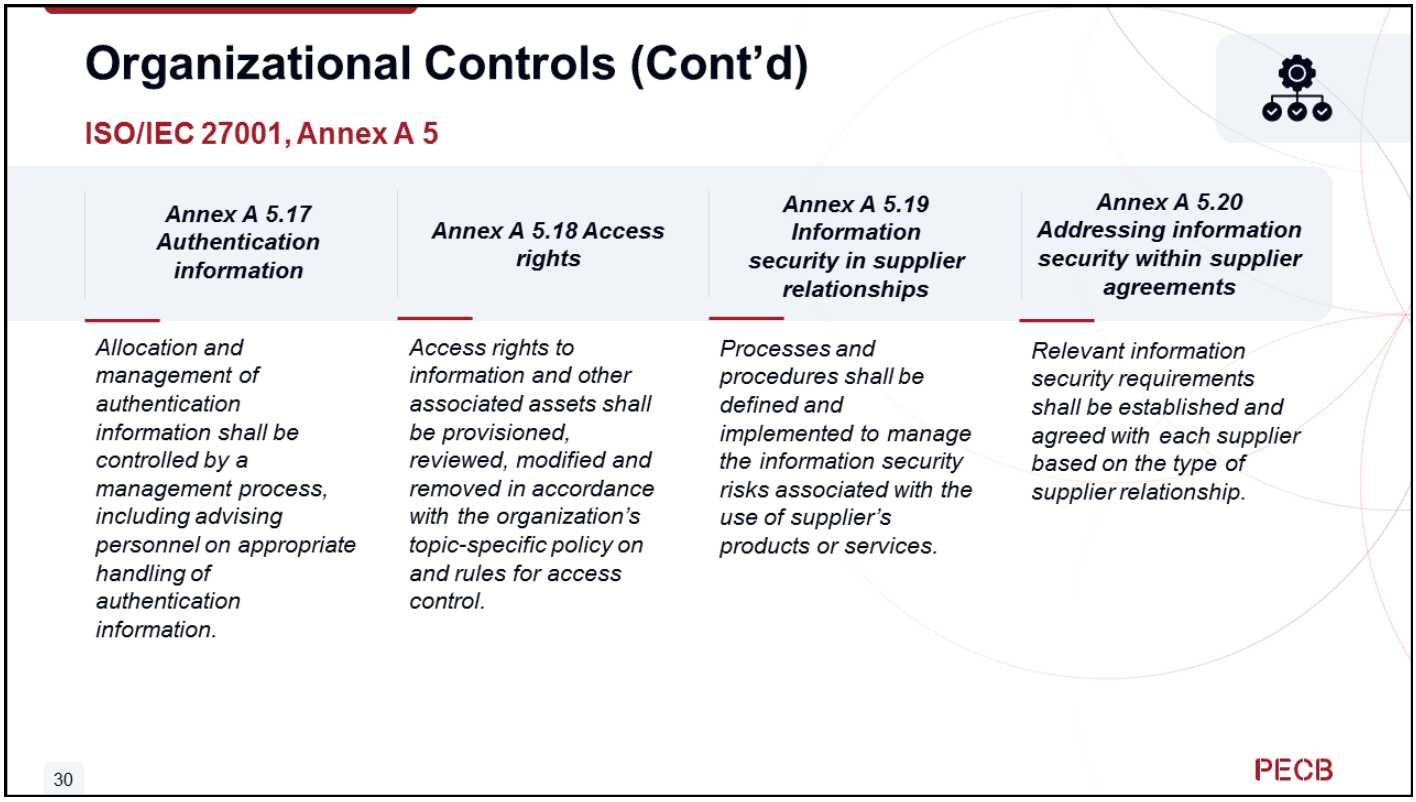
Purpose

To ensure authorized access and to prevent unauthorized access to information and other associated assets.

ISO/IEC 27002, clause 5.16 Identity management

Purpose

To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.



ISO/IEC 27002, clause 5.17 Authentication information

Purpose

To ensure proper entity authentication and prevent failures of authentication processes.

ISO/IEC 27002, clause 5.18 Access rights

Purpose

To ensure access to information and other associated assets is defined and authorized according to the business requirements.

ISO/IEC 27002, clause 5.19 Information security in supplier relationships

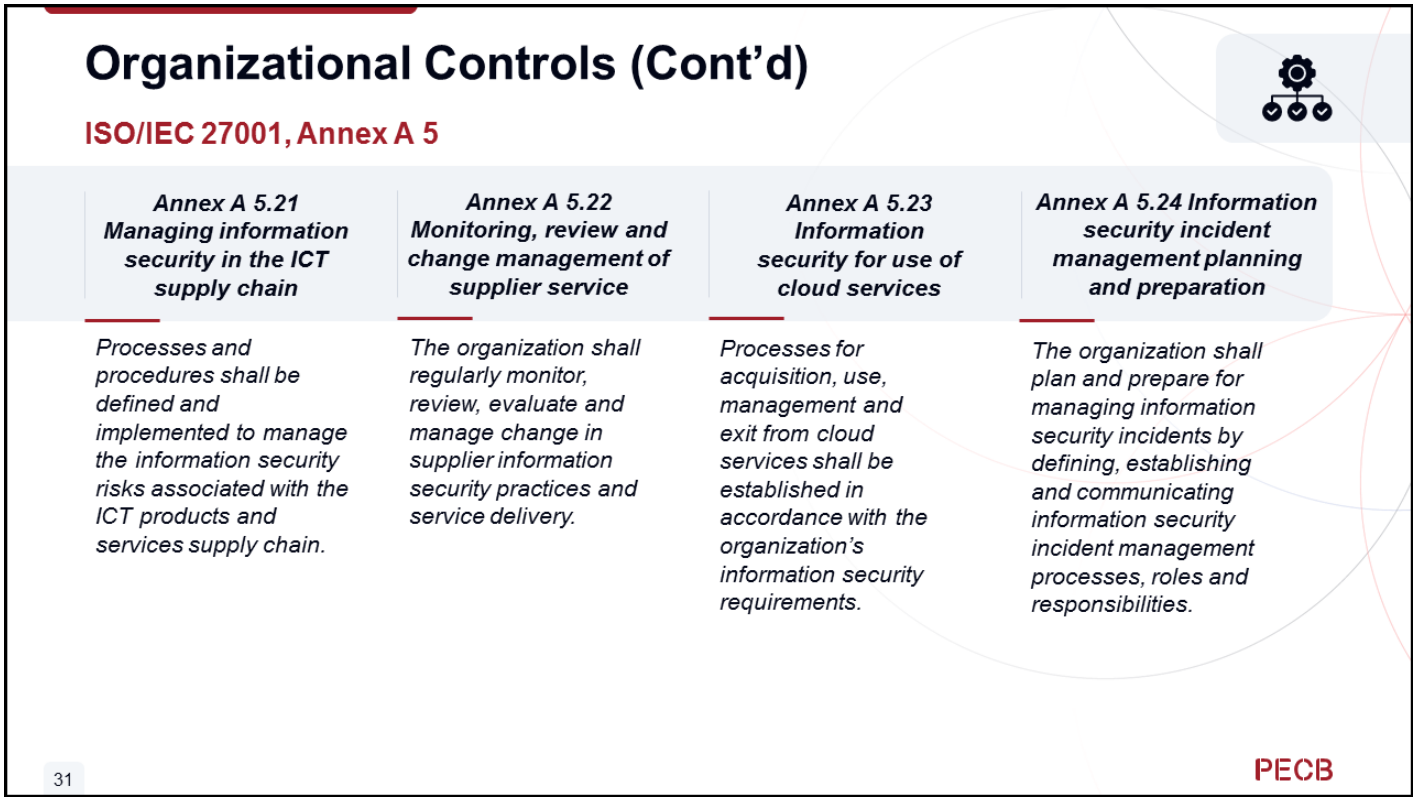
Purpose

To maintain an agreed level of information security in supplier relationships.

ISO/IEC 27002, clause 5.20 Addressing information security within supplier agreements

Purpose

To maintain an agreed level of information security in supplier relationships.



ISO/IEC 27002, clause 5.21 Managing information security in the ICT supply chain

Purpose

To maintain an agreed level of information security in supplier relationships.

ISO/IEC 27002, clause 5.22 Monitoring, review and change management of supplier services

Purpose

To maintain an agreed level of information security and service delivery in line with supplier agreements.

ISO/IEC 27002, clause 5.23 Information security for use of cloud services

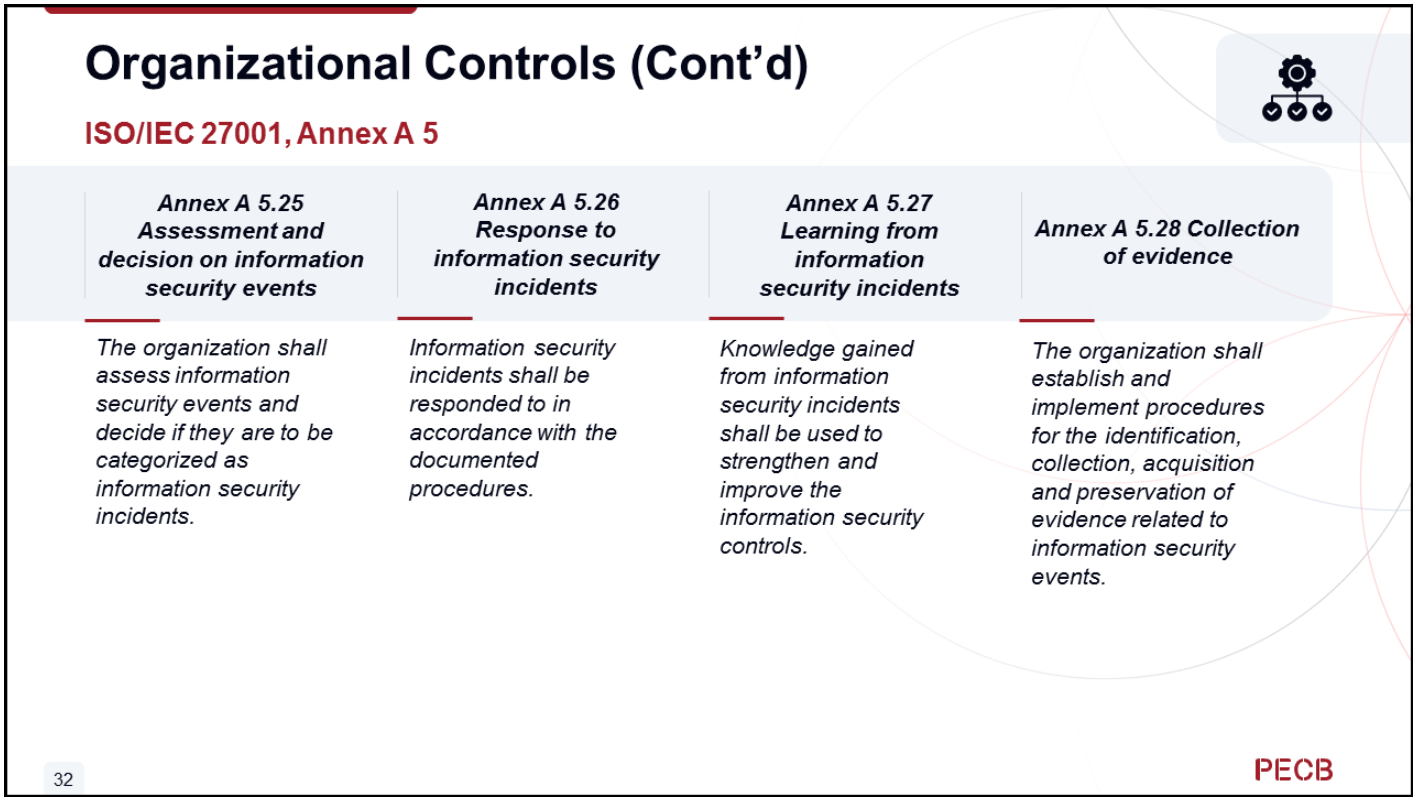
Purpose

To specify and manage information security for the use of cloud services.

ISO/IEC 27002, clause 5.24 Information security incident management planning and preparation

Purpose

To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.



ISO/IEC 27002, clause 5.25 Assessment and decision on information security events

Purpose

To ensure effective categorization and prioritization of information security events.

ISO/IEC 27002, clause 5.26 Response to information security incidents

Purpose

To ensure efficient and effective response to information security incidents.

ISO/IEC 27002, clause 5.27 Learning from information security incidents

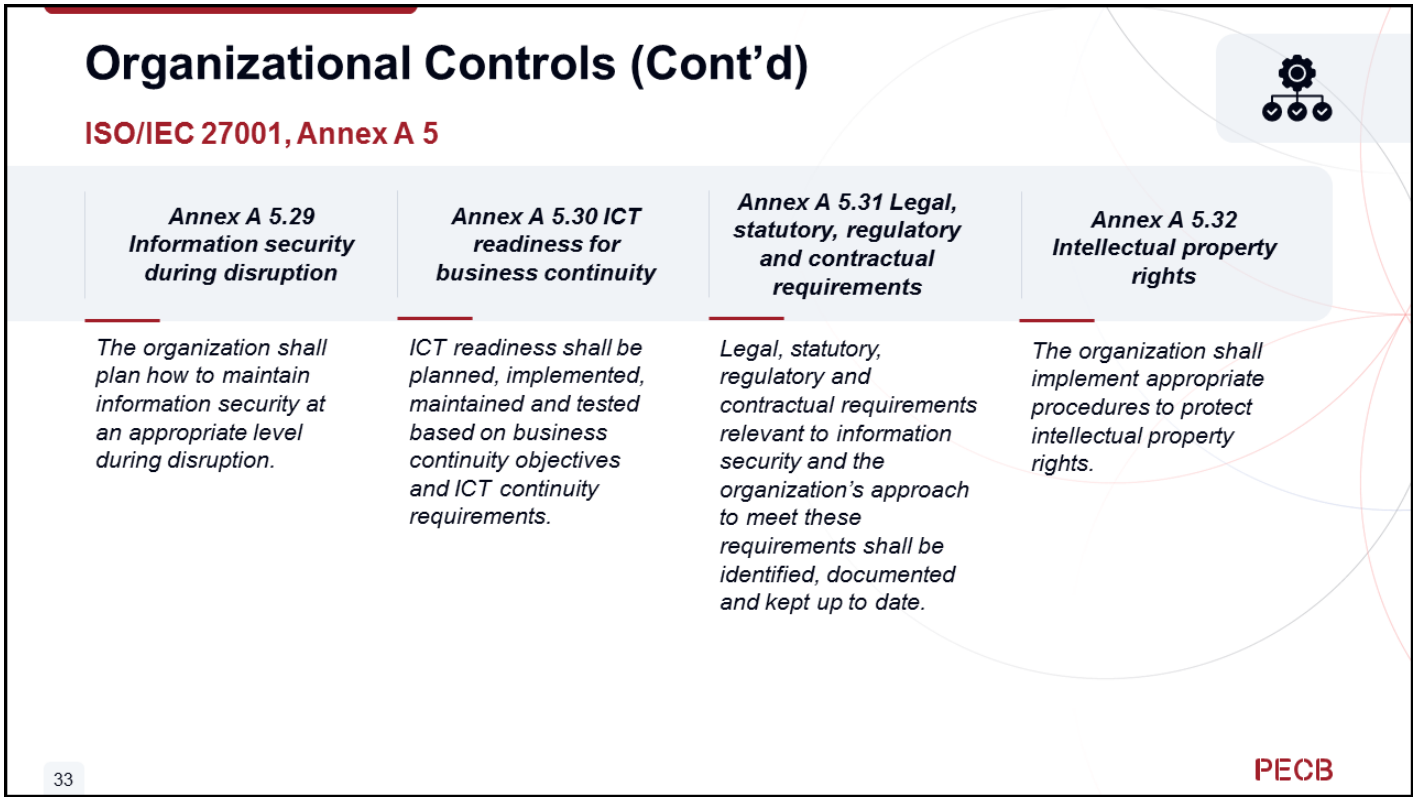
Purpose

To reduce the likelihood or consequences of future incidents.

ISO/IEC 27002, clause 5.28 Collection of evidence

Purpose

To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.



ISO/IEC 27002, clause 5.29 Information security during disruption

Purpose

To protect information and other associated assets during disruption.

ISO/IEC 27002, clause 5.30 ICT readiness for business continuity

Purpose

To ensure the availability of the organization's information and other associated assets during disruption.

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

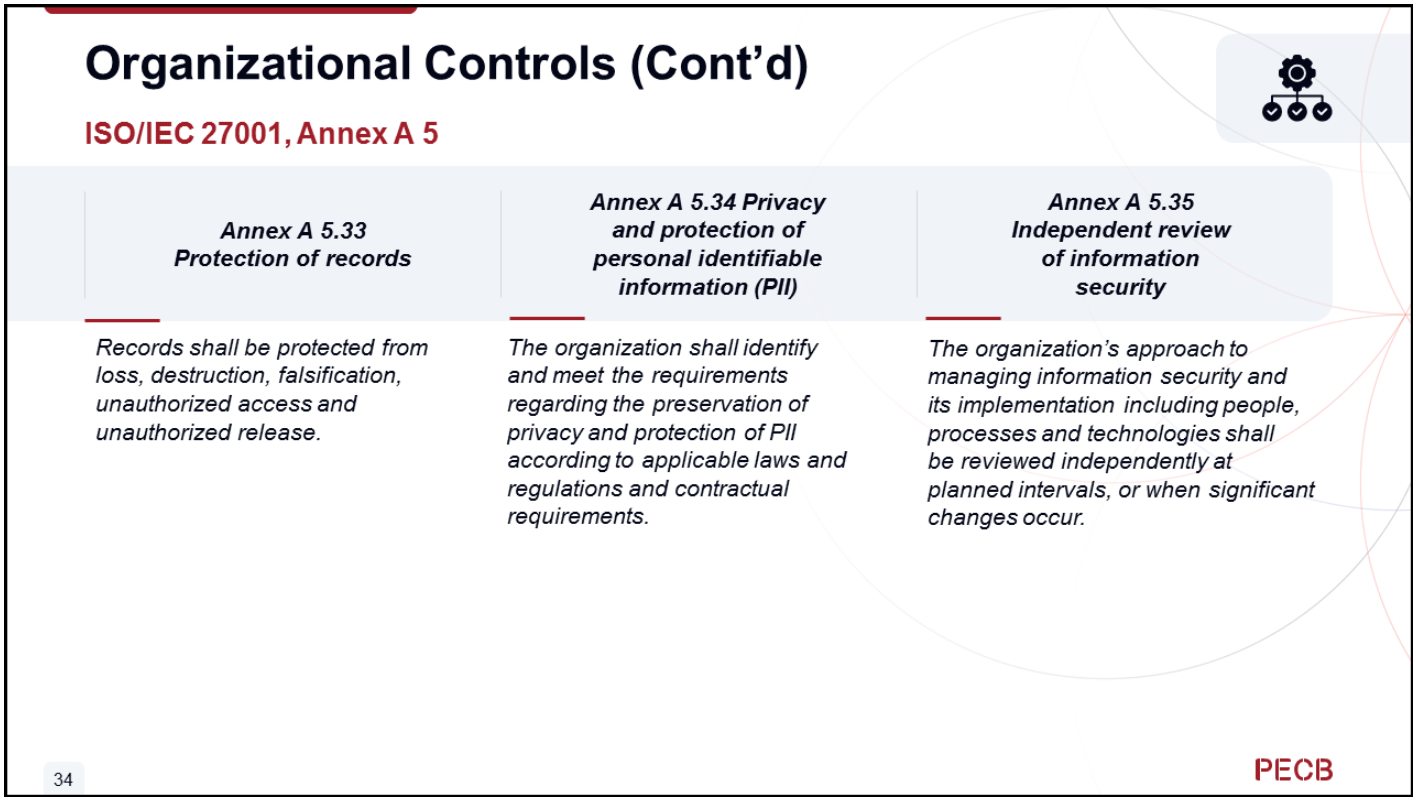
Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.

ISO/IEC 27002, clause 5.32 Intellectual property rights

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.



ISO/IEC 27002, control 5.33 Protection of records

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

ISO/IEC 27002, control 5.34 Privacy and protection of personal identifiable information (PII)

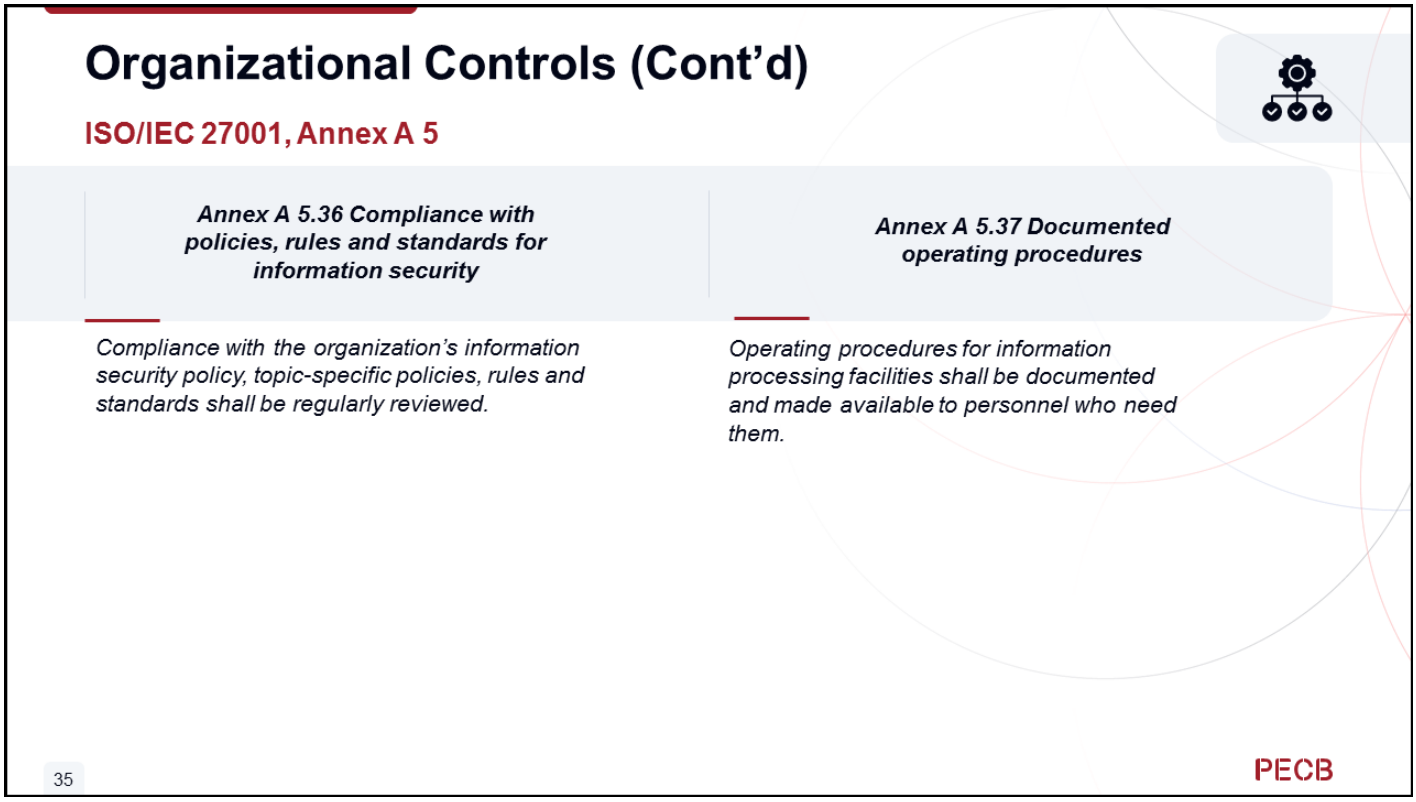
Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.

ISO/IEC 27002, control 5.35 Independent review of information security

Purpose

To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.



ISO/IEC 27002, clause 5.36 Compliance with policies, rules and standards for information security

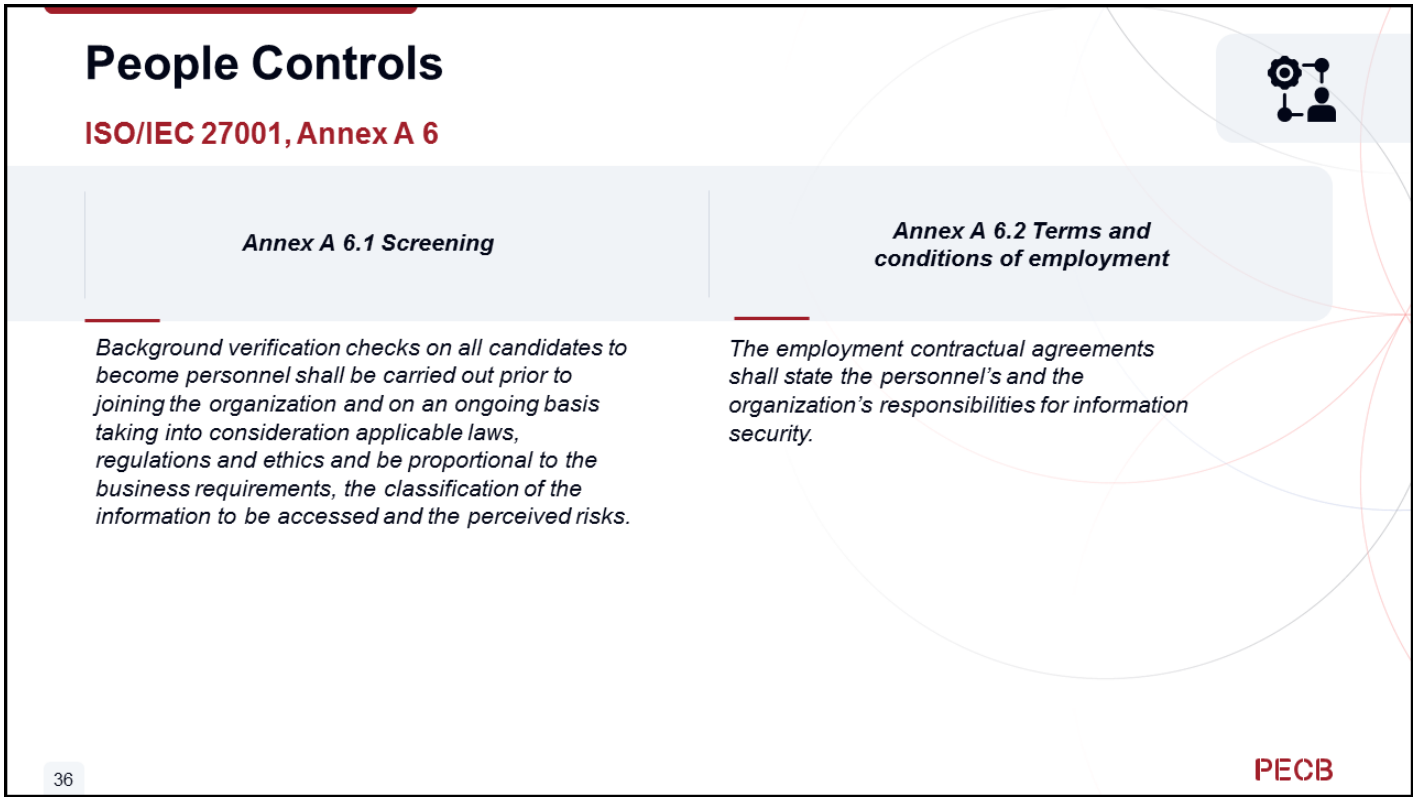
Purpose

To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.

ISO/IEC 27002, clause 5.37 Documented operating procedures

Purpose

To ensure the correct and secure operation of information processing facilities.



ISO/IEC 27002, clause 6.1 Screening

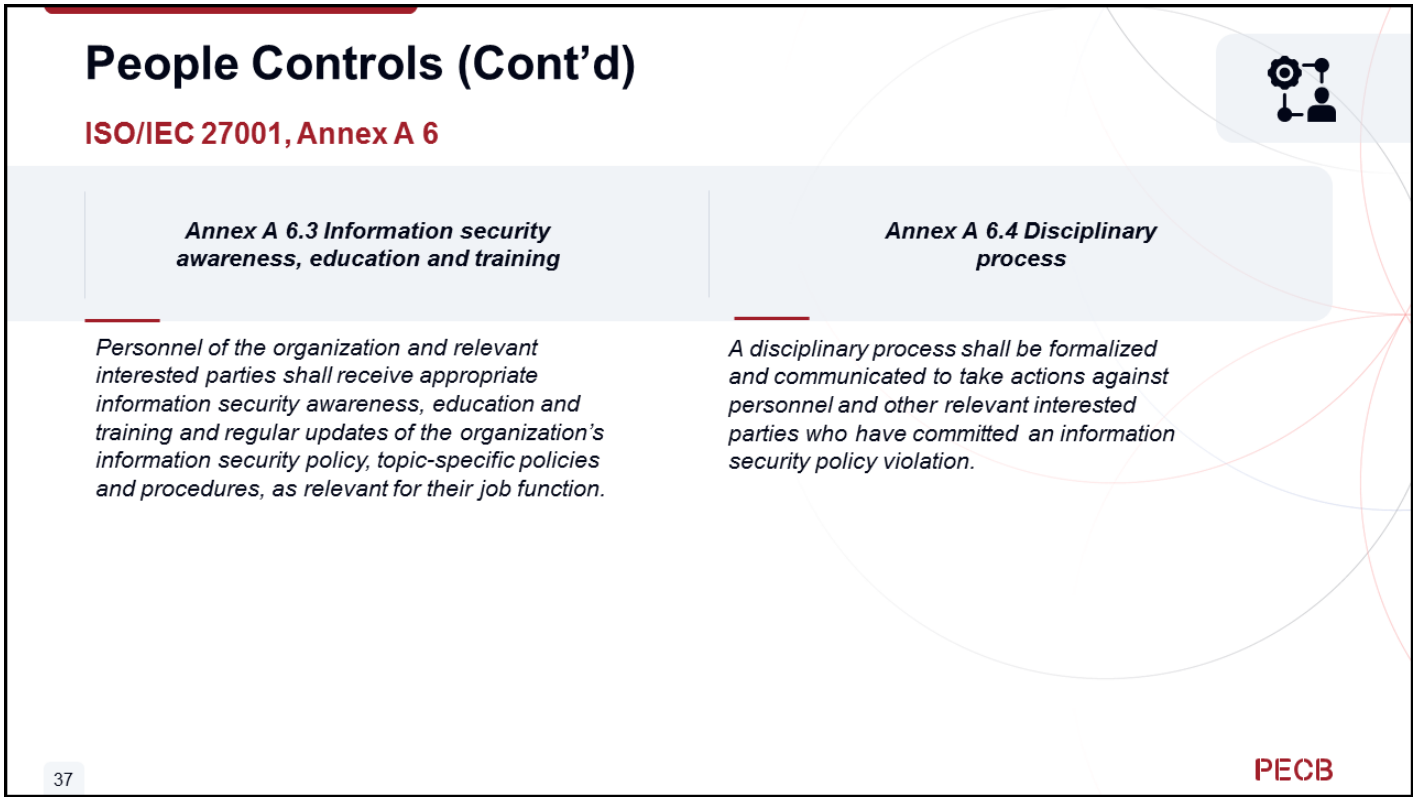
Purpose

To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

ISO/IEC 27002, clause 6.2 Terms and conditions of employment

Purpose

To ensure personnel understand their information security responsibilities for the roles for which they are considered.



ISO/IEC 27002, clause 6.3 Information security awareness, education and training

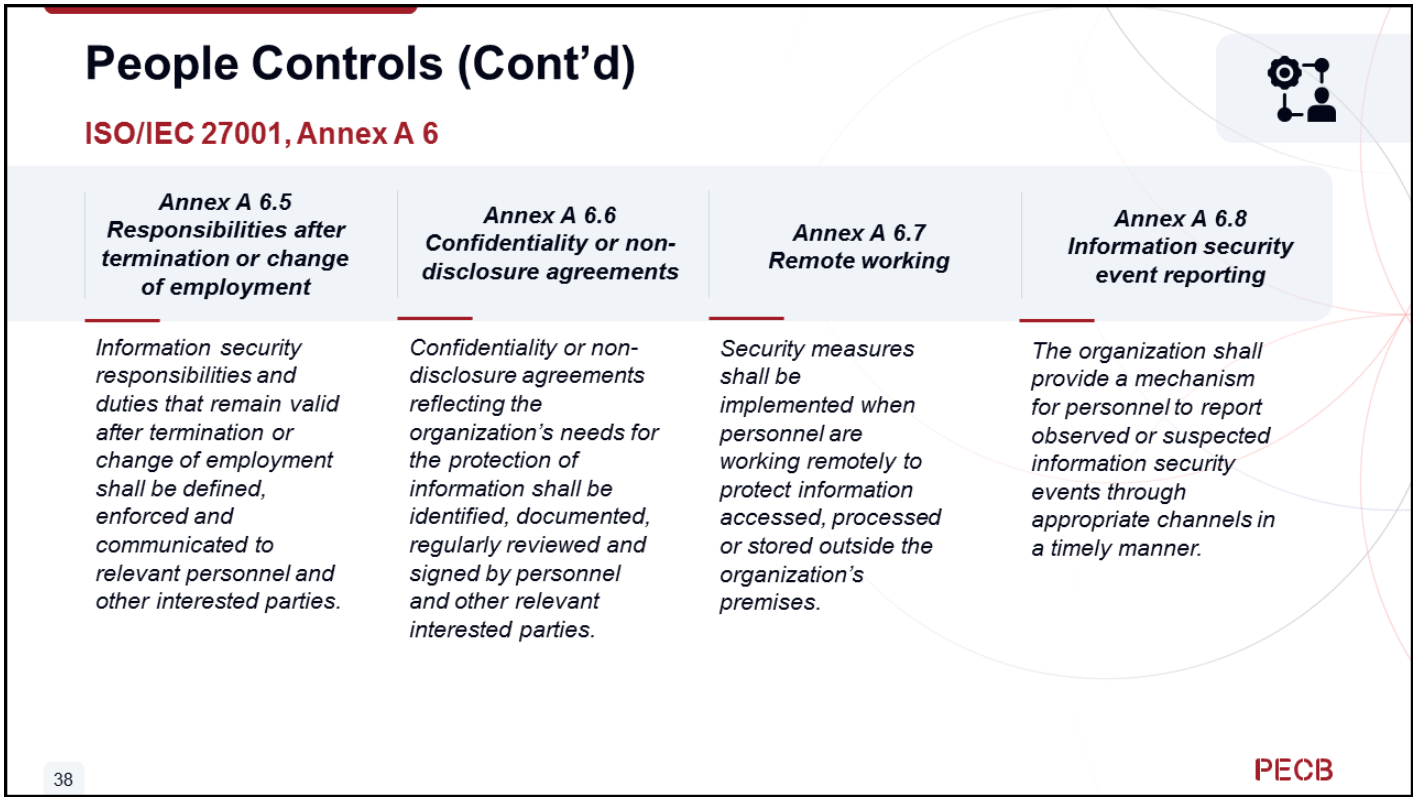
Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

ISO/IEC 27002, clause 6.4 Disciplinary process

Purpose

To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.



ISO/IEC 27002, clause 6.5 Responsibilities after termination or change of employment

Purpose

To protect the organization's interests as part of the process of changing or terminating employment or contracts.

ISO/IEC 27002, clause 6.6 Confidentiality or non-disclosure agreements

Purpose

To maintain confidentiality of information accessible by personnel or external parties.

