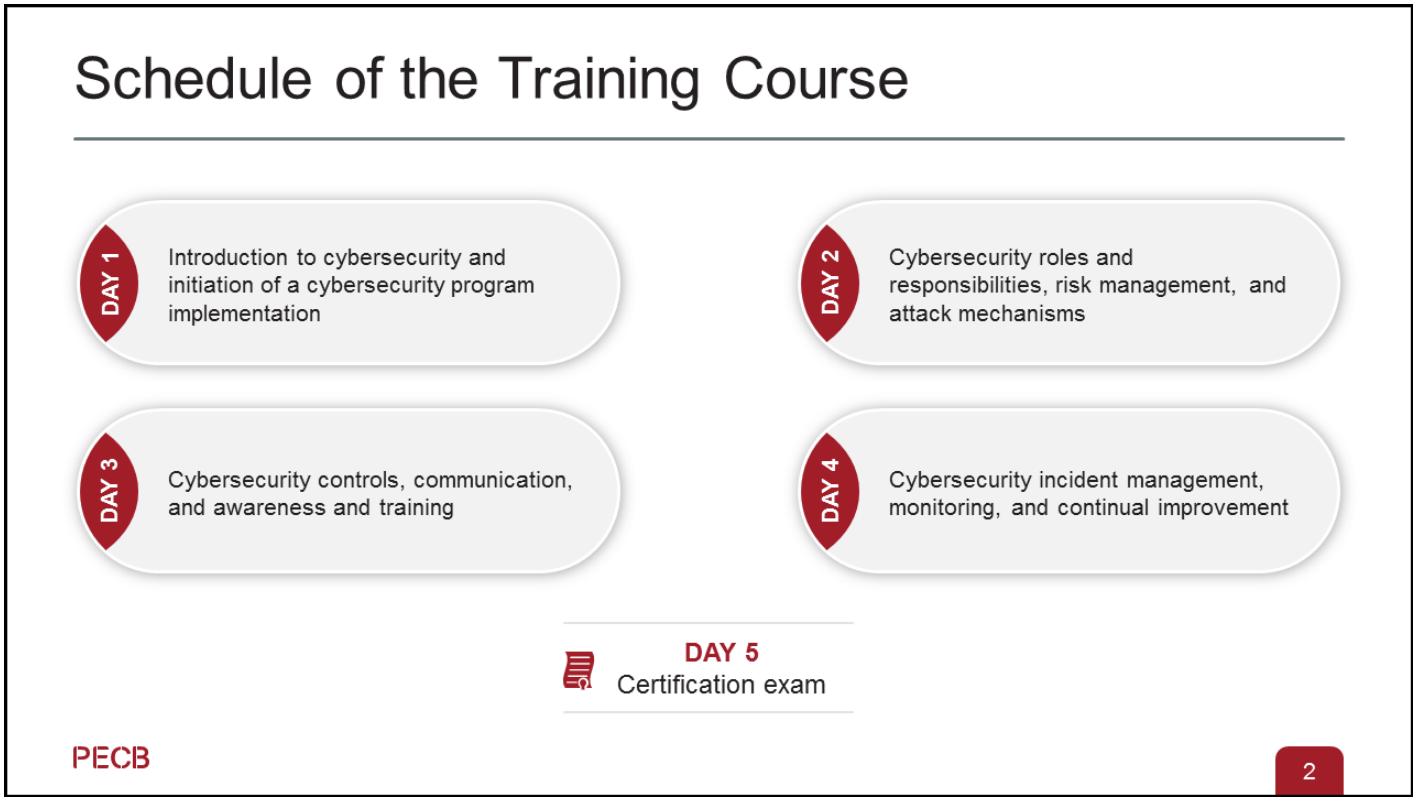
Version 4.0

Document number: LCMD1V4.0



Day 1: Introduction to cybersecurity and initiation of a cybersecurity program implementation

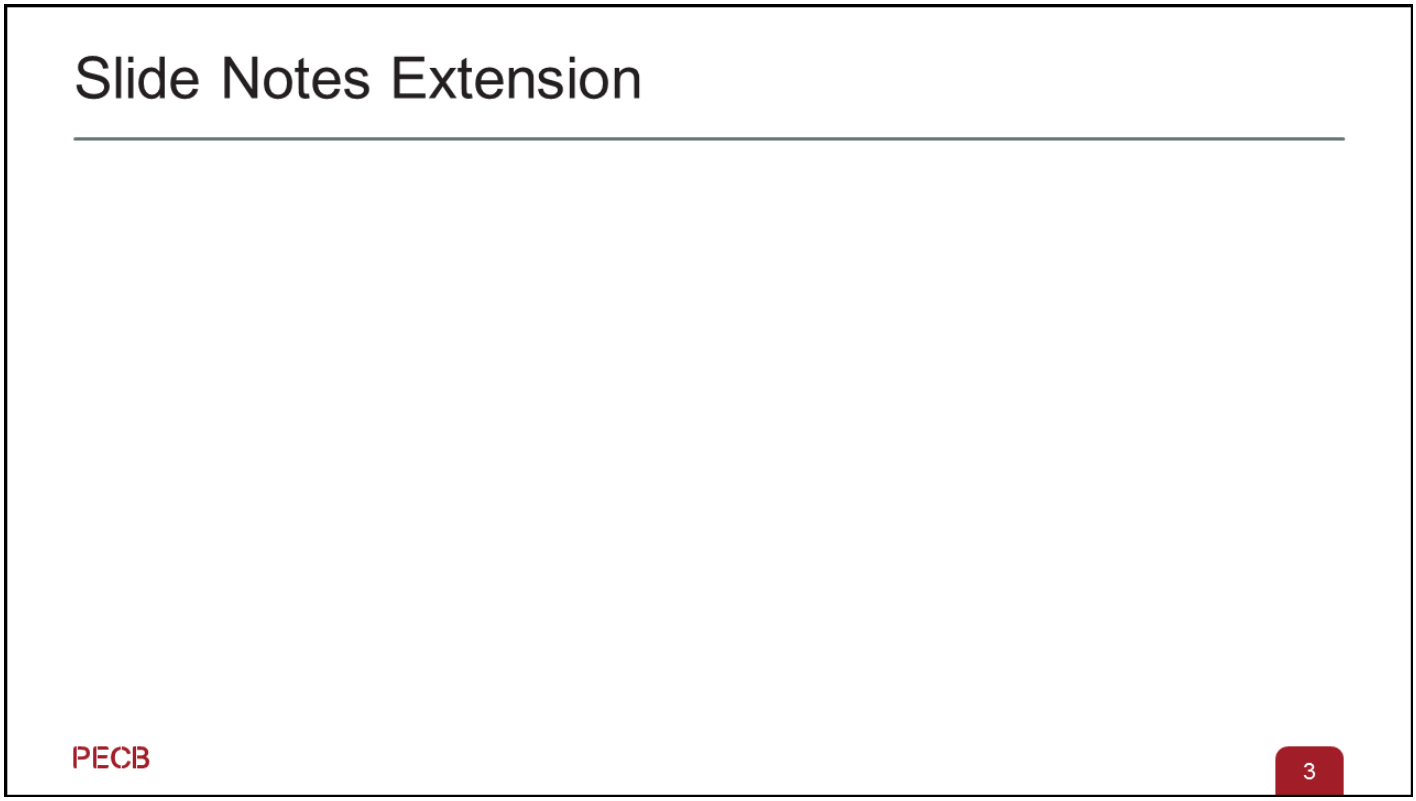
- Section 1: Training course objectives and structure
- Section 2: Standards and regulatory frameworks
- Section 3: Fundamental concepts of cybersecurity
- Section 4: Cybersecurity program
- Section 5: The organization and its context
- Section 6: Cybersecurity governance

Day 2: Cybersecurity roles and responsibilities, risk management, and attack mechanisms

- Section 7: Cybersecurity roles and responsibilities
- Section 8: Asset management
- Section 9: Risk management
- Section 10: Attack mechanisms

Day 3: Cybersecurity controls, communication, and awareness and training

- Section 11: Cybersecurity controls
- Section 12: Cybersecurity communication
- Section 13: Awareness and training

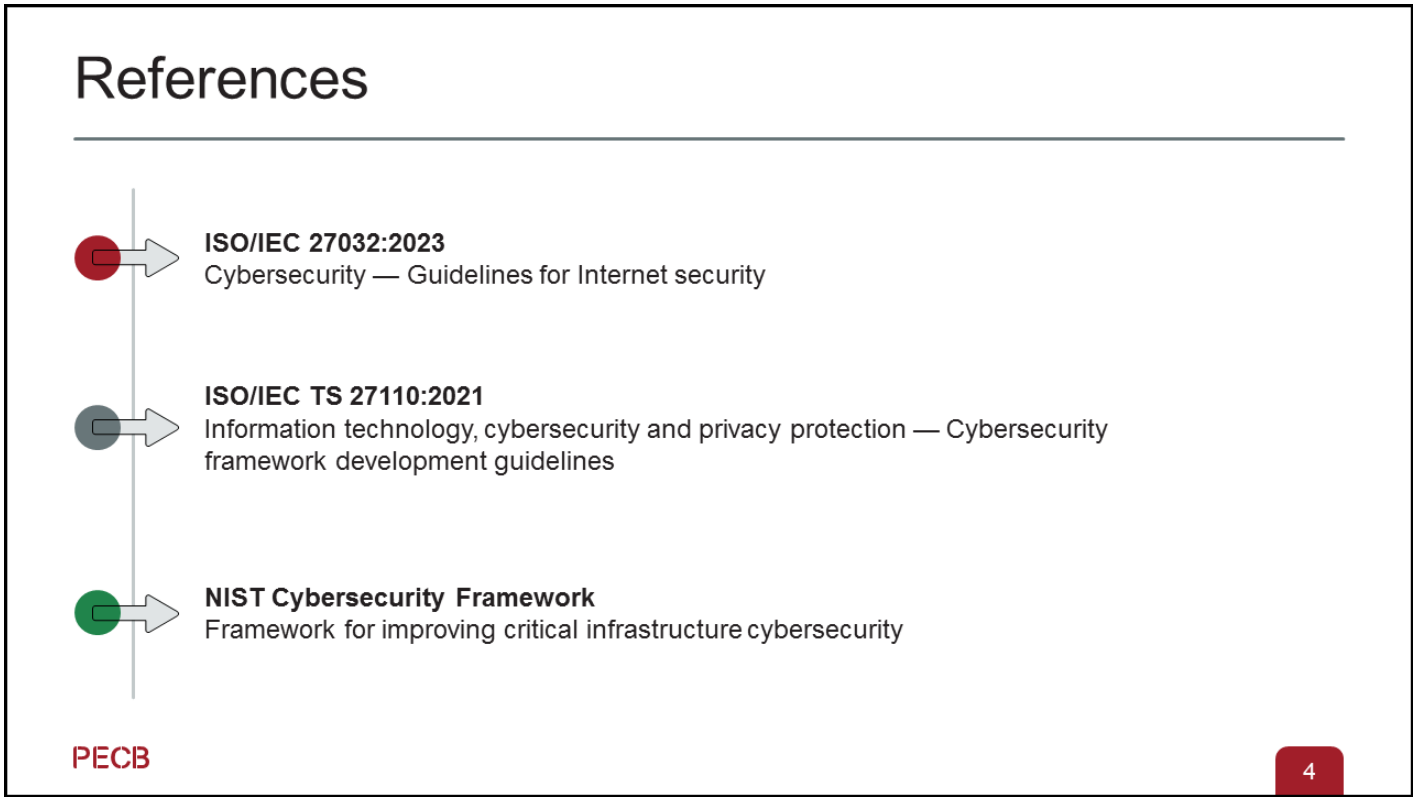


Day 4: Cybersecurity incident management, monitoring, and continual improvement

- Section 14: ICT readiness in business continuity
- Section 15: Cybersecurity incident management
- Section 16: Testing in cybersecurity
- Section 17: Measuring and reporting cybersecurity performance and metrics
- Section 18: Continual improvement
- Section 19: Closing of the training course

Day 5: Certification exam

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



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

List of Acronyms

- **ISO:** International Organization for Standardization
- **LCM:** Lead Cybersecurity Manager
- **PECB:** Professional Evaluation and Certification Board
- **NIST:** National Institute of Standards and Technology

PECB

5

Note: To see the complete list of acronyms used throughout this training course, please go to the Index file.

This section presents the objectives of the training course and its structure, including the examination and certification process, the benefits of being a certified manager, and more information about PECB.

To break the ice, trainer(s) and participants introduce themselves by stating their:

- Name
- Current position
- Knowledge and experience regarding cybersecurity management
- Knowledge and experience regarding cybersecurity standards and guidelines (ISO/IEC 27032, ISO/IEC TS 27110, NIST Cybersecurity Framework, etc.)
- Knowledge and experience regarding management systems and other related standards (ISO/IEC 27001, ISO/IEC 27002, etc.)
- Training course expectations

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

Customer Service

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

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

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

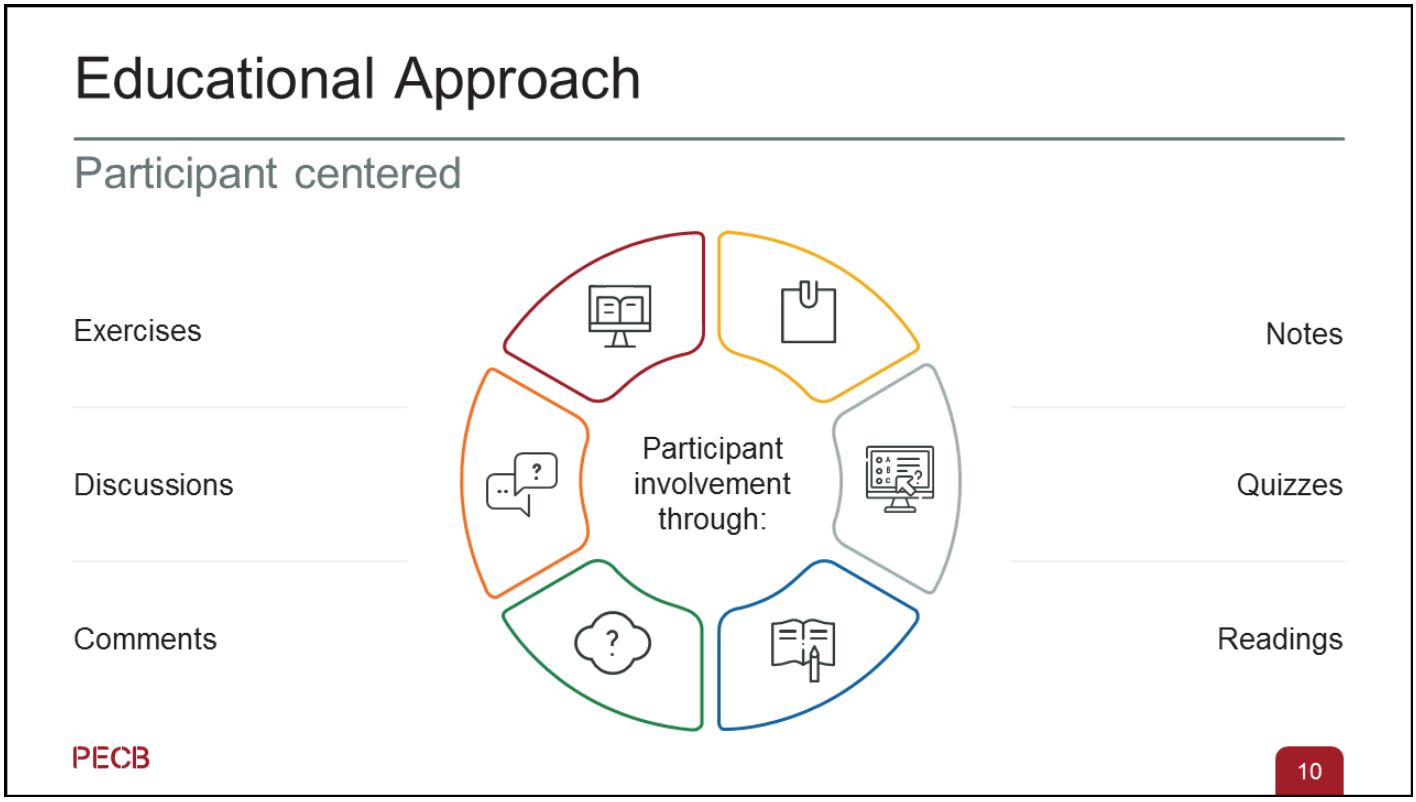
In case of dissatisfaction with the training (trainer, training room, equipment, etc.), the examination, or the certification processes, please open a ticket under **Make a complaint** category on the PECB Help Center (https://pecb.com/help).

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

This training course is intended to help participants develop their competences to participate in the implementation of a cybersecurity program. From an educational perspective, competence consists of the following three elements:

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

This training course provides a comprehensive methodology for the implementation of a cybersecurity program, not merely a list of cybersecurity practices and guidelines. Therefore, general knowledge of the cybersecurity concepts is required for the successful completion of the training course.