ISO/IEC 27002, clause 6.7 Remote working

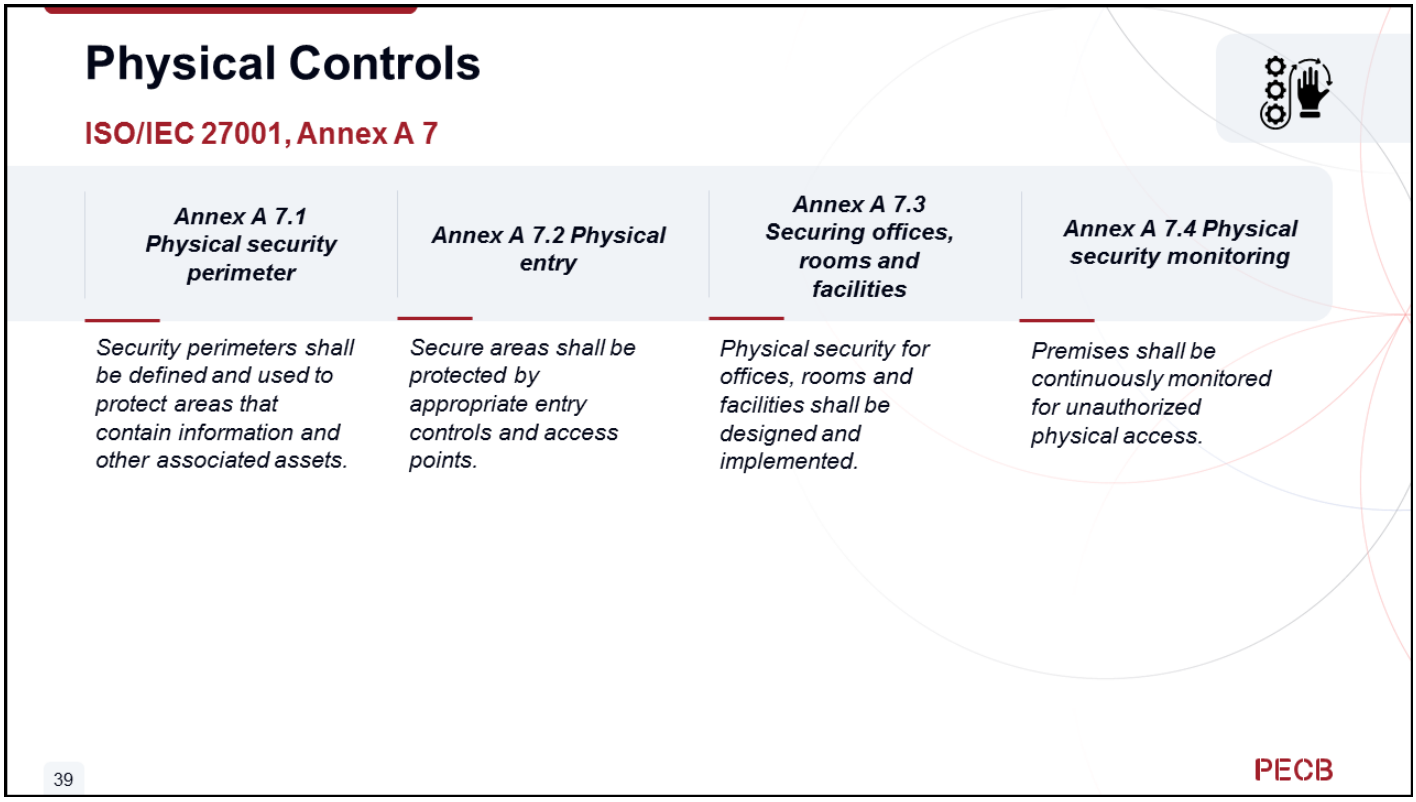
Purpose

To ensure the security of information when personnel are working remotely.

ISO/IEC 27002, clause 6.8 Information security event reporting

Purpose

To support timely, consistent and effective reporting of information security events that can be identified by personnel.



ISO/IEC 27002, clause 7.1 Physical security perimeter

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.

ISO/IEC 27002, clause 7.2 Physical entry

Purpose

To ensure only authorized physical access to the organization's information and other associated assets occurs.

ISO/IEC 27002, clause 7.3 Securing offices, rooms and facilities

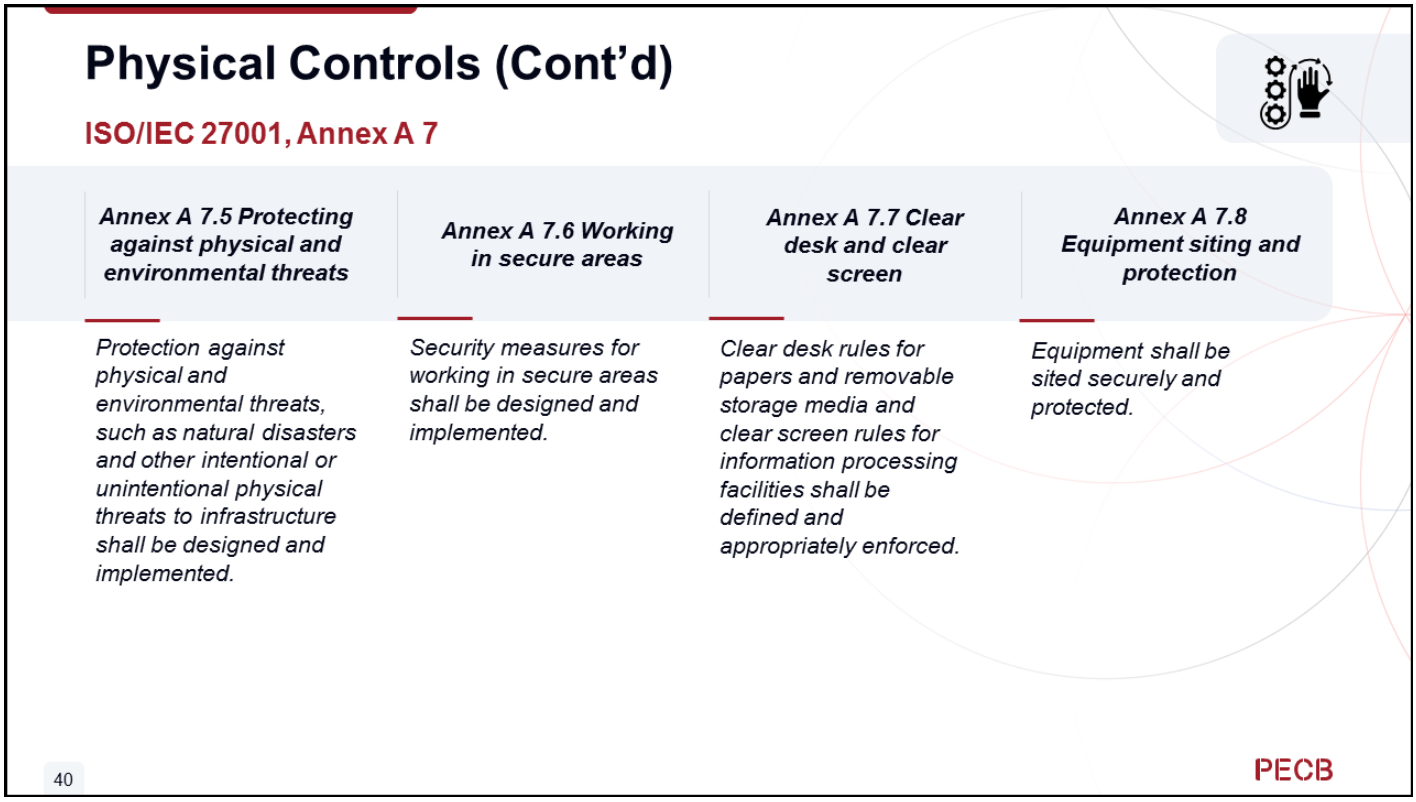
Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

ISO/IEC 27002, clause 7.4 Physical security monitoring

Purpose

To detect and deter unauthorized physical access.



ISO/IEC 27002, clause 7.5 Protecting against physical and environmental threats

Purpose

To prevent or reduce the consequences of events originating from physical and environmental threats.

ISO/IEC 27002, clause 7.6 Working in secure areas

Purpose

To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

ISO/IEC 27002, clause 7.7 Clear desk and clear screen

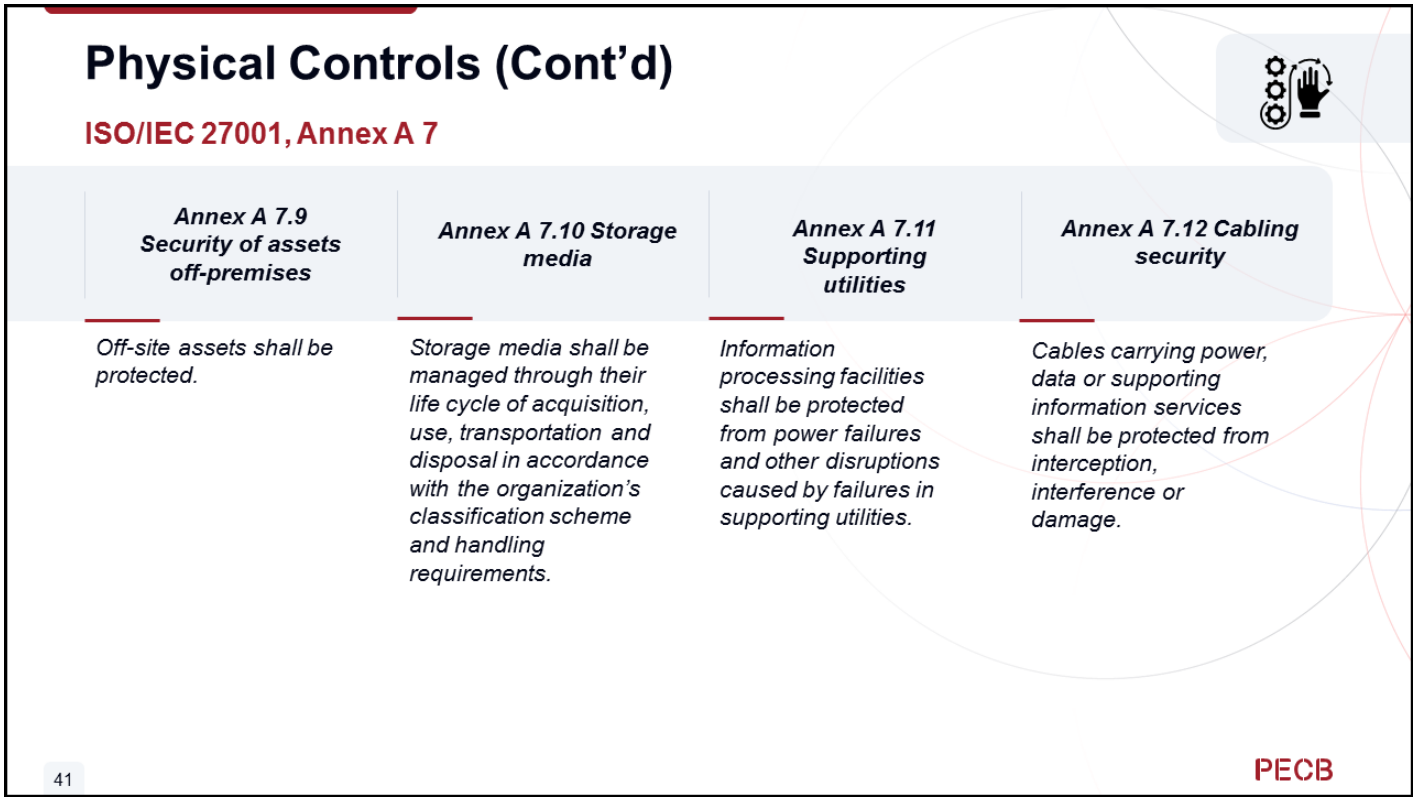
Purpose

To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

ISO/IEC 27002, clause 7.8 Equipment siting and protection

Purpose

To reduce the risks from physical and environmental threats, and from unauthorized access and damage.



ISO/IEC 27002, clause 7.9 Security of assets off-premises

Purpose

To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

ISO/IEC 27002, clause 7.10 Storage media

Purpose

To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

ISO/IEC 27002, clause 7.11 Supporting utilities

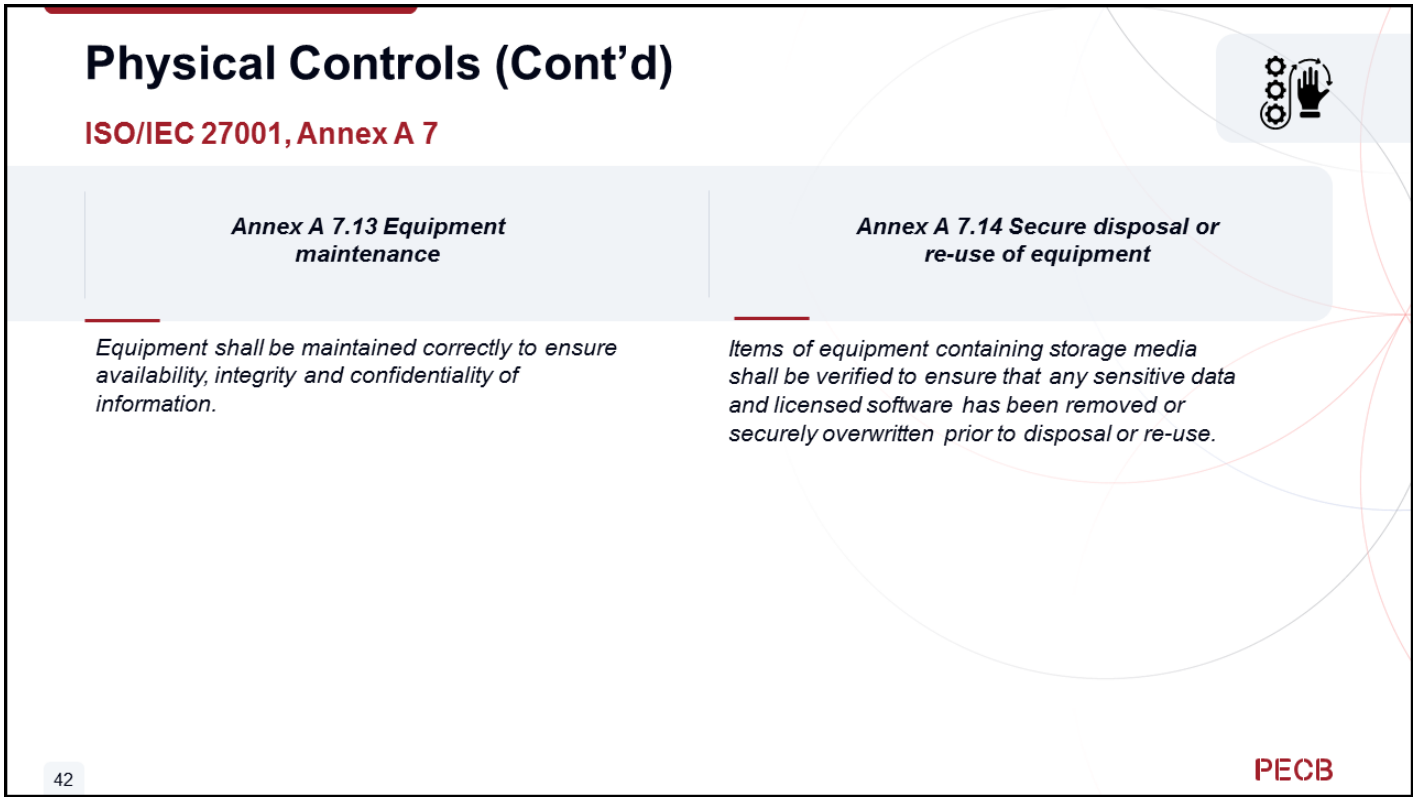
Purpose

To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

ISO/IEC 27002, clause 7.12 Cabling security

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.



ISO/IEC 27002, clause 7.13 Equipment maintenance

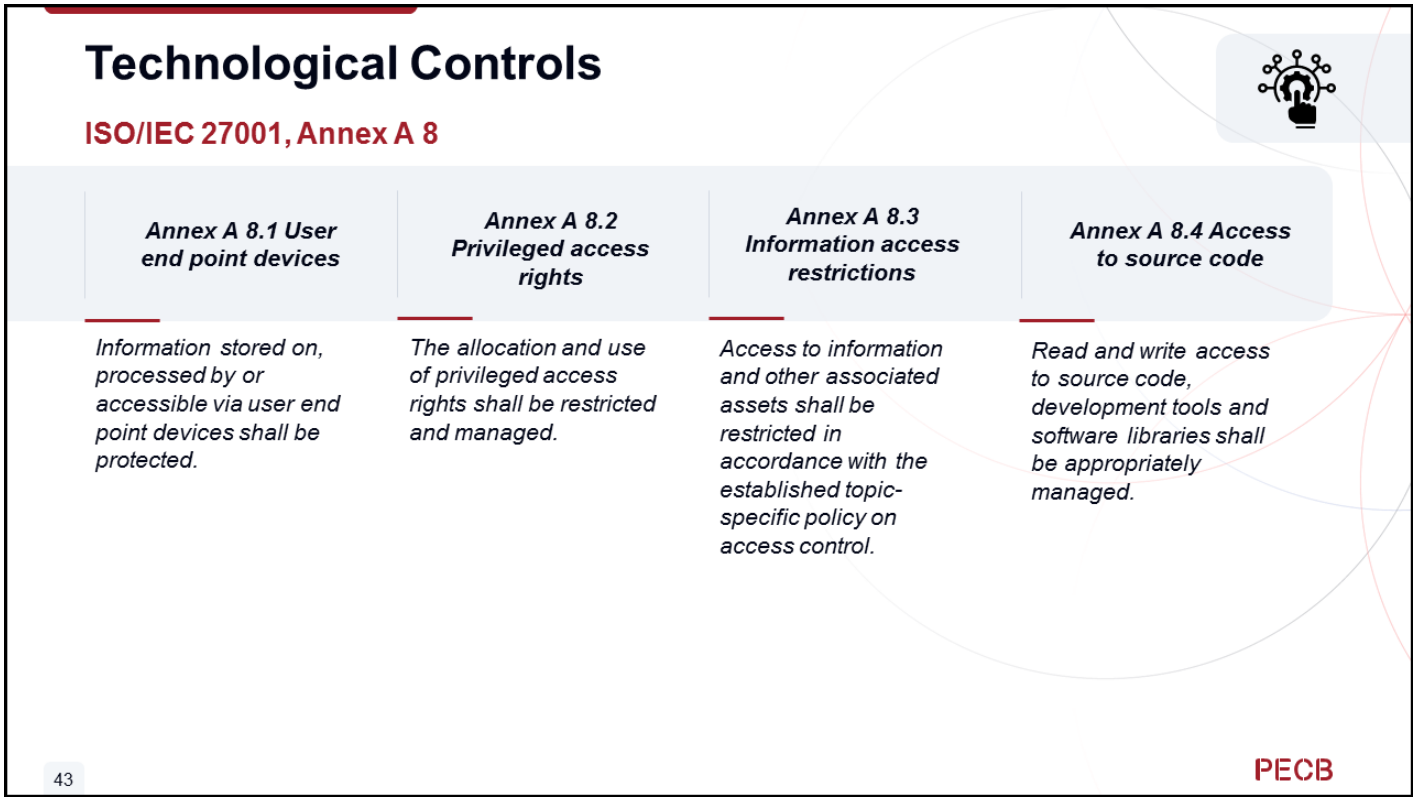
Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

ISO/IEC 27002, clause 7.14 Secure disposal or re-use of equipment

Purpose

To prevent leakage of information from equipment to be disposed or re-used.



ISO/IEC 27002, clause 8.1 User endpoint devices

Purpose

To protect information against the risks introduced by using user endpoint devices.

ISO/IEC 27002, clause 8.2 Privileged access rights

Purpose

To ensure only authorized users, software components and services are provided with privileged access rights.

ISO/IEC 27002, clause 8.3 Information access restrictions

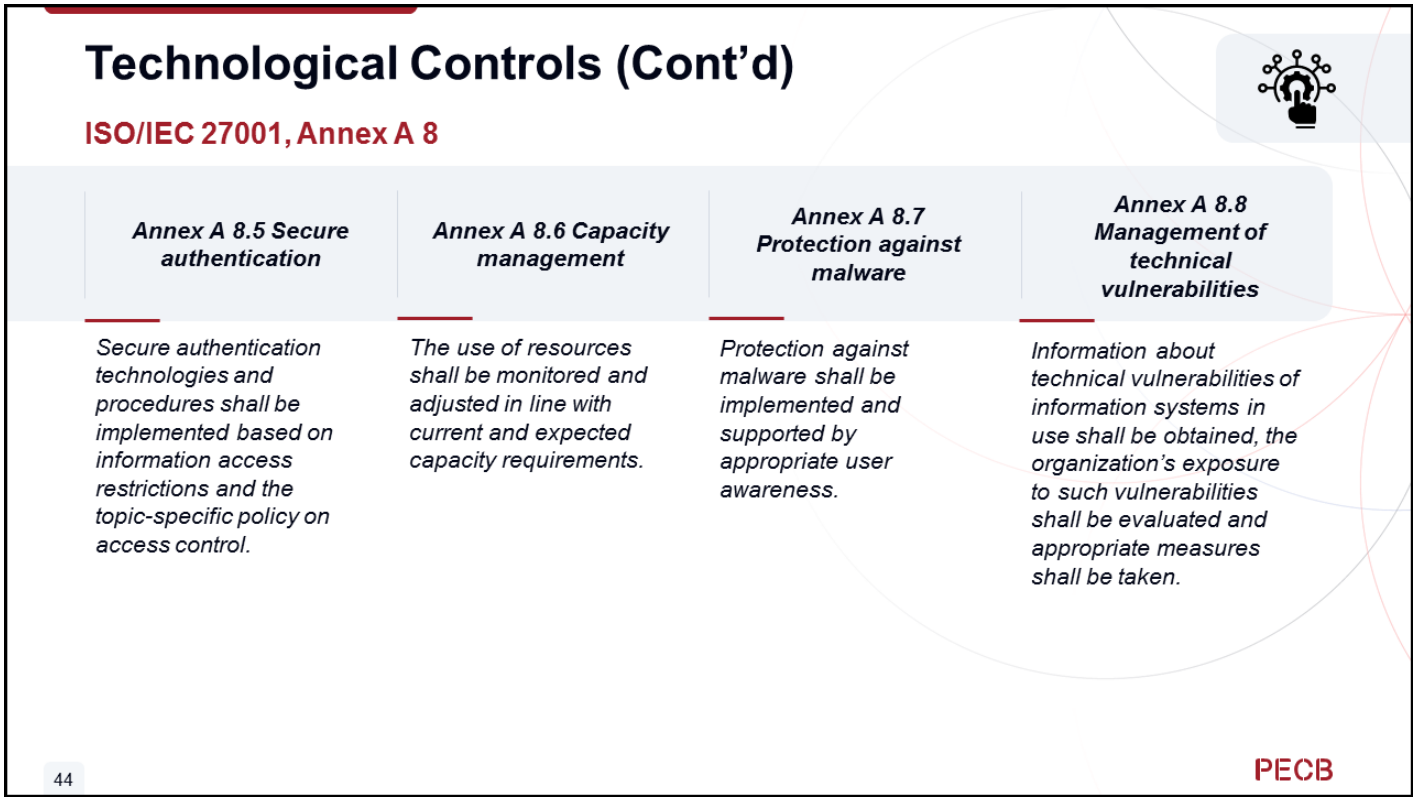
Purpose

To ensure only authorized access and to prevent unauthorized access to information and other associated assets.

ISO/IEC 27002, clause 8.4 Access to source code

Purpose

To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.



ISO/IEC 27002, clause 8.5 Secure authentication

Purpose

To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

ISO/IEC 27002, clause 8.6 Capacity management

Purpose

To ensure the required capacity of information processing facilities, human resources, offices and other facilities.

ISO/IEC 27002, clause 8.7 Protection against malware

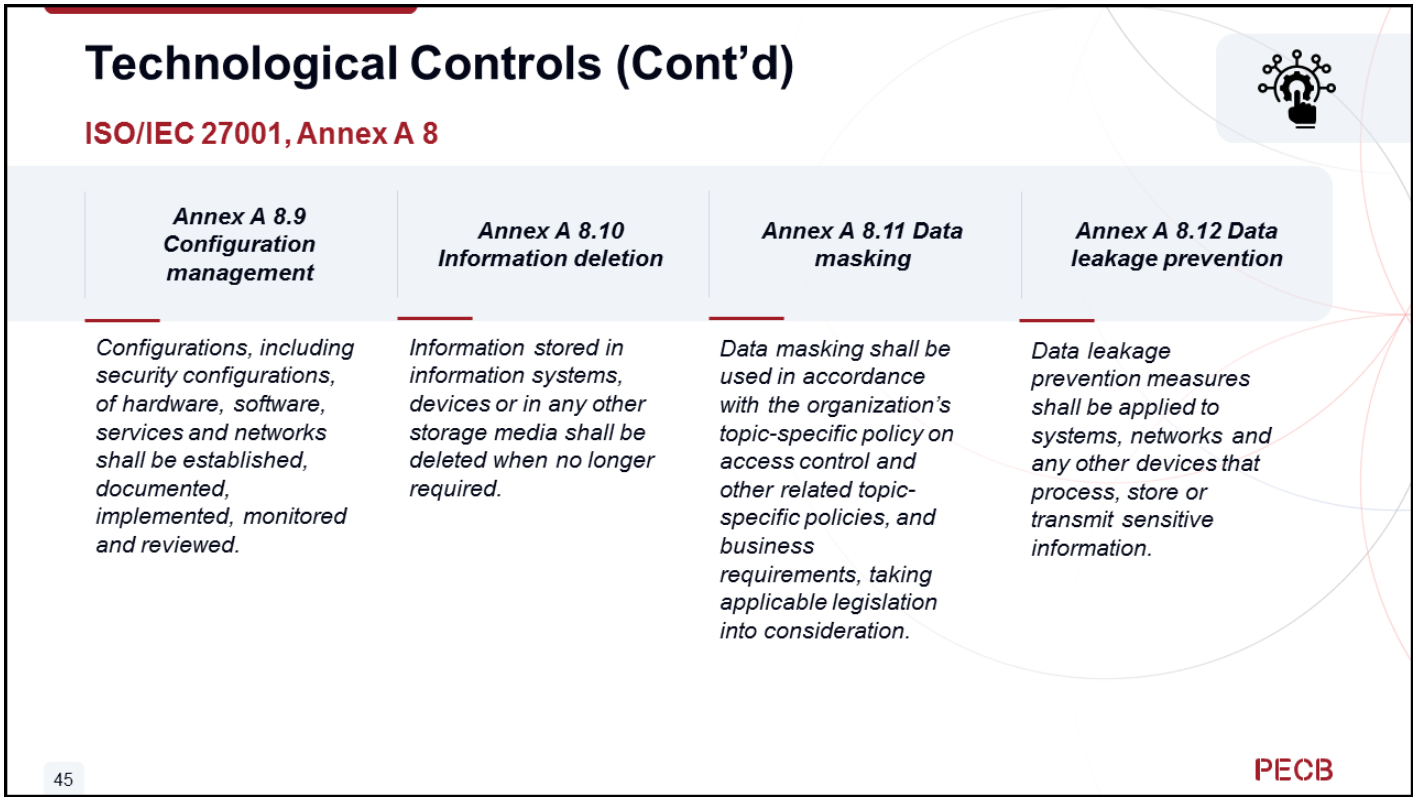
Purpose

To ensure information and other associated assets are protected against malware.

ISO/IEC 27002, clause 8.8 Management of technical vulnerabilities

Purpose

To prevent exploitation of technical vulnerabilities.



ISO/IEC 27002, clause 8.9 Configuration management

Purpose

To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

ISO/IEC 27002, clause 8.10 Information deletion

Purpose

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

ISO/IEC 27002, clause 8.11 Data masking

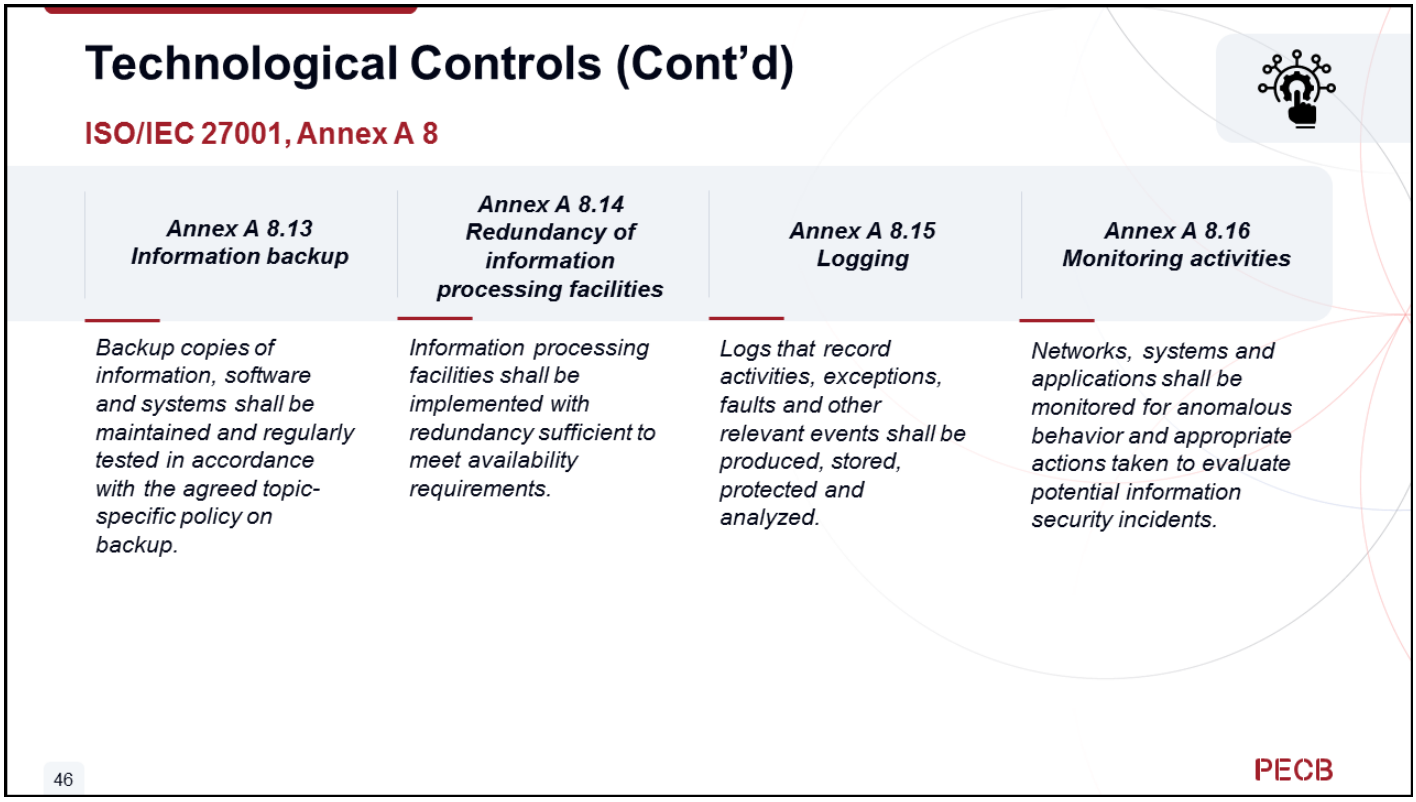
Purpose

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

ISO/IEC 27002, clause 8.12 Data leakage prevention

Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.



ISO/IEC 27002, clause 8.13 Information backup

Purpose

To enable recovery from loss of data or systems.

ISO/IEC 27002, clause 8.14 Redundancy of information processing facilities

Purpose

To ensure the continuous operation of information processing facilities.

ISO/IEC 27002, clause 8.15 Logging

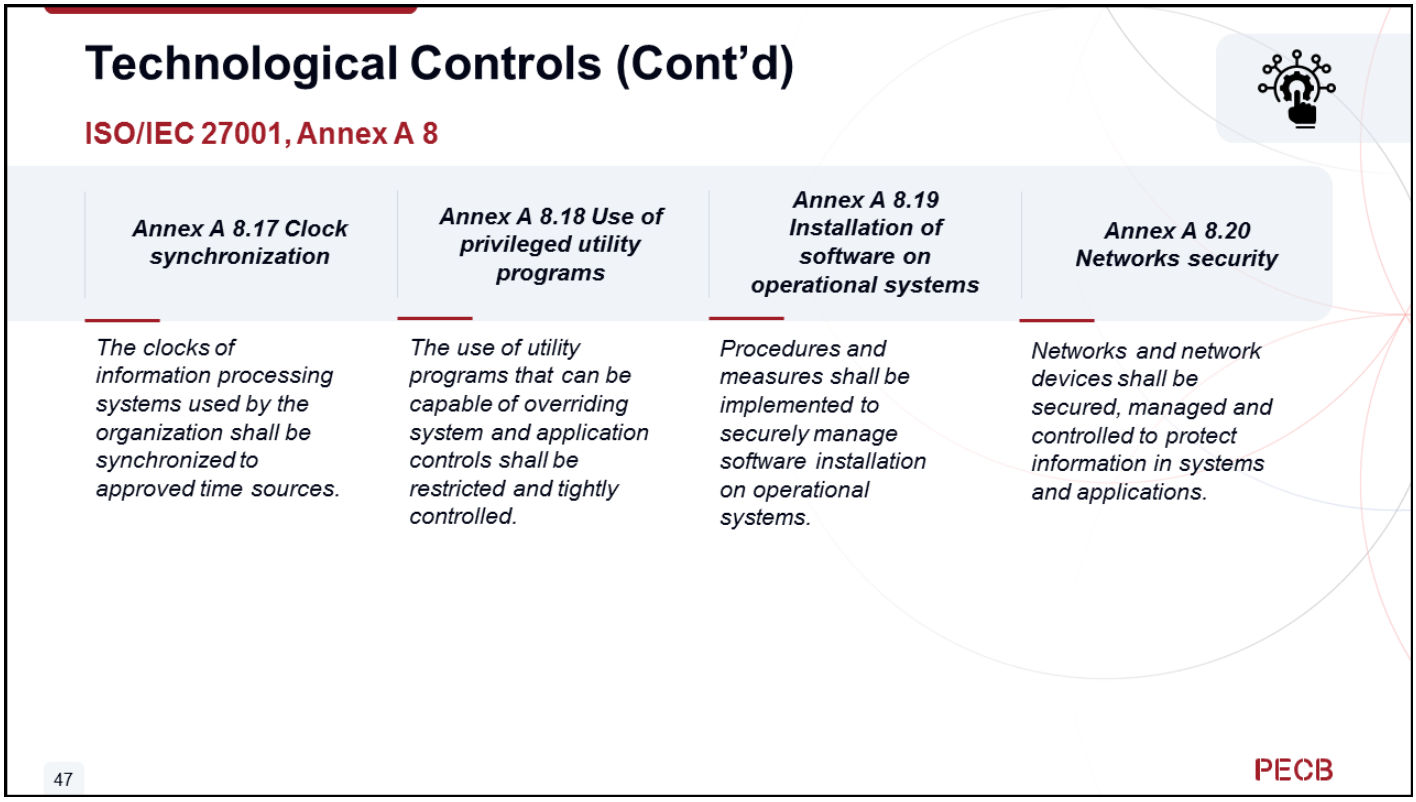
Purpose

To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

ISO/IEC 27002, clause 8.16 Monitoring activities

Purpose

To detect anomalous behavior and potential information security incidents.



ISO/IEC 27002, clause 8.17 Clock synchronization

Purpose

To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.

ISO/IEC 27002, clause 8.18 Use of privileged utility programs

Purpose

To ensure the use of utility programs does not harm system and application controls for information security.

ISO/IEC 27002, clause 8.19 Installation of software on operational systems

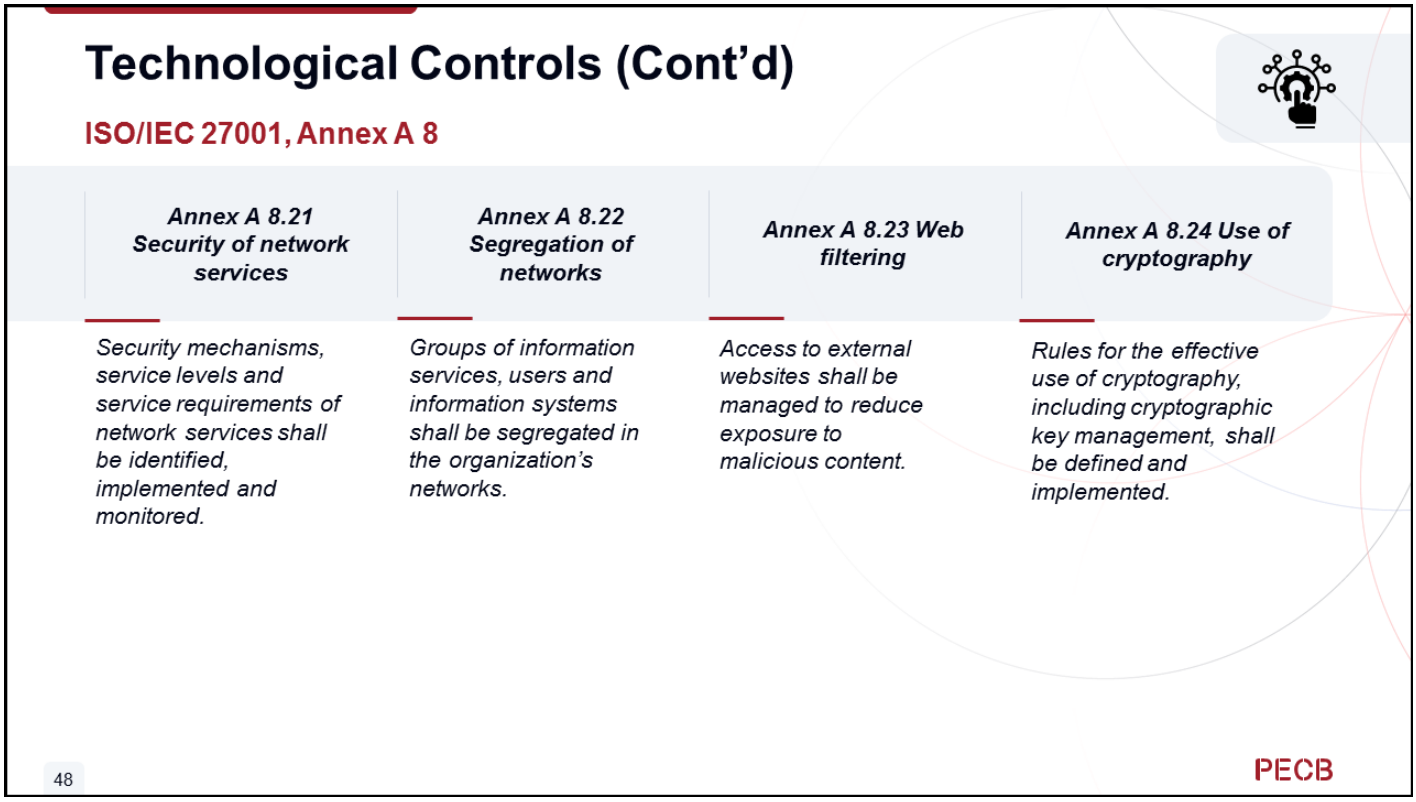
Purpose

To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.

ISO/IEC 27002, clause 8.20 Networks controls

Purpose

To protect information in networks and its supporting information processing facilities from compromise via the network.



ISO/IEC 27002, clause 8.21 Security of network services

Purpose

To ensure security in the use of network services.

ISO/IEC 27002, clause 8.22 Segregation of networks

Purpose

To split the network in security boundaries and to control traffic between them based on business needs.

ISO/IEC 27002, clause 8.23 Web Filtering

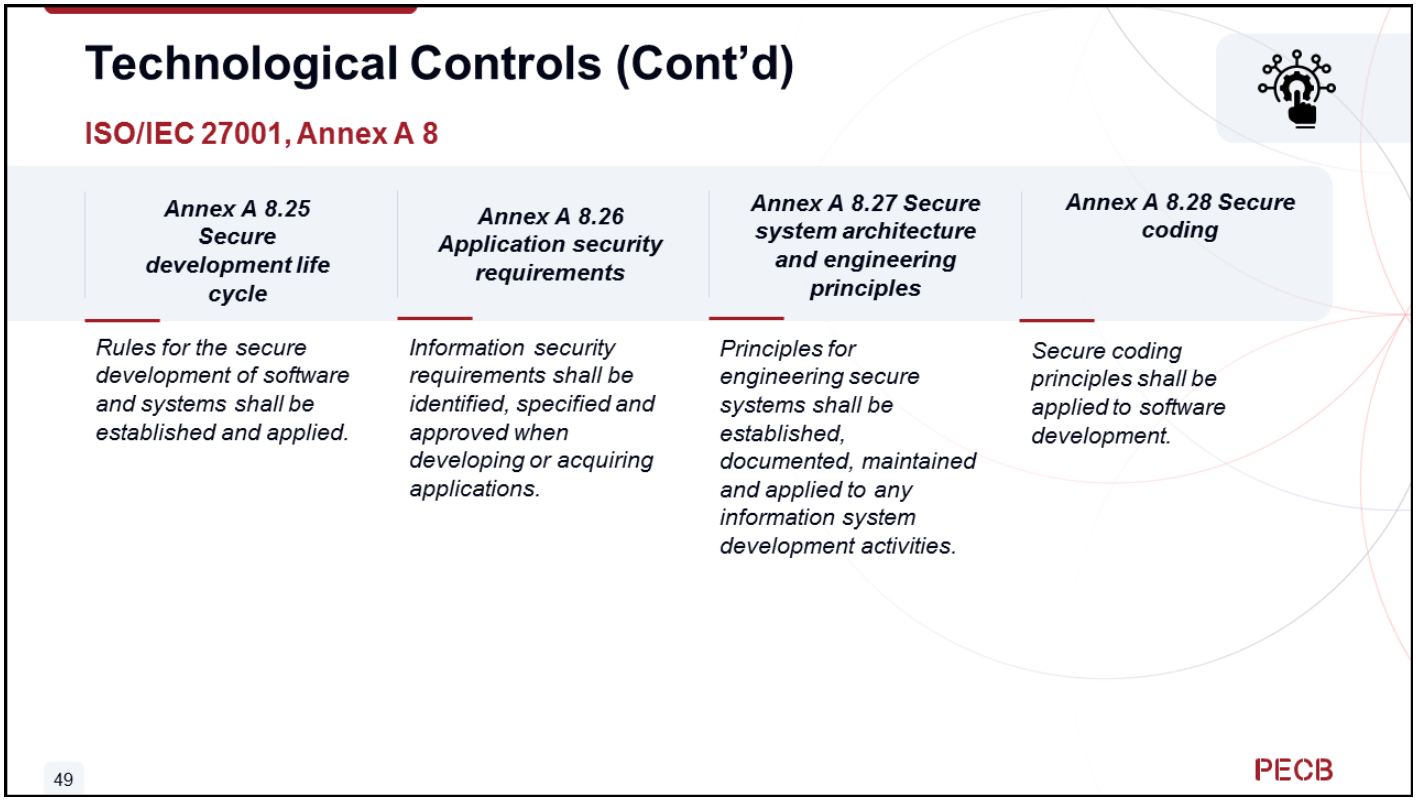
Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

ISO/IEC 27002, clause 8.24 Use of cryptography

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.



ISO/IEC 27002, clause 8.25 Secure development life cycle

Purpose

To ensure information security is designed and implemented within the secure development life cycle of software and systems.

ISO/IEC 27002, clause 8.26 Application security requirements

Purpose

To ensure all information security requirements are identified and addressed when developing or acquiring applications.

ISO/IEC 27002, clause 8.27 Secure system architecture and engineering principles

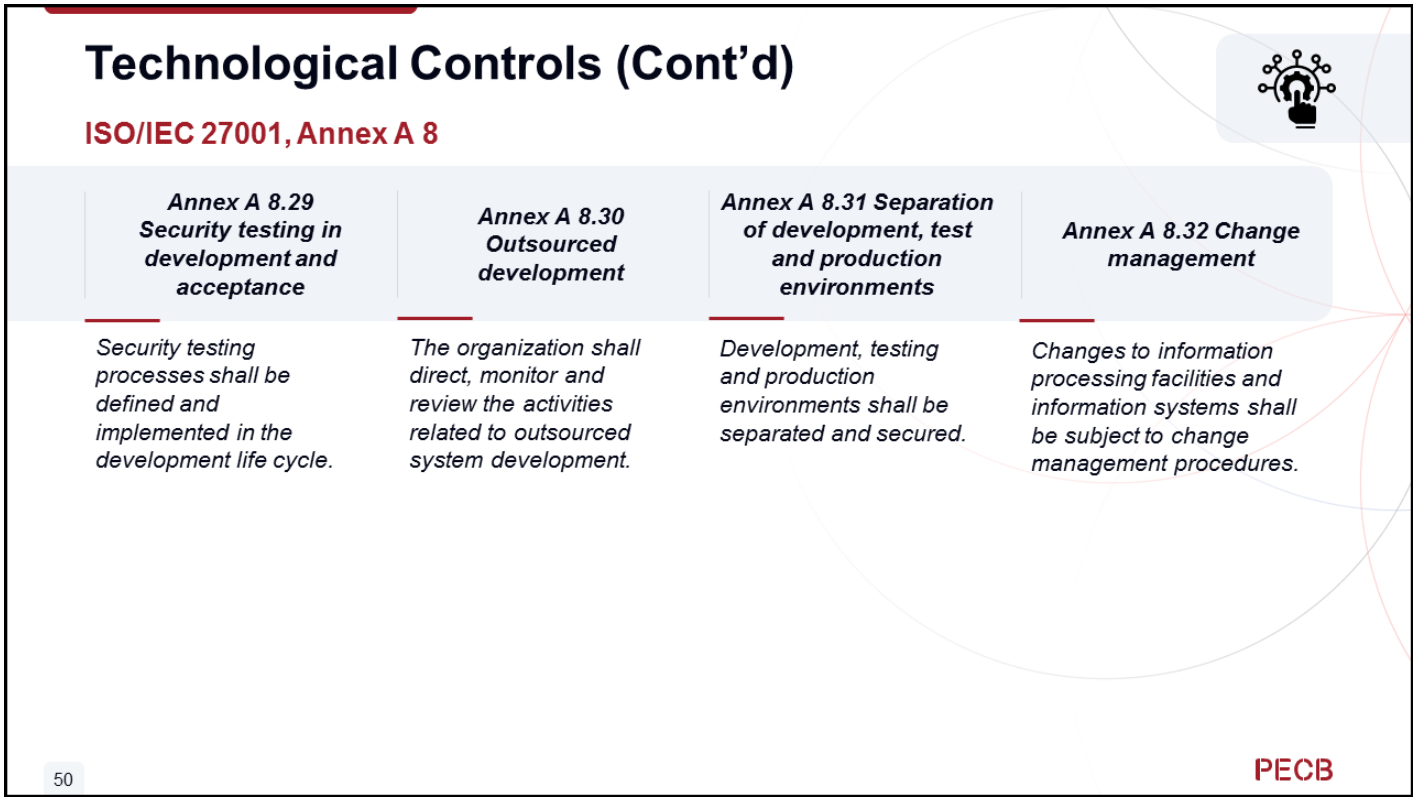
Purpose

To ensure information systems are securely designed, implemented and operated within the development life cycle.

ISO/IEC 27002, clause 8.28 Secure coding

Purpose

To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.



ISO/IEC 27002, clause 8.29 Security testing in development and acceptance

Purpose

To validate if information security requirements are met when applications or code are deployed to the production environment.

ISO/IEC 27002, clause 8.30 Outsourced development

Purpose

To ensure information security measures required by the organization are implemented in outsourced system development.

ISO/IEC 27002, clause 8.31 Separation of development, test and production environments

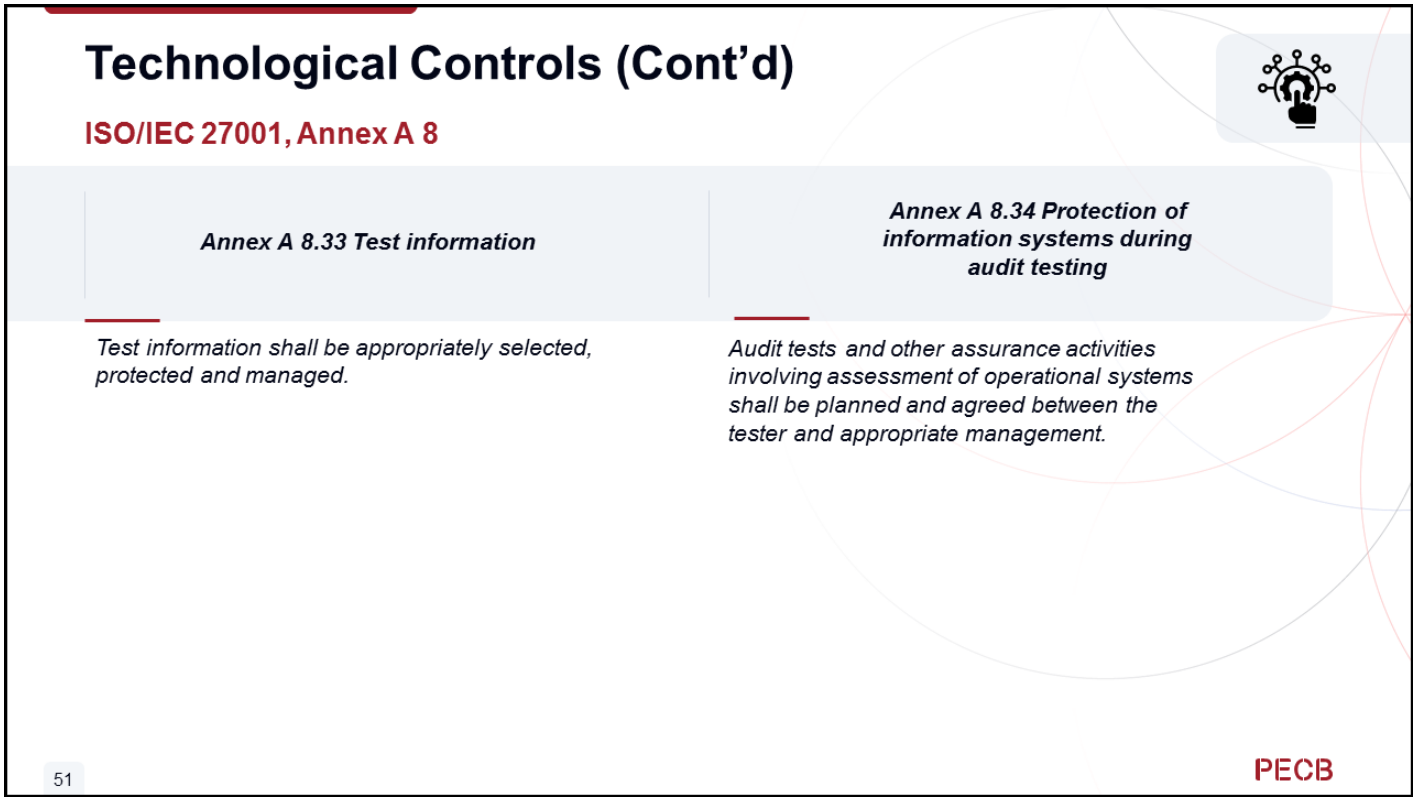
Purpose

To protect the production environment and data from compromise by development and test activities.

ISO/IEC 27002, clause 8.32 Change management

Purpose

To preserve information security when executing changes.



ISO/IEC 27002, clause 8.33 Test information

Purpose

To ensure relevance of testing and protection of operational information used for testing.

ISO/IEC 27002, clause 8.34 Protection of information systems during audit testing

Purpose

To minimize the impact of audit and other assurance activities on operational systems and business processes.

Section 15 Summary

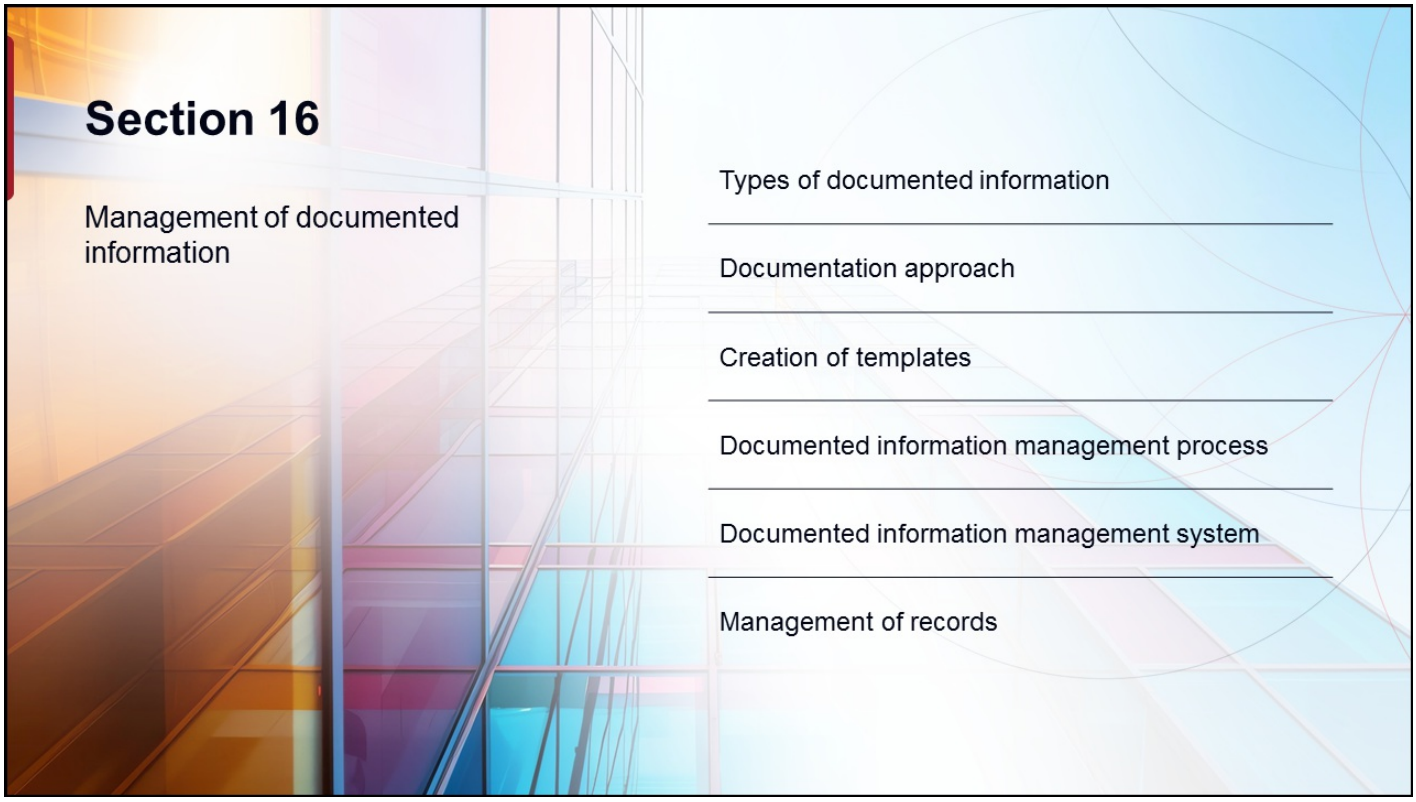
- Organizations must implement the applicable information security controls listed in Annex A of the standard to ensure the security of their information.
- Annex A lists a list of possible information security controls that can be used in context with clause 6.1.3 Information security risk treatment.
- Annex A of ISO/IEC 27001 consists of 93 controls which are grouped into four themes: organizational controls (37 controls), people controls (8 controls), physical controls (14 controls), and technological controls (34 controls).

Questions?

Exercise 3

Quiz 15

Note: To complete Exercise 3 and Quiz 15, please go to the Exercises Worksheet and Quizzes Worksheet respectively.

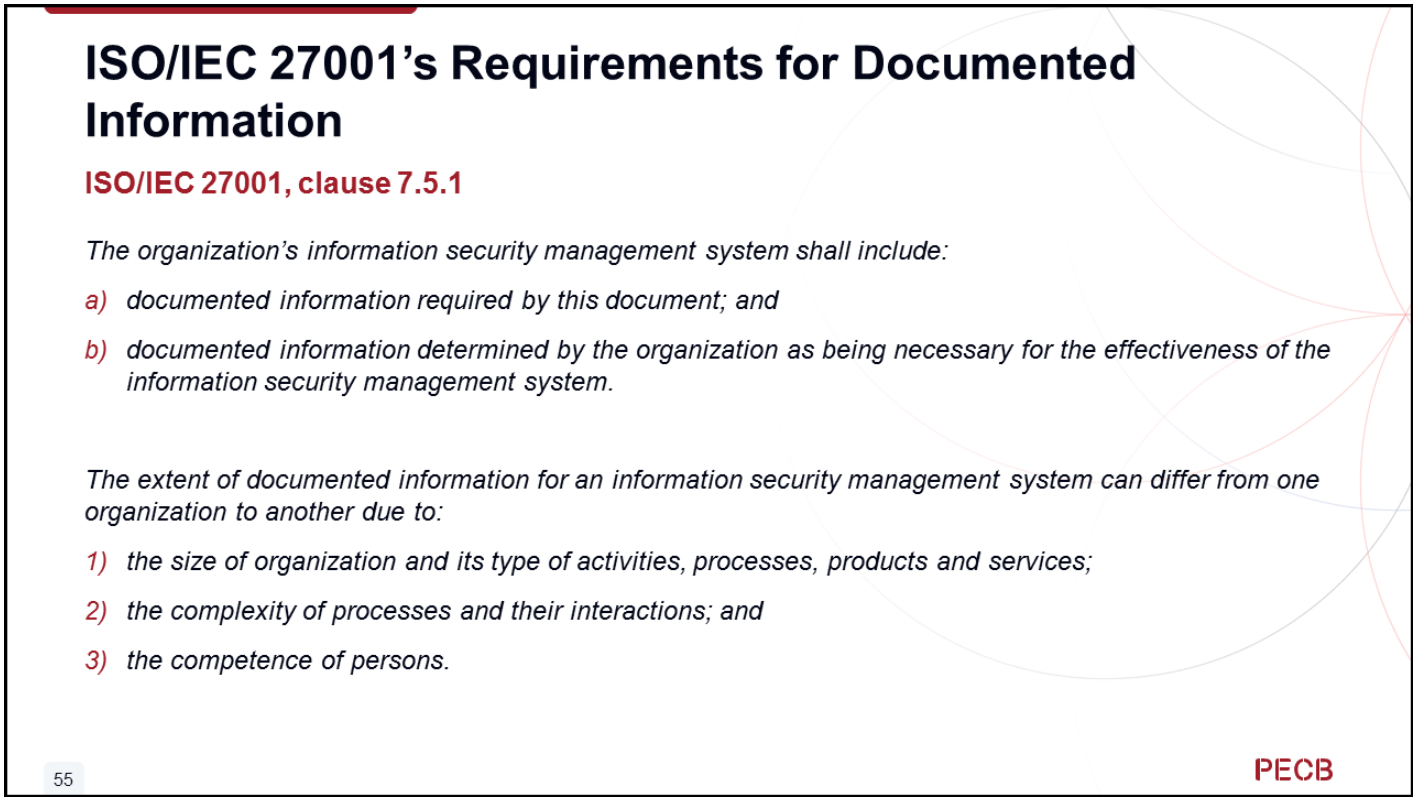


This section provides information that will help the participants gain knowledge on the documented information management process, including the value and types of documented information, the creation of templates, the management of documented information and records, the implementation of a documented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

Management of Documented Information

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

PECB



The documented information of ISMS should be comprehensive and consistent, reflecting the organization's security controls aligned with identified risk scenarios, its adequacy and relevance assessed within the organizational context using reasonable judgment.

ISO/IEC 27003, clause 7.5.1 General

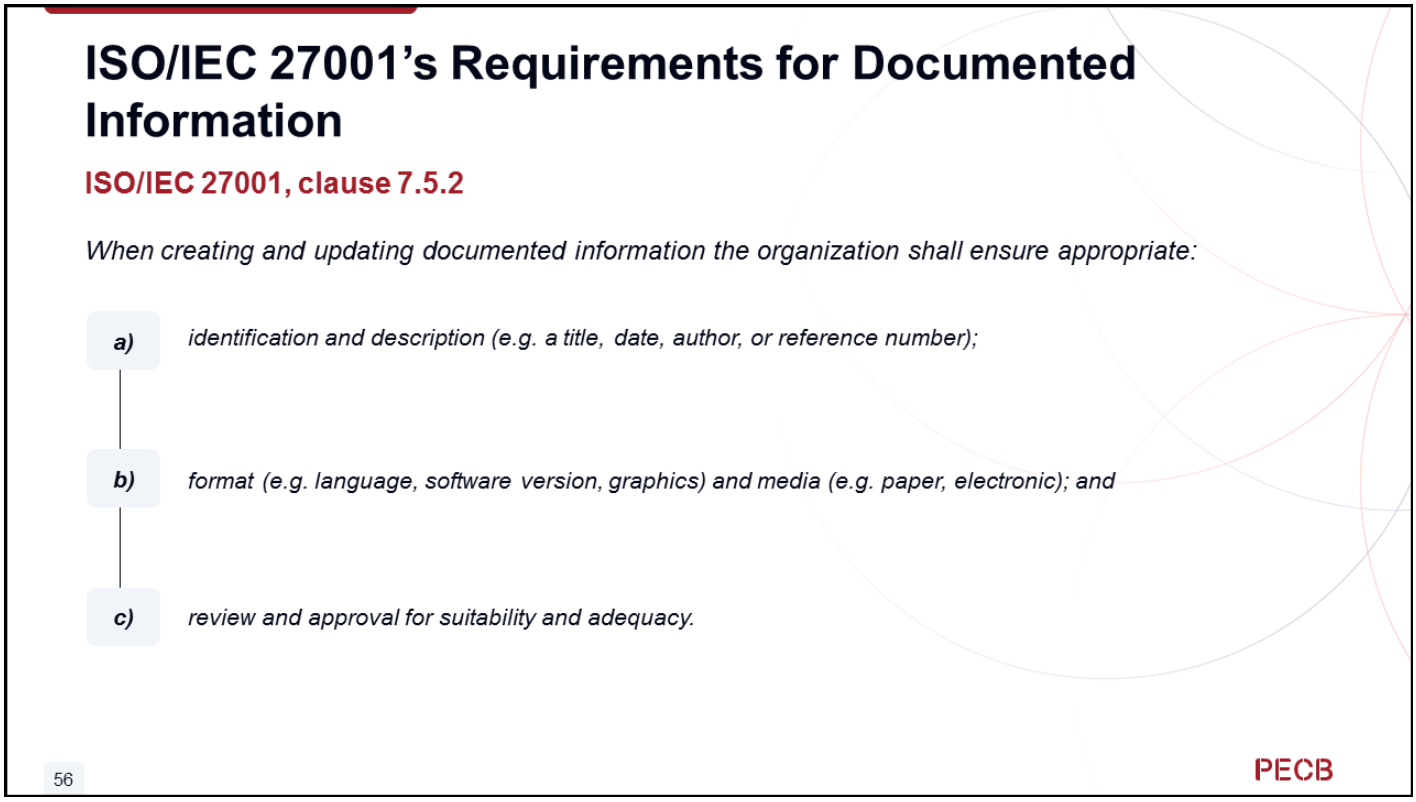
Explanation

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.).*



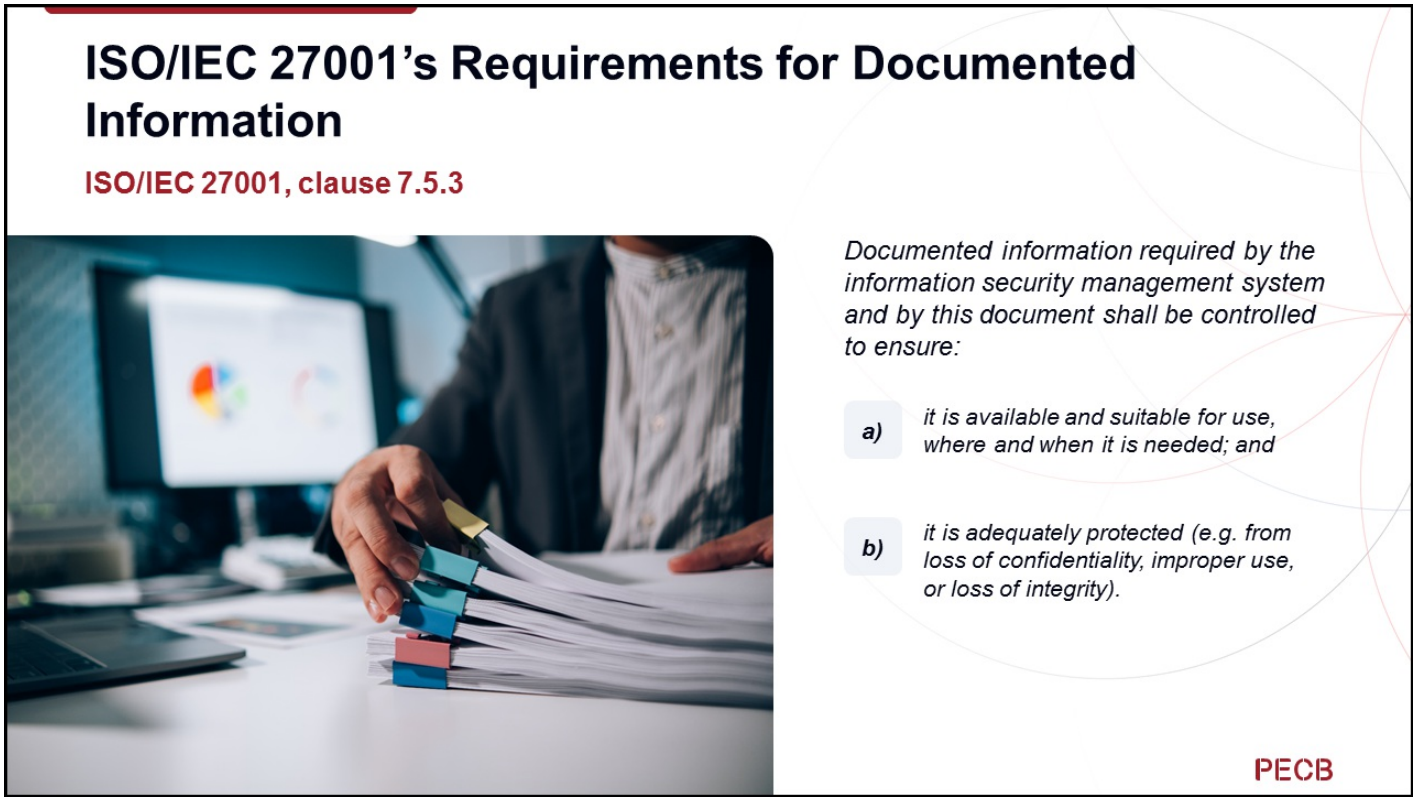
ISO/IEC 27003, clause 7.5.2 Creating and updating

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 authorized 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's Requirements for Documented Information

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 can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.*

PECB

ISMS Documented Information

The organization must approve its ISMS documented information to ensure conformity according to the three following criteria:

Content

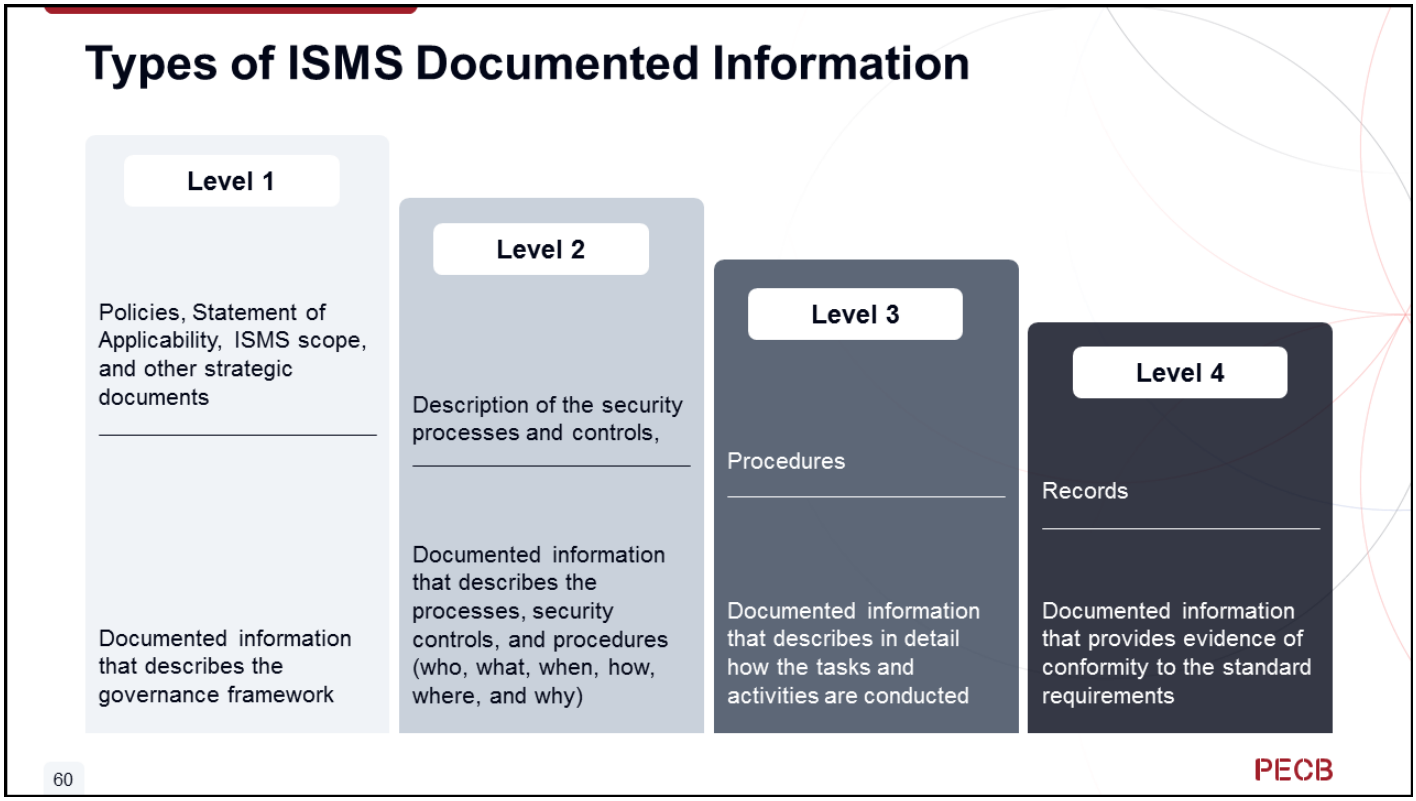
Format

Life cycle

59

PECB

1. **Content:** Each document must contain the information required by the respective clause; however, the document should contain only the minimum required, not unnecessary details.
2. **Format:** Each document must be consistent in format (author identification, production date, version number, approval date of the latest revision, etc.).
3. **Life cycle:** Each document must be controlled, protected, and stored appropriately to meet the requirements of clause 7.5.3 Control of documented information of ISO/IEC 27001.