To successfully complete this training course, two factors are crucial:

- Trainer instructions
- Participant involvement

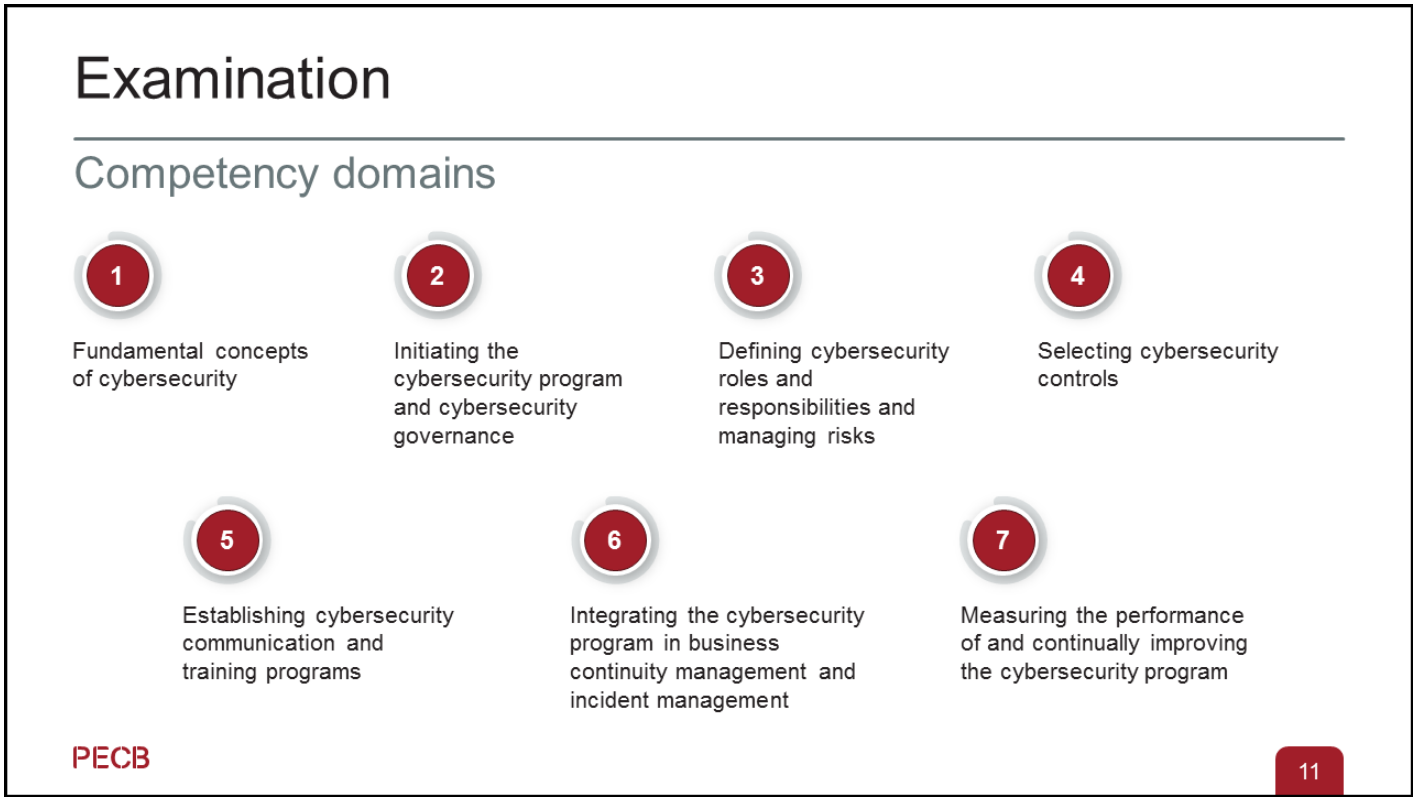
Interaction by means of questions and suggestions is highly encouraged. Participants can best contribute to the training course by partaking in exercises, quizzes, and discussions. Participants are also advised to take personal notes.

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

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

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

- Articles
- Whitepapers
- InfoKits
- Magazine
- Webinars

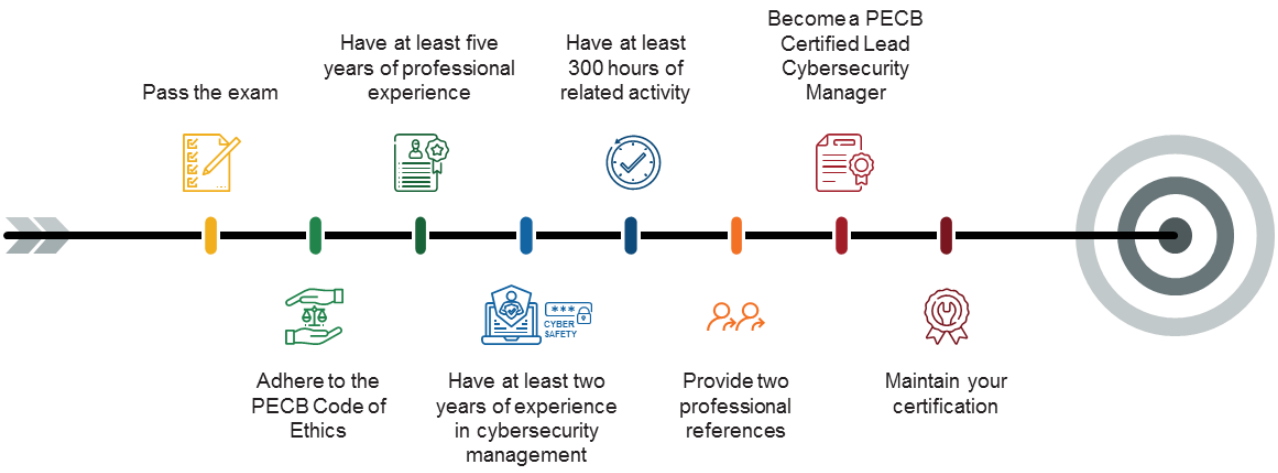


The purpose of the certification exam is to evaluate whether candidates have mastered the cybersecurity management concepts, methods, and techniques so that they are able to participate in cybersecurity management project assignments.

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

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

Prerequisites for Certification



PECB

12

Individuals who do not meet all the prerequisites for certification cannot claim to be PECB Certified Lead Cybersecurity Manager-certified.

A less experienced candidate can apply for and obtain the “PECB Certified Lead Cybersecurity Manager” credential or “PECB Certified Cybersecurity Provisional Manager” credential.

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

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

PECB Certificate

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

PECB

13

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

PECB Digital Badges

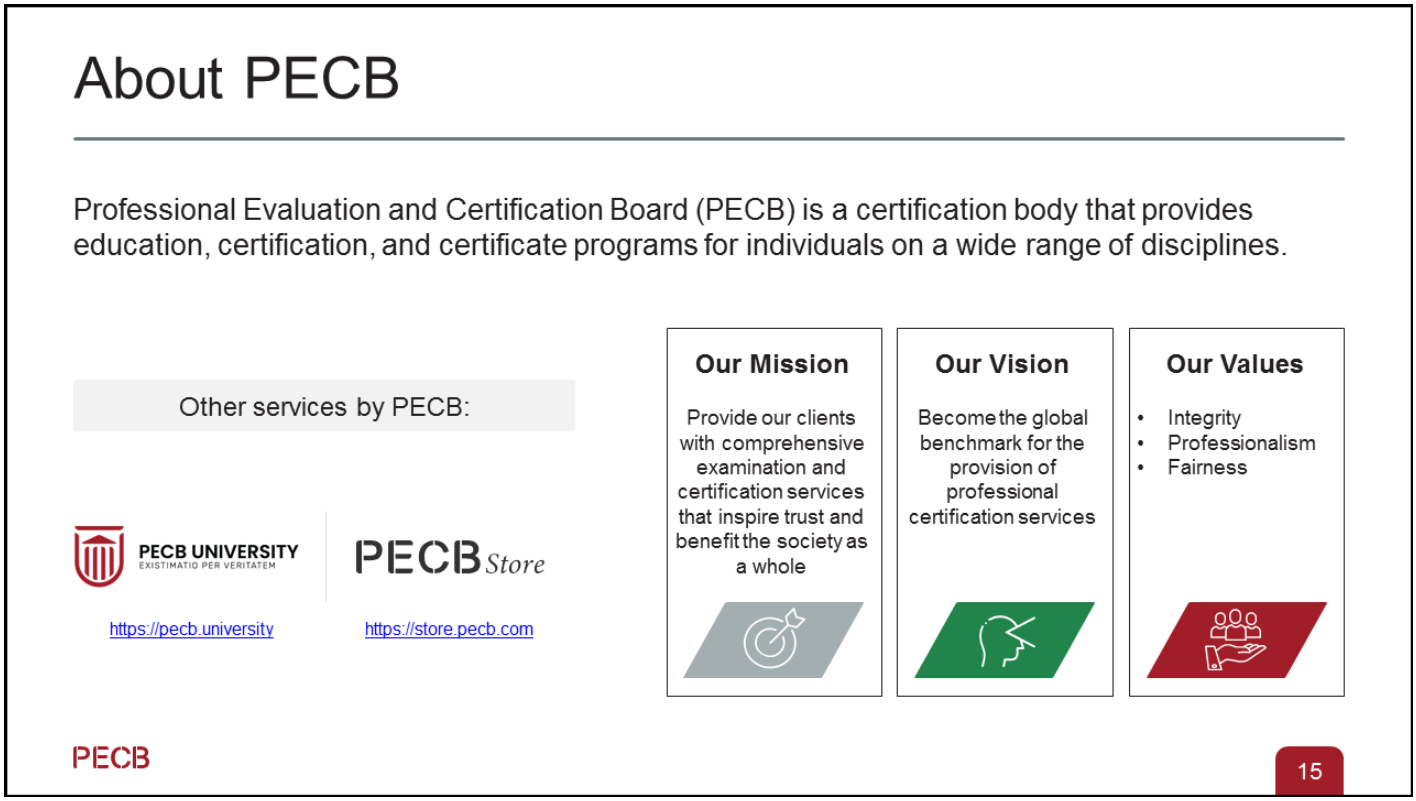
- In addition to the certificate, candidates can now also claim their digital badge on Credly, through their PECB account.
- Digital badges contain shareable information about who has issued the badge, who has earned it, what the criteria for earning the badge were, issue and expiration date, and achievement evidence.
- Digital badges are a powerful online representation that allows candidates to demonstrate professional knowledge and skills obtained.
- Candidates can easily and safely share their digital badges on social media platforms or add it to their resume and business cards.
- It is important to note that candidates can claim digital badges for their existing PECB certificates as well. All they need to do is to head to their PECB accounts. To learn more about this, please visit PECB Digital Badges.

PECB

14

Digital badges have many benefits. Some of them include:

- They demonstrate a candidate's competence and commitment to the profession.
- They demonstrate a candidate's willingness to learn and develop in a profession.
- They demonstrate that a candidate is up to date with the latest industry developments.
- They increase candidates' opportunities in a profession.



PECB helps professionals show commitment and competence by providing them with valuable education, evaluation, and certification against internationally recognized standards.

Our principal objectives and activities are:

1. Establishing the minimum requirements necessary to certify professionals
2. Reviewing and verifying the qualifications of applicants for eligibility to be considered for the certification evaluation
3. Developing and maintaining reliable, valid, and current certification evaluations
4. Granting certificates to qualified candidates, maintaining records, and publishing a directory of the holders of valid certificates
5. Establishing requirements for the periodic renewal of certification and determining compliance with those requirements
6. Ascertaining that our clients meet ethical standards in their professional practice
7. Representing its members, where appropriate, in matters of common interest

This section introduces the International Organization for Standardization (ISO) and main ISO standards for cybersecurity. It also introduces other cybersecurity frameworks and guidelines, such as the NIST Cybersecurity Framework and NIST SP 800 publications.

ISO applies the following principles when developing international standards:

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

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

2.ISO standards are based on global expert opinion.

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

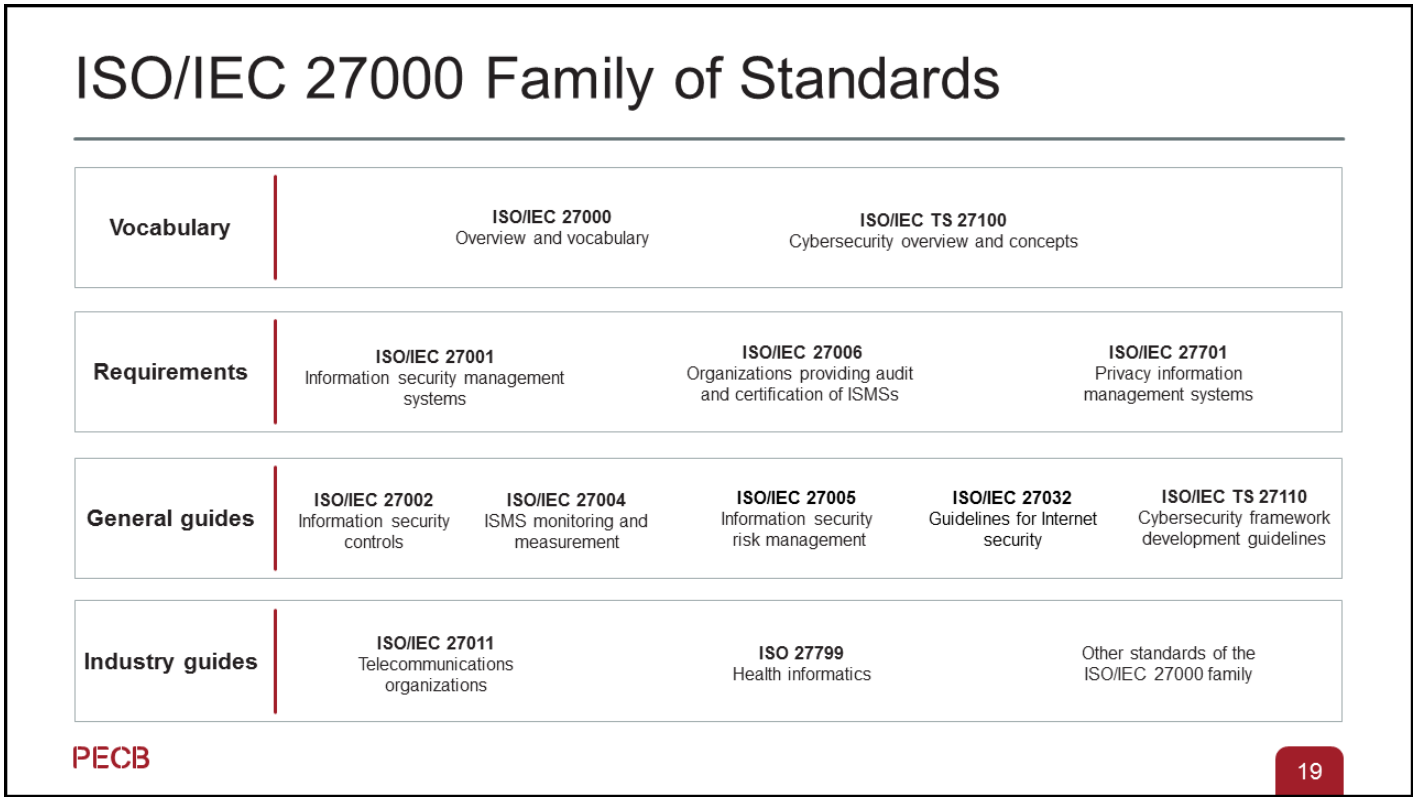
3.ISO standards are developed through a multi-stakeholder process.

The technical committees consist of experts from relevant industries, but also from consumer associations, academia, NGOs, and governments.

4.ISO standards are based on consensus.

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

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



The ISO 27000 family includes the following standards:

- **ISO/IEC 27000** gives a general overview of information security management systems (ISMS). In addition, it provides common terms and definitions used in the ISMS family of standards. A free copy of this standard can be downloaded on the ISO website.
- **ISO/IEC 27001** specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS.
- **ISO/IEC 27002** provides a reference set of generic information security controls including implementation guidance.
- **ISO/IEC 27004** provides guidance on evaluating the information security performance and the effectiveness of an ISMS.
- **ISO/IEC 27005** provides guidelines for managing information security risks, in accordance with the requirements of ISO/IEC 27001.
- **ISO/IEC 27006** specifies requirements for organizations auditing and certifying ISMSs.
- **ISO/IEC 27007** provides guidelines for managing an ISMS audit program.
- **ISO/IEC TS 27008** provides guidance on reviewing and assessing the implementation and operation of information security controls.
- **ISO/IEC 27011** provides guidelines supporting the implementation of information security controls in telecommunications organizations.
- **ISO/IEC 27032** provides guidelines for addressing threats associated with Internet security.
- **ISO/IEC TS 27100** provides an overview of cybersecurity and describes relevant cybersecurity concepts.
- **ISO/IEC TS 27110** provides guidelines for developing a cybersecurity framework.
- **ISO/IEC 27701** specifies requirements and provides guidance for establishing, maintaining, and continually improving a privacy information management system (PIMS) as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management.
- **ISO 27799** provides guidelines for organizations in the health informatics industry in implementing the controls provided in ISO/IEC 27002.

Source: https://www.iso.org

ISO/IEC 27001

- This standard specifies requirements for establishing, implementing, maintaining, and improving an ISMS.
- Requirements (clauses) are expressed with the verb “shall.”
- It is applicable to all organizations, regardless of their size, type, or industry in which they operate.
- Annex A contains 93 information security controls categorized into four groups.
- Organizations can obtain certification against this standard.

PECB

20

ISO/IEC 27001, clause 0.1 General

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

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

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

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

ISO/IEC 27002

- This standard provides a set of information security controls and guidelines for their implementation.
- Clauses are expressed with the verbal form “should.”
- Organizations cannot obtain certification against this standard.