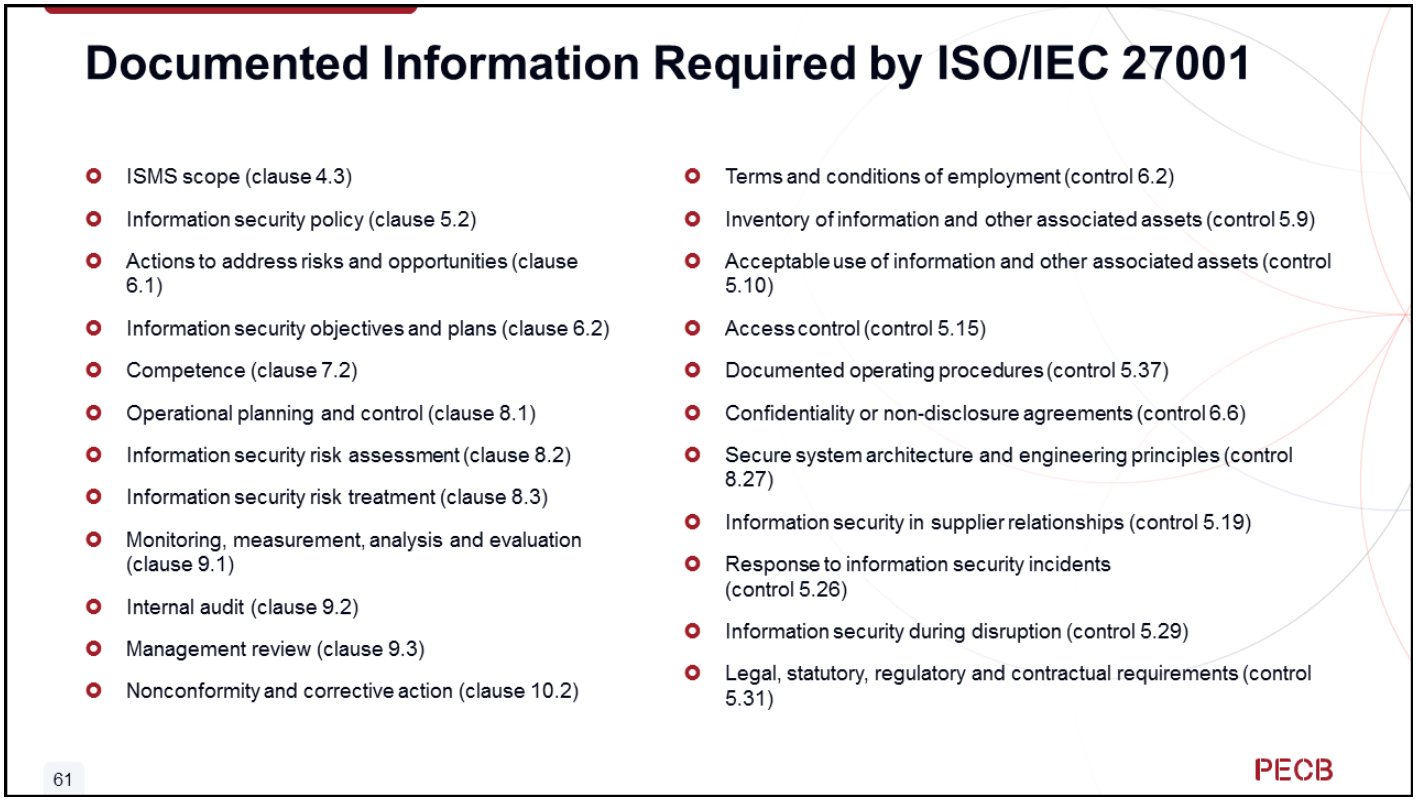
There is no mandatory requirement on how to document processes and security controls. This can be done using diagrams, textual descriptions, spreadsheets, etc.

ISO/IEC 27003, clause 7.5.3 Control of documented information

Guidance

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

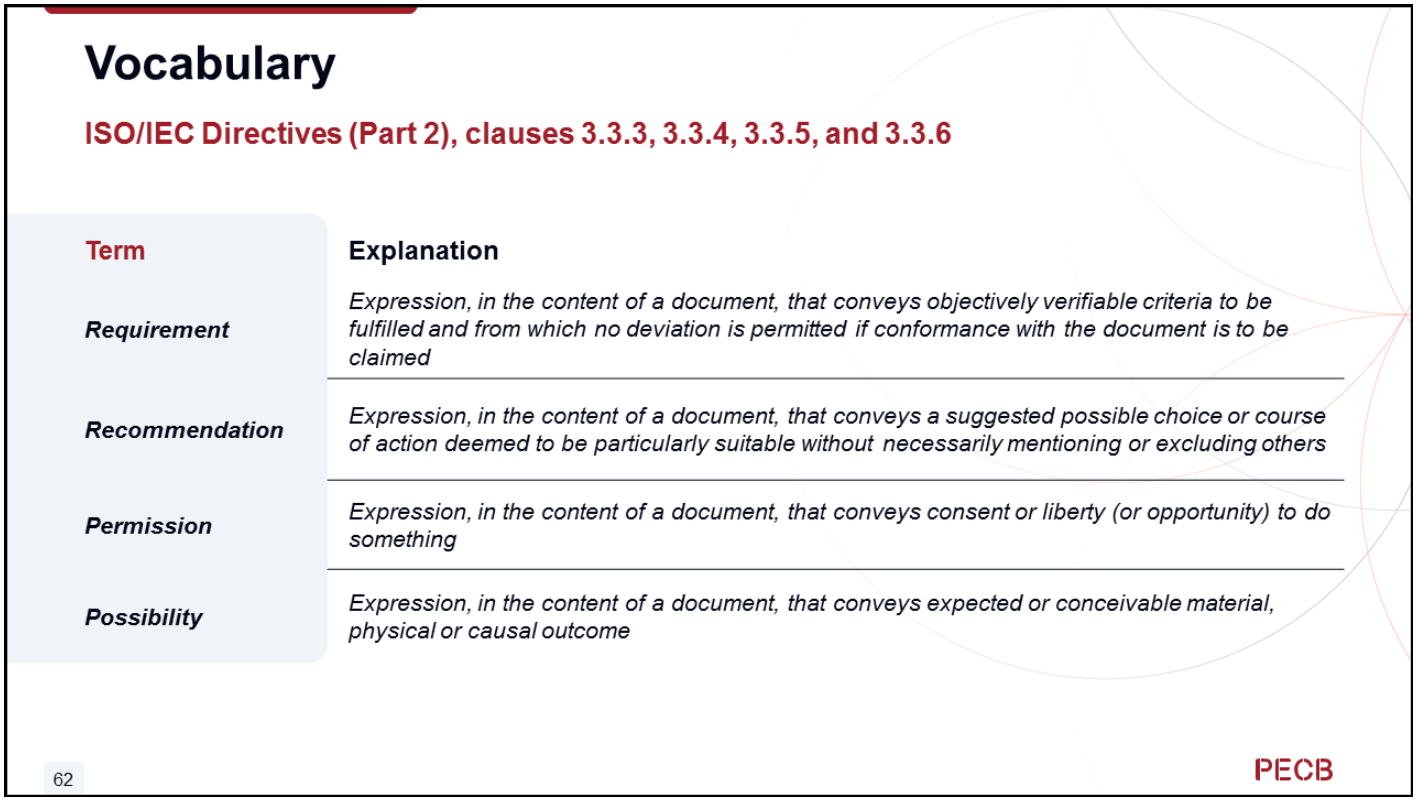
- *the results of the context establishment;*
- *the roles, responsibilities and authorities;*
- *reports of the different phases of the risk management;*
- *resources determined and provided;*
- *the expected competence;*
- *plans and results of awareness activities;*
- *plans and results of communication 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.)*



Documented information is implicitly required on the following clauses and controls of ISO/IEC 27001:

- *Communication* (clause 7.4)
- *Documented information* (clause 7.5)
- *Organizational roles, responsibilities and authorities* (clause 5.3)
- *Leadership and commitment* (clause 5.1)
- *Improvement* (clause 10)
- *Remote working* (control A.6.7)
- *Classification of information* (control A.5.12)
- *Access rights* (control A.5.18)
- *Storage media* (control A.7.10)
- *Secure disposal or re-use of equipment* (control A.7.14)
- *Working in secure areas* (control A.7.6)
- *Clear desk and clear screen* (control A.7.7)
- *Change management* (control A.8.32)
- *Information backup* (control A.8.13)
- *Information transfer* (control A.5.14)
- *Redundancy of information processing facilities* (Control A.8.14)

The availability of these documents supports operations and helps demonstrate conformity during the certification audit.



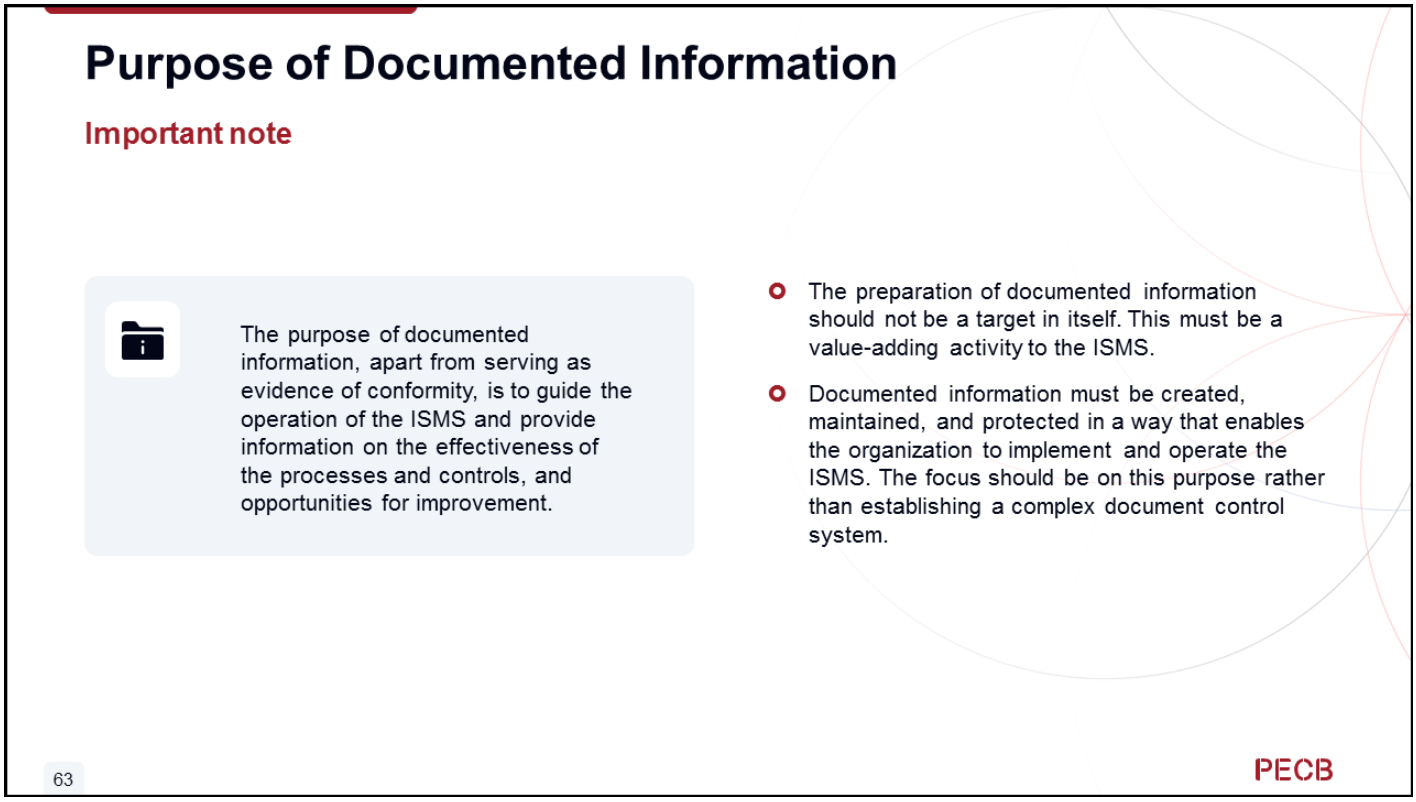
During the implementation of an ISMS, particular attention should be given to the use of verbal expressions to indicate the nature of specific provisions.

- The verbal form “shall” is used to express a requirement.
- The verbal form “should” is used to indicate a recommendation.
- The verbal form “may” is used to indicate a permission, whereas “can” is used to express a possibility or capability.

The organization must 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 expressed by the verb “should” as guidelines rather than adopting them as requirements.

However, if a process or a control that is not a standard requirement is documented by the organization with the verb “shall,” it becomes a requirement of the ISMS. 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 states that backups “shall” be checked every morning at 10:00 a.m., but during the audit the auditor notes that this is not followed, this indicates 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.



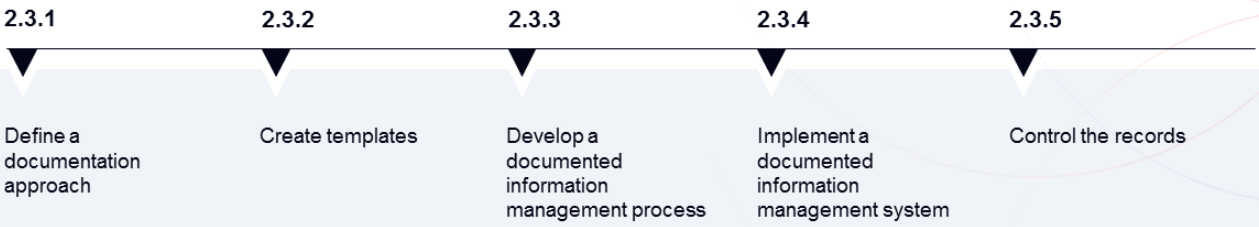
The extent of the necessary documentation and media types to use depends on factors such as the type and size of the organization, the complexity and interaction of processes, information systems and technologies available, the requirements of interested parties, and the applicable regulatory requirements.

Documented information helps the organization to:

- Comply with legal, regulatory, and contractual obligations
- Provide media for communication and training
- Ensure consistency and traceability
- Evaluate the effectiveness of the information security processes and controls
- Improve ISMS processes and information security controls
- Demonstrate conformity to ISO/IEC 27001

2.3 Management of Documented Information

List of activities



Define a documentation approach

Create templates

Develop a documented information management process

Implement a documented information management system

Control the records

PECB

2.3.1 Define a Documentation Approach

It is recommended to create a list of all documented information related to the ISMS that includes common attributes of every document, which allow clear and unique identification.

These attributes include:

- 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

65

PECB

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.

2.3.2 Create Templates

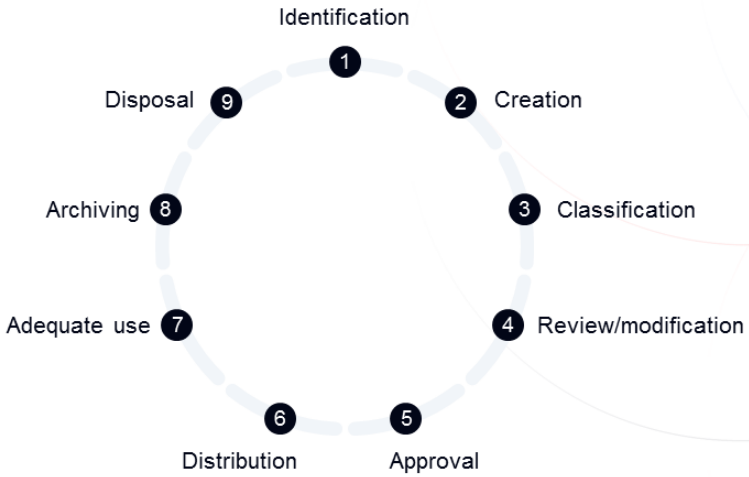
Types of documents

Type of document	Objectives
Policy	To express the objectives and the strategic direction of an organization as outlined by its management
Procedure	To outline the specific instructions on the steps to be taken
Guidelines	To provide general guidance on good practices to be followed in order to achieve the policy objectives
Security manual	To consolidate different types of documents related to information security and data protection
Charter	To provide a description of the established agreements between the organization and other interested parties, such as users, employees, suppliers, service providers, etc.
Schematic diagram	To illustrate how a process works
Narrative processes	To explain the function of a process
Form	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	To provide detailed instructions on the use or installation, maintenance, or operation of something
Datasheet	To summarize the technical information (specifications) needed to install, use, maintain, and improve equipment, software, etc.

PECB

2.3.3 Develop a Documented Information Management Process

A procedure must be established to manage the document life cycle:



67

PECB

Establishing procedures for controlling and managing documents is essential for maintaining, communicating, and further improving the ISMS.

1. **Identification:** The document that needs to be produced has been identified.
2. **Creation:** A draft document is produced.
3. **Classification:** The draft document is classified and determined to whom it will be accessible.
4. **Review/modification:** The draft is formally reviewed; the draft 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.

2.3.4 Implement a Documented Information Management System

A documented information management system ensures:

- Facilitated access, referencing, dissemination, and archiving of documented information
- Effective management of the documents throughout their life cycle
- Traceability
- Secured access

Optimizing searching and updating

68

PECB

Types of available solutions:

1. **Electronic document management system (EDMS):** EDMS is a computerized system for the acquisition, classification, storage, and archiving of documents (e.g., mass digitization of paper documents). An example is SharePoint (Microsoft).
2. **Content management system (CMS):** CMS is 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.

2.3.5 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, identifiable, and accessible.

VISITORS REGISTER

Date	Visitors name	Email address	Time (in)	Time (out)
2022-02-06	Abbey Martin	abbey.martin@gmail.com	10:15	11:27
2022-02-10	Barren Miller	miller-b@gmail.com	09:07	10:41
2022-02-14	David Wilson	da.willson@gmail.com	12:10	13:44
2022-02-19	Lynda Brown	lyndaBrown@gmail.com	10:15	11:27
2022-02-21	Sofia Morris	ssofia@hotmail.com	14:22	15:15
2022-02-24	Tricia Zylker	tricia.Z@hotmail.com	10:15	11:27
2022-02-26	Jackson Rivera	jack-riv@gmail.com	15:20	16:20
2022-02-28	Peter Diaz	peter82@hotmail.com	09:50	10:30
2022-03-02	Jim Walker	walker.jim@gmail.com	10:58	11:40

PECB

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

PECB

Documented Information Management

Most common problems

Problems	Potential causes
Difficulty in finding or managing a document	A large number of misclassified and not indexed documents
Inability to quickly extract useful information from a document	Voluminous documents, too literary, often with multiple annexes
Inefficient update of documents	The processes for managing documented information are established ineffectively
Incoherence between records and actual business processes	Employees are not involved in the process of drafting the documents
Ambiguous or incomprehensible texts or graphics	Lack of validation with users, lack of training and awareness, incompetent editors
Proliferation of document versions	Lack of documented information management system

PECB

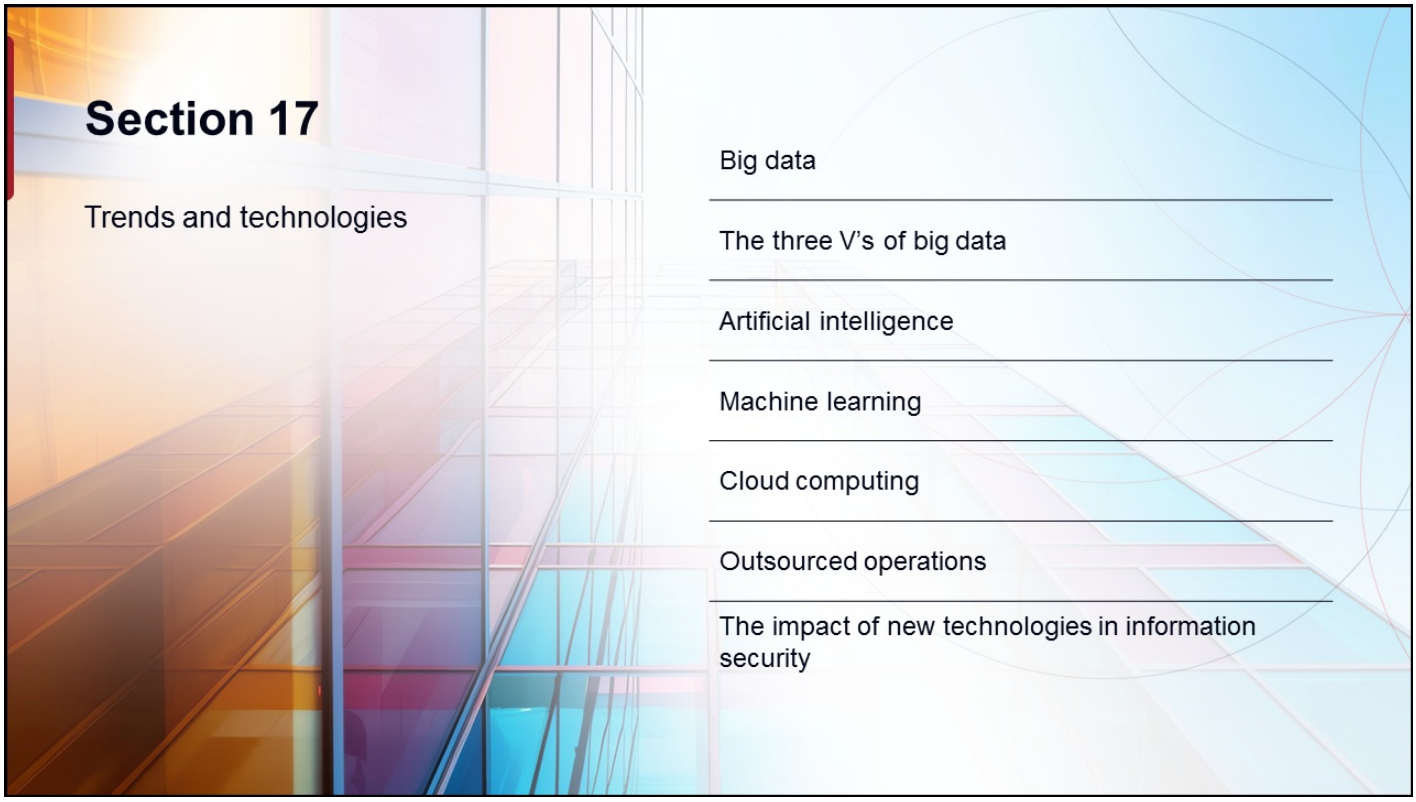
Section 16 Summary

- Documented information serves as evidence of conformity, guides the operation of the ISMS, and provides information on the effectiveness of the processes and controls, and opportunities for improvement.
- Documented information related to the ISMS must have attributes which allow clear and unique identification.
- ISO/IEC 27001 does not specify how to document processes and security controls or the types to be used. Common documents related to the ISMS include policies, procedures, guidelines, security manuals, forms, data sheets, etc.
- A document life cycle includes the following steps: identification, creation, review/modification, approval, distribution, adequate use, archiving, and disposal.
- A documented information management system ensures facilitated access, referencing, dissemination, and archiving of documented information; effective management of the documents throughout their life cycle; traceability; and secured access.

Questions?

Quiz 16

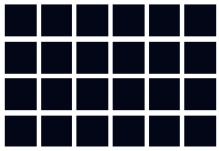
Note: To complete Quiz 16, please go to the Quizzes Worksheet.



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 Merriam-Webster dictionary 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[1]:



Structured data are organized and easily reachable. It is included in an organization's traditional spreadsheet and database, such as business processes, customers lists, and product information.

Unstructured data cannot be organized in relational databases and are not easily reachable. It includes large information that could be hard to fit in an organization's database, such as Google translate data or IoT sensors.

74

PECB

The difference between structured and unstructured data:

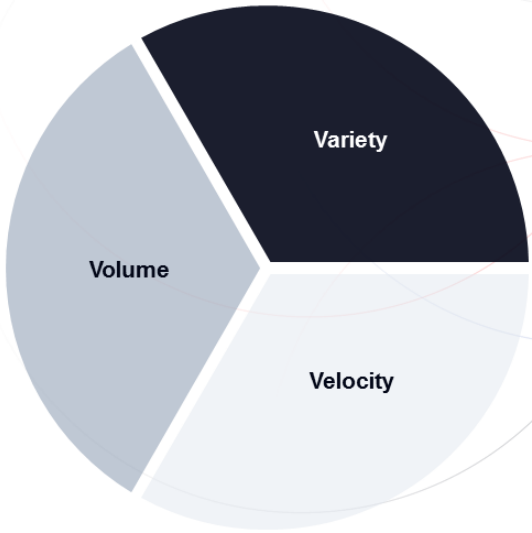
- Structured data have a defined data model and are based on a relational database. Examples of structured data include SQL (Structured Query Language) databases and Microsoft Excel files which have structured tables, rows, and columns.
- Unstructured data do not have a predefined data model and are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

The Three V's of Big Data

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

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

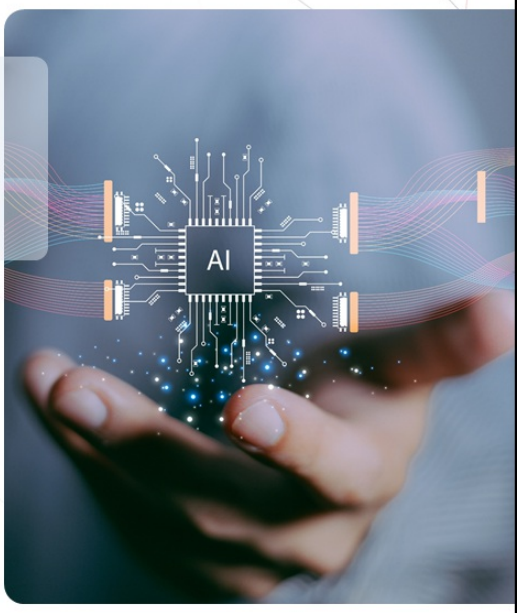
Velocity refers to the speed of data processing generated in real time, online and offline, in streams, batches, or bits.



PECB

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.

AI is typically used in:

Banking	Marketing	Healthcare	Autonomous vehicles

PECB

Weak and Strong AI [2][3]

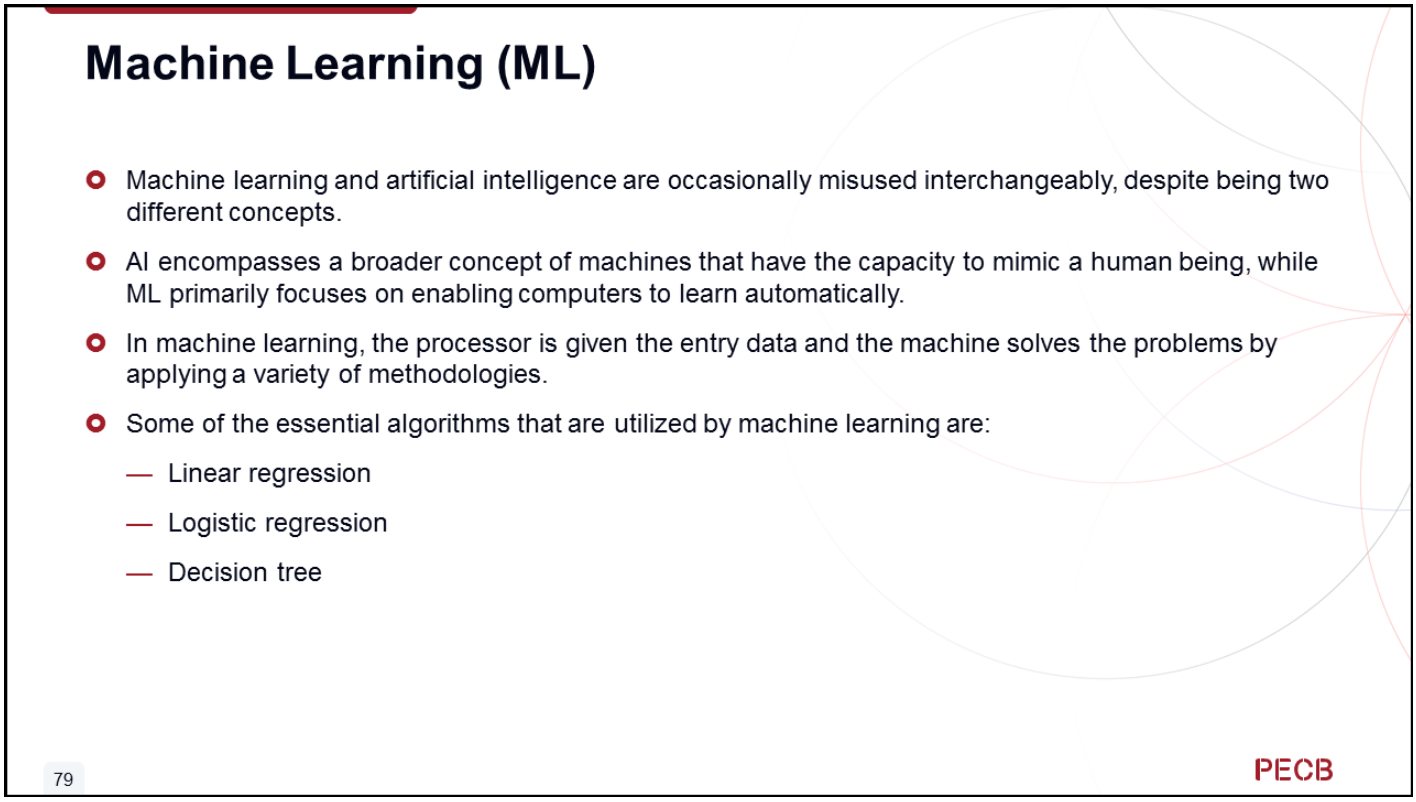
Weak AI	• Weak AI is also known as narrow AI. It is focused on a specific task and outperforms humans when conducting technical and automated tasks. However, when weak AI has to conduct a task that it does not recognize, it will not be able to complete it, unless it is specifically programmed to do so. • The benefit of weak AI is the automation of tasks. • Examples of weak AI include Meta's newsfeed (formerly Facebook), Apple's Siri, Alexa, Amazon's product recommendation algorithms, etc.
Strong AI	• Strong AI is also known as artificial general intelligence (AGI). • AGI has the capacity to understand newly presented problems and derive solutions based on prior knowledge. • The benefit of strong AI is problem-solving. • Although there are no practical examples of strong AI yet, strong AI may include AI that can communicate in natural language, use critical thinking, etc.

PECB

Artificial intelligence risks may impact individuals, organizations, and society. Potential negative consequences of AI for individuals include risks related to physical safety, privacy and reputation, digital safety, financial health, and equity and fair treatment. AI risks that may impact organizations are related to financial and nonfinancial performance, legal and compliance, and reputational integrity. AI risks that may impact the society are related to national security, economic stability, political stability, and infrastructure integrity.

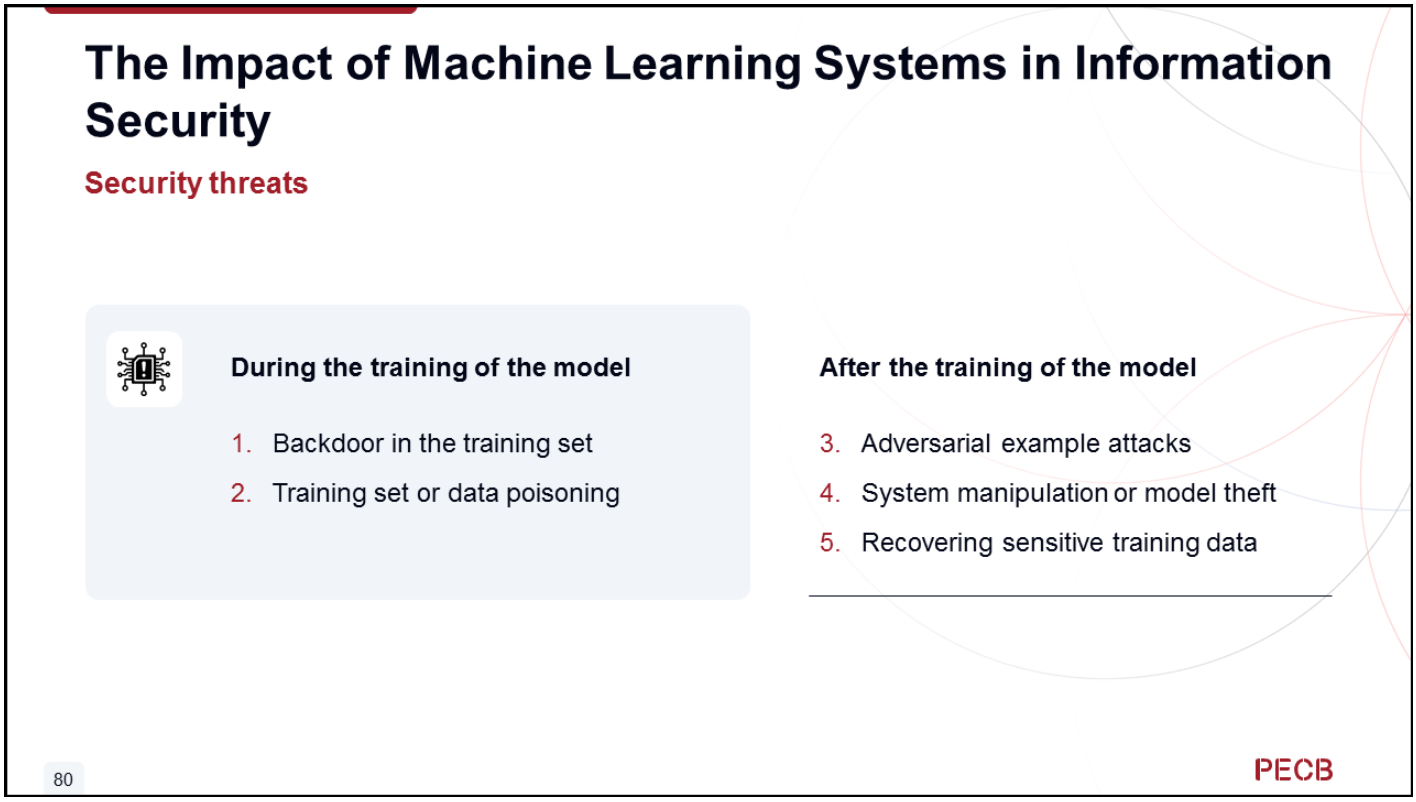
Some common AI risks include[4]:

1. **Data difficulties:** Due to the large amount of unstructured data in various sources including the web, social media, mobile devices, sensors, and the Internet of Things, managing such data has become difficult. Thus, the risk of revealing important information has increased.
2. **Technology troubles:** The performance of AI systems can suffer from challenges with technology and operational procedures across all working environments. A financial institution, for instance, encountered difficulties when its compliance software failed to identify trading concerns since the data feeds did not contain all customer activities.
3. **Security snags:** Insufficient security measures may result in unauthorized users gaining access to marketing, health, and financial data used for AI systems.
4. **Models misbehaving:** Some AI models may provide biased outcomes, lack stability, or produce wrong conclusions.
5. **Interaction issues:** This is a key risk area of AI risks that involves the interaction between humans and machines (e.g., in automated transportation, manufacturing, and infrastructure systems).



There are three main types of machine learning[5]:

1. **Supervised machine learning** 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.
2. **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.
3. **Reinforcement learning** establishes a reward and punishment system for correct or incorrect behavior. The model uses the data from this system to learn to maximize the reward.



There are five main threats that ML faces during its life cycle[6]:

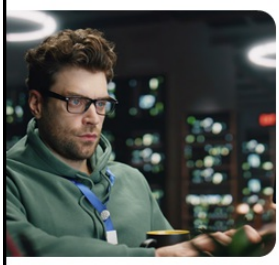
1. **Backdoor in the training set:** Attackers can hide a backdoor in the training data to send signals and easily manipulate model's parameters. Backdoors, also known as Trojans, can be mitigated through measures such as preprocessing, re-training, and anomaly detection.
2. **Training set or data poisoning:** Due to the sensitive nature of data used in ML, attackers exploit vulnerabilities to manipulate the training data and impact the outcomes.
3. **Adversarial example attacks:** This type of attack manipulates the ML system into predicting information that is not accurate, while affecting its integrity and reliability.
4. **System manipulation or model theft:** Adversaries can steal machine learning models by gaining the output labels from choosing different inputs.
5. **Recovering sensitive training data:** It uses model inversion attack and membership interference attack. The model inversion attack evaluates sensitive attributes while using black-box to access the model, whereas membership interference attack trains a model to differentiate training and non-training data.