PECB

21

ISO/IEC 27002, clause 1 Scope

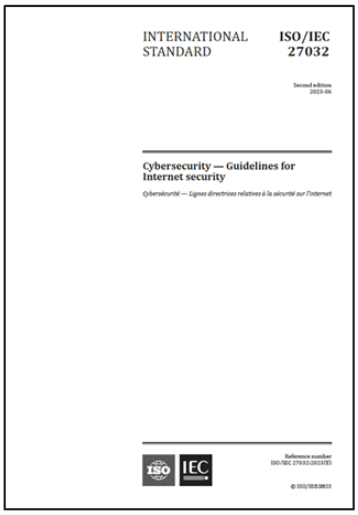
This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

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

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

ISO/IEC 27032

- The standard provides guidelines for security practices that address internet security threats.
- The standard explains the relationship between internet security, web security, network security, and cybersecurity.
- The standard provides an overview of the internet security risk assessment and treatment process as well as security controls for internet security.
- Organizations cannot obtain certification against this standard.



PECB

22

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.

ISO/IEC TS 27100

- This standard outlines the fundamental concepts of cybersecurity and highlighting its relationship with information security.
- It establishes the context and significance of cybersecurity, emphasizing its relevance in various organizational settings.
- This document applies to organizations of all types and sizes, including commercial enterprises, government agencies, and not-for-profit organizations.
- Organizations cannot obtain certification against this standard.

PECB

23

ISO/IEC TS 27100, clause 1 Scope

This document provides an overview of cybersecurity.

This document:

- *describes cybersecurity and relevant concepts, including how it is related to and different from information security;*
- *establishes the context of cybersecurity;*
- *does not cover all terms and definitions applicable to cybersecurity; and*
- *does not limit other standards in defining new cybersecurity-related terms for use.*

ISO/IEC TS 27110

- This standard provides guidance on how to develop a cybersecurity framework.
- These guidelines are relevant to individuals or organizations involved in creating a cybersecurity framework.
- Guidelines (clauses) are expressed with the verb “should.”
- The scope of this document encompasses cybersecurity framework creators in organizations of different types, sizes, and industries.
- Organizations cannot obtain certification against this standard.

PECB

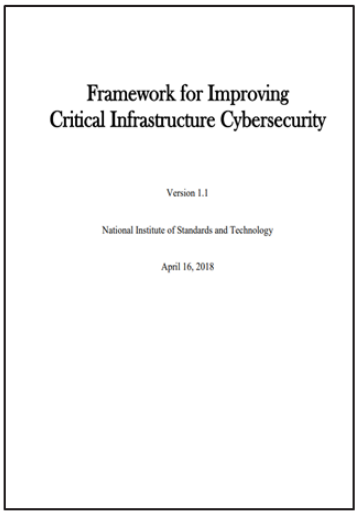
24

ISO/IEC TS 27110, clause 1 Scope

This document specifies guidelines for developing a cybersecurity framework. It is applicable to cybersecurity framework creators regardless of their organizations’ type, size or nature.

NIST Cybersecurity Framework

- The framework created by NIST is designed for the US Federal Government, but can be used by any organization worldwide.
- It provides guidelines and best practices to help organizations build and improve their cybersecurity posture.
- The framework is built upon five high-level functions: Identify, Protect, Detect, Respond, and Recover.
- Organizations cannot obtain certification against this framework.



PECB

25

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.

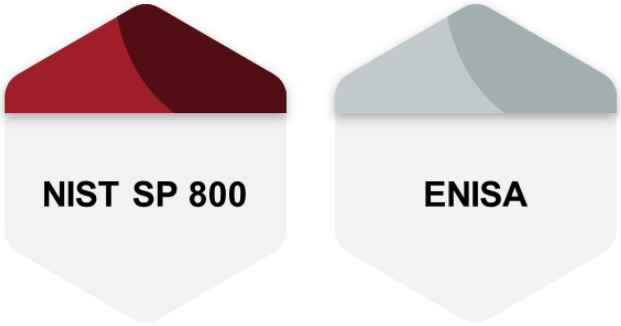
It is important to note that the framework is not limited to a specific industry, and the standardized taxonomy of standards, guidelines, and practices it provides is not exclusive to any particular country. Organizations worldwide can leverage the framework to enhance their cybersecurity efforts. Moreover,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

Sources:

NIST. “Questions and Answers | NIST.” *NIST*. Last modified January 6, 2023. https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics.

Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity."https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Other Sources



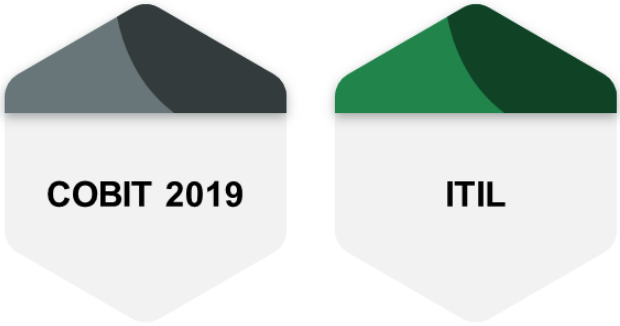
PECB

26

NIST SP 800 series comprises documents that outline US government computer security policies, procedures, and guidelines. These publications result from extensive research and offer cost-effective methods to optimize the security of IT systems and networks proactively. They cover NIST-recommended procedures, criteria for assessing threats and vulnerabilities, and implementing security measures. The documents serve as guidelines for enforcing security rules and legal references in security-related litigation. They are useful for businesses, educational institutions, and government agencies. Several publications within the series focus on cybersecurity, including NIST SP 800-53, NIST SP 800-61, NIST SP 800-171, NIST SP 800-30, and NIST SP 800-137.

ENISA (European Union Agency for Cybersecurity) is a center of network and cybersecurity expertise for the EU, its member states, the private sector, and EU citizens. ENISA works with these groups to develop advice and recommendations on best practices in cybersecurity. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. (www.enisa.europa.eu)

Other Sources (cont'd)



PECB

27

COBIT 2019 is a framework issued by ISACA (Information Systems Audit and Control Association). The Control Objectives for Information and Related Technology (COBIT) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT embodies the collective expertise of industry experts and is specifically geared towards effective control rather than operational execution. Its recommended practices play a crucial role in optimizing investments in IT-enabled initiatives, ensuring the smooth delivery of services, and establishing benchmarks to evaluate and address potential issues.

ITIL (Information Technology Infrastructure Library) is a collection of five core volumes that serve as a comprehensive guide for IT service management (ITSM). By using ITIL, organizations can establish a baseline from which they can plan, implement, and measure IT service management. ITIL encompasses non-organization-specific processes, procedures, tasks, and checklists that organizations can utilize to align with their strategy, deliver value, and maintain competency.

NIST SP 800 Publications

Provides a comprehensive set of security controls for federal information systems and organizations, including cybersecurity controls.

Offers guidance on establishing computer security incident response capabilities and handling cybersecurity incidents effectively.

Provides security requirements for protecting controlled unclassified information (CUI) in nonfederal systems, particularly for organizations working with the US government.

Focuses on conducting risk assessments for information systems, including assessing risks related to cybersecurity.

Provides guidance on establishing and maintaining an effective continuous monitoring program for information systems to ensure ongoing cybersecurity.

PECB

Section Summary:

- The International Organization for Standardization (ISO) responds to market demands by publishing international standards. These standards are developed through a collaborative process involving interested parties, incorporating global expert opinions and achieving consensus.
- ISO/IEC 27032 is a guideline standard for internet security practices.
- ISO/IEC 27001 specifies the requirements for an ISMS.
- ISO/IEC 27002 is a guideline standard of information security management best practices.
- Other important sources in cybersecurity include the NIST SP 800 series, ENISA, COBIT 5, and ITIL.

Questions?

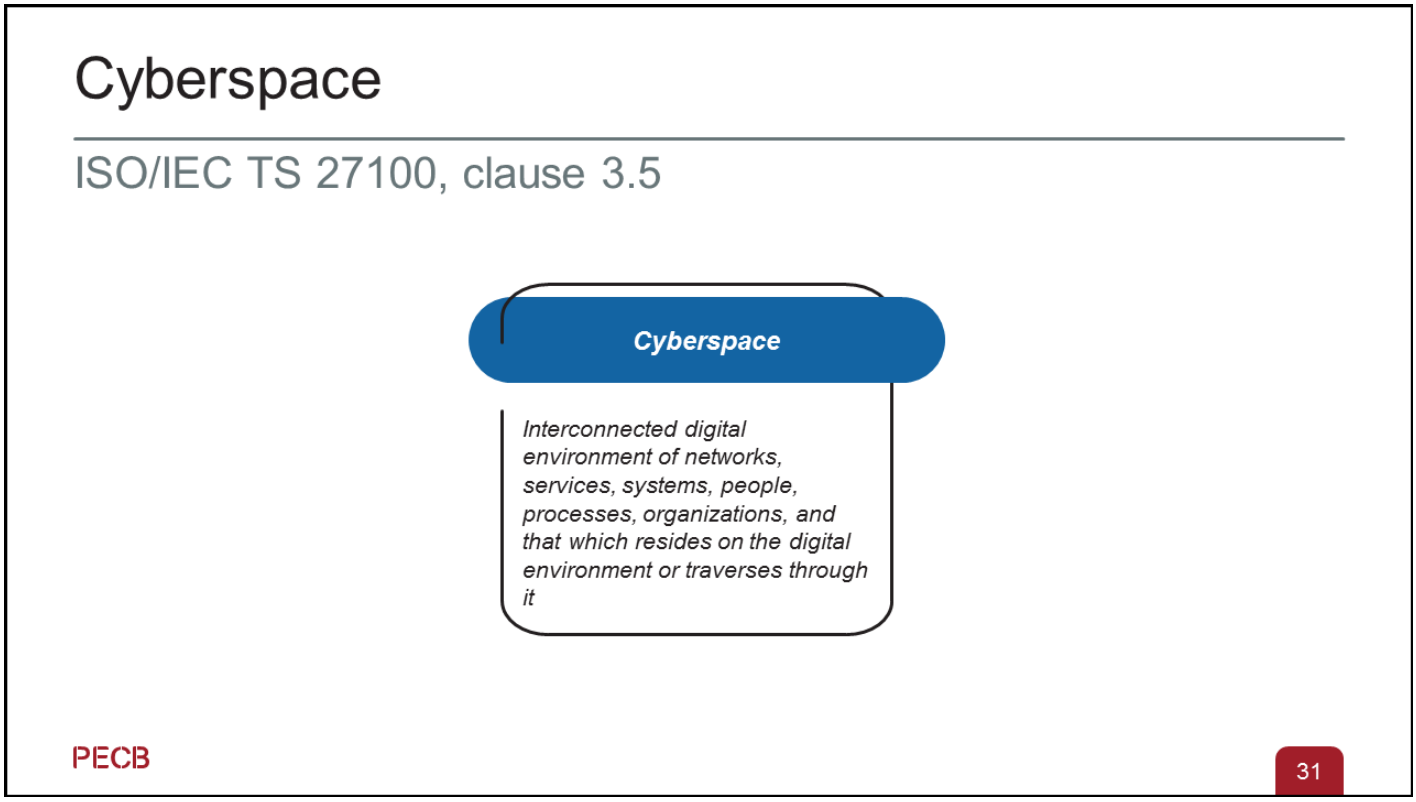
Quiz 1

PECB

29

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

This section provides information that will help participants gain knowledge on the fundamental concepts of cybersecurity, such as cyberspace, cybercrime, confidentiality, integrity, availability, vulnerability, threat, information security risk, and security controls. In addition, it elaborates on the difference between cybersecurity and information security.



ISO/IEC TS 27100, clause 4.1 Cyberspace

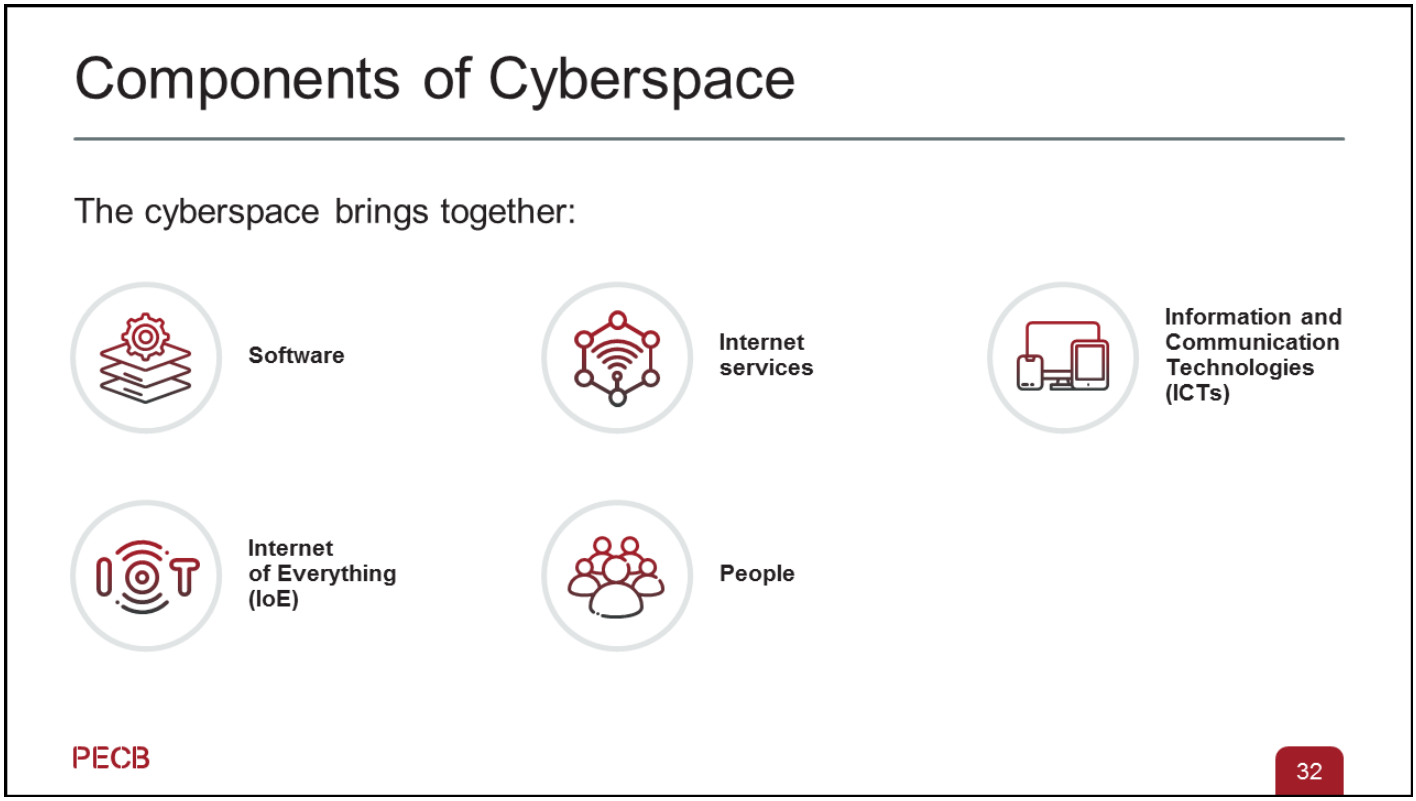
Cyberspace is a complex environment based on digital technologies that provides a global place for digital interaction among people including formal and informal interactions with public or private entities such as businesses, governments, non-profit organizations and other groups. Cyberspace is public but as individual components of cyberspace are owned by a variety of entities, it can be considered both public and private space. People and entities interact in cyberspace for many different purposes. This interaction is manifested as sharing, exchange, processing or receipt of information. Any interaction taken in cyberspace by an individual or an entity potentially has a near-instantaneous impact anywhere, in the world.

While interactive actions in cyberspace create knowledge and power, the following features of cyberspace can bring both advantageous and adverse consequences:

a. *cyberspace is borderless;*
b. *anyone can enter and leave cyberspace freely or at a very low cost;*
c. *cyber actors can be anonymous or obfuscated; and d) a threat agent can be anywhere in cyberspace from the opposite side of the globe to a close neighbour of the target.*

An action in cyberspace and its impacts can be asymmetric. The originating action can have consequences disproportionate in difficulty and cost of counteraction. In order to take advantage of cyberspace, it is important to prevent adverse consequences, that is, to ensure cybersecurity.

Cyberspace application services have gained a very important role and place in everyday life. They are moving beyond the traditional one-on-one business and consumer interactions, as well as consumer-to-consumer relationships, to a more complex and inclusive system where multiple parties can interact and transact with one another. This situation has also caused the increase of threats and vulnerabilities toward cyberspace applications, so cyberspace is becoming the target of cybercrime.



The cyberspace is a virtual network comprised of people and the technological means necessary for the communication and interaction between them.

Software

A software is an intangible part of the computer that includes a set of instructions with the intent of completing a certain task. The most common types of software in a cyberspace are databases, operating systems, antiviruses, communication and audio programs, device drivers, word processors, etc.

Internet services

For the user to be connected to the internet, they have to use an internet service. Some categories of internet services include communication services, information retrieval services, web services, and the World Wide Web.

Information and Communications Technologies (ICTs)

This term refers to various communications technologies associated with network and computer hardware, such as satellite systems, cell phones, radio, TV, remote learning, online video conferencing, and more.

Internet of Everything (IoE)

According to Cisco, the Internet of Everything (IoE) is defined as the interconnection of people, process, data, and things. The combination of these elements enables the transformation of information into actionable insights, leading to the emergence of new capabilities, enhanced experiences, and unprecedented economic prospects for business, individuals, and countries.