The first two attacks usually take place during the training of the model, while the other three attacks after the training of the model.

Cloud Computing

NIST Glossary

A model for enabling ubiquitous, convenient, on-demand networks 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.

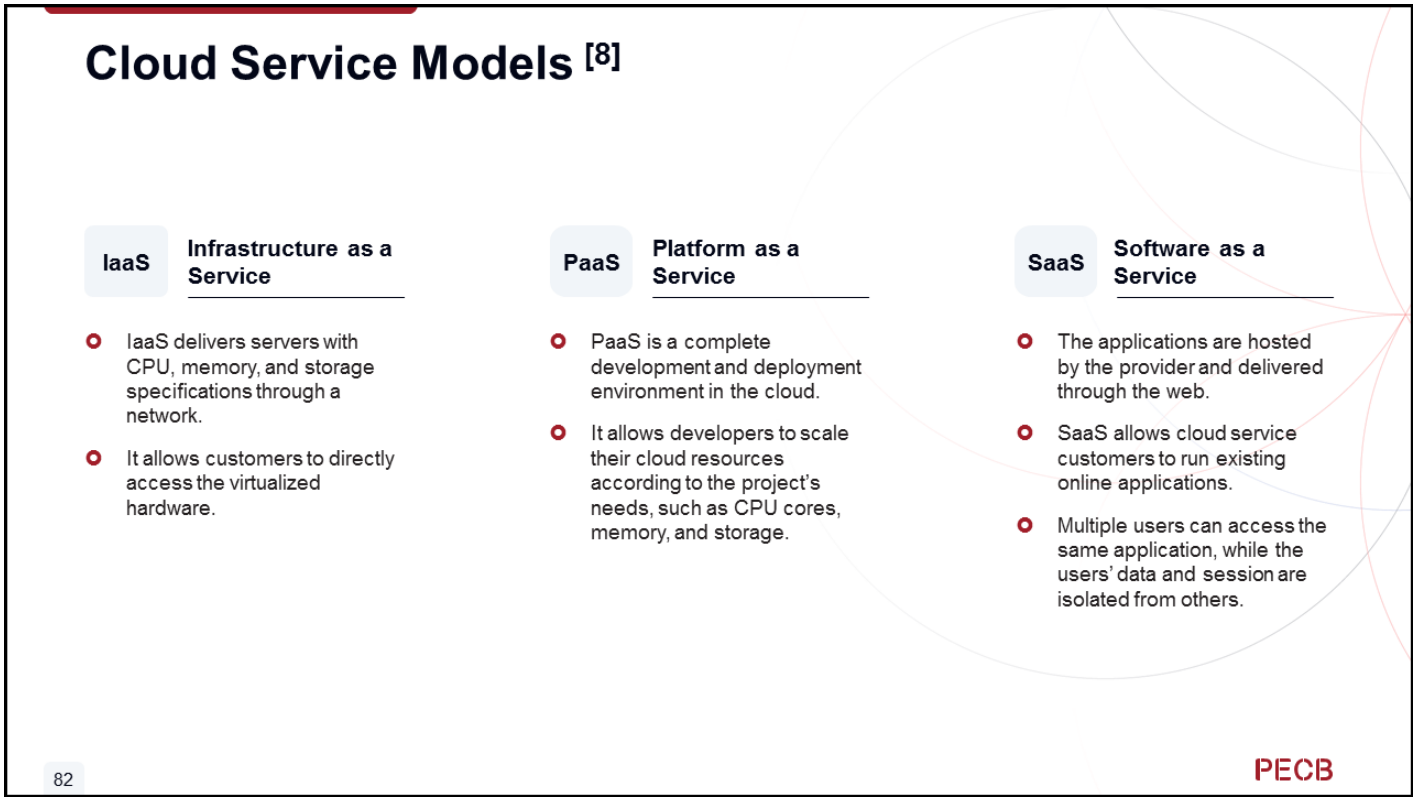


- Cloud service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- It has three main deployment models known as private, public, and hybrid cloud.

81

PECB

- **Public cloud:** Similarly to internet, the services in public cloud can be accessed from anywhere. The public cloud is a multi-tenant environment, where the same computing resources are shared among multiple customers.
- **Private cloud:** Private cloud computing dedicates the hardware, storage, and network to a single client. The private cloud is similar to the concept of intranet.
- **Hybrid cloud:** It combines public and private cloud computing. It allows data and applications to be used among both private and public clouds, enabling flexibility and more deployment options.[7]

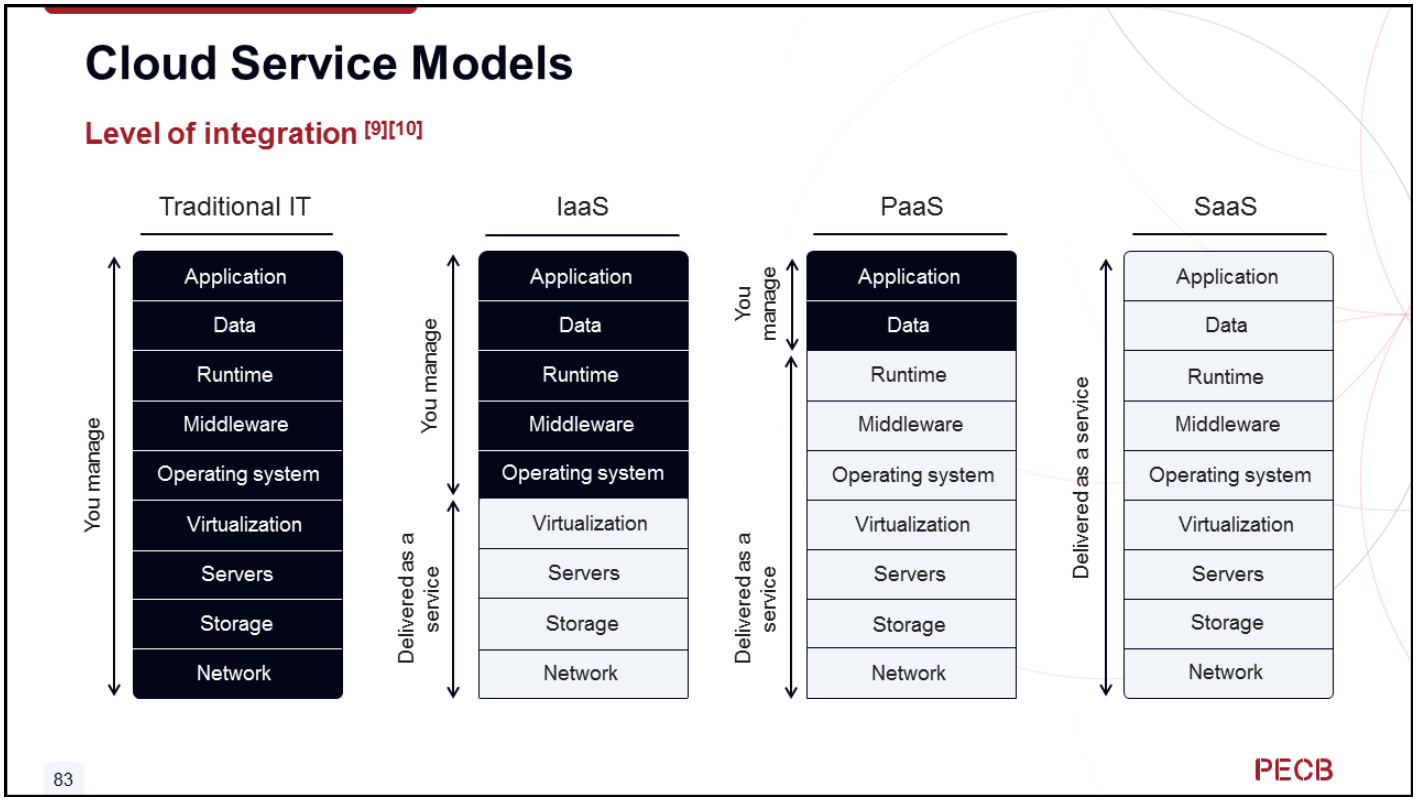


NIST SP 800-145, Service models

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).



Note: The slide provides a visual representation of the customer's and provider's management responsibilities for each cloud service model. Services that you manage are in dark background and the services that are delivered as a service by the cloud service provider are in white background.

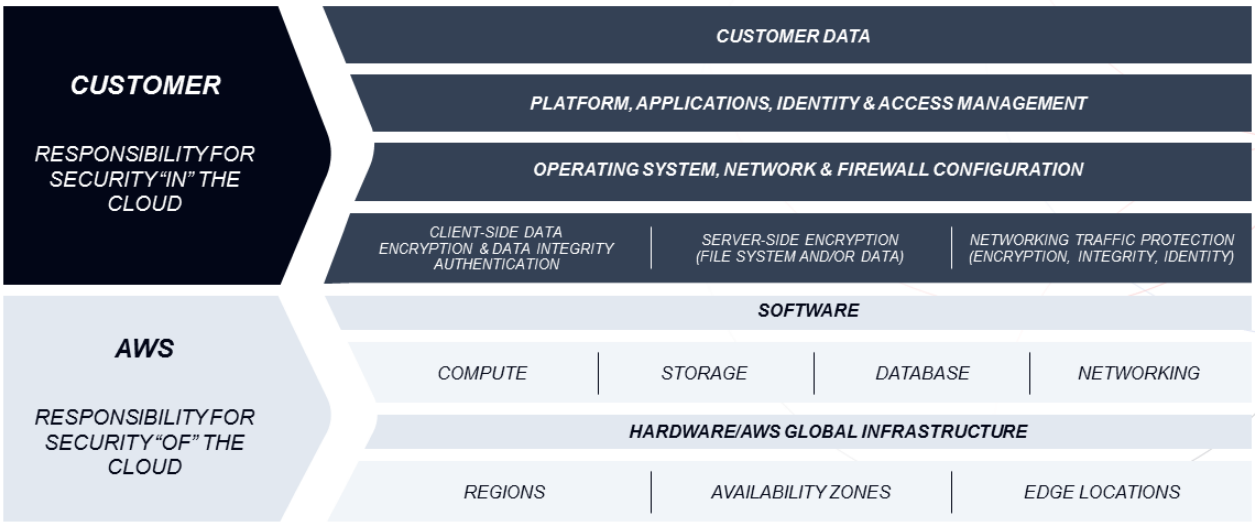
As shown on the slide, in a SaaS cloud service model, all services are provided by the cloud service provider, including data. Although data in SaaS is managed by the cloud service provider, it is created, owned, and controlled by the cloud service customer.

The Software-Platform-Infrastructure (SPI) model is the most widely used cloud computing classification used by NIST and most cloud service providers. The SPI framework is also known as SPI tiers and comprises IaaS, PaaS, and SaaS. These three cloud computing service models can the established as part of public cloud, private cloud, hybrid cloud, and multi-cloud architecture, within the SPI framework.

Some examples of top cloud providers for the cloud service models of the SPI model are:

- **IaaS:** Amazon Web Services (AWS), Google Cloud, IBM Cloud, and Microsoft Azure
- **PaaS:** AWS Elastic Beanstalk, Google App Engine, Microsoft Windows Azure, and Red Hat OpenShift on IBM Cloud
- **SaaS:** Salesforce, HubSpot, Trello, Slack, and Canva

Shared Responsibility Model in Cloud [11]



84

PECB

The figure on the slide outlines the shared responsibility model for security and compliance between the cloud service provider and cloud service customer.

- **Security of the cloud:** The cloud service provider is responsible for safeguarding the underlying infrastructure, including hardware, software, networking, and facilities that support the cloud environment.
- **Security in the cloud:** Customers are responsible for managing the guest operating system, application software, and the configuration of security features provided by the cloud service provider, such as security groups. The extent of customer responsibility depends on the specific services that the cloud service provider used.

Customer responsibilities for different cloud service models:

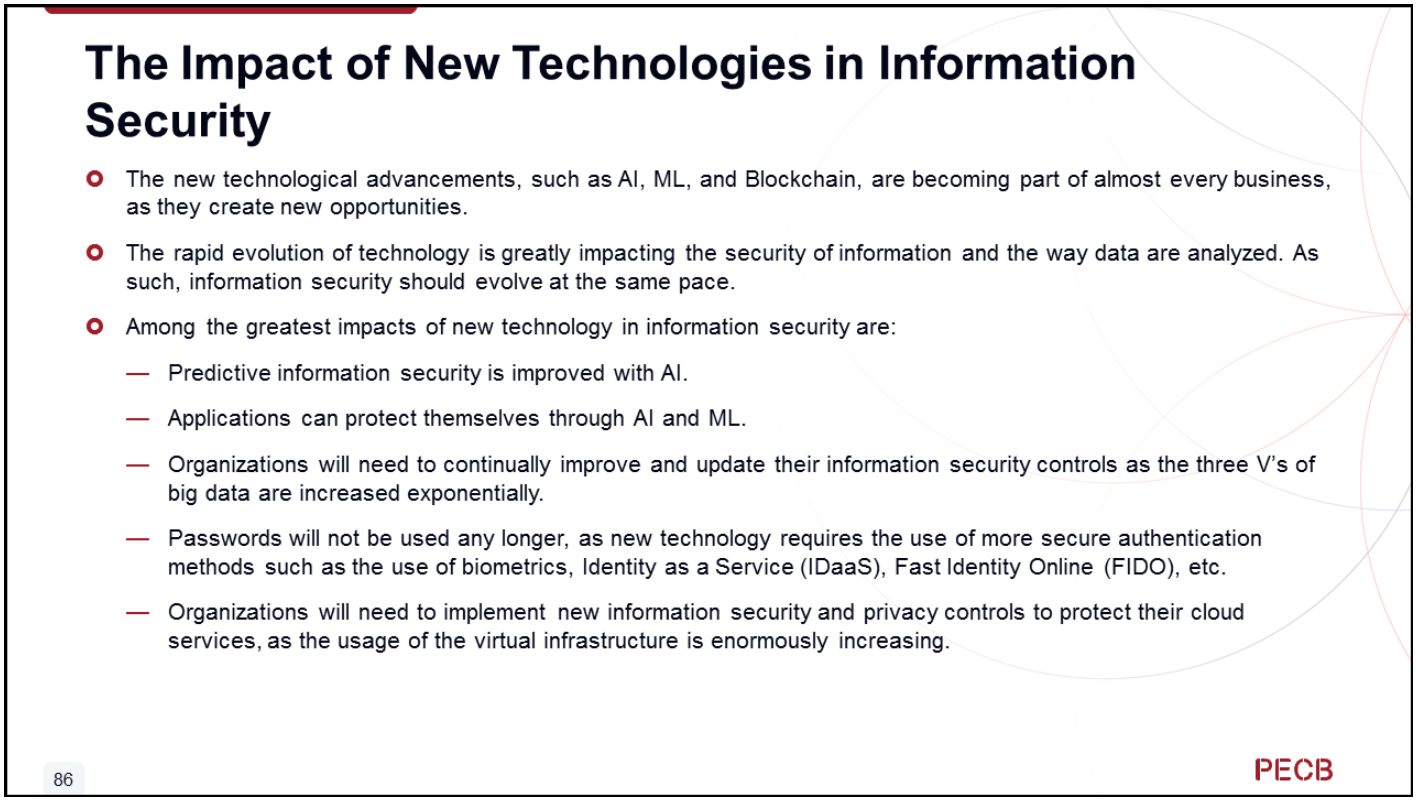
- For Infrastructure as a Service (IaaS), customers are responsible for the entire security configuration and management, including the guest operating system, applications, and firewall settings.
- For abstracted services, the cloud service provider manages the infrastructure layer, operating system, and platforms, while customers focus on managing their data, encryption options, asset classification, and permissions using IAM tools.

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, etc.

Organizations outsource in order to reduce their costs, ensure efficiency, and focus on key business operations.

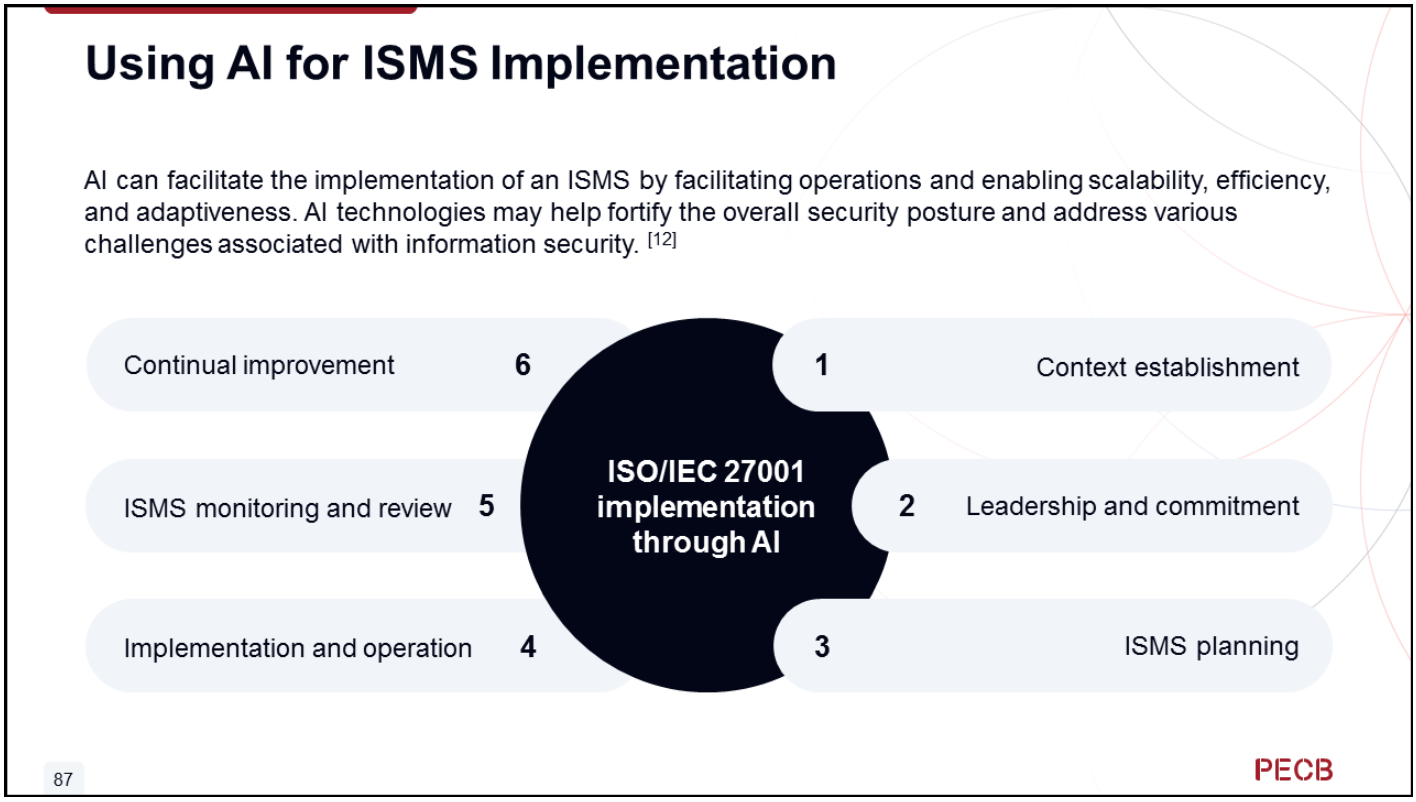


Predictive information security is an approach that uses predictive, strategic, and intelligent analytics through AI to anticipate and assess information security in real time. For instance, as the issues of fraud and money laundering constantly arise, machine learning models are able to automatically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

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. **Context establishment:**
   - AI is crucial in information security as organizations must identify internal and external factors influencing their ISMS to manage risks effectively. AI enhances efficiency by automating the scanning of both internal IT environments and external threat landscapes using machine learning to map out connections, creating a visual topology, and employing graph databases to track relationships for easy analysis.
   - AI systems continuously monitor diverse sources for emerging threats, leaked credentials, zero-day vulnerabilities, and high-risk vulnerabilities through natural language processing, enabling a comprehensive establishment of the information security context at a faster pace than human analysts.
2. **Leadership and commitment:**
   - AI aids executives in developing effective policies, defining roles, setting objectives, and guiding strategic direction in information security.
   - AI-driven chatbots and virtual assistants provide customized resources, such as sample policies and training materials, ensuring efficient collaboration for geographically dispersed leaders in planning the ISMS.
3. **ISMS planning:**
   - AI assists in ISMS implementation by automating the identification of information assets using scanning, crawling, and mapping techniques, and employs machine learning to track changes in asset inventories over time.
   - Algorithms in AI systems assimilate intelligence feeds, scan the dark web, simulate ethical hacking scenarios, and model attack probabilities to systematically recognize potential threats, allowing for informed selection of controls from ISO/IEC 27001 Annex A based on asset sensitivity and exposure.
   - Automated planning tools use synthesized data on assets and risks to generate comprehensive ISMS implementation roadmaps, including phases, activities, schedules, and resource allocations, with dashboards for tracking the progress of the plan.

Slide Notes Extension

4.Implementation and operation:

- AI facilitates ISMS implementation tasks, including the establishment and execution of robust processes for ISMS by automating routine tasks such as configuring firewalls, deploying endpoint agents, defining access rules, and installing hardware. This automation allows security personnel to prioritize strategic and high-value activities during ISMS implementation.
- Cloud-based AI platforms with centralized dashboards enable seamless orchestration and provisioning of security controls across the entire IT environment. Application programming interfaces (APIs) further integrate diverse security products into a unified framework, enhancing the effectiveness of the ISMS implementation.
- The deployment of powerful cybersecurity analytics, driven by machine learning algorithms, automates monitoring activities across various domains. In the face of security threats, AI-driven security orchestration, automation, and response (SOAR) platforms swiftly validate incidents, isolate affected systems, terminate unnecessary processes, revoke user access, and halt malware propagation. This automated response significantly minimizes the overall damage caused by security incidents.

5.ISMS monitoring and review:

- AI enhances ISMS effectiveness by providing continuous performance monitoring, surpassing the intermittent nature of human reviews. Virtual assistants use AI to assess key performance indicators such as patch latencies, virus scan frequencies, encryption coverage, and access request approvals.
- Machine learning algorithms are employed to randomly sample log, event, and traffic data, identifying potential lapses in controls. Natural language processing sifts through various communication channels to detect instances of high-risk behavior, misuse, and policy violations.
- AI significantly improves auditing capabilities by systematically examining network traffic, open ports, cloud configurations, access controls, and system settings for any deviations from ISO/IEC 27001’s best practices. Intelligent dashboards fueled by AI provide easily digestible security metrics, audit findings, risk scores, performance trends, and benchmarks tailored to the specific needs of both management and operators.

6.Continual improvement:

- AI contributes to ongoing enhancement in ISMS implementation by continuously assimilating new external threat data and internal monitoring intelligence, allowing systems to refine risk models and anticipate

emerging threats at an earlier stage.

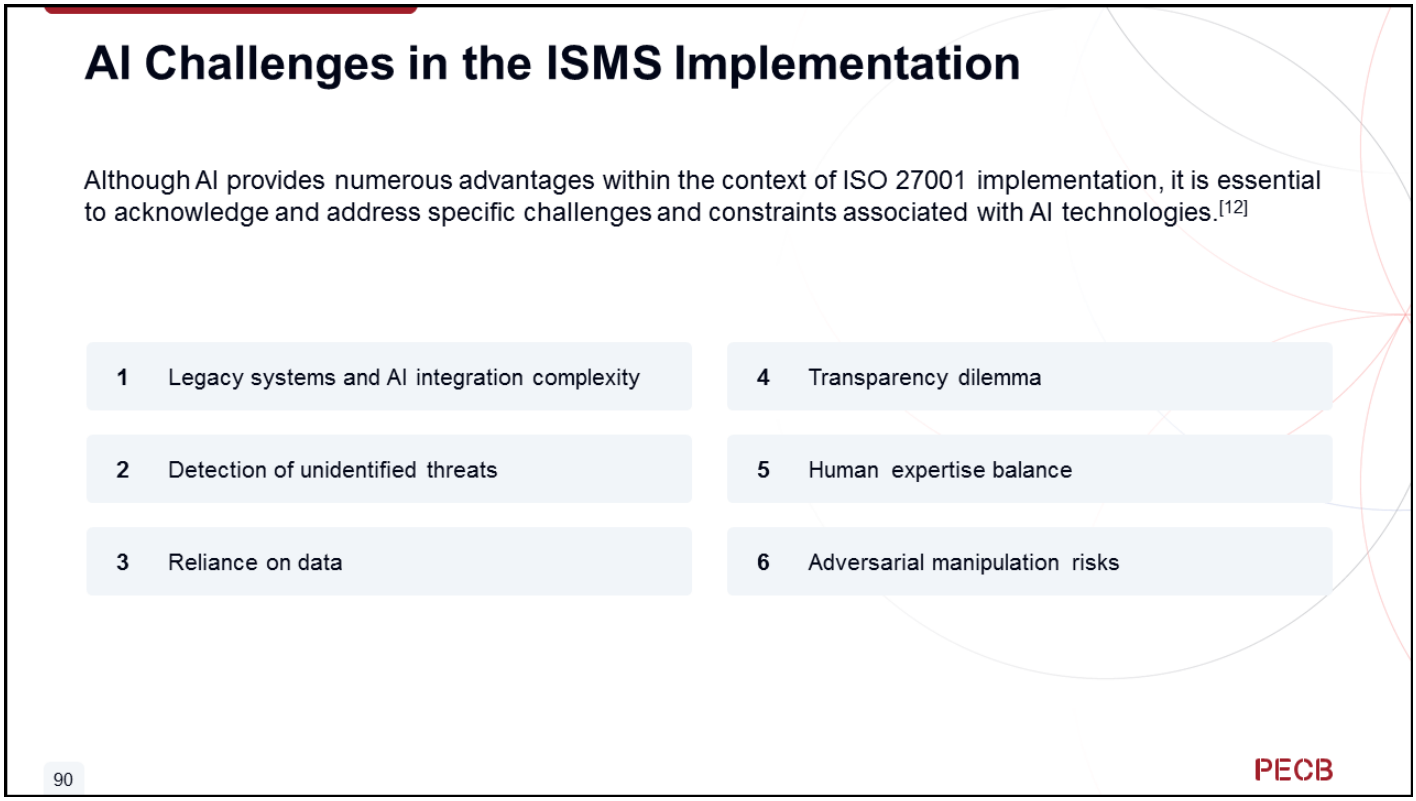
- Machine learning algorithms systematically analyze incident, audit, and control data, providing analytical insights that enable targeted enhancements to processes and technologies, thereby reinforcing defense mechanisms within the ISMS.
- Natural language AI is used to assess sentiment from employee and customer surveys, emails, chats, and social media, identifying both strengths to be reinforced and weaknesses requiring remediation. Virtual assistants leverage aggregated performance data and sentiment analysis to deliver tailored recommendations to executives, while expert systems conduct cost-benefit analyses to maximize the return on security investments in the ISMS.

AI-Driven ISO/IEC 27001 Evolution

There are five pivotal areas where AI is impacting fundamental aspects of ISO/IEC 27001 implementation[13]:

- **Automating compliance tasks:** AI revolutionizes the ISO/IEC 27001 compliance process by automating time-intensive activities like risk assessment, incident response, and training for security awareness, thereby streamlining and enhancing conformance.
- **Enhancing risk management**: AI is employed for scrutinizing extensive data sets sourced from diverse sources with the aim of detecting and consistently evaluating potential risks. This proactive approach empowers organizations to maintain a vigilant stance on security measures, thereby minimizing potential threats.
- **Optimizing security controls:** The use of AI facilitates the development and implementation of more robust security controls, empowering organizations to safeguard their information assets. This includes preventing unauthorized access, utilization, disclosure, alteration, or destruction.
- **Streamlining incident response:** The integration of AI into incident response tasks leads to process automation, enabling organizations to respond to incidents with greater speed and effectiveness. This, in turn, strengthens their overall cybersecurity posture.
- **Revolutionizing security awareness:** AI is instrumental in designing security awareness training that is both more compelling and conducive to productivity. This innovative approach plays a crucial role in reducing the risk of human error, contributing to a more informed and vigilant workforce.

PECB



1. **Legacy systems and AI integration complexity:** Organizations lacking modern IT infrastructure face challenges integrating AI with legacy systems, particularly those without APIs or cloud connectivity. Securely migrating data to the cloud introduces additional complexities, necessitating careful consideration within the ISMS framework.
2. **Detection of unidentified threats:** AI's reliance on learning from data patterns may result in the oversight of entirely new attack methods. Analyzing blind spots becomes challenging due to the opaque nature of deep learning models, making it difficult to identify potential threats.
3. **Reliance on data:** Inaccurate data can lead to inaccurate results, which is why acquiring comprehensive and reliable data is pivotal for maximizing the potential of AI.
4. **Transparency dilemma:** When organizations cannot easily comprehend how an AI system arrives at its decisions, it creates a lack of transparency while implementing an ISMS. Effective oversight is highlighted as a crucial element, ensuring that AI systems operate in a transparent, accountable, and trustworthy manner.
5. **Human expertise balance:** Relying too heavily on AI without maintaining and valuing human expertise could result in a diminished ability to understand, interpret, and act upon information in a nuanced and context-specific manner.
6. **Adversarial manipulation risks:** Adversarial vulnerabilities in AI systems may arise from the potential for external actors to manipulate data inputs or training processes, leading to deceptive outcomes that can be exploited for malicious purposes.

Section 17 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.
- The new technology has an enormous influence on information security as well. It has brought information security into another level of development and evolution.

Questions?

Quiz 17

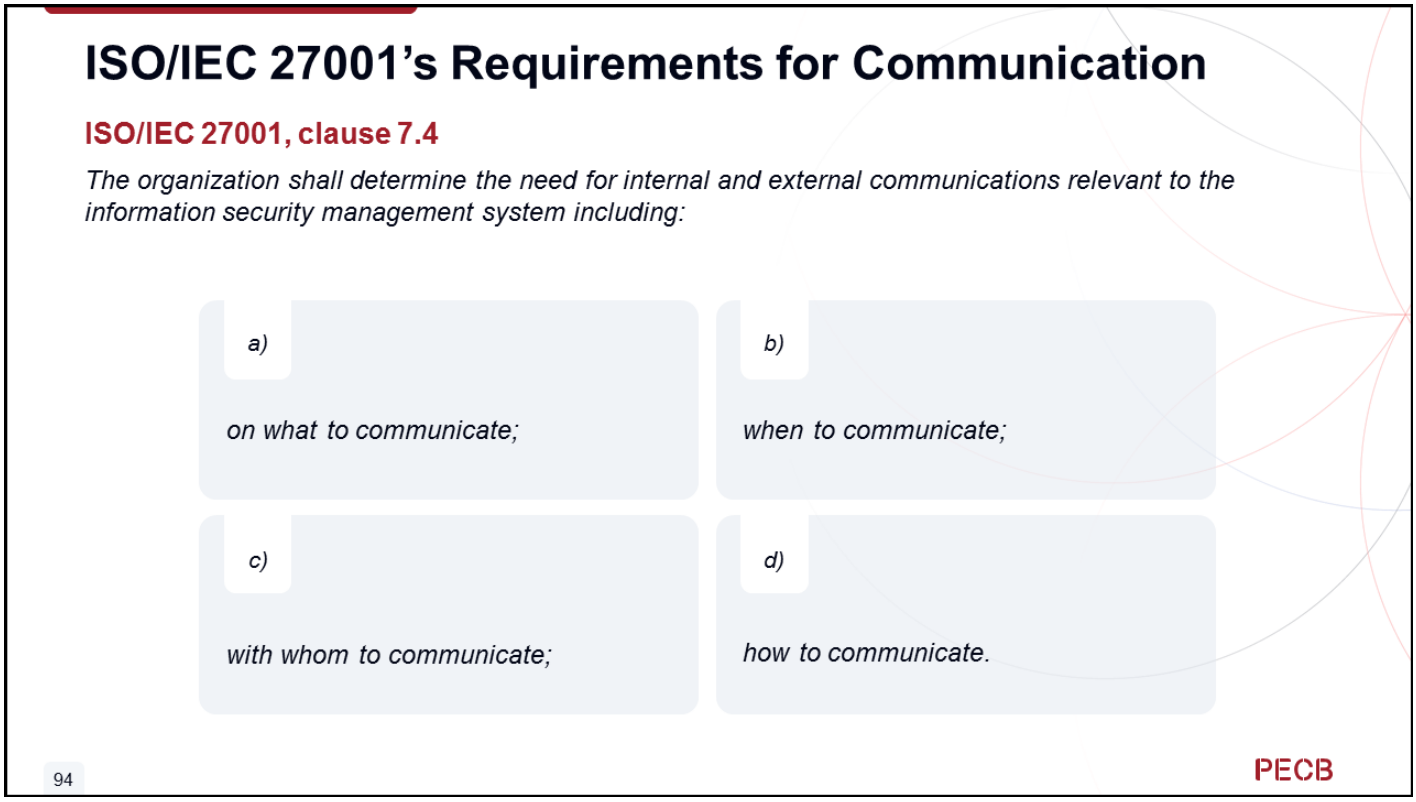
Note: To complete Quiz 17, please go to the Quizzes Worksheet.

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.

Communication

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

PECB



The aim of communication is to inform the concerned parties about a given subject.

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.*

Slide Notes Extension

ISO/IEC 27003, clause 7.4 Communication (cont'd)

Guidance

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. Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system.

The principles of effective communication are:

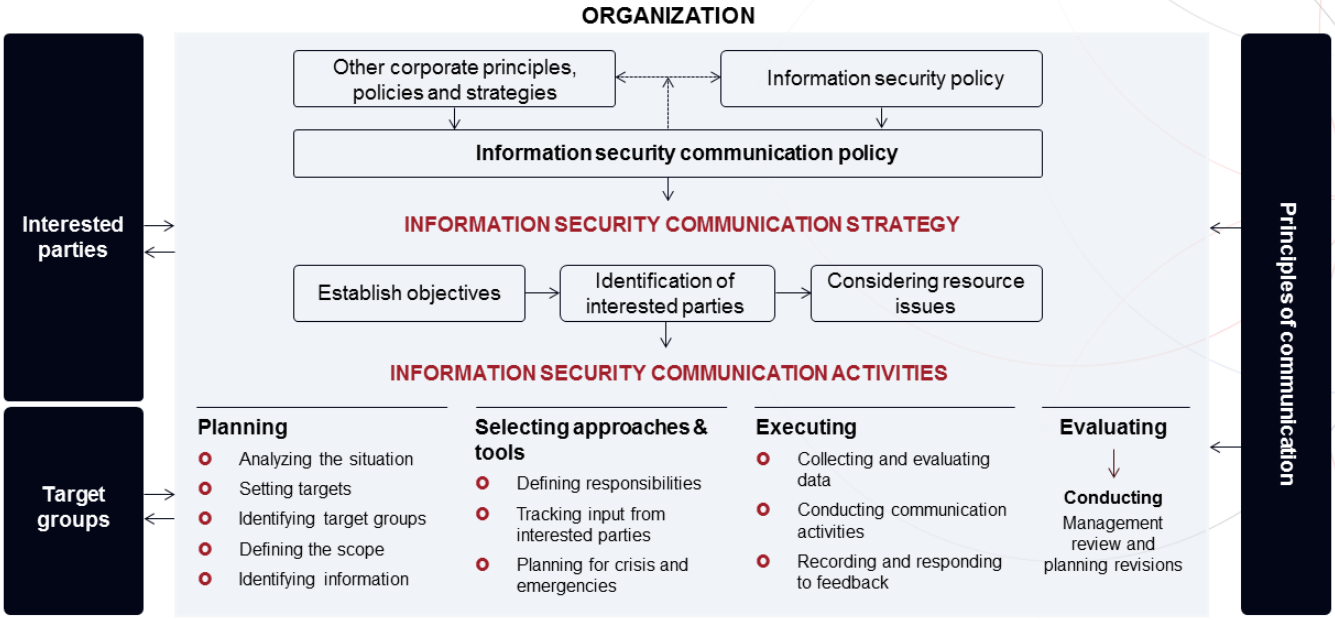
1. **Transparency**: Properly communicate the processes, procedures, methods, data sources, and assumptions to all interested parties, taking into account the confidentiality of information.
2. **Appropriateness**: Provide relevant information to interested parties using formats, language, and media that meet their interests and needs, enabling them to fully participate.
3. **Credibility**: Conduct communication in an honest and fair manner and provide information that is truthful, accurate, and substantive.
4. **Responsiveness**: Respond to the queries and concerns of interested parties in a full and timely manner and inform interested parties on how their queries and concerns have been addressed.
5. **Clarity**: Ensure that the language of communication is easily understood by all interested parties in order to avoid ambiguity.

2.4 Communication

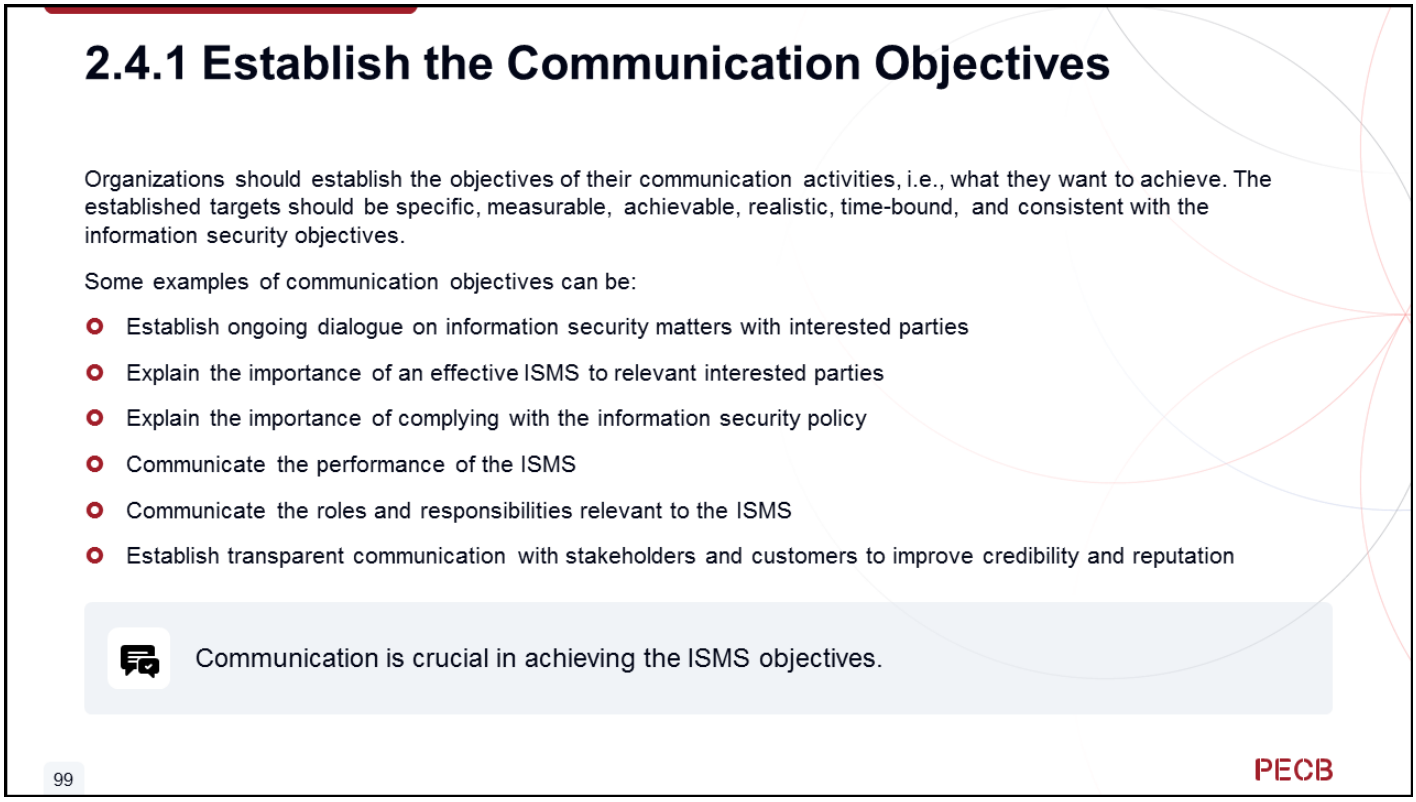
List of activities

PECB

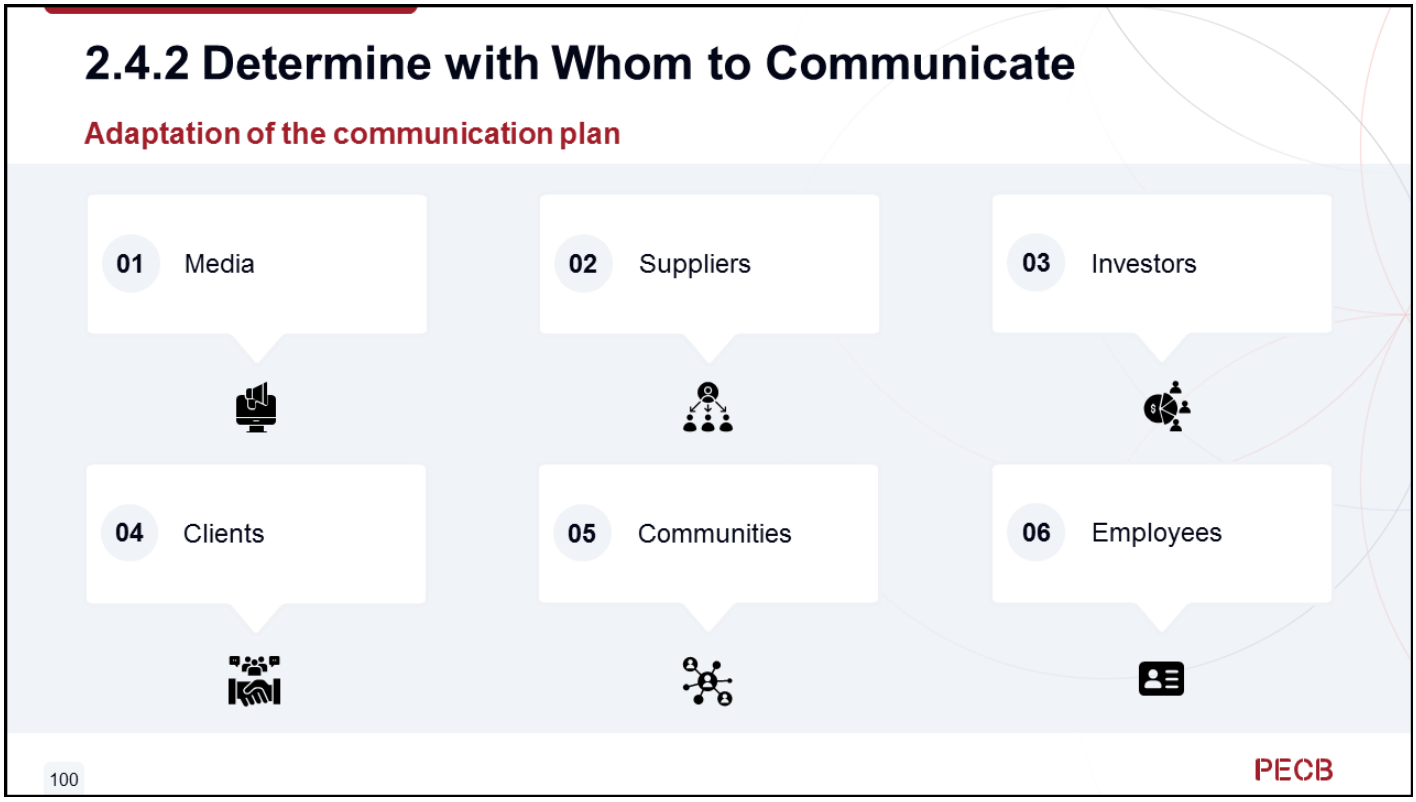
Information Security Communication Process



PECB



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.



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. 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. In addition, It should 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 Develop the Communication Strategy

- The organization's top management should develop a strategy to implement communication activities.
- Among others, the strategy should include the following:
  - Communication objectives
  - Interested parties
  - An indication of when and what the organization plans to communicate
  - 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.

101

PECB

Information security communication should be integrated with the organization's broader activities and aligned with its management system, policies, strategies, and relevant undertakings.

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 on information security issues related to the organization's specific context

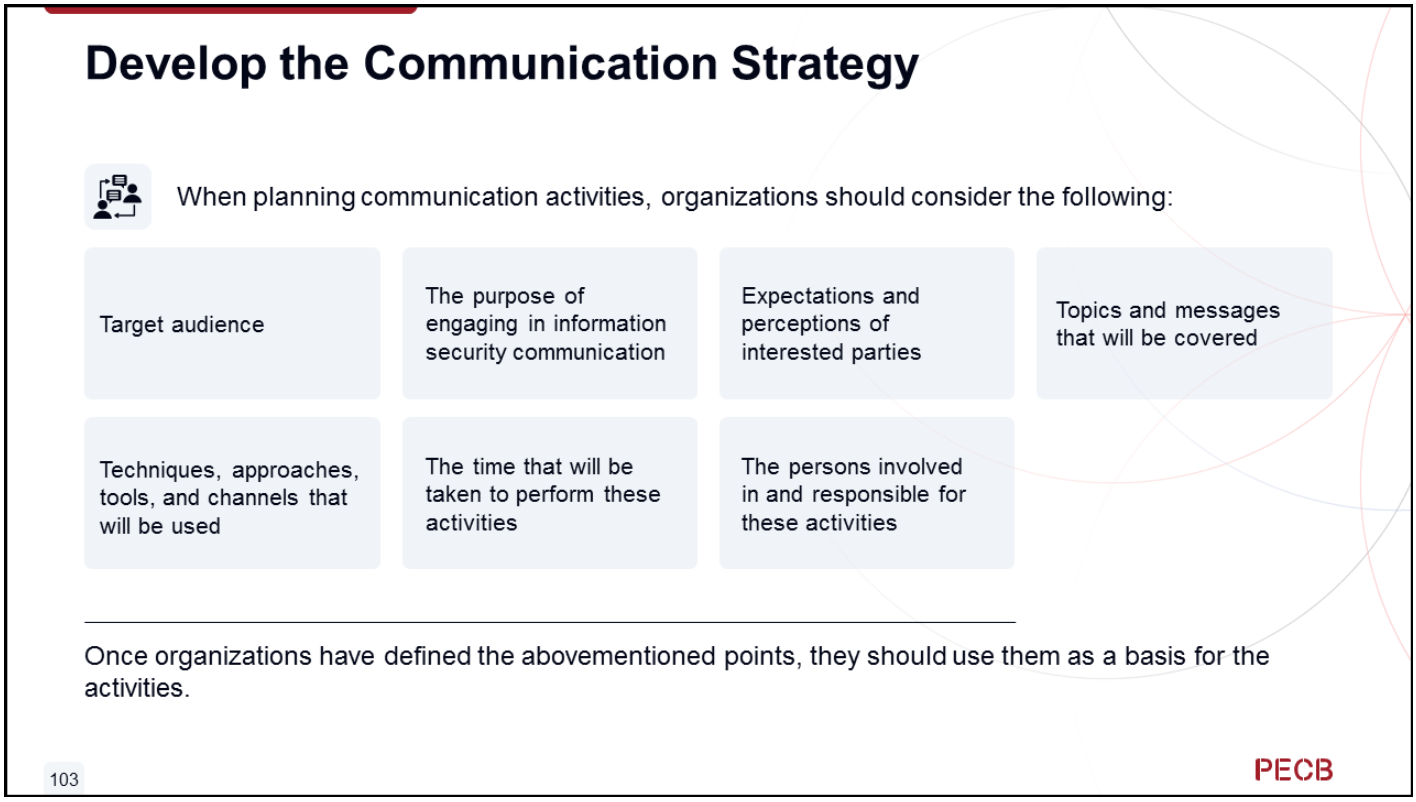
When evaluating the context for an information security communication activity, it is also important to consider the potential costs and consequences of not communicating. Such consequences can be material; they can cost more than information security communication in the long run, and also impose other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

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.



Organizations will typically undertake a range of information security communication activities in implementing their information security communication strategy. 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 approaches or tools to use to conduct communication activities largely depend on whether organizations aim to consult, understand, inform, persuade, or simply involve the target group.

Organizations should make the information they communicate appropriate to the target group. This could be done by:

- Taking into account some aspects, such as the social, cultural, educational, economic, and political interests of target groups
- Using appropriate language
- Using appropriate visual images or electronic media, where appropriate
- Being consistent in the approach or tool selected

Before actually implementing and performing the communication with the target group, organizations should test the selected approaches and tools.

2.4.5 Evaluate the Effectiveness of the Communication Process

It is important that organizations give plenty of time to the communication activities to be effective and performed appropriately. In particular, the time needed will depend on the extent of the communication activity and the type of approach used.

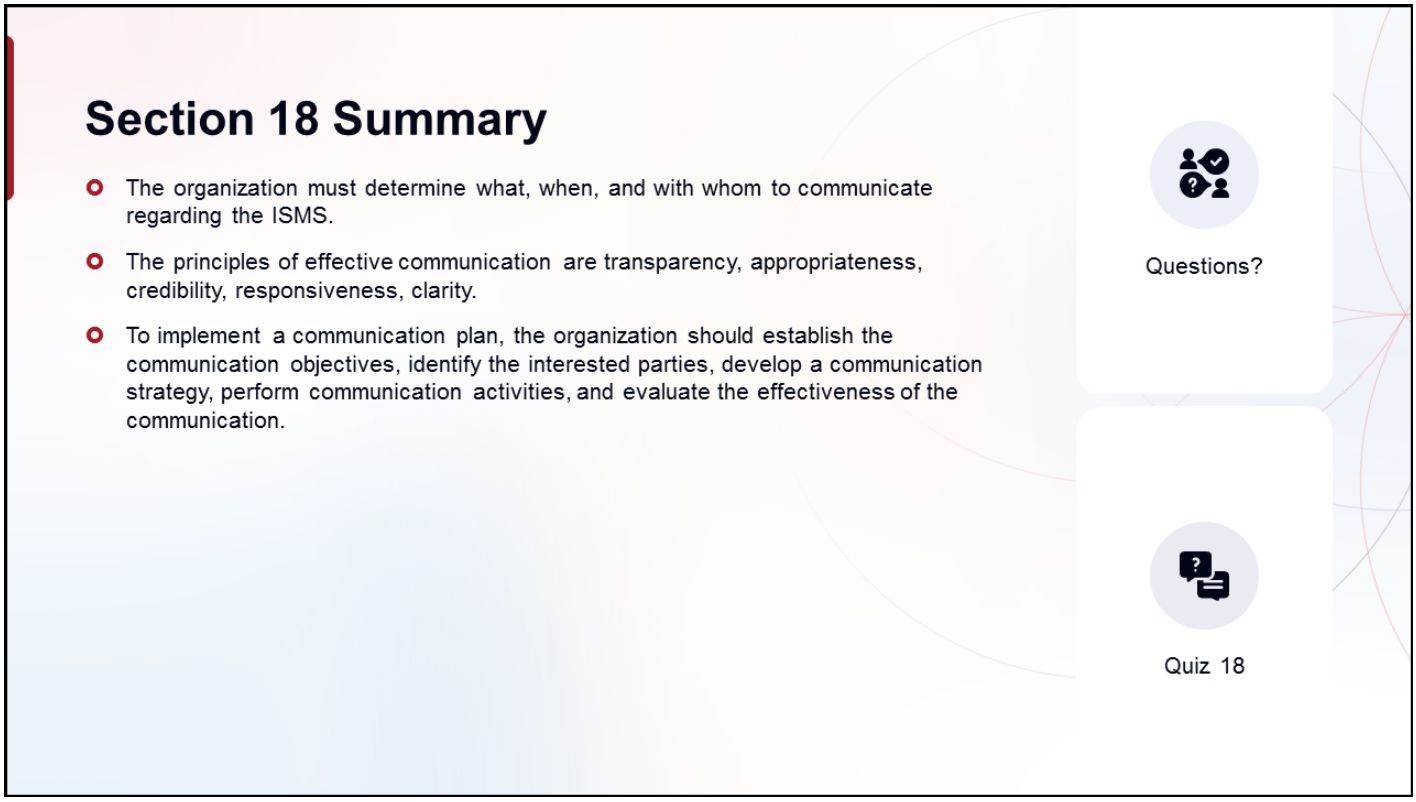
Organizations should periodically review and evaluate the effectiveness of the communication process. This way, organizations will close any gaps and further increase the effectiveness of their ISMS.

105

PECB

When evaluating the effectiveness of the communication process, the organization should consider, among others, whether:

- The information security policy is understood and followed by the target group.
- The principles of effective communication are followed.
- The objectives of communication activities have been achieved.
- The approaches or tools used to conduct communication activities are appropriate.
- The information and language are appropriate.
- The responses of the target group show positive results and support the achievement of objectives.
- The target groups' issues, suggestions, and remarks are addressed.
- The target groups fully understand the purpose and content of the activities.



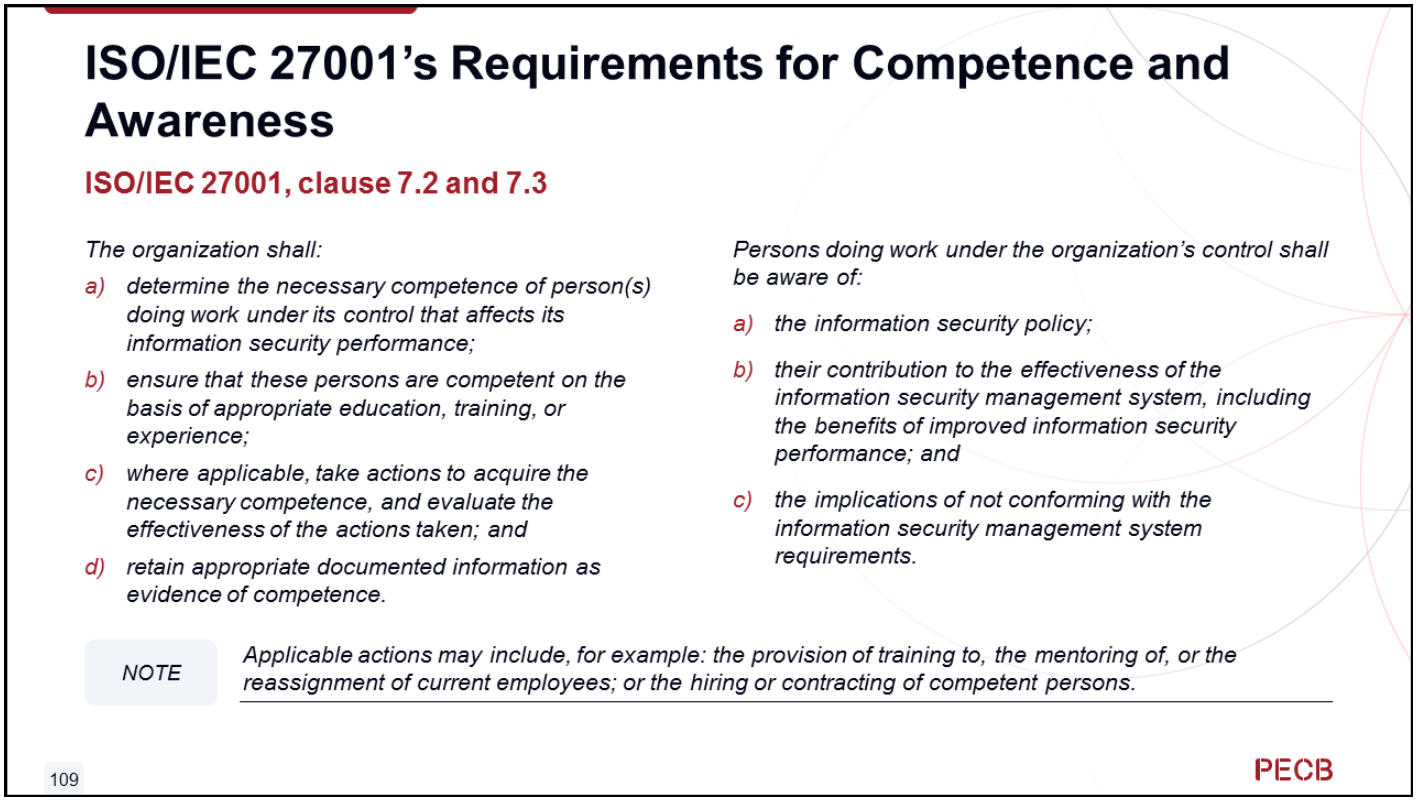
Note:To complete Quiz 18, please go to the Quizzes Worksheet.

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.

Competence and Awareness

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

PECB



ISO/IEC 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.*

ISO/IEC 27003, clause 7.3 Awareness

Guidance

The organization should:

c.*prepare a program 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'*

behavior to reinforce the message.

Competence and People Development

ISO 9000, clause 3.10.4 and ISO 10015, clause 3.2

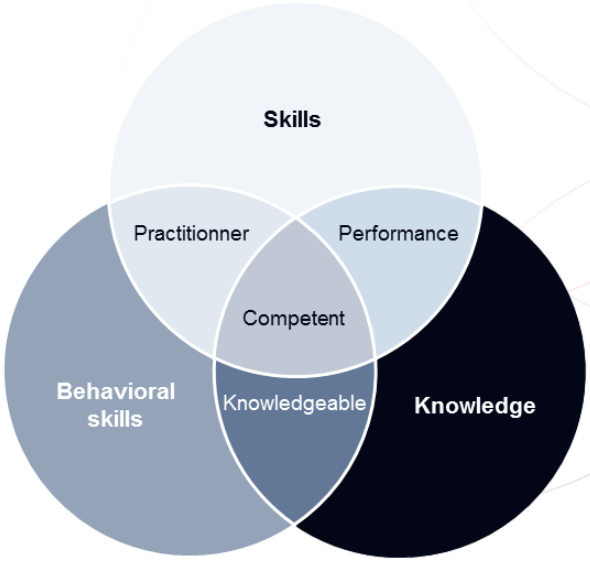
Competence

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



110

PECB

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 and Awareness

Training

The aim of a training program is to help an individual acquire the knowledge, skills, and behavior required to meet specific requirements.

Awareness

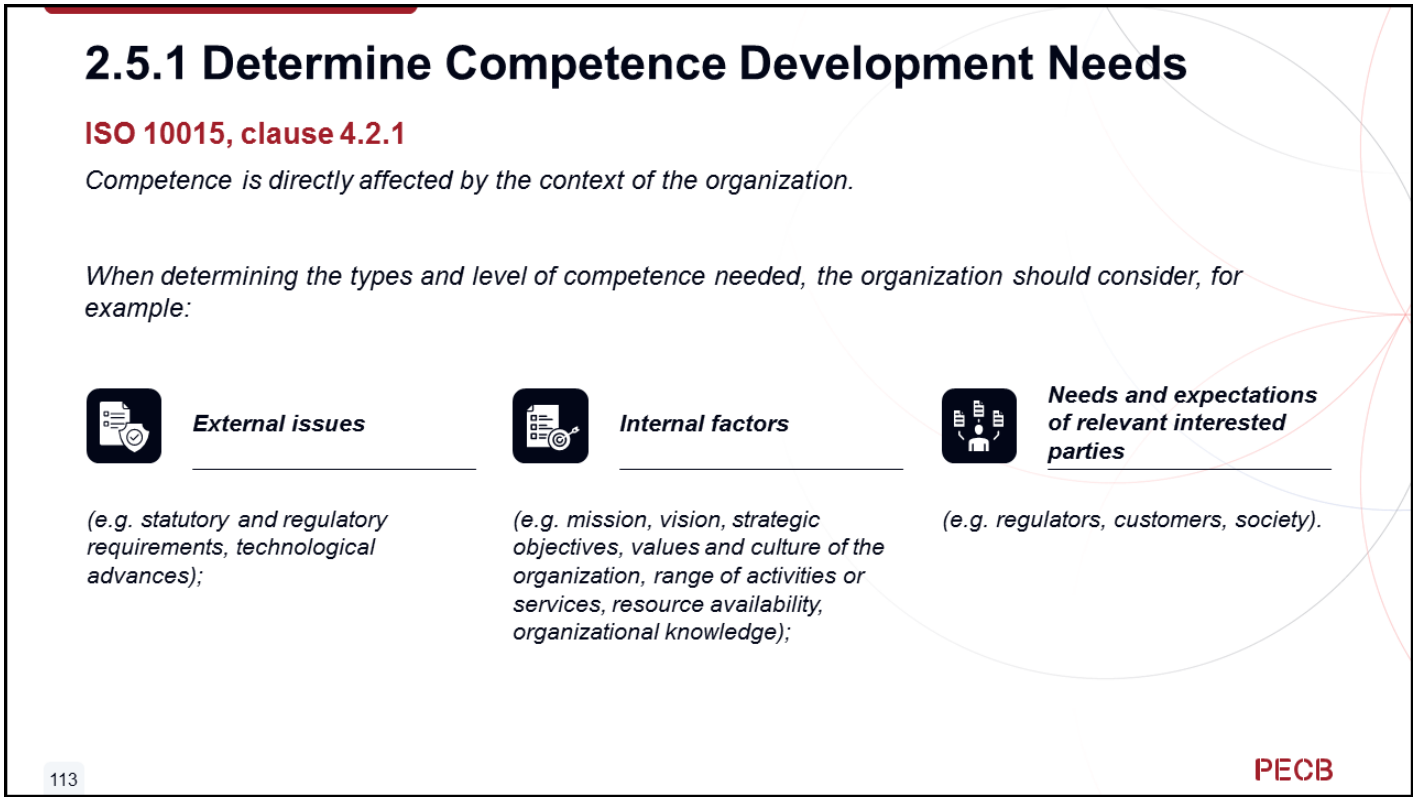
The aim of an awareness session is to inform and engage the target audience about a specific issue, potentially leading to a shift in their approach and behavior.

PECB

2.5 Competence and Awareness

List of activities

PECB



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 programs 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. *behaviors (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:

— *consider existing competence levels;*

— *compare these with required competence levels;*

— *use risk-based thinking to prioritize actions to address competence gaps.*

PECB

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

After assessing their employees' competencies, organizations must address the identified competency gaps through activities. Such activities include:

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

The competence development program should take into account the following points:

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

116

PECB

ISO 10015, clause 5.4.2

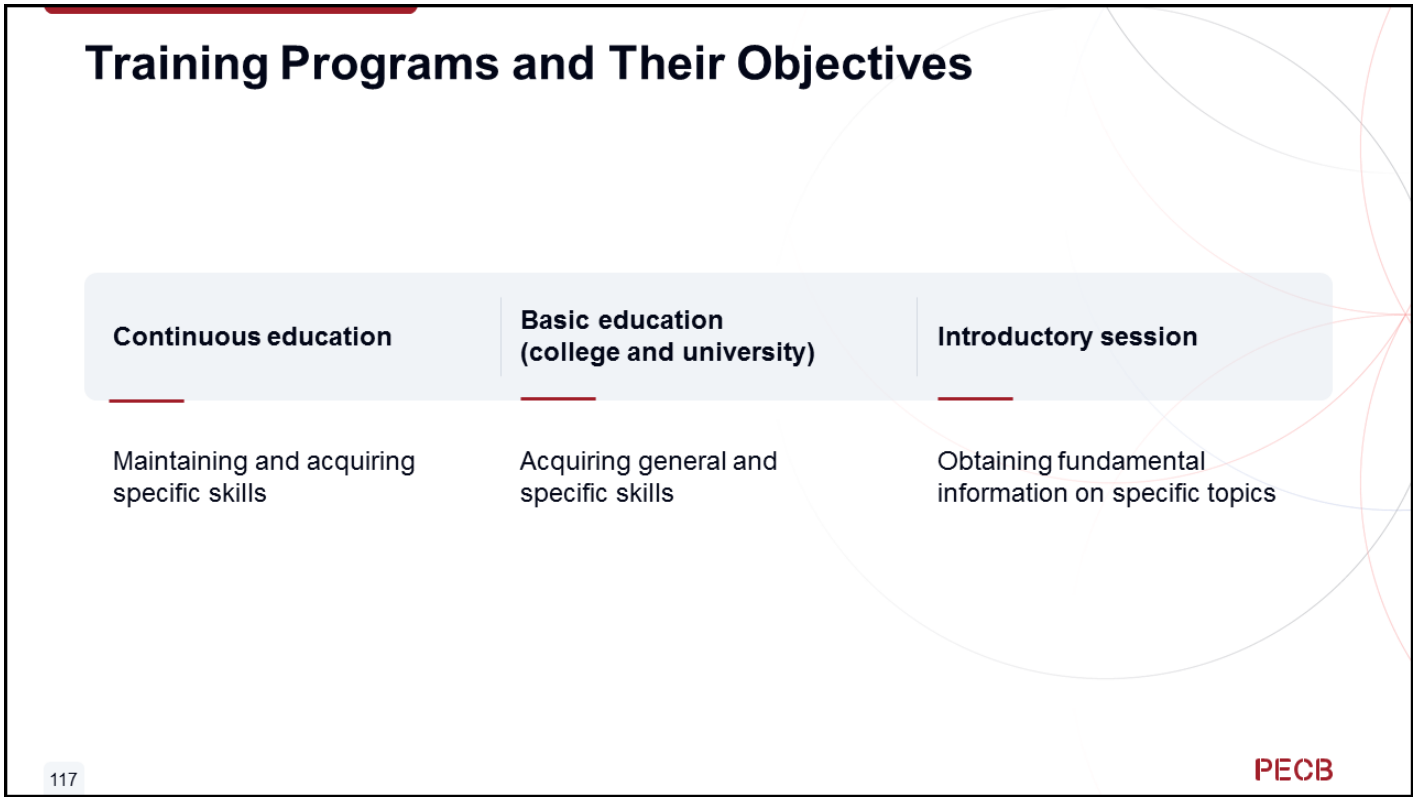
Competence management and people development activities at the team or group level should address:

a. *establishing and delivering team or group training programs;*
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 Program structure

The competence management and people development program 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).*



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

Nowadays, many universities and colleges offer complete specialized courses in information security. Such courses can provide the necessary expertise and specialization to the employees who are responsible for information security on specific areas.

Introductory sessions 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, several professional certifications in information security have been developed. These certifications can help enhance personal development and ensure recognition.

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.

118

The “human” factor is essential in ensuring the effectiveness of the ISMS. If humans are the key strength, they can also be the main weakness, which is why they require attention. The organization’s employees should be aware of and understand their responsibilities, how they can contribute to the effectiveness of the ISMS, 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 change 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 malware
- 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 organization must provide the necessary resources for the successful delivery of the training. It should support both the trainer and the trainees and ensure that the training is qualitative and achieves its intended results.

120

PECB

- **Before the training,** the organization should provide information to the trainer about the nature of the training and the competence gaps that have been identified during the training needs assessment.
- **During the training,** the organization should provide the necessary resources to successfully deliver the training. Such resources include tools, documentation, equipment, etc.
- **After the training,** the organization should acquire feedback regarding the training from the trainees and the trainer. 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 determine whether its objectives have been achieved. This evaluation involves obtaining feedback from the trainer, trainees, and other people involved. The results of the evaluation can be used to further improve the quality of the training program.

121

PECB

Kirkpatrick's four-level training evaluation model is an effective method to understand what the trainees have learned from the training and determine the effectiveness of the training.[1]

Level 1: Reaction

During this level, the organization measures the trainees' involvement in the training and determines their general impressions of the training. To evaluate the overall learning experience, different methodologies can be employed, such as surveys, questionnaires, or direct conversations with the trainees. Key points to address during the discussion can include:

- Assess the course content for its relevance and clarity
- Check employees' understanding and identify key takeaways
- Evaluate the program's strengths and weaknesses
- Determine if the training suits the trainees' preferred learning style

Level 2: Learning

During this level, the organization assesses the knowledge and skills acquired by trainees through the training. For this level to be measured, a variety of metrics can be employed, including:

- Scores and assessments conducted during and after training
- Assessment of hands-on learning projects
- Influence on key performance indicators (KPIs)
- Confirmation through the completion of the course and certification
- Report and feedback

Slide Notes Extension

Level 3: Behavior

During this level, the organization assesses the impact of the training on the trainees' performance and workplace behavior. It can be evaluated through a combination of the following methods:

- Self-evaluation surveys
- Informal input from colleagues and supervisors
- Involvement in the focus group
- Observation during on-the-job activities
- Review of KPIs associated with real job performance
- Evaluation of customer feedback, survey, or complaints

Level 4: Results

During this level, the organization evaluates the results of the training such as cost reduction, boosted morale, enhanced quality, and improved marketing leads. Key metrics to measure this level can include:

- Enhanced business outcomes
- Improved productivity and work quality
- Retention rates for employees
- Enhanced morale
- Index of customer satisfaction

Section 19 Summary

- The organization must conduct competence development activities such as training and awareness programs for employees whose work affects the ISMS. Such activities help organizations conform to the information security objectives.
- To implement competence development activities, organizations should determine competence and development needs, assess current needs, plan competence development activities, define their type and structure, provide training and awareness sessions, and 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 policies, the use of passwords, the risk associated with emails, the security of laptops and smartphones, etc.

Questions?

Quiz 19

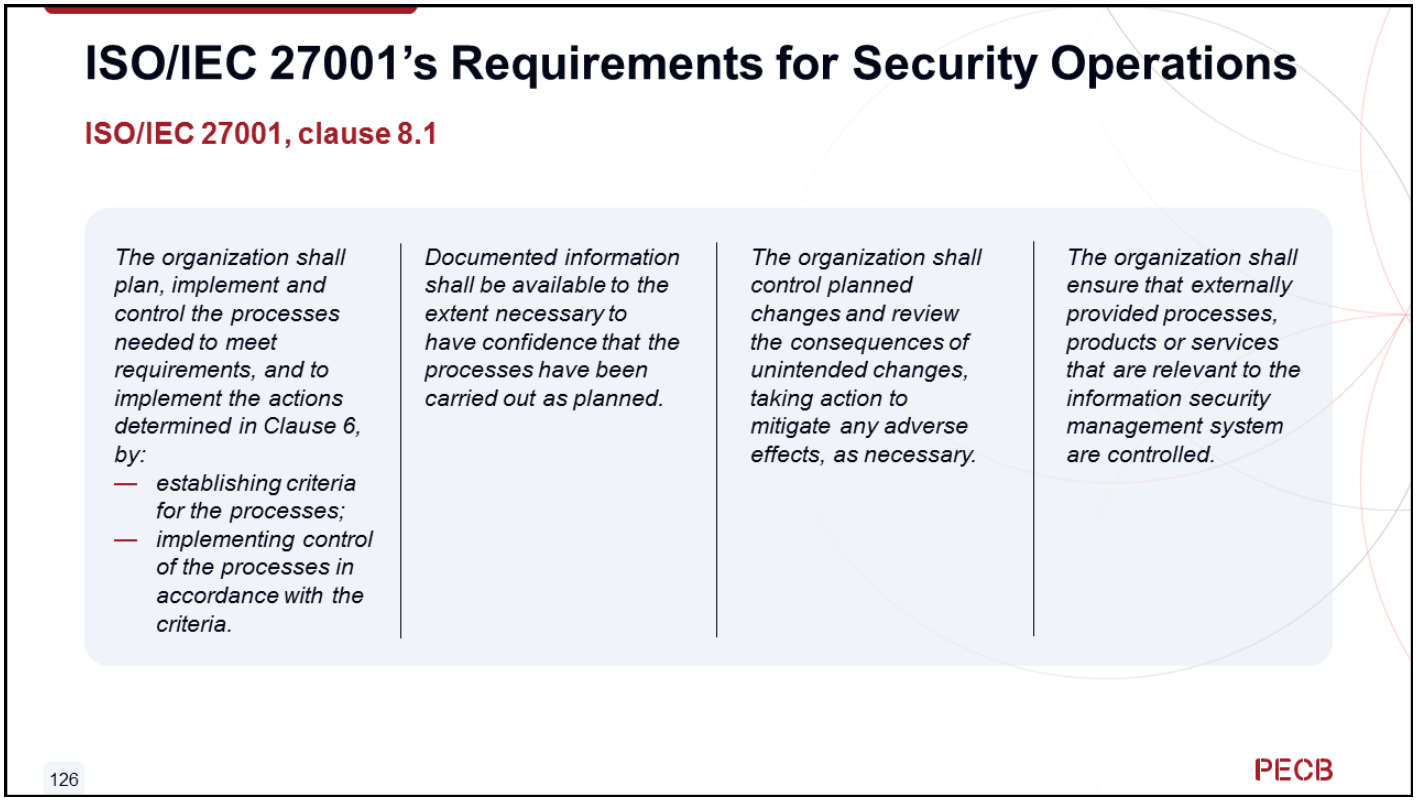
Note: To complete Quiz 19, please go to the Quizzes Worksheet.