People

People are the intelligent users, capable of using and manipulating the computerized devices and the components of the cyberspace.

Cybercrime

NIST Cybersecurity Glossary

Criminal offenses committed on the internet or aided by the use of computer technology.

PECB

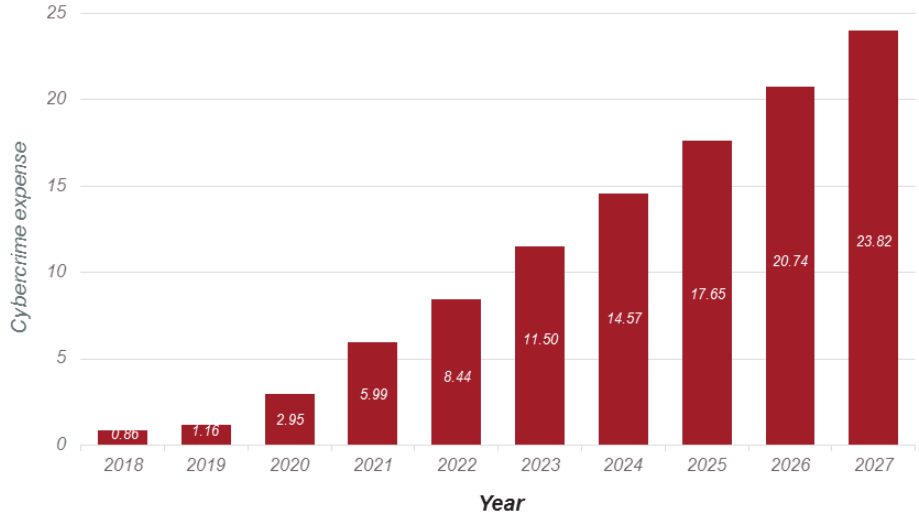
33

Sensitive customer information, intellectual property, and the control of key machinery are increasingly at risk from cyberattacks. The targeting of electronic assets has the potential to make a material impact on the entire organization and possibly its partners. Various actors can initiate these attacks, exhibiting various characteristics that include the type of target, attack methods employed, and the scale of impact caused.

Cybercrime actors can be cybercriminals who are interested in making money through fraud, employees who have access in different sensitive data and do this accidentally or on purpose, hackers who find the challenge of hacking enjoyable or who have different political or ideological motives, or competitors who are interested in gaining an economic advantage for their organizations or interests.

Cybercrime Expenses

Recent facts and studies



PECB

34

The evolution of cybercrime is driven by evolving techniques, impacts, and targets. The economic impact of cyberattacks can be devastating. Thus, organizations should consider investing in their cybersecurity programs.

Statista's Cybersecurity Outlook estimates that the worldwide expense of cybercrime is projected to increase significantly over the next four years. It is predicted to rise from $8.44 trillion in 2022 to $23.84 trillion by 2027.

Source: Fleck, Anna. "Cybercrime Expected to Skyrocket in Coming Years." Statista. Last modified December 2, 2022.https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Cybersecurity

ISO/IEC TS 27100, clause 3.2

Safeguarding of people, society, organizations and nations from cyber risks

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

PECB

35

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

ISO/IEC TS 27100, clause 4.2 Cybersecurity

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

Areas of concern for cybersecurity include:

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

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

Information Security

ISO/IEC 27000, clause 3.28

Preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

PECB

36

ISO/IEC TS 27100, clause 5.2.1 Cyberspace as a field of risk sources for an ISMS

An information security management system (ISMS) is applicable within an organization with interfaces and interactions with external entities. Specifically, the scope of the ISMS and the scope of risk identification are within an organization. Information security objectives aim at protection of information that has value to the organization or of the information of other entities that are in custody of the organization.

Cybersecurity transcends the boundaries and control of an organization because of the interconnectedness of cyberspace. Organizations frequently interface and interact with external entities by using cyberspace. As such, the use of cyberspace represents risks to the organization that need to be managed as a part of an organization's ISMS. If the organization has an ISMS, cyberspace shapes part of context of the ISMS as referred to in ISO/IEC 27001:2013, 4.1. Threat vectors that originate in cyberspace can expose the organization to information security risks. The organization identifies risks from threats in cyberspace, along with other risks, during the process of risk identification as required in ISO/IEC 27001:2013, 6.1.2 c).

ISO/IEC 27000, clause 3.6 Authenticity

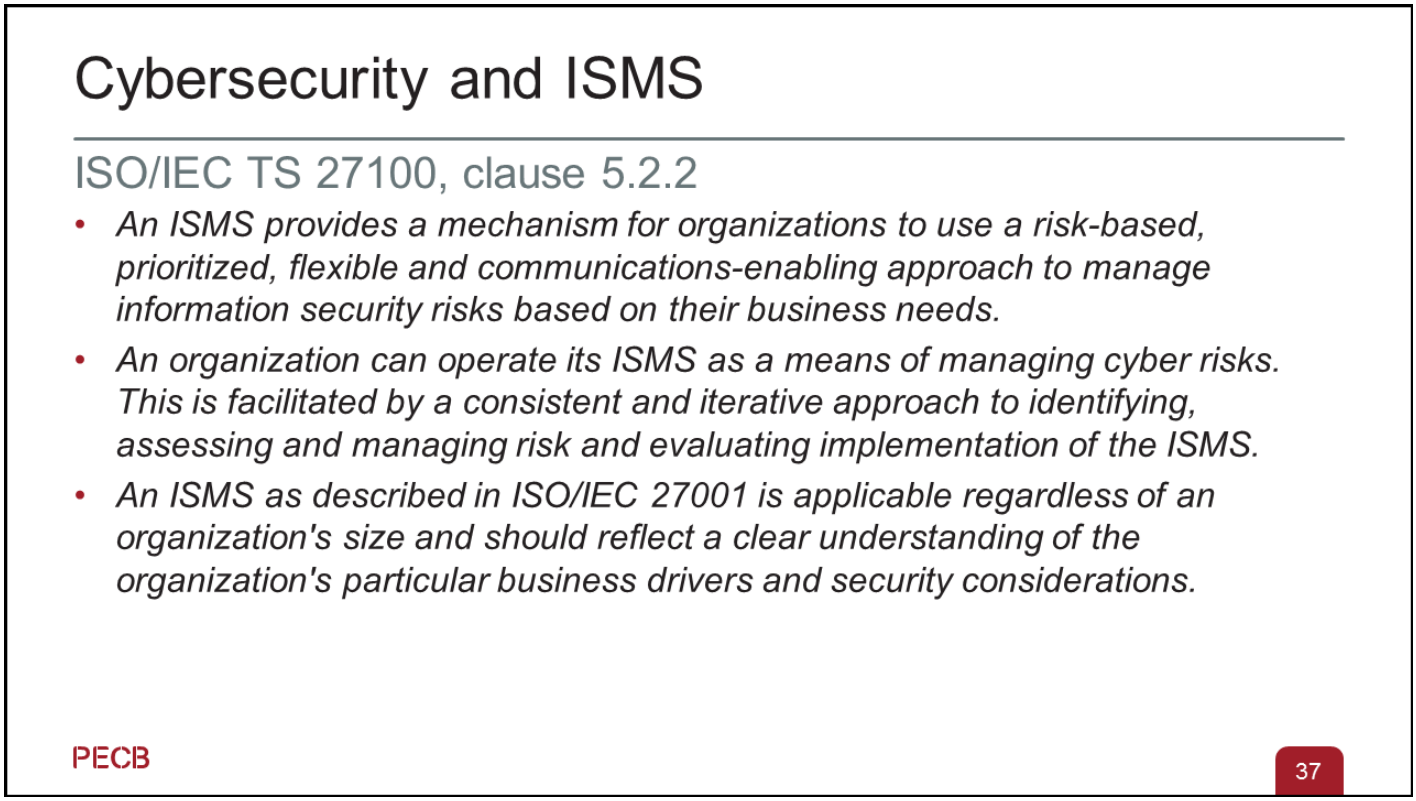
Property that an entity is what it claims to be

ISO/IEC 27000, clause 3.48 Non-repudiation

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

ISO/IEC 27000, clause 3.55 Reliability

Property of consistent intended behaviour and results

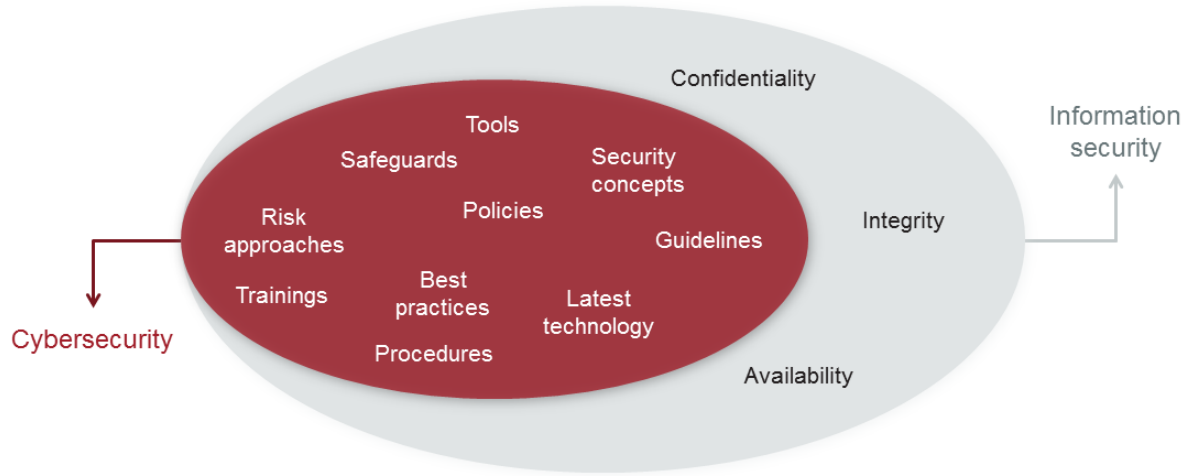


ISO/IEC TS 27100, clause 5.2.2 ISMS in support of cybersecurity (cont'd)

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

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

Difference between Information Security and Cybersecurity



PECB

38

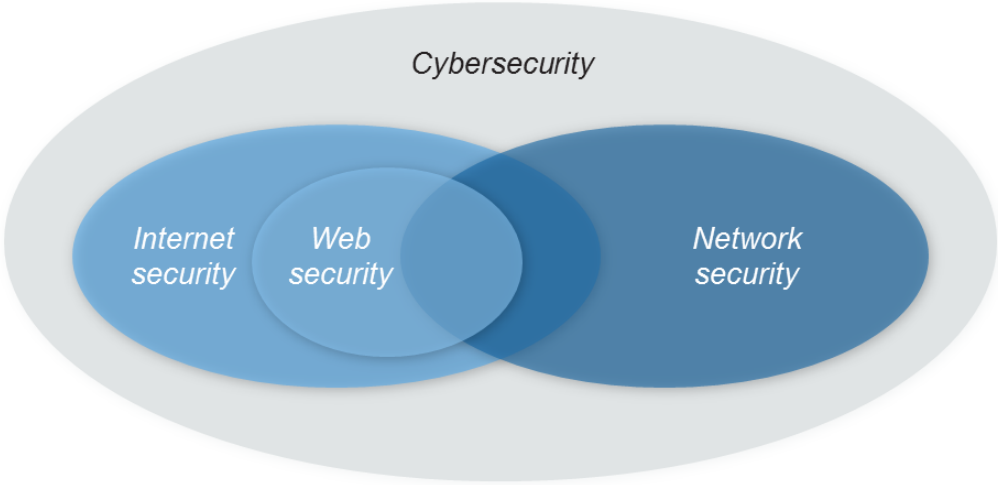
The term cybersecurity is frequently used interchangeably with information security due to their close association. There are also technical definitions derived from it, including cyberwarfare and protection of critical infrastructure. However, it is crucial to note that there are significant distinctions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

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

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

Relationship between Cybersecurity and Other Security Domains

ISO/IEC 27032, Figure 1



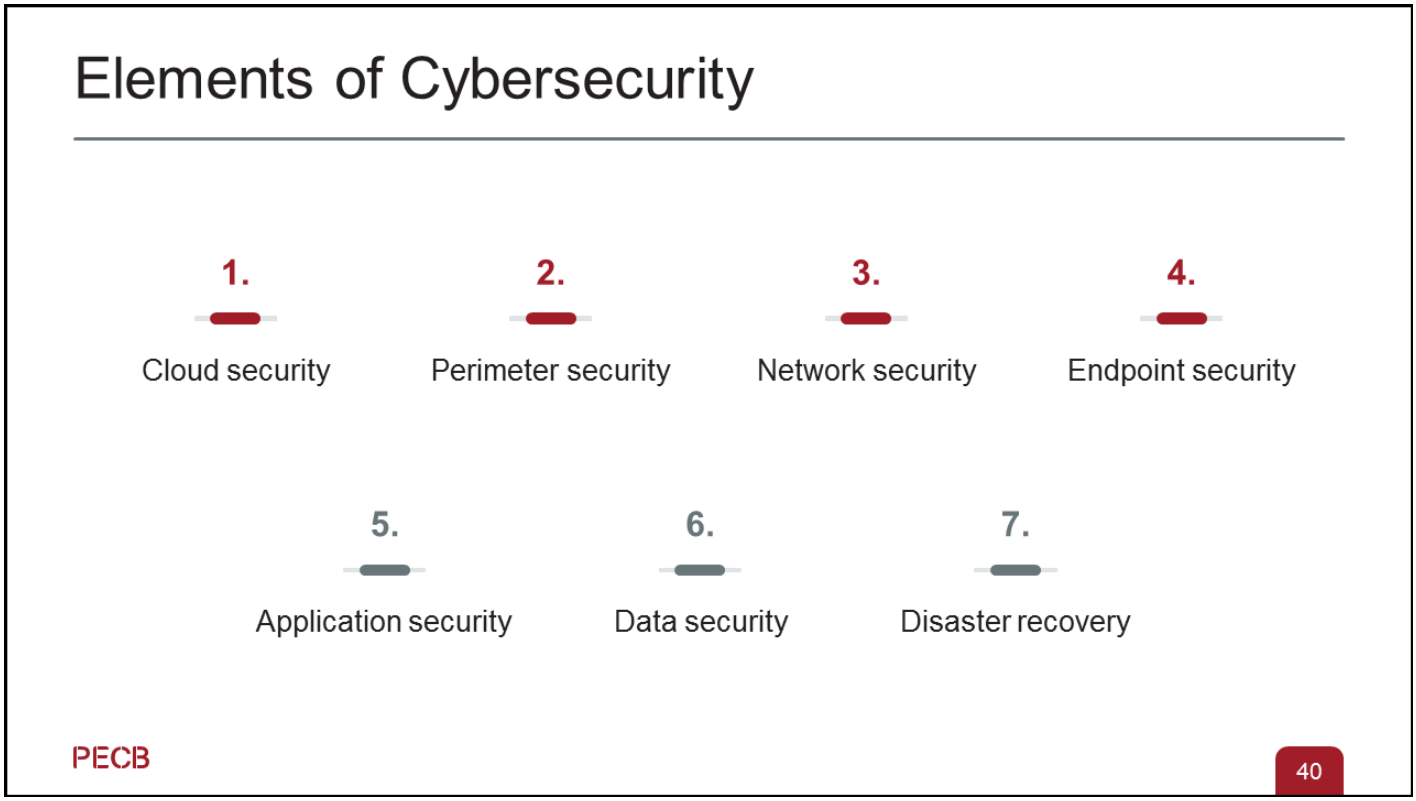
PECB

39

ISO/IEC 27032, clause 5 Relationship between Internet security, web security, network security and cybersecurity

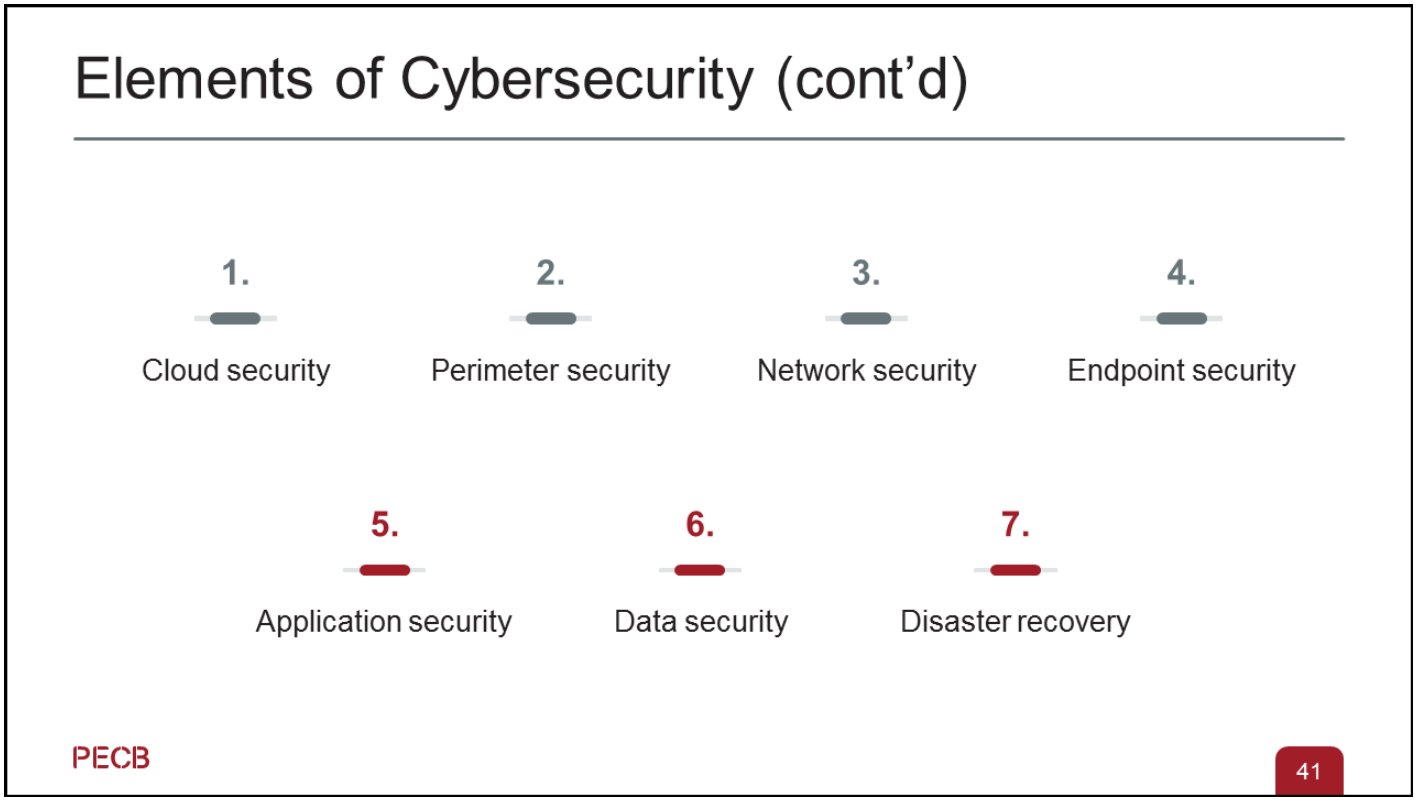
Cybersecurity concerns managing information security risks when information is in digital form in computers, storage and networks. Many of the information security controls, methods, and techniques can be applied to manage cyber risks.

Cybersecurity also deals with protecting Internet-connected systems including hardware, software, programs and data from potential attacks. Many of these attacks are characterized by targeted and blended attacks with a high degree of sophistication and persistence. The threats can be Internet-based and/or threats due to connectivity with other networks and systems within the organization or customer and service provider's network, to which the organization communicates during the normal course of business.



Various elements of cybersecurity include:

1. **Cloud security** involves protecting private and public cloud instances used by companies, which can be set up on-site or off-site. Measures such as cloud governance solutions and managed security service providers help enforce policies, manage vulnerabilities, and defend against targeting cloud instances.
2. **Perimeter security** serves as the primary defense for on-site corporate infrastructure, using intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and block external malicious traffic. Demilitarized zones (DMZ) and data loss prevention (DLP) solutions enhance network segregation and asset isolation, ensuring secure transmission of network packets.
3. **Network security** involves implementing measures and protocols to protect computer networks from unauthorized access and potential threats. It includes using identity control and access management solutions to detect and prevent external and insider threats, virtual firewalls to block malicious web traffic, web proxy content filtering for identifying anomalous behavior in mail and web servers, and deploying mobile and wireless security solutions to support BYOD policies.
4. **Endpoint security** refers to the implementation of measures and practices to secure the entry points or the endpoints of end-user devices, including desktops, laptops, and mobile devices, against exploitation by malicious actors and attacks. This involves utilizing advanced solutions like XDR (extended detection and response) instead of traditional host-based IDS/IPS, as well as employing next-generation antivirus (NGAV) solutions to detect, prevent and mitigate host-based cyber risks and threats. The primary goal of endpoint security is to protect these endpoints within a network or cloud environment from various cybersecurity threats.



5.Application security refers to the implementation of security measures and practices to protect applications from cyberattacks. It involves utilizing tools such as web application firewalls (WAF) to detect and prevent malicious web traffic from impacting web servers.

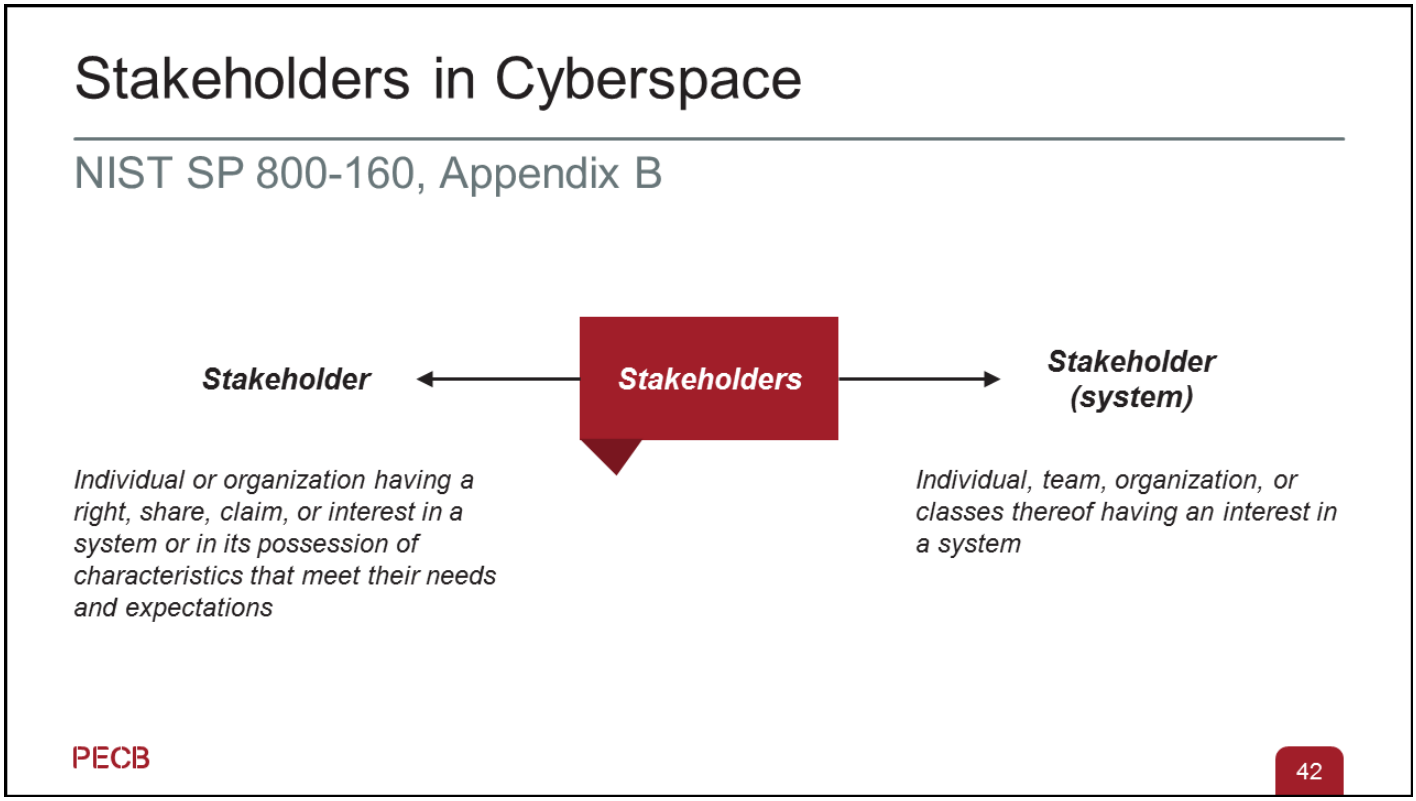
6.Data security refers to the implementation of measures and practices to protect the integrity, confidentiality, and availability of data. It involves utilizing data integrity and monitoring techniques, along with file integrity monitoring (FIM) solutions, to enable security personnel to monitor and classify different types of data stored in data base servers. The objective of data security is to ensure that data is protected from unauthorized access, manipulation, or disclosure, and that appropriate safeguards are in place throughout its lifecycle.

7.Disaster recovery planning refers to the process of creating a strategy that ensures the continuity of work in an efficient and rapid manner after a disaster occurs. The key objectives of such planning include protecting the organization during a crisis, instilling a sense of security, reducing downtime, ensuring the dependability of backup systems, and minimizing ad hoc decision-making in critical situations.

Sources:

Subhani, Abdul. "Essential Elements Of Cybersecurity." Forbes. Last modified August 30, 2022. https://www.forbes.com/sites/forbestechcouncil/2022/08/30/essential-elements-of-cybersecurity/?sh=6872caa015cd.

GeeksforGeeks. "Elements of Cybersecurity." Accessed June 16, 2022. https://www.geeksforgeeks.org/elements-of-cybersecurity/.



Stakeholders play a critical role in ensuring the protection and maintenance of cyberspace.

Note: The term “stakeholders” is synonymous with the term “interested parties.” Therefore, these terms are used interchangeably.

Confidentiality, Integrity, Availability

ISO/IEC 27000, clause 3.10 Confidentiality

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

ISO/IEC 27000, clause 3.36 Integrity

Property of accuracy and completeness

ISO/IEC 27000, clause 3.7 Availability

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

PECB

43

According to NIST, the security objectives of confidentiality, integrity, and availability, as well as security requirements, are used to inform the security capabilities for a system, product, or service.

Confidentiality means ensuring that the protected and sensitive information is only accessible to authorized individuals. Some of the practices employed to ensure confidentiality are:

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

Integrity ensures that:

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

Availability means ensuring that information must be easily accessible as required, when required, where required, and to the person(s) requiring it. To ensure the availability of information, organizations should maintain and improve their infrastructure, such as servers and disks where information is stored. In addition, organizations should establish record retention policies, data backup and recovery procedures, incident management procedures, information processing procedures, and procedures to control the usage of systems.

Vulnerability

ISO/IEC 27000, clause 3.77

Vulnerability

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

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

PECB

44

ISO/IEC 27032, clause 8.3 Vulnerabilities

Vulnerability is weakness of an asset or control that can be exploited by a threat. Manufacturers, software developers and other technology developers produce security updates and patches to fix these weaknesses once they are found and solved. As systems receive patches, updates or new elements are added. As systems become outdated or unsupported by the vendor or not patched to the latest version, new vulnerabilities can be introduced. Interested parties should have a thorough knowledge and understanding of the asset or control in question, as well as the threats, threat agents and risks involved, in order to perform a comprehensive assessment. Interested parties should be aware of the zero-day vulnerabilities for which there is no patch available.

Examples of Vulnerabilities

ISO/IEC 27005, Table A.11 (excerpt)

Category	Examples of vulnerabilities
Hardware	Insufficient maintenance/faulty installation of storage media
	Lack of care at disposal
Software	No or insufficient software testing
	Complicated user interface
Network	Unprotected communication lines
	Single point of failure
Personnel	Insufficient security training
	Unsupervised work by outside or cleaning staff
Site	Unstable power grid
	Location in an area susceptible to flood
Organization	Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective
	Audits (supervision) not conducted on a regular basis

PECB

45

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

The lists can provide help during the assessment of threats and vulnerabilities, to determine relevant risk scenarios. In some cases, other threats can exploit these vulnerabilities as well.

Threat

ISO/IEC 27000, clause 3.74

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

- A threat is any circumstance or activity that has the potential to exploit vulnerabilities and negatively impact the organization.
- By definition, a threat has the potential to harm assets such as information, processes, and systems and, therefore, harm the organization. Threats are associated with the negative aspect of risk and, as such, refer to undesirable occurrences.

PECB

Threats

Threats related to assets

- Online identity stolen or masqueraded
- Unauthorized access to a person's financial information, theft of the person's money, and fraud

- Website defacement
- Domain name theft by cyber-squatters
- Financial reports breach
- Unauthorized access to sensitive information

Examples of Typical Cyber Threats

ISO/IEC TS 27100, clause 7.2

Performance of a business organization is supported by the ICT infrastructure of its own and its connectedness to the global network. Cyber threats for the organization communicating and interacting with other entities in the network can include:

a) attacks through networks, e.g. intrusion to the intranet, malware infection, advanced persistent threat (APT) attack and a denial of service (DoS) attack;

b) information theft by personnel to include external parties, external threat actors and remote workers;

c) quality issues of ICT devices and systems resulting in failure of their operation; and

d) system management and operational issues that result in a failure to effectively implement cybersecurity controls.

PECB

48

ISO/IEC TS 27100, clause 7.3 Industrial organization and industrial automation and control systems

Industrial organizations have information systems that control operations of product lines, machines and equipment in the factory, collectively called industrial automation and control systems (IACSs). While each IACS has processes specific to its application, there is a series of processes generally observed in IACS:

a. *sensing states or movement of equipment or materials;*
b. *transmitting the sensed data over the network to an information system;*
c. *processing of the data;*
d. *generating controlling data;*
e. *transmitting the controlling data over the network; and*
f. *actuating the controlling data into the states or movement of equipment or materials.*

Cyber threats in these processes are:

a. *attacks on the systems and networks;*
b. *quality issue of the IACS;*
c. *loss of integrity or availability of the sensed data or control data;*
d. *failure in operation of hardware and software; and*
e. *incorrect or halt of physical operations.*

Within these cyber threats, there are cascading relationships of causes and consequences.

An IACS can be a system of devices, machines and other equipment as "things" connected to the network through sensors and actuators.

Threat Agent

ISO/IEC 27032, clause 8.2

- *A threat agent is an individual or group of individuals who have any role in the execution or support of an attack.*
- *Thorough understanding of their motives (religious, political, economic, etc.), capabilities (knowledge, funding, size, etc.) and intentions (fun, crime, espionage, etc.) is critical in the assessment of vulnerabilities and risks, as well as in the development and deployment of controls.*

Threat Landscape

- Threat landscape encompasses a wide range of possible and identified cyber threats, such as vulnerabilities, malware, specific threat agents, and their techniques, that pose a danger to a sector, user, or time period in a specific context.
- The context for a cyber threat varies by the sector, organization, or even individual. Some of the factors include the possession of valuable information, the level of security, and geopolitical factors.

PECB

50

Source: Encyclopedia by Kaspersky. “Threat Landscape.” Accessed June 27, 2023. https://encyclopedia.kaspersky.com/glossary/threat-landscape/.