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.

Management of Security Operations

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

PECB



ISO/IEC 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:

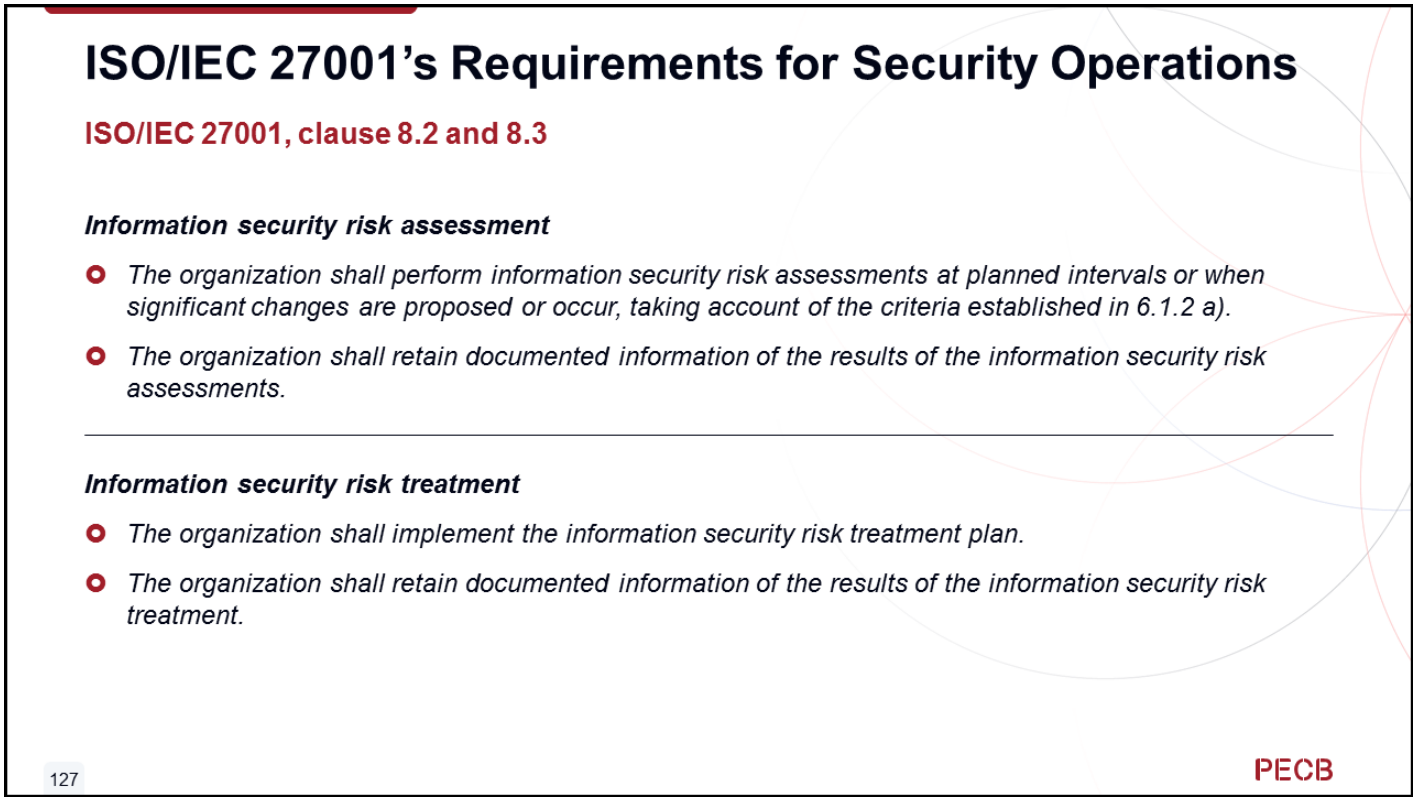
q.*determine all outsourcing relationships;*

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

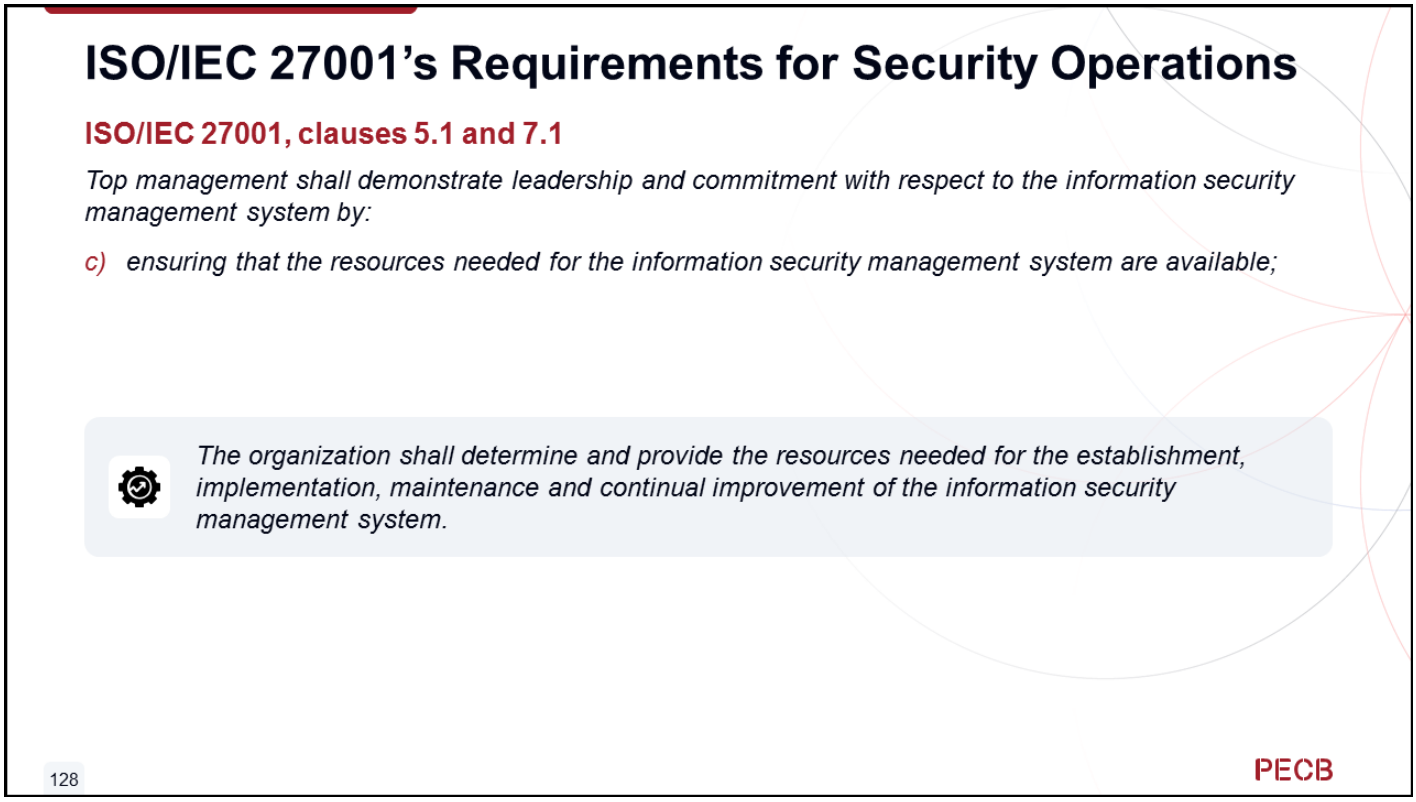
In order to treat information security risks, the organization needs to carry out the information security risk treatment process defined in 6.1.3. During operation of the ISMS, whenever the risk assessment is updated according to 8.2, the organization then applies the risk treatment according to 6.1.3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

Slide Notes Extension

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 Management of Security Operations

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 Establish an information security incident management process

2.6.5 Define the processes and draft the procedures

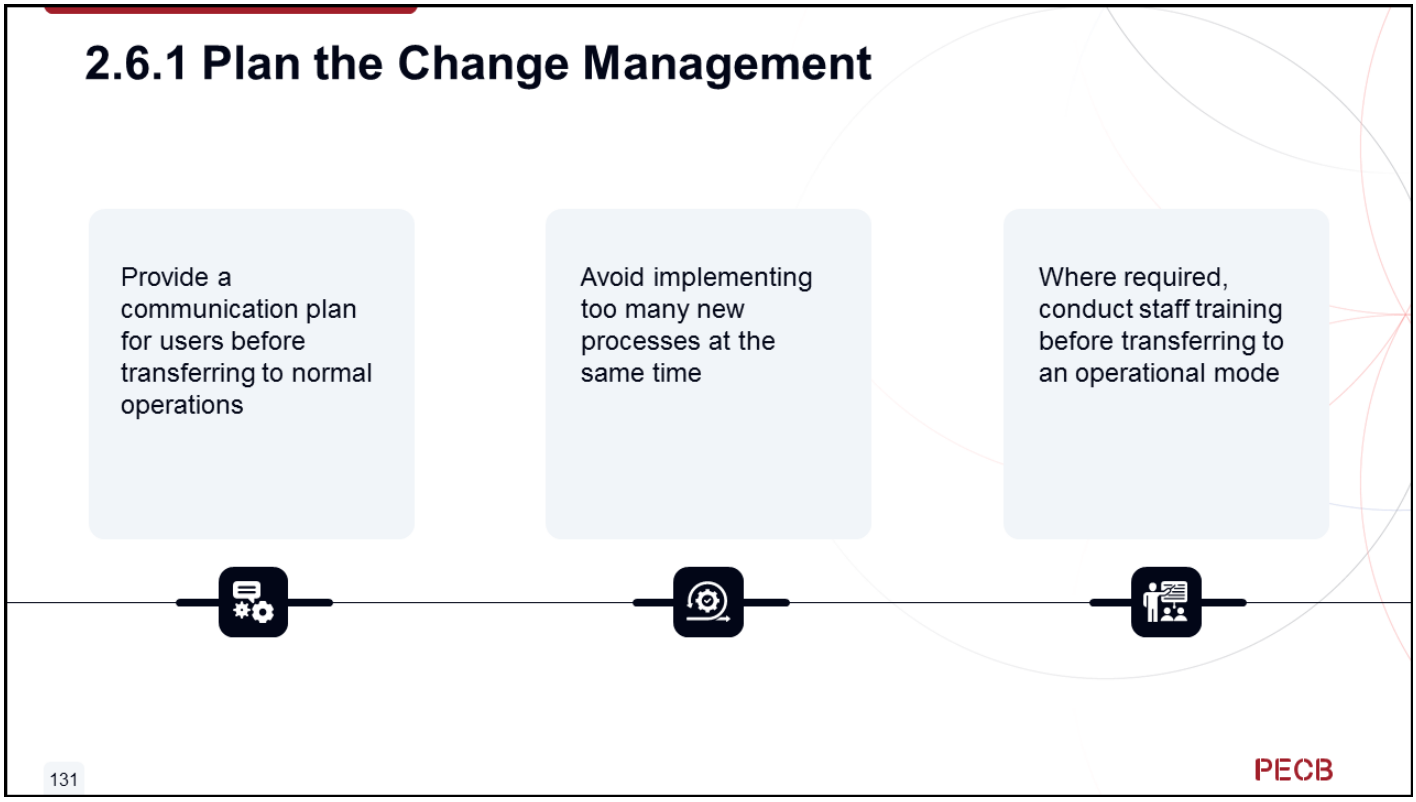
2.6.6 Establish an incident management team

2.6.7 Define a forensics process

2.6.8 Record the information related to security incidents

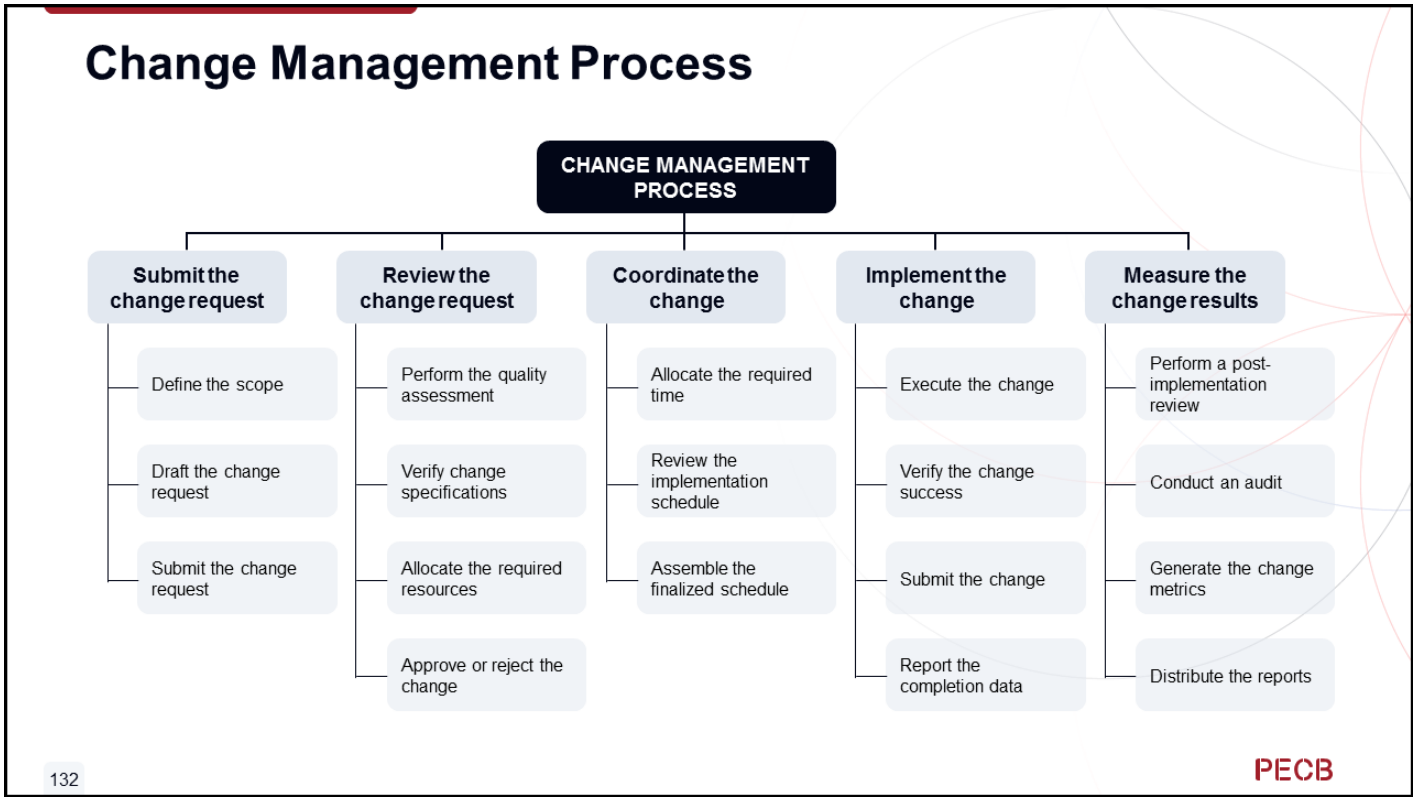
2.6.9 Measure and review the incident management process

PECB



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.

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: after the change is submitted, it should be reviewed.

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

Implement the change: the appointed person implements 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 approves the implemented change.

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

- Change request documentation
- Final implementation status
- Metrics

2.6.2 Manage the Operations

Management of operations

After the ISMS implementation has been completed, it should start operating. This transition should be smooth and should not interrupt the normal business processes.

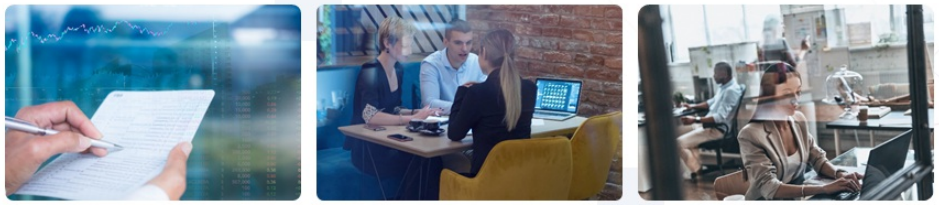
133

PECB

Although there may be an official launch of the ISMS (that is, it formally passes into an operational mode), it is more likely that this process will be completed gradually. 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 be effective until they are put into operation mode. Thus, this transition should be 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

134

PECB

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*

2.6.4 Establish an Information Security Incident Management Process

- The objective of information security incident management is to reduce the impact of security incidents on an organization's information systems and data. This can be achieved by identifying, managing, and responding to security incidents in a systematic and structured manner, with the aim of minimizing their impact and preventing their recurrence.
- The ultimate goal is to ensure the confidentiality, integrity, and availability of an organization's information assets.
- An effective incident management program includes policies, procedures, and tools to ensure that incidents are promptly identified, reported, assessed, and responded to in a timely and effective manner, with the aim of minimizing the impact of incidents and mitigating their consequences.
- ISO/IEC 27001 requires from organizations to have a well-defined incident management process for managing information security incidents.

135

PECB

ISO/IEC 27035-1, clause 4.2 Objectives of incident management

As a key part of an organization's overall information security strategy, the organization should put controls including procedures in place to enable a structured well-planned approach to the management of information security incidents. From an organization's perspective, the prime objective is to avoid or contain the impacts of information security incidents in order to minimize the direct and indirect damage to its operations caused by the incidents. Since damage to information assets can have a negative consequence on operations, business and operational perspectives should have a major influence in determining more specific objectives for information security incident management.

More specific objectives of a structured well-planned approach to incident management should include the following:

a. *information security events are detected and efficiently dealt with, in particular deciding whether they should be classified as information security incidents;*
b. *identified information security incidents are assessed and responded to in the most appropriate and efficient manner and within the predetermined time frame;*
c. *the adverse impact(s) of information security incidents on the organization and involved parties and their operations are minimized by appropriate controls as part of incident response;*
d. *a link with relevant elements from crisis management and business continuity management through an escalation process is established. There is a need for a swift transfer of responsibility and action from incident management to crisis management when the situation requires it, with this order reversed once the crisis is resolved to allow for a complete resolution of the incident;*
e. *information security vulnerabilities involved with or discovered during the incident are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the incident response team (IRT) or other teams within the organization and involved parties, depending on duty distribution;*
f. *lessons are learnt quickly from information security incidents, related vulnerabilities and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.*

Slide Notes Extension

Definitions related to information security incidents

ISO/IEC 27035-1, clause 3.1.4 Information security event

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

ISO/IEC 27035-1, clause 3.1.5 Information security incident

Related and identified information security event(s) that can harm an organization's assets or compromise its operations

ISO/IEC 27035-1, clause 3.1.6 Information security incident management

Collaborative activities to handle information security incidents in a consistent and effective way

ISO/IEC 27035-1, clause 3.1.7 Information security investigation

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

ISO/IEC 27035-1, clause 3.1.2 Incident response team

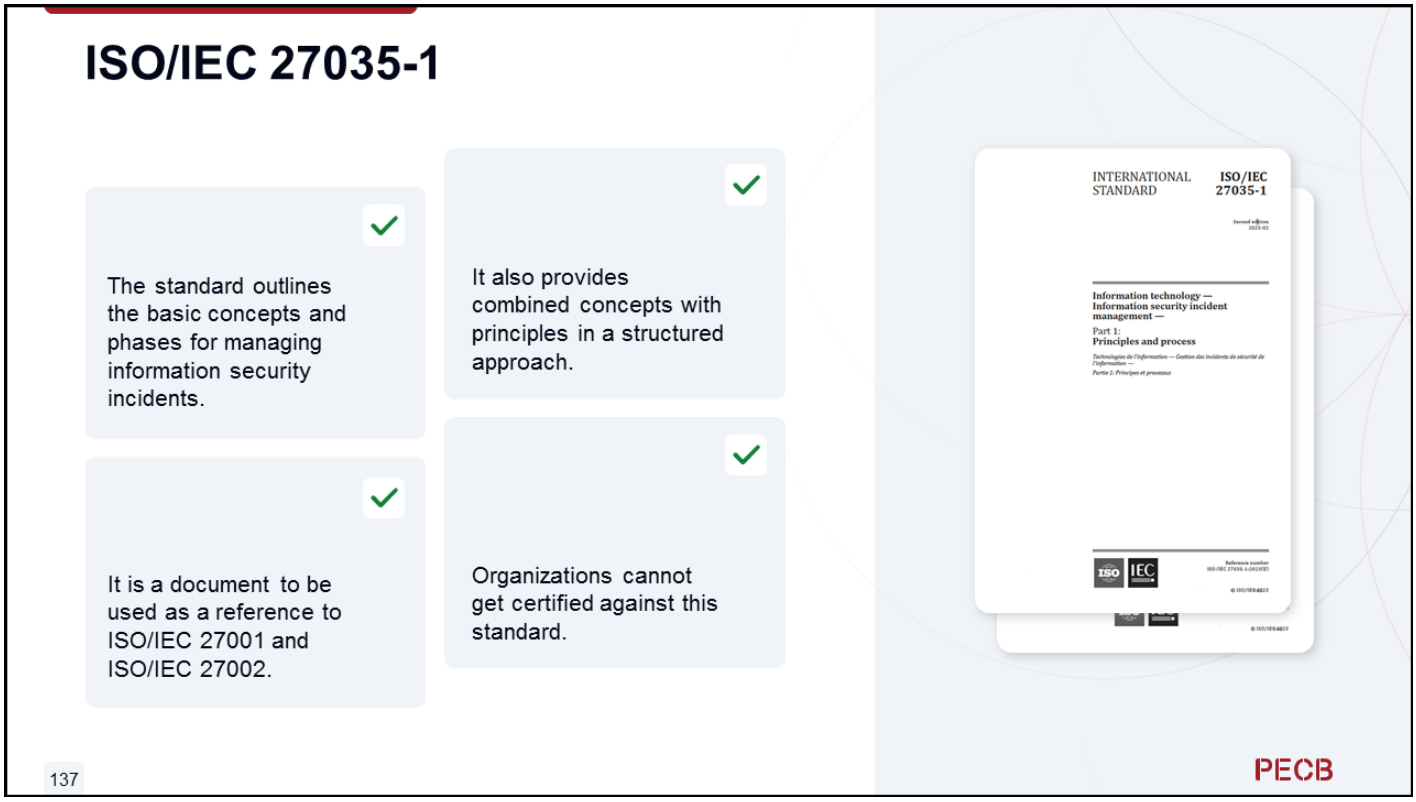
IRT

Team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way

Notes on terminology:

1. *ISO/IEC 27035-1 distinguishes an incident from a security event. According to the standard, an incident indicates a high probability that operations have been compromised, whereas, an event only indicates a possible breach. A security incident is the realization of a risk that threatens the confidentiality, integrity, and/or availability of informational resources and threatens, depending on its severity, the conduct of activities of the organization.*
2. *ISO/IEC 27001 describes the occurrence of incident scenarios as "security breaches."*
3. *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."

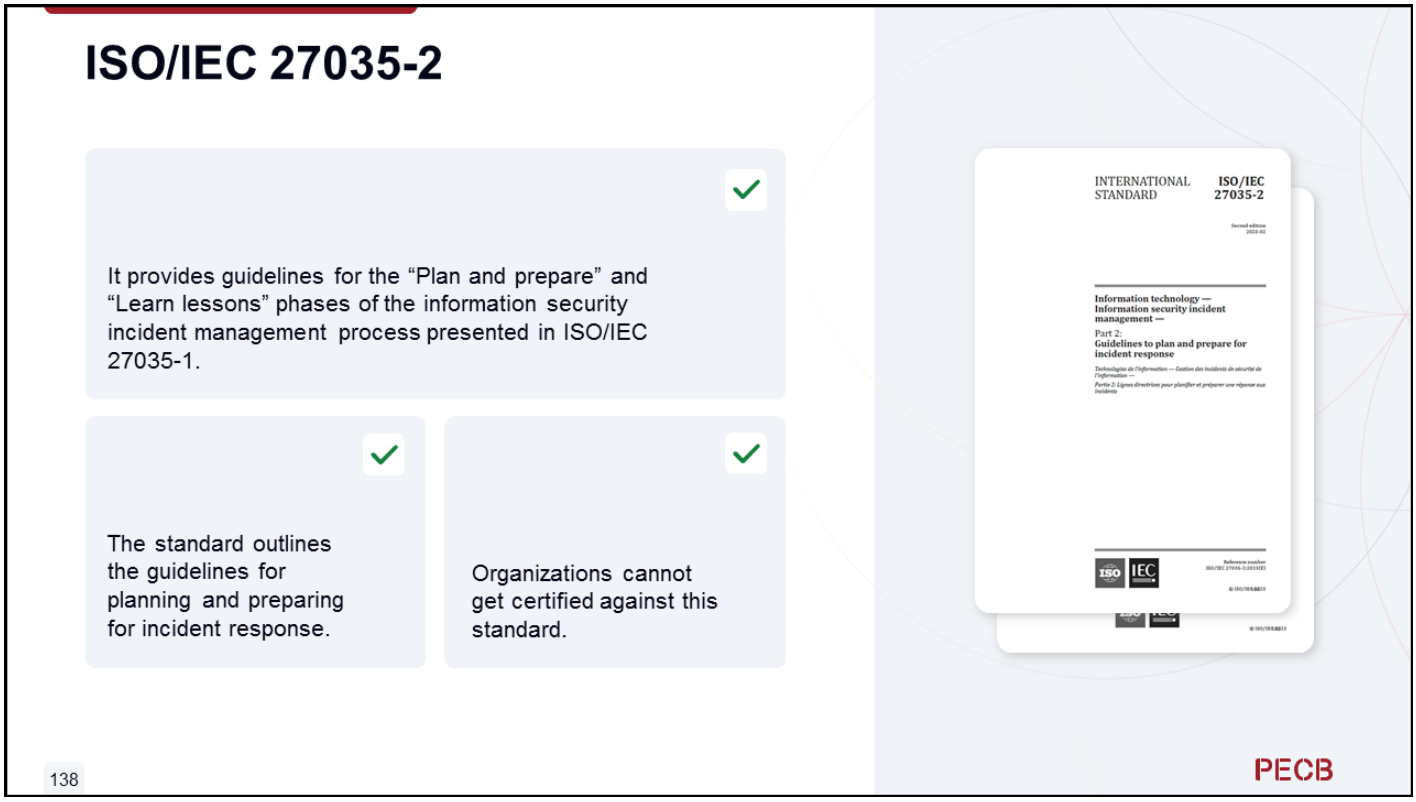


ISO/IEC 27035-1 provides guidance to plan, implement, manage, and improve a process for incident management for an organization in the context of the implementation of an ISMS. This standard provides additional information on security controls described in ISO/IEC 27001 and ISO/IEC 27002. It should be 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 document is the foundation of the ISO/IEC 27035 series. It presents basic concepts, principles and process with key activities of information security incident management, which provide a structured approach to preparing for, detecting, reporting, assessing, and responding to incidents, and applying lessons learned.

The guidance on the information security incident management process and its key activities given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance according to their type, size and nature of business in relation to the information security risk situation. This document is also applicable to external organizations providing information security incident management services.



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 incident management controls that can help organizations to comply with the requirements of Annex A of ISO/IEC 27001. 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

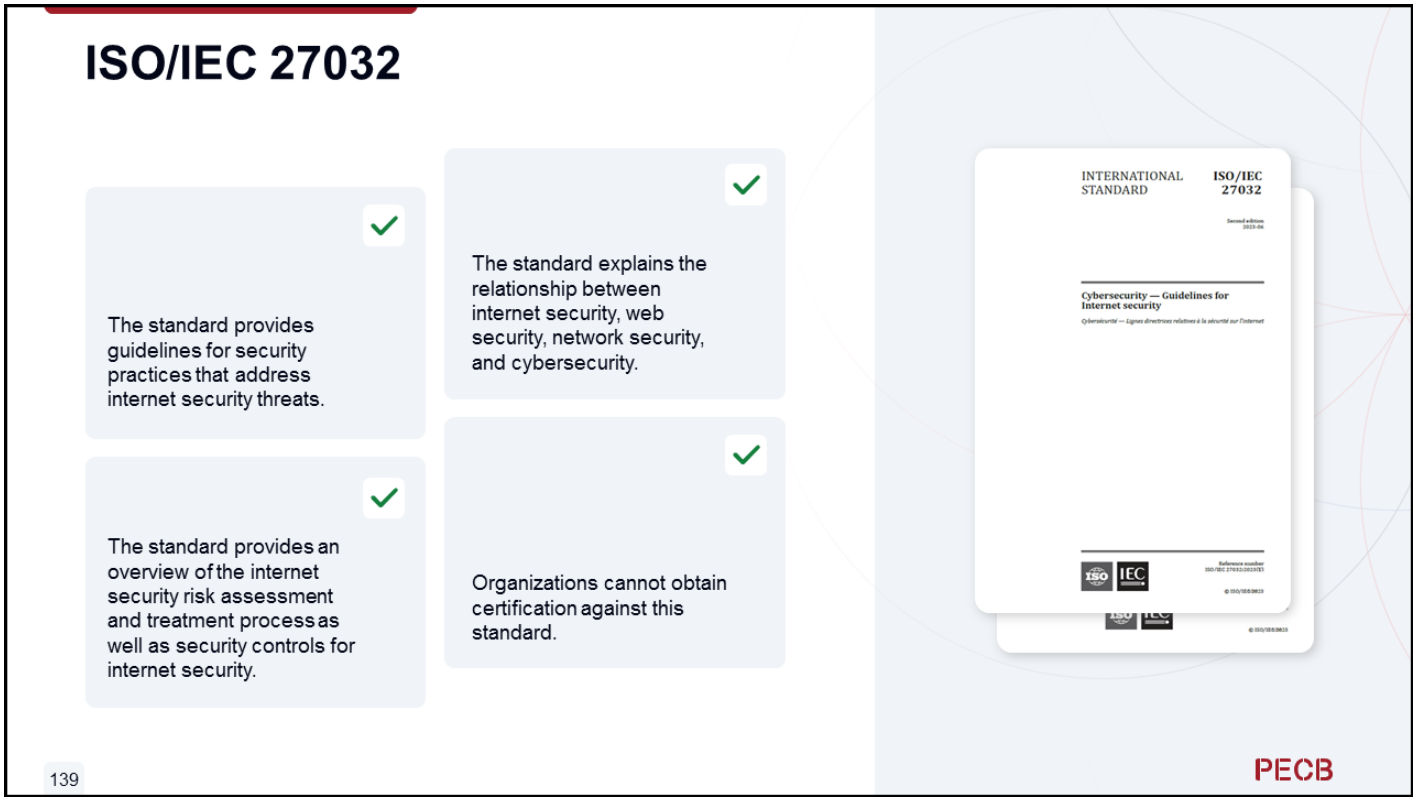
This document provides guidelines to plan and prepare for incident response and to learn lessons from incident response. The guidelines are based on the "plan and prepare" and "learn lessons" phases of the information security incident management phases model presented in ISO/IEC 27035-1:2023, 5.2 and 5.6.

The major points within the "plan and prepare" phase include:

information security incident management policy and commitment of top management;

- *information security policies, including those relating to risk management, updated at both organizational level and system, service and network levels;*
- *information security incident management plan;*
- *Incident Management Team (IMT) establishment;*
- *establishing 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.*
- *The "learn lessons" phase includes:*
- *identifying areas for improvement;*
- *identifying and making necessary improvements;*
- *Incident Response Team (IRT) evaluation.*

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



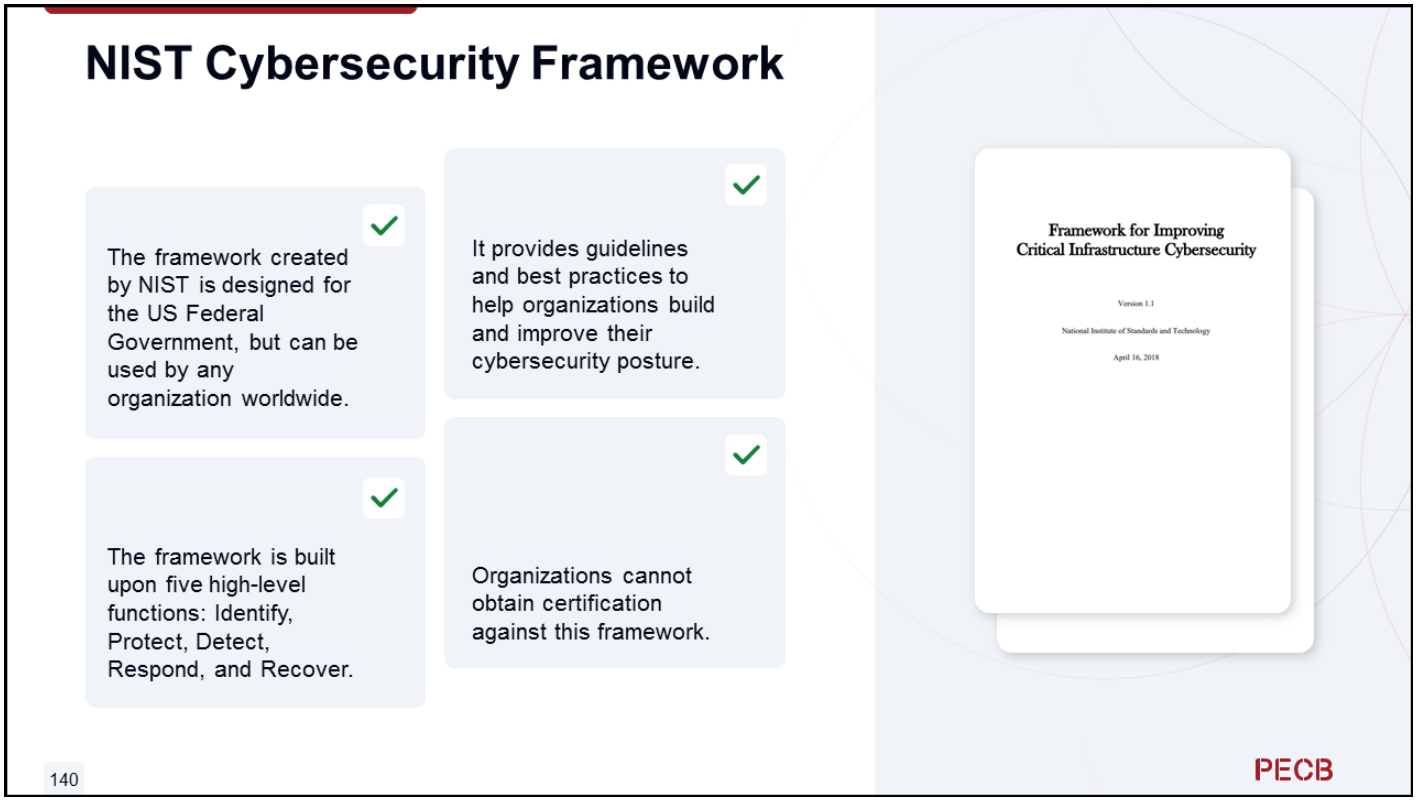
ISO/IEC 27032 helps organizations identify and assess internet security risks, enabling them to prioritize their efforts and allocate resources effectively to mitigate those risks.