Relationship between Vulnerability and Threat

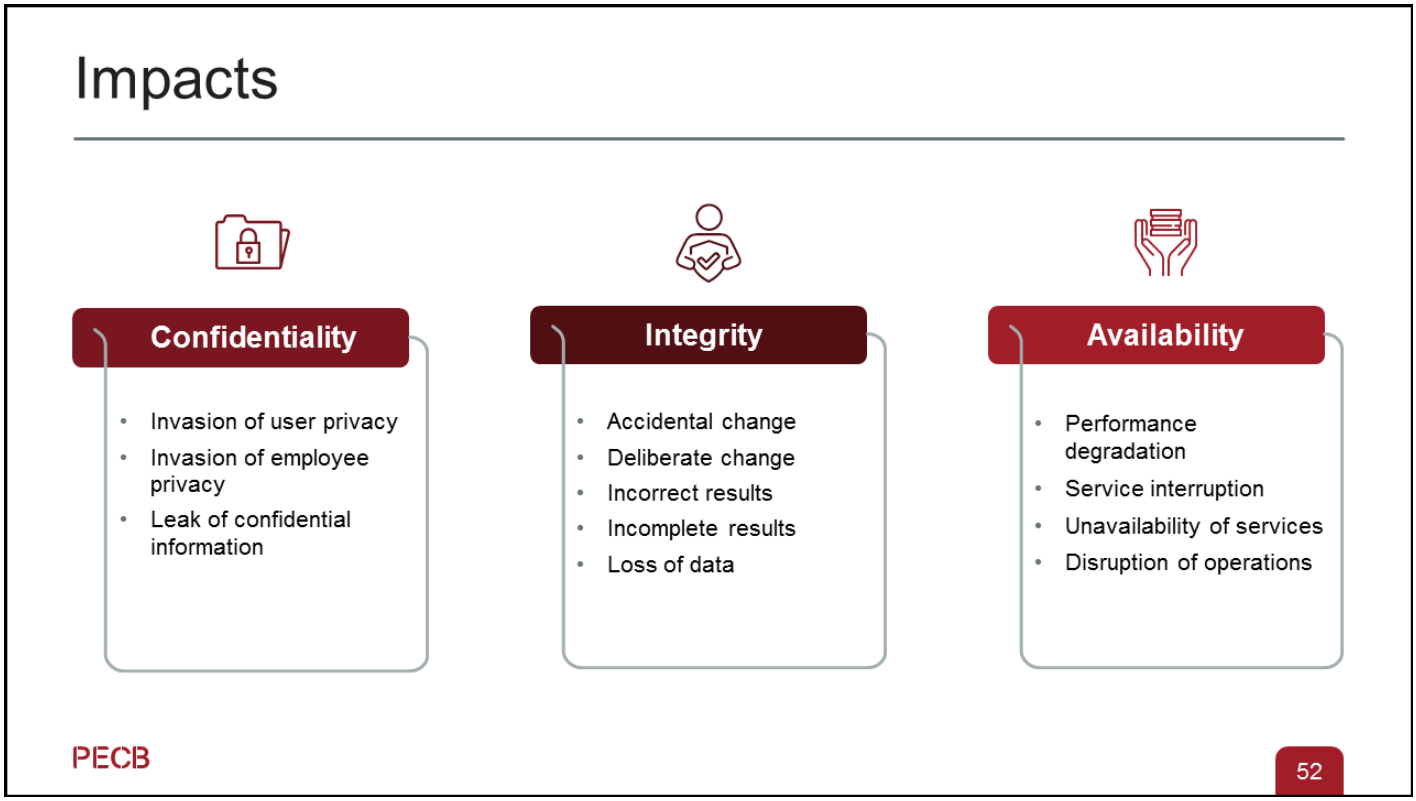
Examples

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

PECB

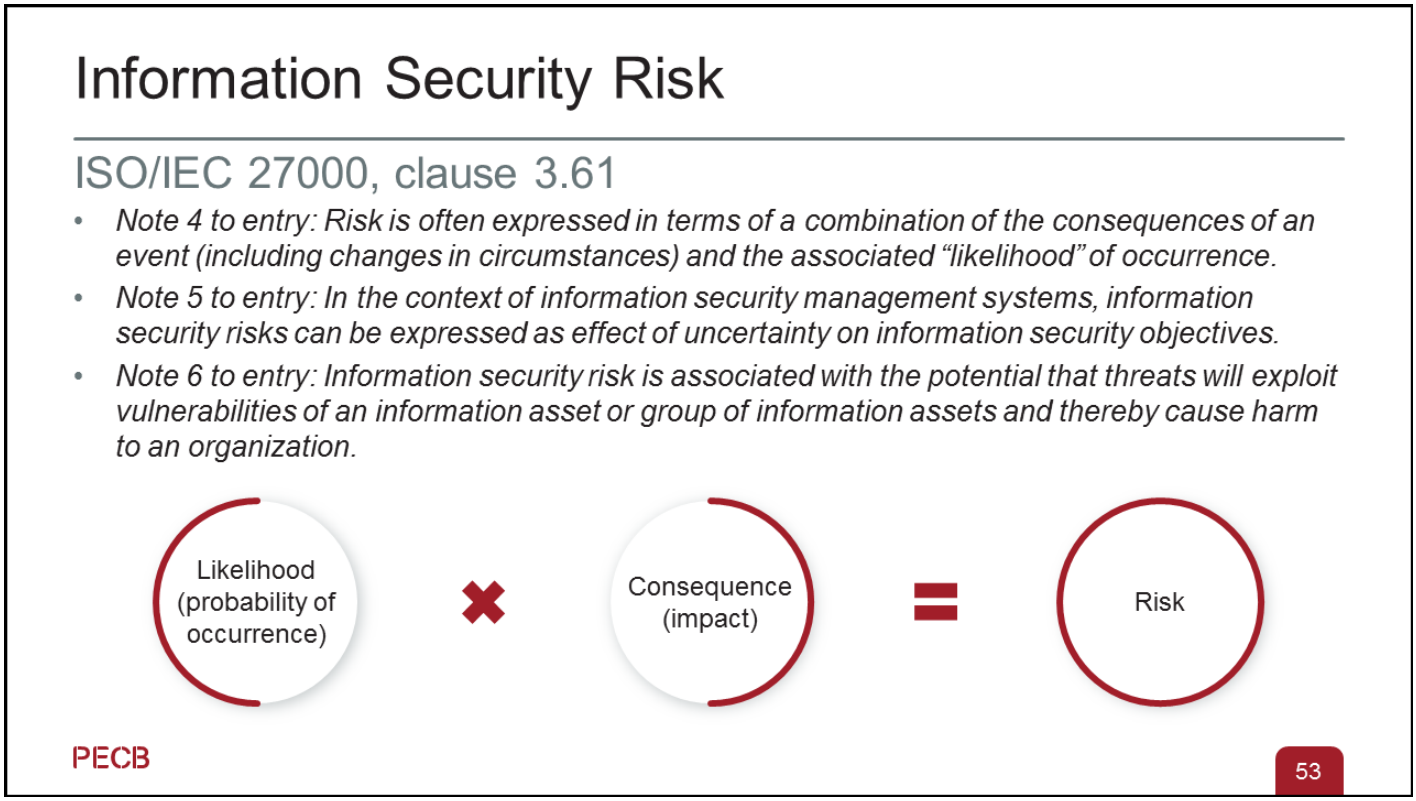
51

The incorrect implementation, use, or malfunction of a control could, in itself, represent a threat.



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

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



ISO/IEC 27000 clause 3.57 Residual risk

Risk remaining after risk treatment

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

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

ISO/IEC 27000, clause 3.61 Risk

Effect of uncertainty on objectives

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

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

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

ISO/IEC 27000, clause 3.62 Risk acceptance

Informed decision to take a particular risk

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

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

ISO/IEC 27000, clause 3.63 Risk analysis

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

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

Note 2 to entry: Risk analysis includes risk estimation.

ISO/IEC 27000, clause 3.64 Risk assessment

Overall process of risk identification, risk analysis and risk evaluation

Information Security Risk – Definitions

ISO/IEC 27000, clauses 3.66 to 3.72

Term	Definition
Risk criteria	*Terms of reference against which the significance of risk is evaluated*
Risk evaluation	*Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable*
Risk identification	*Process of finding, recognizing and describing risks*
Risk management	*Coordinated activities to direct and control an organization with regard to risk*
Risk management process	*Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk*
Risk owner	*Person or entity with the accountability and authority to manage a risk*
Risk treatment	*Process to modify risk*

PECB

54

ISO/IEC 27000, clause 3.66 Risk criteria (cont'd)

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

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

ISO/IEC 27000, clause 3.67 Risk evaluation (cont'd)

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

ISO/IEC 27000, clause 3.68 Risk identification (cont'd)

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

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

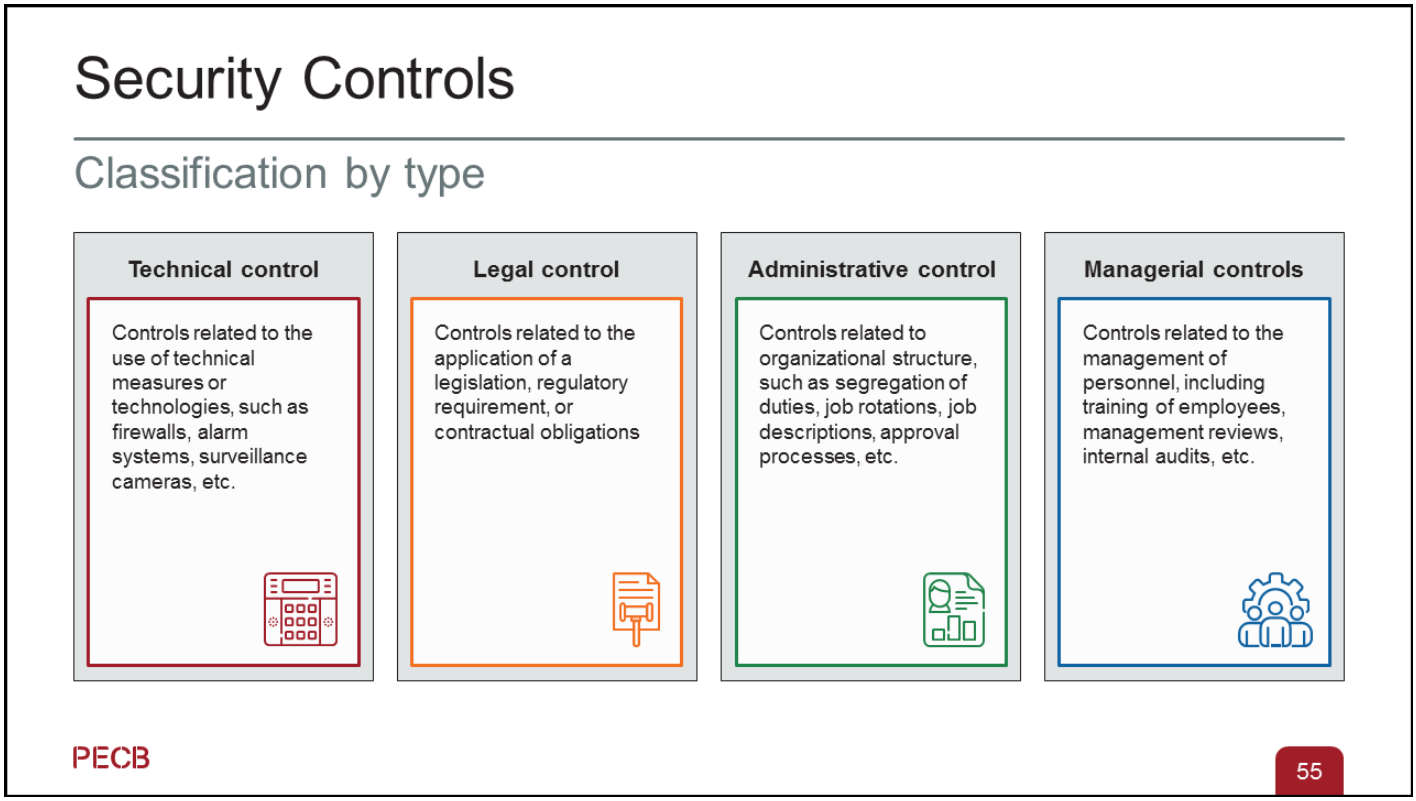
ISO/IEC 27000, clause 3.70 Risk management process (cont'd)

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

ISO/IEC 27000, clause 3.72 Risk treatment (cont'd)

Note 1 to entry: Risk treatment can involve:

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



ISO/IEC 27000, clause 3.14 Control

Measure that is modifying risk

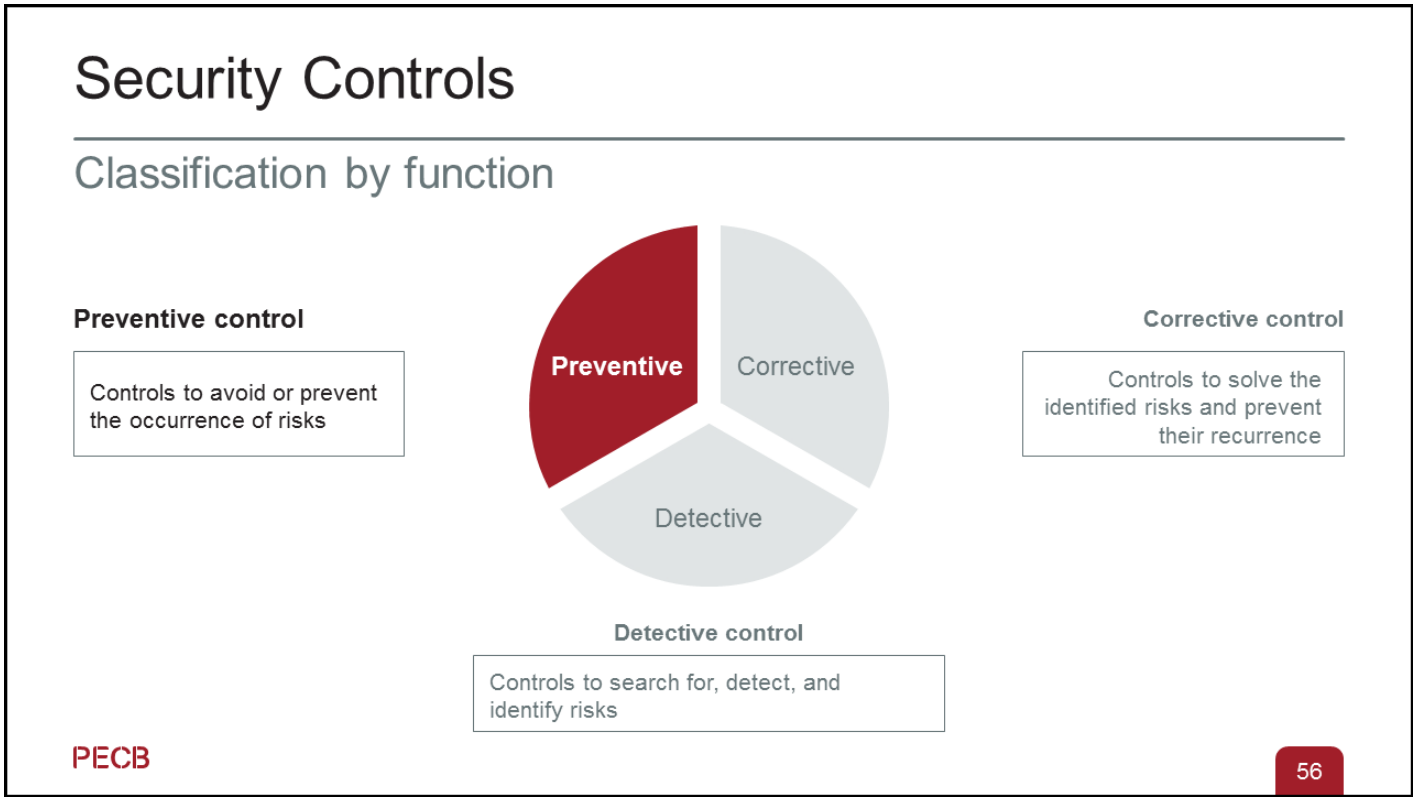
ISO/IEC 27000, clause 3.15 Control objective

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

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

Note:

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



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

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

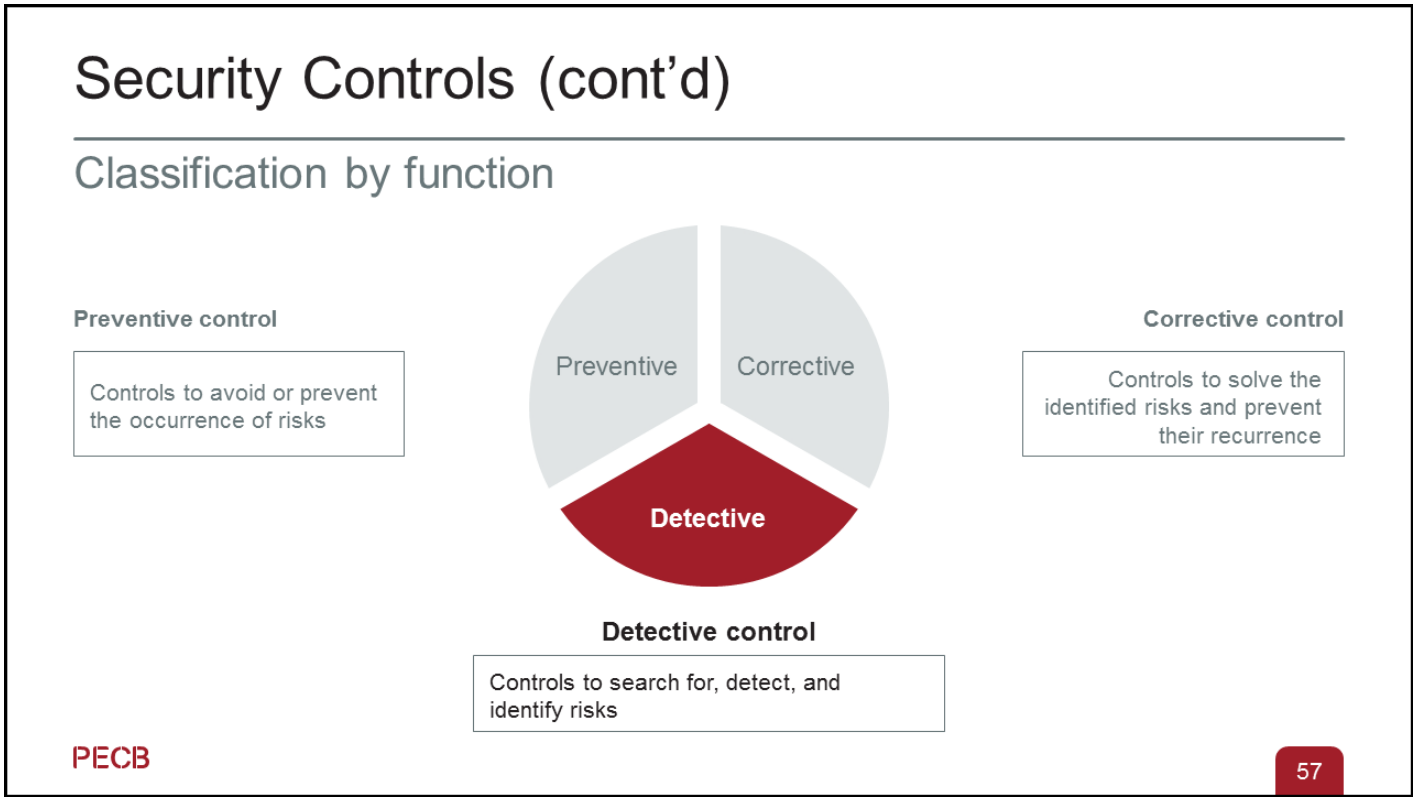
1.Preventive control

Purpose: Avoid or prevent the occurrence of risks

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

Examples:

- Separate the development, testing, and operating equipment
- Secure offices, rooms, and equipment
- Use clearly defined procedures (to prevent errors and mistakes)
- Use cryptography
- Use an access control software that only allows authorized employees to access sensitive files