ISO/IEC 27032, clause 1 Scope

This document provides:

- *an explanation of the relationship between Internet security, web security, network security and cybersecurity;*
- *an overview of Internet security;*
- *identification of interested parties and a description of their roles in Internet security;*
- *high-level guidance for addressing common Internet security issues.*

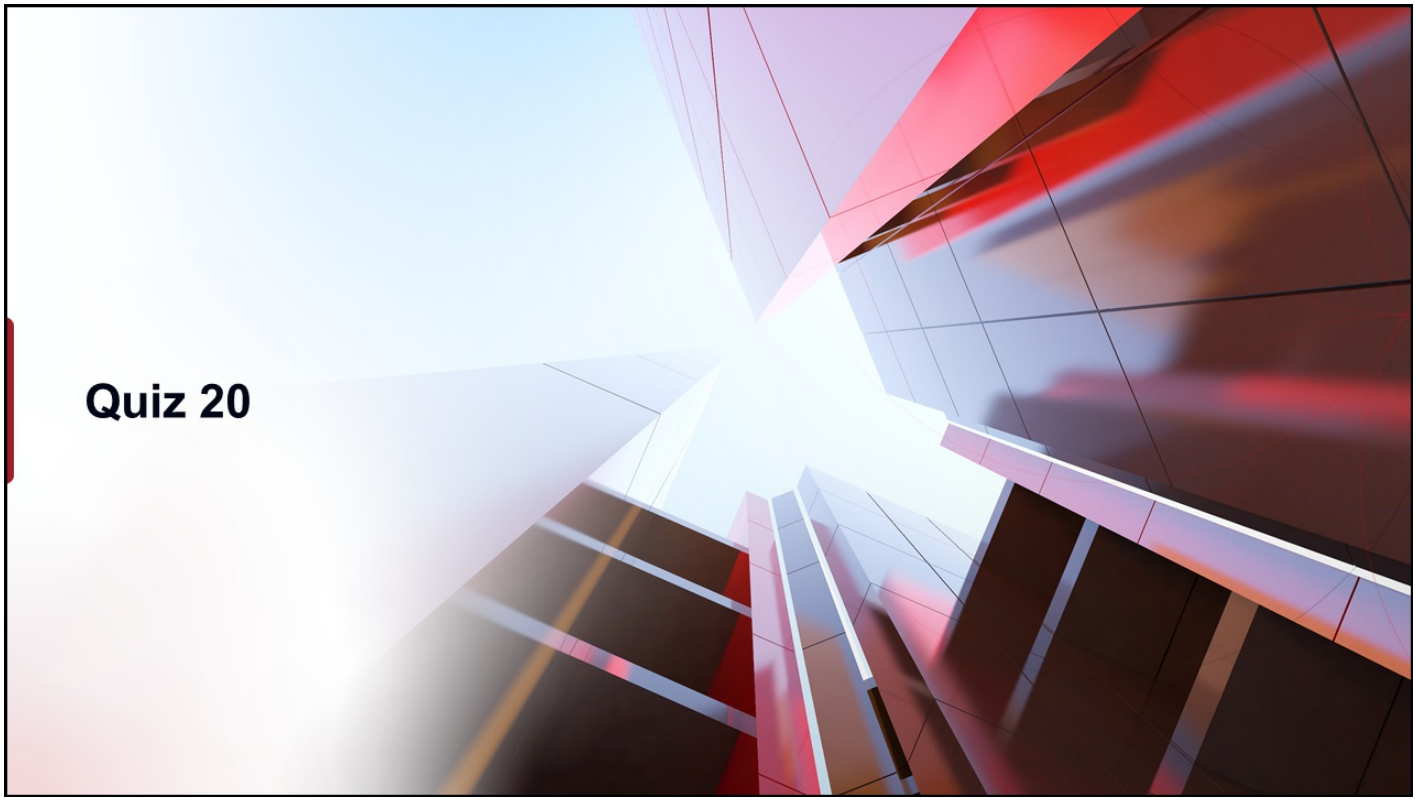
This document is intended for organizations that use the Internet.



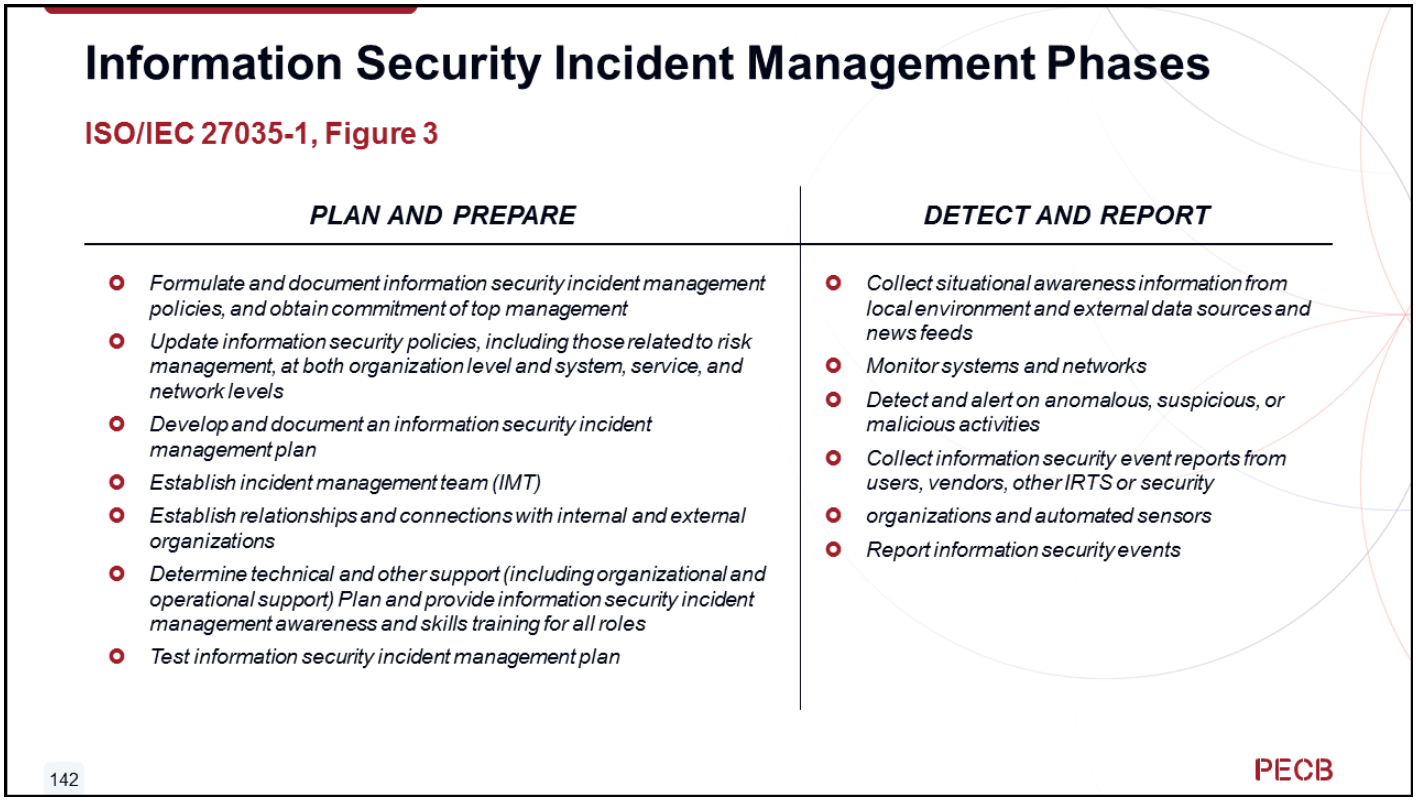
Since its establishment in 1901, NIST has served as a federal agency operating within the United States Department of Commerce. Its primary goal is to enhance economic security and improve the quality of life in the United States through the advancement of measurement science, standards, and technology, with a particular focus on cybersecurity.

The framework serves as a complement rather than a replacement for an organization's existing risk management process and cybersecurity program. By utilizing the framework alongside their current procedures, organizations can identify areas for improvement and effectively communicate their cybersecurity risk management while aligning with industry standards. Furthermore, organizations can use this framework as a reference for establishing and implementing their own cybersecurity program.

It is important to note that the framework is not limited to a specific industry, and the standardized taxonomy of standards, guidelines, and practices it provides is not exclusive to any particular country. Organizations worldwide can leverage the framework to enhance their cybersecurity efforts. Moreover, the framework plays a role in fostering the creation of an universally understood language for international cooperation on cybersecurity measures pertaining to critical infrastructure.[1][2]



Note: To complete Quiz 20, please go to the Quizzes Worksheet.



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 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.

Information Security Incident Management Phases (Cont'd)

ISO/IEC 27035-1, Figure 3

ASSESS AND DECIDE	RESPOND	LEARN LESSONS
• *Assess information security event, and determine if it constitutes an information security incident* • *Categorize, correlate and prioritize the incidents* • *Establish the necessary IRTs*	• *Investigate and determine whether information security incidents are under control Contain and eradicate information security incidents* • *Invoke BCP/DRP measures for those incidents that exceed organizationally-determined limits for IRTs* • *Recover from information security incidents* • *Resolve and close the information security incidents*	• *Identify, document and communicate the lessons learnt* • *Identify and make improvements to information security* • *Identify and make improvements to information security risk assessment and management review results* • *Identify and make improvements to information security incident management policy and plan* • *Evaluate the performance and effectiveness of the IRTs*

143

PECB

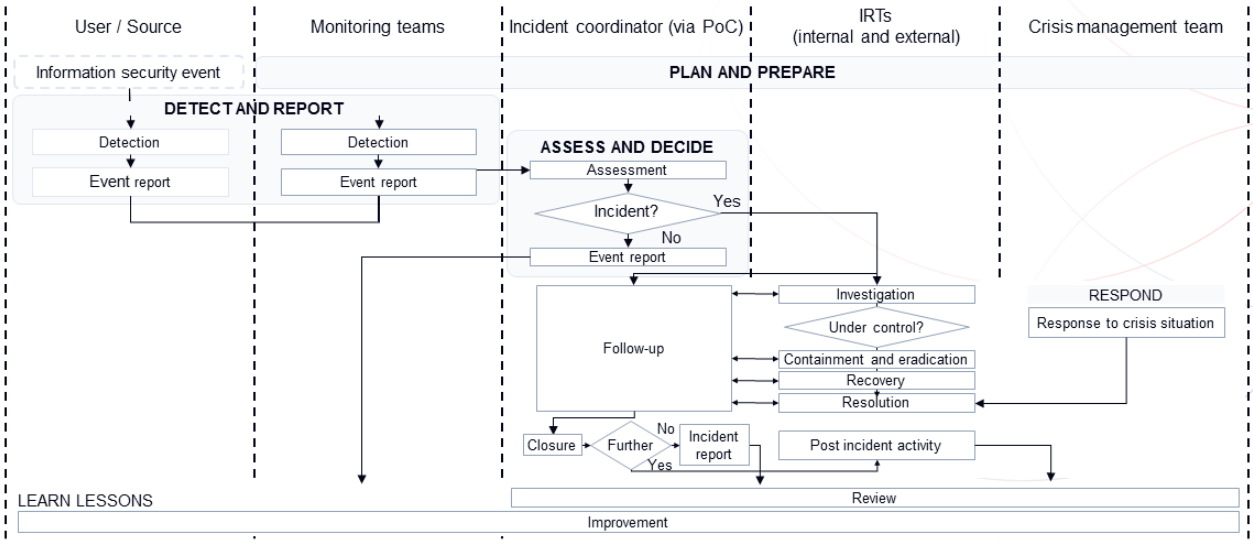
Business continuity planning (BCP) and disaster recovery planning (DRP) refer to strategies and procedures designed to help an organization recover from disasters and continue operating or quickly resume its critical functions.

ISO/IEC 27035-2, clause 4.3 highlights the importance of a clear and effective information security incident management policy. 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:** Information security awareness is critical to the overall security posture of organizations. 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 are aware that understanding the relevant laws and regulations is critical for 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

ISO/IEC 27035-1, Figure 4



PECB

1.Plan and prepare

During this phase, organizations should create a foundation for incident management, involving monitoring teams, incident coordinator, internal and external incident response teams (IRTs), and crisis management team. Additionally, organizations should create the information security incident management policy and ensure top management's commitment. Organizations should also develop an incident management plan, and establish the Incident Management Team (IMT). To ensure comprehensive support and coordination the organization should establish the relations with internal and external entities. Lastly, organizations should plan and deliver trainings to enhance incident management awareness and skills of employees and test their incident management plan to ensure its effectiveness.

2.Detect and report

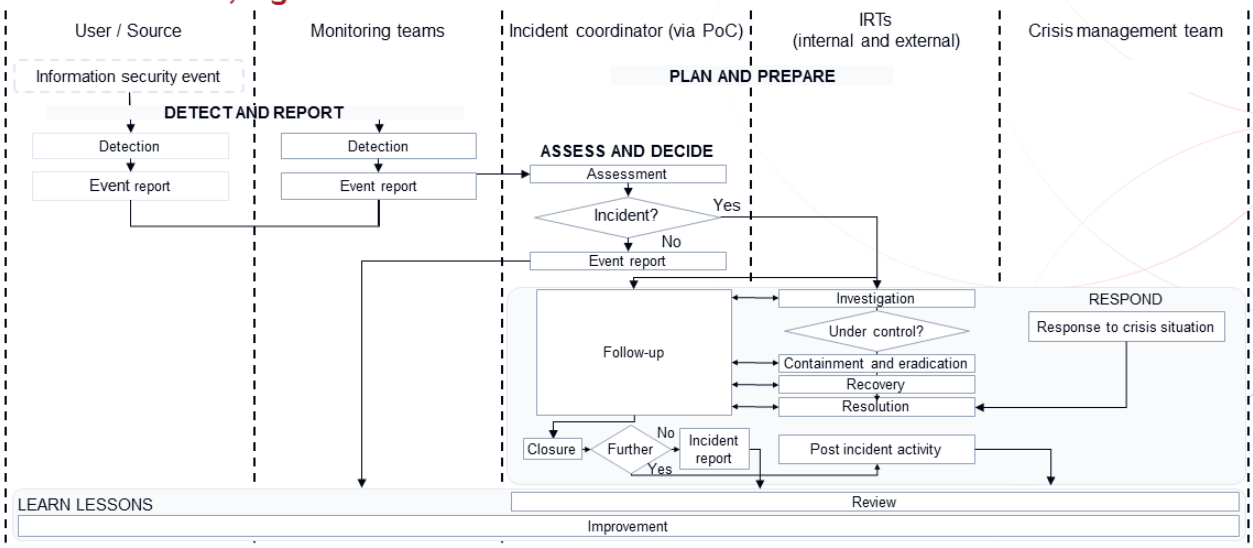
This phase involves gathering information for potential information security issues and reporting on the occurrences of information security events and vulnerabilities. Organizations should monitor systems and networks for anomalies, and set up alerts for suspicious or malicious activities. Detect and report phase includes the collection of security event reports from various sources like users, monitoring teams, vendors, other incident response teams, or security organizations. Such events should be reported to the incident coordinator for further action. Therefore, all interested parties should be aware of and have access to procedures for reporting information security events.

3.Assess and decide

In this phase, the reported information security events should be evaluated by the incident coordinator based on the report and the criteria defined in the plan and prepare phase to determine if they should be categorized as incidents. This phase involves categorizing, correlating, and prioritizing incidents based on their nature and impact. If it is determined that the event is not an incident, it is stored in the incident register maintained by the IMT and analyzed in the lessons learn phase, if needed. If the event is categorized as an information security incident, it should be reported to internal or external IRTs for further investigation.

2.6.5 Define the Processes and Draft the Procedures (Cont'd)

ISO/IEC 27035-1, Figure 4



146

PECB

4.Respond

In this phase, the IRT should investigate the incident to determine if it is under control. If the incident is under control, the IRT should initiate the necessary containment and eradication measures. After the incident is neutralized, recovery actions should be taken to restore operations and resolve the incident. If the incident is not under control, it should be reported to the crisis management team that perform the response to crisis situations. This may include activating the business continuity plan (BCP) or disaster recovery plan (DRP) for severe incidents. During the respond phase, the incident coordinator should follow up with the involved teams to make sure that the incident is closed and documented in the incident report.

5.Learn lessons

After an incident is handled, it is critical to reflect and learn from it. Lessons learned should be documented and communicated. Based on these, improvements to the information security framework, risk assessment and management processes, and the incident management policies and plans should be identified and implemented. This step also helps organizations evaluate the performance and effectiveness of the IRTs and continually improve incident response capabilities.

2.6.6 Establish an Incident Management Team

ISO/IEC 27035-2, clause 7.1 and 7.2.1

The aim of establishing an incident management organizational structure 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.

Incident management organizational structure can be structured differently depending on the organization size, its staff members and industry type.

An incident management team (IMT) is the group responsible for managing the end to end incident management capability for the organization. The main activities of IMT may include, but are not limited to, the following:

- *Managing integrated security systems: monitoring information security event management agents installed on heterogeneous systems (e.g. intrusion detection system, intrusion prevention system, firewall, network resource, etc.).*
- *Implementing a consistent policy: minimizing risks to the information system by applying a consistent set of response tasks according to the defined policy.*
- *Responding promptly: defining the most appropriate detection and response mechanisms to react quickly to threats, breaches, and attacks to minimize damage and reduce cost of recovery.*

147

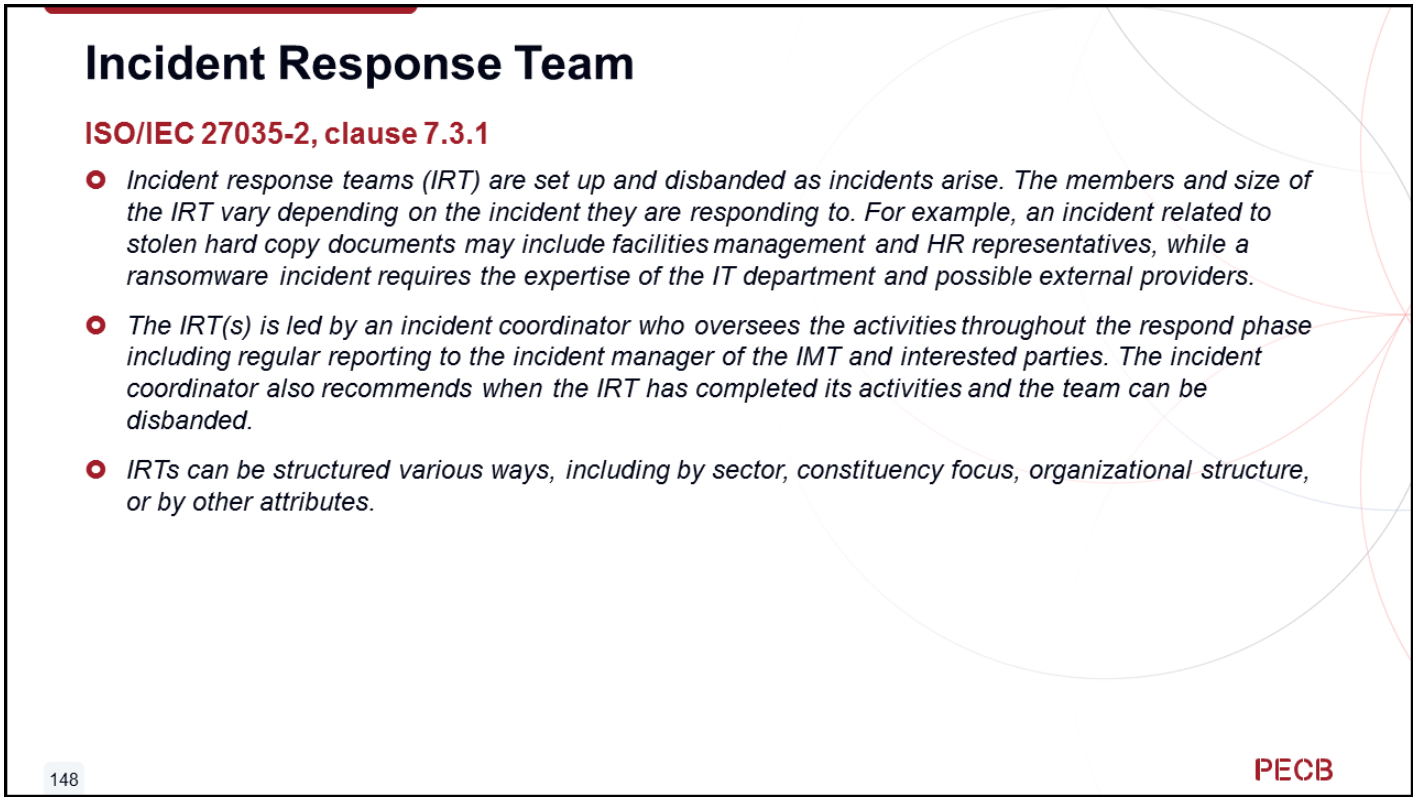
PECB

ISO/IEC 27035-2, clause 7.2.1 IMT structure (cont'd)

Duties of an IMT may also include monitoring and management activities as follows.

- *Integrated management and monitoring: 24 h x 365 d monitoring of targets, proactive monitoring and responses against incidents, log management.*
- *Reports management: periodic security reporting, security patch management, incident reporting.*
- *Administrative management: policy management for various system environments including task control and IRT operations.*
- *Technical management: network, system, application, contents, and service security management.*
- *System operation and management: system capacity, performance, security configuration, and environment configuration management.*

NOTE: Some of the above duties can be shared with or performed by other organizational units outside of the IMT.



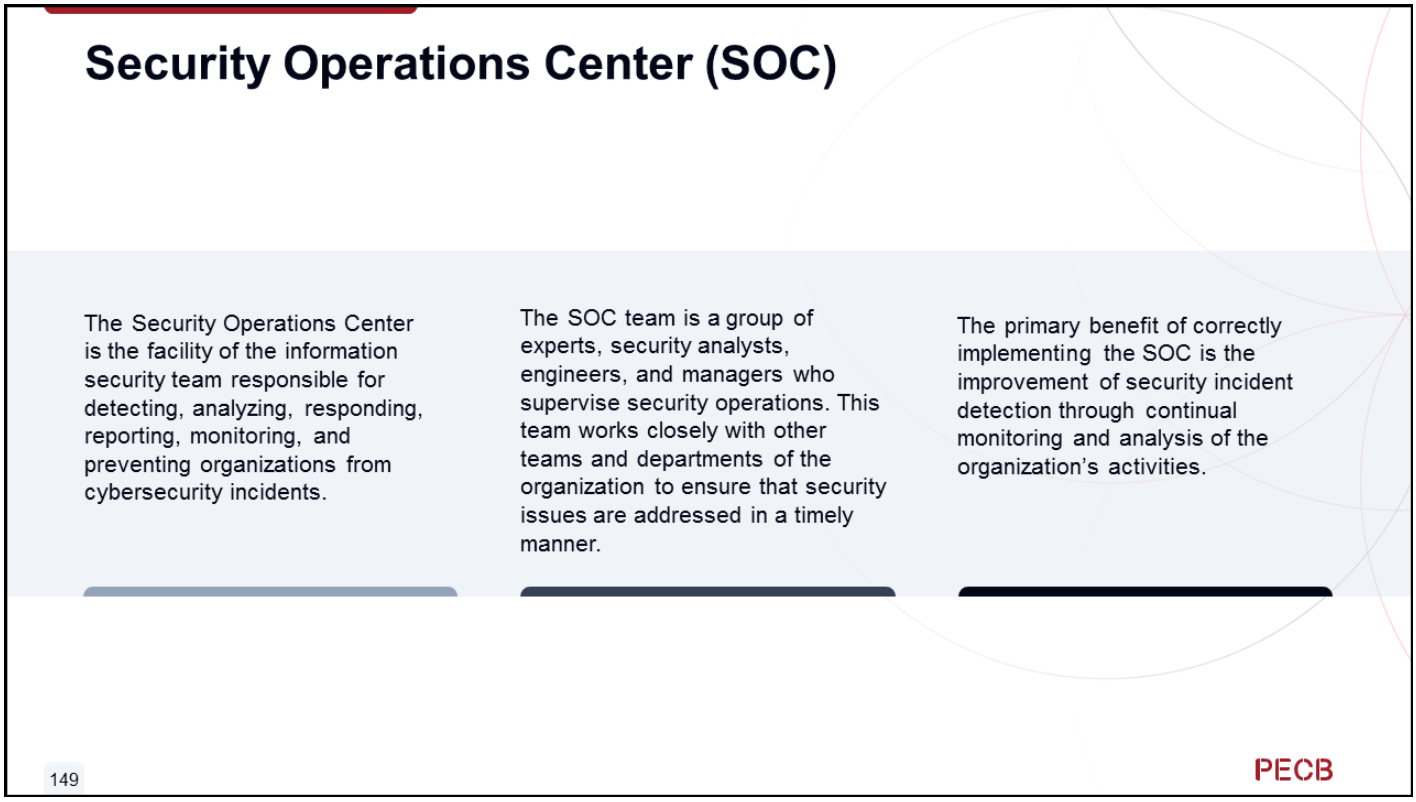
There are differences between “security team,” “CSIRT,” and “coordinating CSIRT”:

- The security team consists of individuals, such as system, network, and security administrators, who perform internal and external defense functions and ad hoc incident handling.
- The CSIRT may include the entire security team or a separate entity from the security team.
- 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.

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. 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.[3]

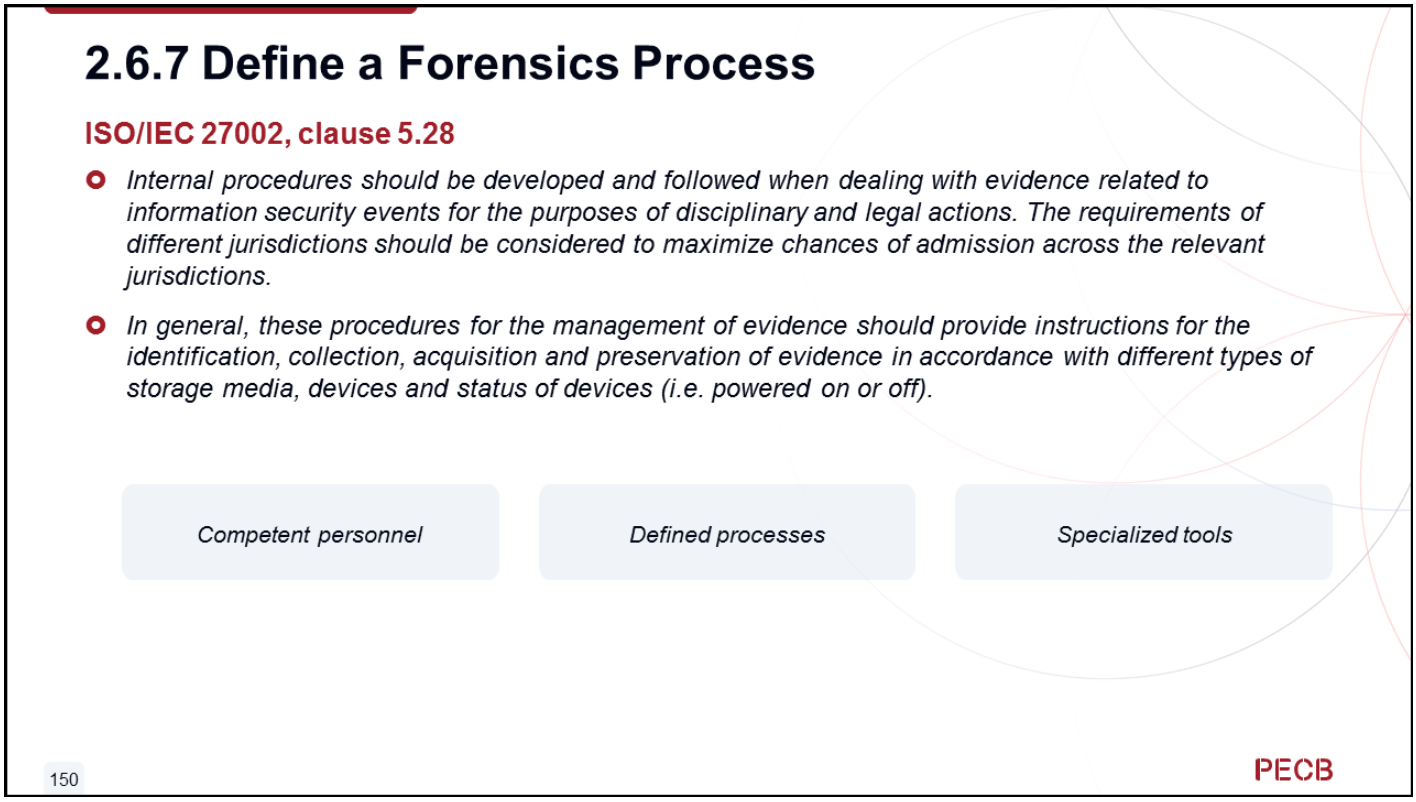
The incident response team (IRT) has the option to provide a range of services, which should be tailored in accordance with the team’s mission, purpose, and composition. Such services can be classified into:

1. **Reactive services:** These services are activated in response to specific events or requests, including reports of compromised hosts, the dissemination of malicious code, software vulnerabilities, or incidents detected through intrusion detection or logging systems. Reactive services constitute the fundamental and central aspect of the IRT's operations.
2. **Proactive services:** These services assist in preparing and securing systems to prevent future incidents. They reduce the likelihood of potential attacks and issues.
3. **Security quality management services:** These services complement established functions within an organization, which are not directly related to incident handling, and are typically carried out by departments like IT, audit, or training. When the IRT engages in or supports these services, their unique perspective and expertise offer valuable insights to enhance the overall security of the organization. This helps identify risks, threats, and system vulnerabilities.



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.



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.

According to NIST SP 800-86, there are four main steps in a forensic process:

1. Collection that includes the identification, recording, and acquisition of information
2. Examination that involves the processing of the collected information using automated and manual methods
3. Analysis that includes the analysis of the outcomes of the examination
4. Reporting that includes the reporting of the results of analysis and defining the actions to be performed

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.5.28 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

151

PECB

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

Reevaluated:

To identify corrective and preventive actions

152

PECB

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.

Slide Notes Extension

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.

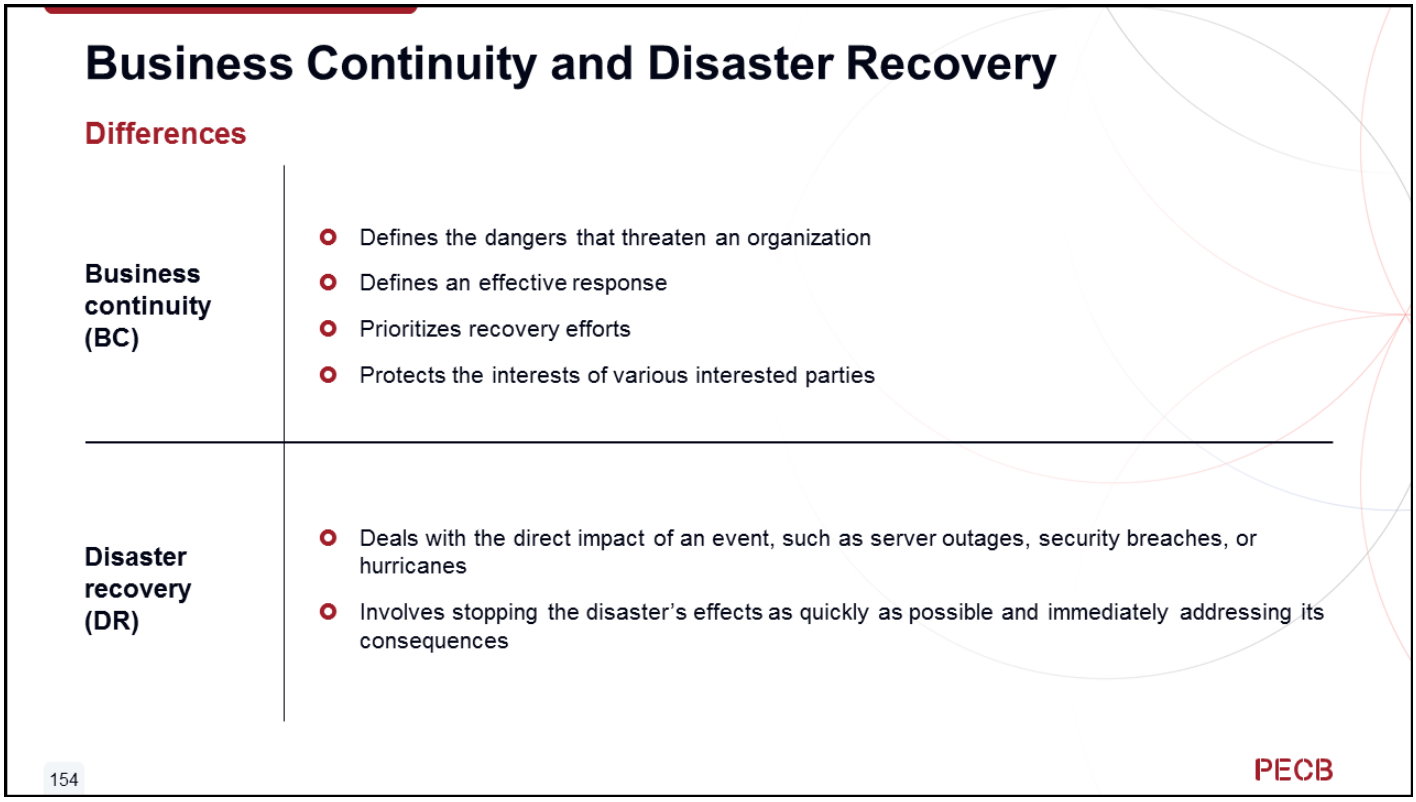
Identification of scheme improvements

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.



The three following questions, with a primary focus on continuing business operations, are related to business continuity and disaster recovery:

- 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 any server used by the organization daily gets damaged or fails, another server will automatically replace the damaged server; therefore, the organization's operations will continue without disruption. This resilience of the IT data is provided by a disaster recovery device. Although disaster recovery can exist on its own, it is an essential component of the business continuity management, given that it offers the required resources that facilitate the operations of a business.

Another example of ensuring failover resilience is an organization that implements a hybrid cloud infrastructure, which allows it to seamlessly move workloads between on-premises data centers and public cloud providers. This not only provides additional failover options but also enables the organization to take advantage of the scalability and flexibility of cloud computing while maintaining control over sensitive data.

Section 20 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 establish an incident management policy and an incident response team.
- The incident response team (IRT) is responsible to provide the coordination, management, feedback, and communication in regards to information security incidents.
- Documented information related to security incidents may include the unique 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 reevaluated on a regular basis to identify corrective and preventive actions.

Questions?

Quiz 21

Note: To complete Quiz 21, please go to the Quizzes Worksheet.

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

Day 3 Summary

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

- The definition of the documented information management process
- The implementation of a documented information management system
- The design and implementation of security controls
- Introduction of Annex A controls
- Trends and technologies including big data, artificial intelligence, machine learning, cloud computing, and outsourced operations
- Principles of an efficient communication strategy
- Planning of communication activities
- Competence, training, and awareness
- Designing and planning of training programs
- Management of security operations
- Resource management necessary to maintain the ISMS
- Information security incident management process and policy

Note: To complete Homework 8-10, please go to the Exercises Worksheet.