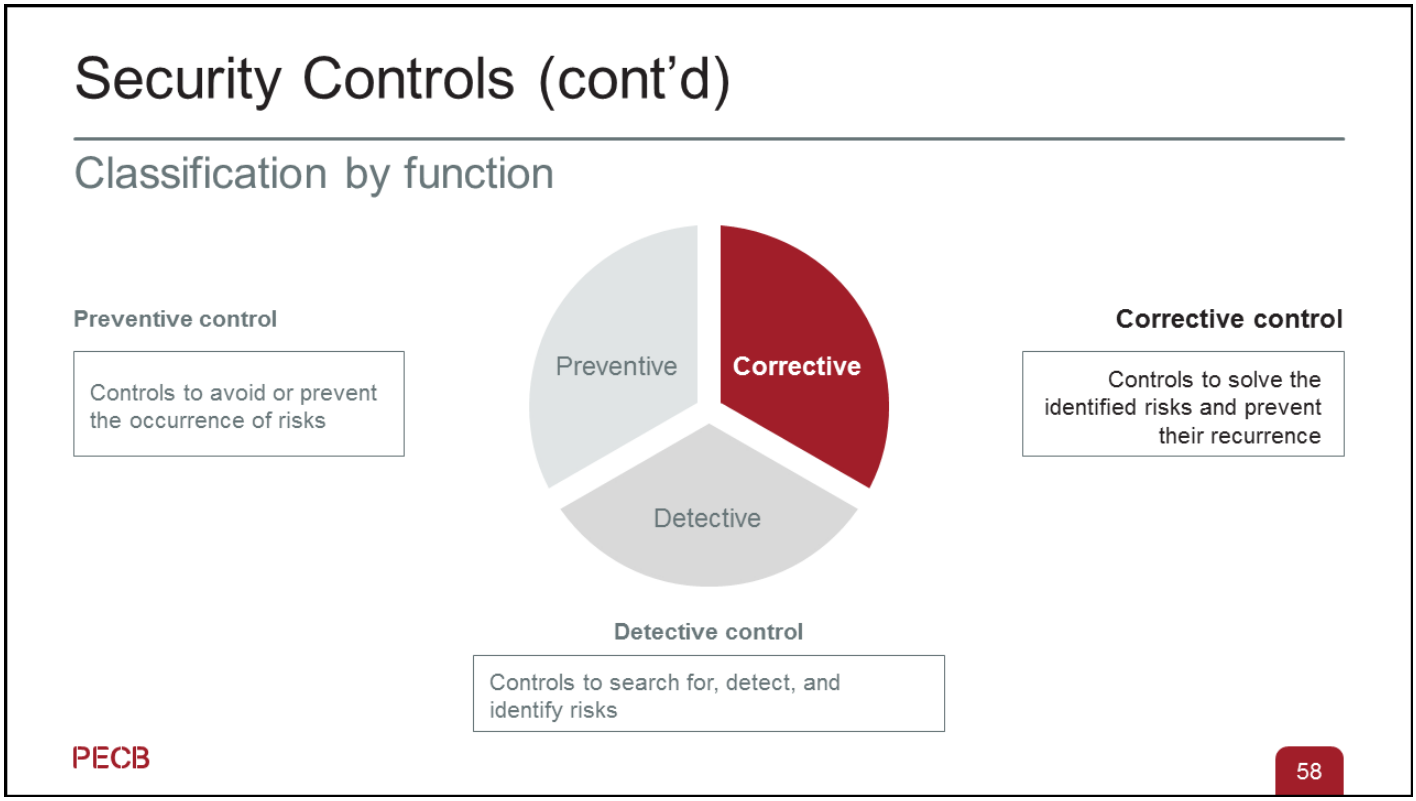


2.Detective controls
Purpose: Search for, detect, and identify risks

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

Examples:

- Integrate checkpoints in the applications in production
- Use echo control in telecommunications
- Use alarms to detect risks related to heat, smoke, fire, or water
- Verify duplicate calculations in data processing
- Detect break-ins with video cameras
- Detect potential intrusions on networks with an intrusion detection system (IDS)
- Review user access rights
- Conduct a technical review of applications after modifying the operating system



3.Corrective controls
Purpose: Solve the identified risks and prevent their recurrence

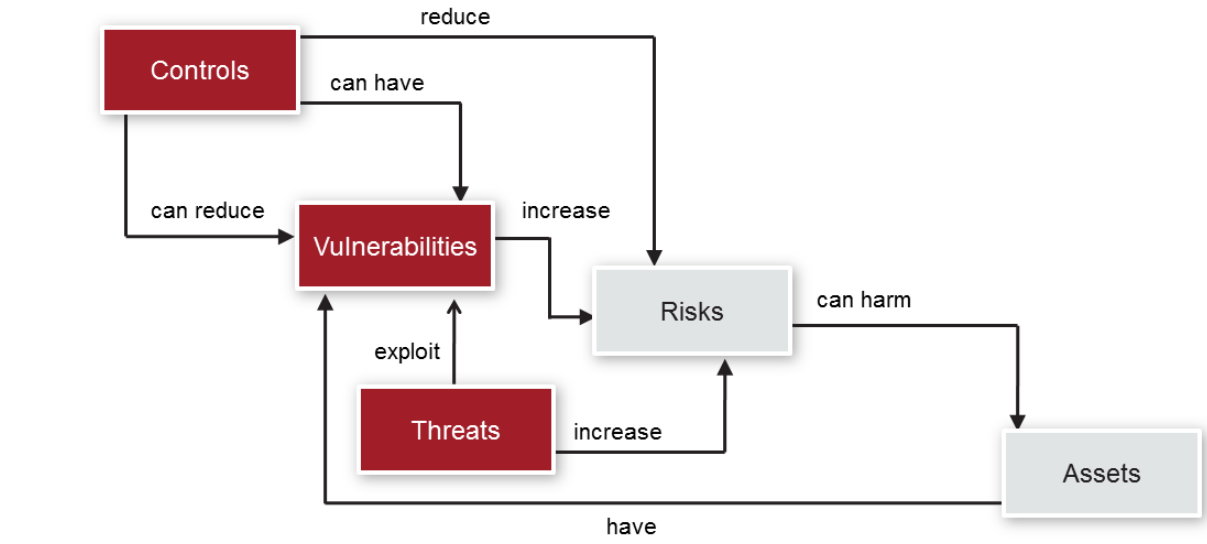
- Minimize the impact of a threat
- Solve the risks detected by detective controls
- Identify the causes of risks
- Modify the processing system to reduce future risks to a minimum

Examples:

- Review the security policy after the integration of a new division in the organization
- Appeal to authorities to report a computer crime
- Change all passwords of all systems when a computer network intrusion has been detected
- Recover the transactions with the backup procedure after discovering that some data has been corrupted
- Disconnect idle sessions automatically
- Implement patches following the identification of technical vulnerabilities

Relationships between Security Elements

Overview



PECB

59

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

Section Summary:

- The cyberspace is a complex virtual world comprised of software, internet services, communications technology (ICT) devices, connected networks, and people.
- Cybercrime is the usage or subjection of the administrations or applications in the cyberspace for a crime, or where the cyberspace is the source, apparatus, target, or spot of a crime.
- Cybersecurity falls under the umbrella of information security. They both deal with the value of the data under protection. However, cybersecurity determines the technologies needed to implement the important data and identifies the important data and their location.
- Stakeholders in cyberspace are categorized as consumers and providers.
- Vulnerability is a weakness found in the system that, when exploited by a threat, can be used to gain unauthorized access to an asset.
- A threat refers to any situation or action that has the capacity to exploit vulnerabilities and have a detrimental effect on the organization.
- Risk can be defined as the potential impact or deviation, whether positive or negative, on objectives due to the presence of uncertainty.

PECB

Questions?

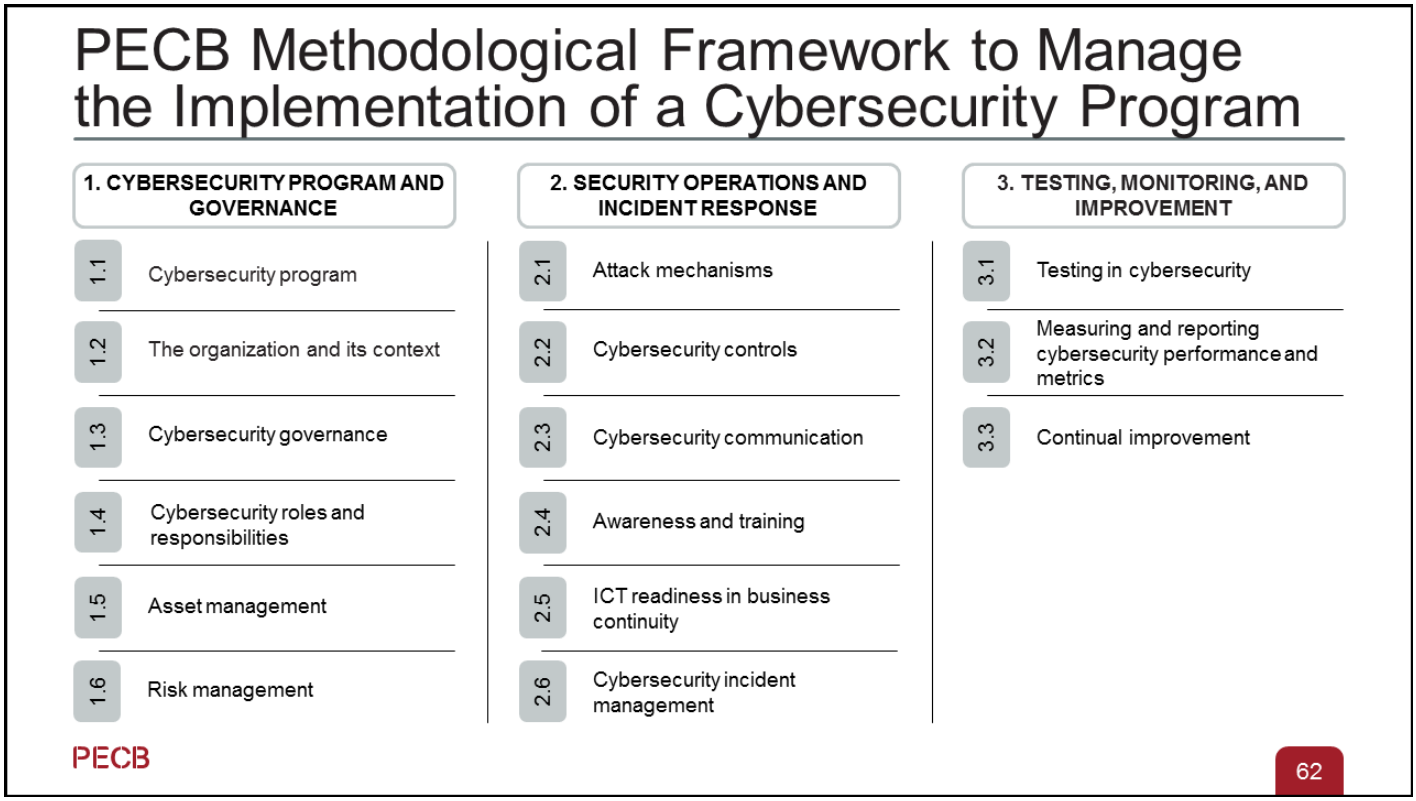
Exercise 1

Quiz 2

60

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

This section provides information about the process of finding an approach to successfully implement the cybersecurity program.



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

Important notes:

1. The organization must adapt the methodology to its particular context (requirements, size, scope, objectives, etc.) and not apply it strictly.
2. The sequence of steps can be changed (inversion, merging, etc.). For example, the implementation of risk management can be completed before the development of policies.
3. Many processes are iterative because of the need for progressive development throughout the implementation program (e.g., awareness and training).

Cybersecurity Program

- The implementation of a robust cybersecurity program is crucial in establishing a secure virtual environment for sensitive data.
- Such program should be tailored to meet the specific needs of an organization taking into account its size, complexity, and the nature of the sensitive data it handles.

PECB

63

A well-designed cybersecurity program is not a one-size-fits-all solution; rather, it is customized to address the unique challenges and risks faced by each organization. Factors such as the type of data being handled, the industry in which the organization operates, and the potential threats it faces play a significant role in shaping the cybersecurity strategy.

To ensure comprehensive protection, the cybersecurity program must be implemented organization-wide, encompassing all business functions and IT-related activities.

Cybersecurity is not solely the responsibility of the IT department; instead, it requires a collaborative effort between business units and IT specialists. While IT professionals possess technical expertise and knowledge, business leaders bring a deeper understanding of the organization's overall goals, operations, and risk tolerance. A cooperative approach ensures that security measures align with the organization's objectives and that potential security vulnerabilities are adequately addressed across all levels of the organization.

Cybersecurity Frameworks

- Organizations can use cybersecurity frameworks to create a new cybersecurity program or improve their existing one.
- Cybersecurity frameworks are designed to complement existing business and cybersecurity operations.
- The following key points help choosing the right framework for an organization:
  - The state of the current cybersecurity program, if there is one
  - The goal of the cybersecurity program
  - Cybersecurity risks
  - Compliance requirements of applicable legislations and industry standards

PECB

64

When identifying the cybersecurity frameworks, it is important to establish the framework's role, scope, and form of interaction with other standards and guidelines.

Cybersecurity frameworks are commonly applicable to all organizations, regardless of their size or industry.

Source: Cybersecurity & Infrastructure Security Agency. "Cybersecurity Framework Implementation Guidance." Last modified May, 2020.
https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Impl

Cybersecurity Program Framework

1. CYBERSECURITY PROGRAM AND GOVERNANCE		2. SECURITY OPERATIONS AND INCIDENT RESPONSE		3. TESTING, MONITORING, AND IMPROVEMENT	
1.1	**Cybersecurity program**	2.1	Attack mechanisms	3.1	Testing in cybersecurity
1.2	The organization and its context	2.2	Cybersecurity controls	3.2	Measuring and reporting cybersecurity performance and metrics
1.3	Cybersecurity governance	2.3	Cybersecurity communication	3.3	Continual improvement
1.4	Cybersecurity roles and responsibilities	2.4	Awareness and training		
1.5	Asset management	2.5	ICT readiness in business continuity		
1.6	Risk management	2.6	Cybersecurity incident management		

PECB

1.1 Cybersecurity Program

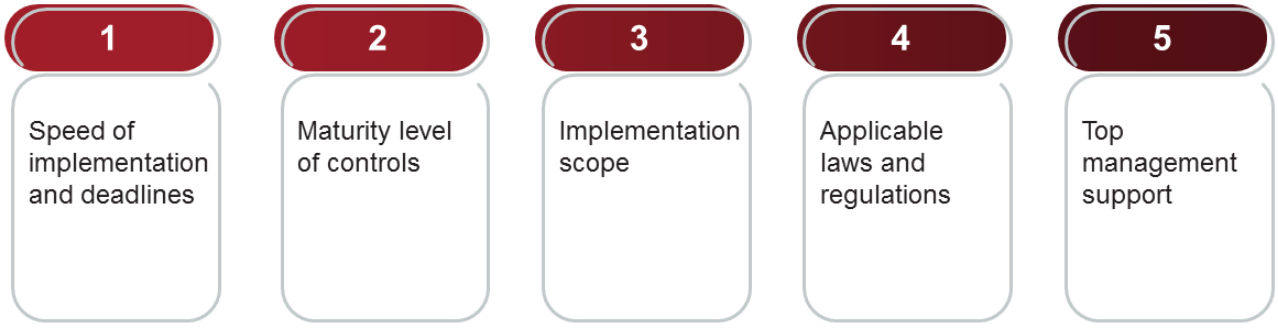
List of activities

1.1.1 Define an approach for the implementation of the cybersecurity program

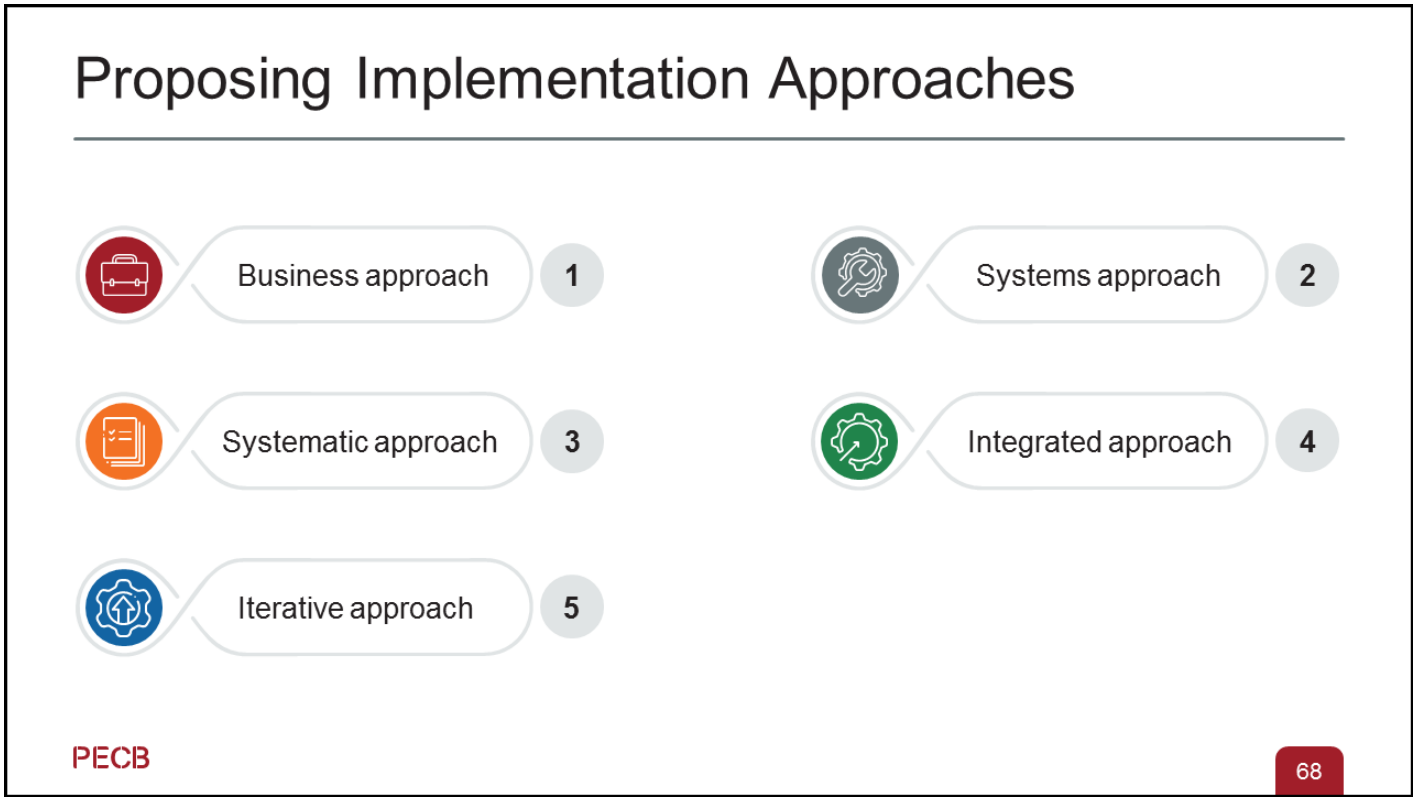
1.1.2 Align with best practices

1.1.1 Define an Approach for the Implementation of the Cybersecurity Program

Factors determining the implementation approach



PECB



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

The approach proposed in this training course as a response to overcoming the difficulties mentioned above based on the following:

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

Applying the Proposed Implementation Approach

Recommendations

1. Avoid the integration of new technologies
2. Integrate the cybersecurity program into existing processes
3. Apply the principles of continual improvement
4. Involve interested parties in the organization
5. Obtain top management support
6. Identify and appoint a cybersecurity program manager

PECB

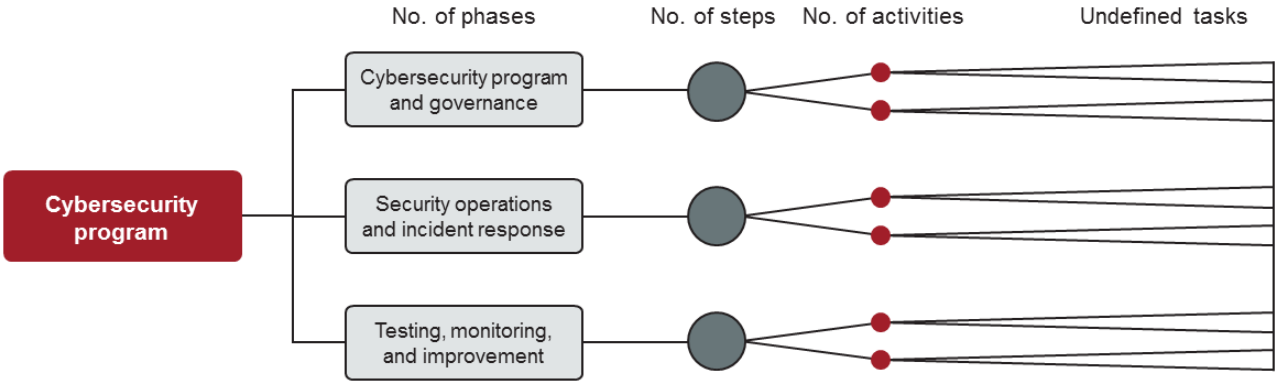
69

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

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

Integrated Implementation Methodology for the Cybersecurity Program

PECB methodology



PECB

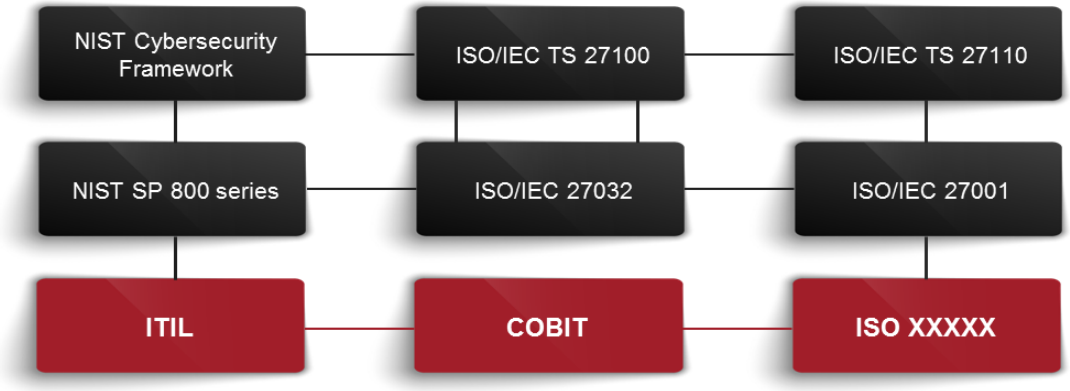
70

PECB has developed a methodology based on best practices for implementing a cybersecurity program. This methodology is aligned with the cybersecurity guidelines provided in industry best practices, including ISO standards and NIST Cybersecurity Framework.

The methodology is built upon three main phases: Cybersecurity Program and Governance, Security Operations and Incident Response, and Testing, Monitoring, and Improvement. In turn, these phases are divided into steps, steps into activities, and activities into tasks. During this training course, the steps and activities will be presented in the chronological order of the course of an implementation program.

Tasks will not be detailed because they are specific for each project and depend on the organization’s context.

1.1.2 Align with Best Practices



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

PECB

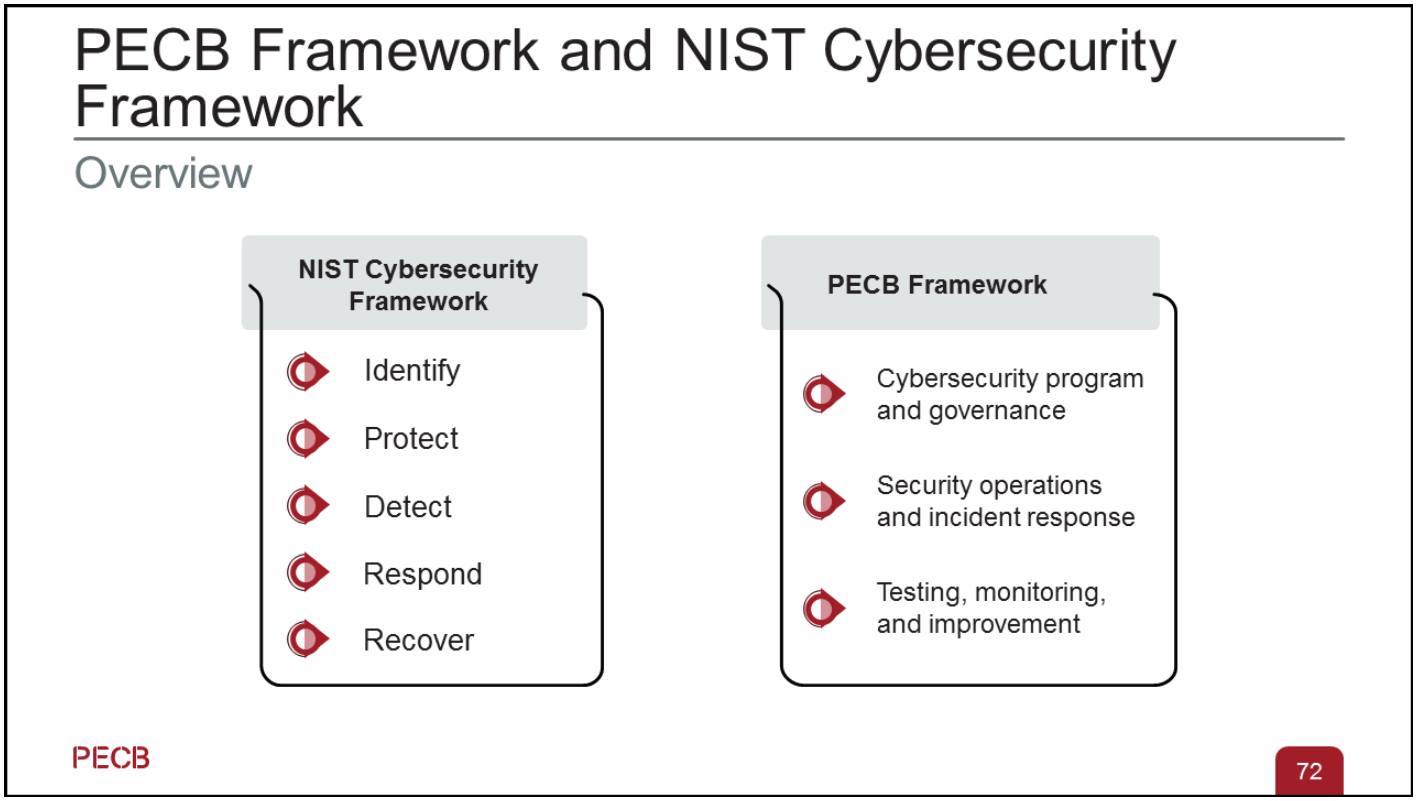
71

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

Good practices published in various ISO standards and NIST SP 800 series are presented in this training. However, there are several other sources of good practices, such as COBIT and the ITIL library.

Note on terminology

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



The PECB proposed framework closely aligns with the well-established steps outlined in NIST Cybersecurity Framework, providing organizations with a comprehensive approach to implement a cybersecurity program. By incorporating the five core principles of NIST Cybersecurity Framework, it offers an adaptable approach to address cybersecurity incidents.

Section Summary:

- A cybersecurity program is necessary to create a secure virtual environment of data.
- Frameworks can be used to create or improve the cybersecurity program.
- A structured methodology should be followed, but it can be adapted to the organization's needs.
- Many processes are iterative throughout the implementation of the cybersecurity program.
- There are some activities that should be followed to initiate the cybersecurity program. These activities include defining the approach to the cybersecurity program implementation, choosing a methodological framework to manage the implementation of a cybersecurity program, and aligning it with best practices.
- There are some factors that should be taken into account when defining the approach for the implementation of the cybersecurity program, such as the speed of implementation and deadlines, targeted maturity level of controls, expectations and scope, applicable laws and regulations, and management support.

Questions?

Quiz 3

PECB

73

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

This section provides information that will help participants understand the importance of identifying internal and external factors that affect the implementation of a cybersecurity program, the key processes and activities, identify business requirements and interested parties, and understand the process of conducting a gap analysis.

Cybersecurity Program Framework

1. CYBERSECURITY PROGRAM AND GOVERNANCE		2. SECURITY OPERATIONS AND INCIDENT RESPONSE		3. TESTING, MONITORING, AND IMPROVEMENT	
1.1	Cybersecurity program	2.1	Attack mechanisms	3.1	Testing in cybersecurity
1.2	**The organization and its context**	2.2	Cybersecurity controls	3.2	Measuring and reporting cybersecurity performance and metrics
1.3	Cybersecurity governance	2.3	Cybersecurity communication	3.3	Continual improvement
1.4	Cybersecurity roles and responsibilities	2.4	Awareness and training		
1.5	Asset management	2.5	ICT readiness in business continuity		
1.6	Risk management	2.6	Cybersecurity incident management		

PECB

NIST Recommendation

NIST Cybersecurity Framework

Business Environment (ID.BE): *The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.*

ID.BE-1: *The organization's role in the supply chain is identified and communicated*

ID.BE-2: *The organization's place in critical infrastructure and its industry sector is identified and communicated*

ID.BE-3: *Priorities for organizational mission, objectives, and activities are established and communicated*

ID.BE-4: *Dependencies and critical functions for delivery of critical services are established*

ID.BE-5: *Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations*

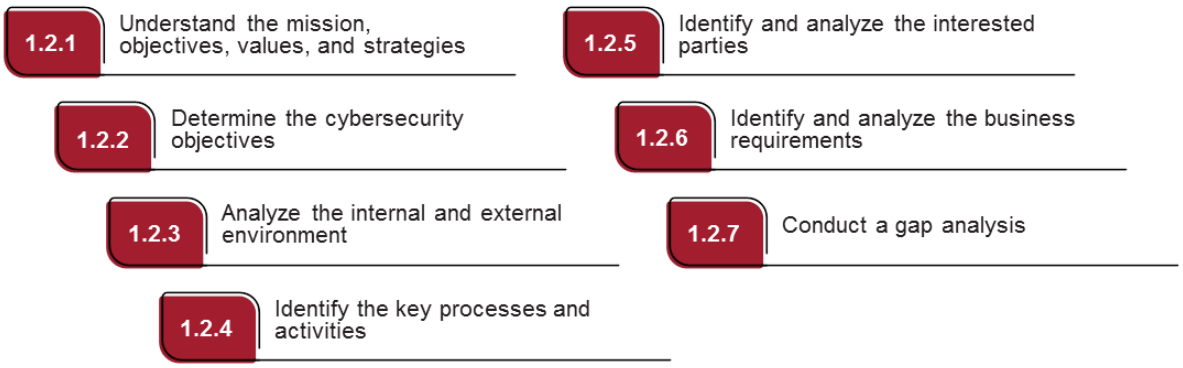
PECB

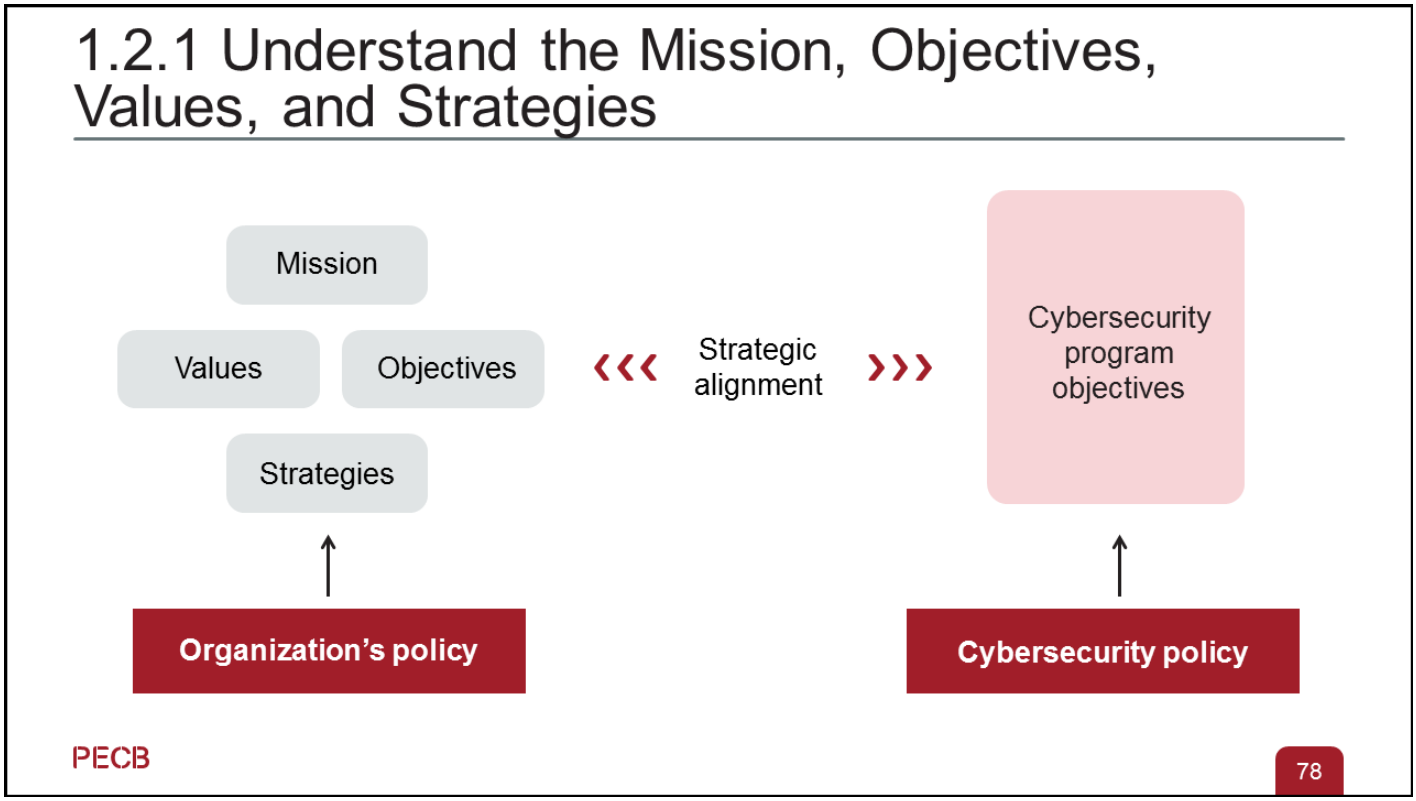
76

NIST Cybersecurity Framework core is a list of functions, categories, subcategories, and informative references describing cybersecurity activities. Each function and category have unique identifiers. Business environment (BE) is a category of the Identify (ID) function. Thus, its identifier is stated as ID.BE.

1.2 The Organization and Its Context

List of activities





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

Mission: The mission is what justifies and defines an organization's existence. It serves as a reference point to keep everyone clear on where the organization is headed.

Implications for cybersecurity program: The cybersecurity program aims to support the organization in fulfilling its mission, that is the protection of its information assets from cyber attacks. The cybersecurity program must, therefore, be aligned with the organization's mission.

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

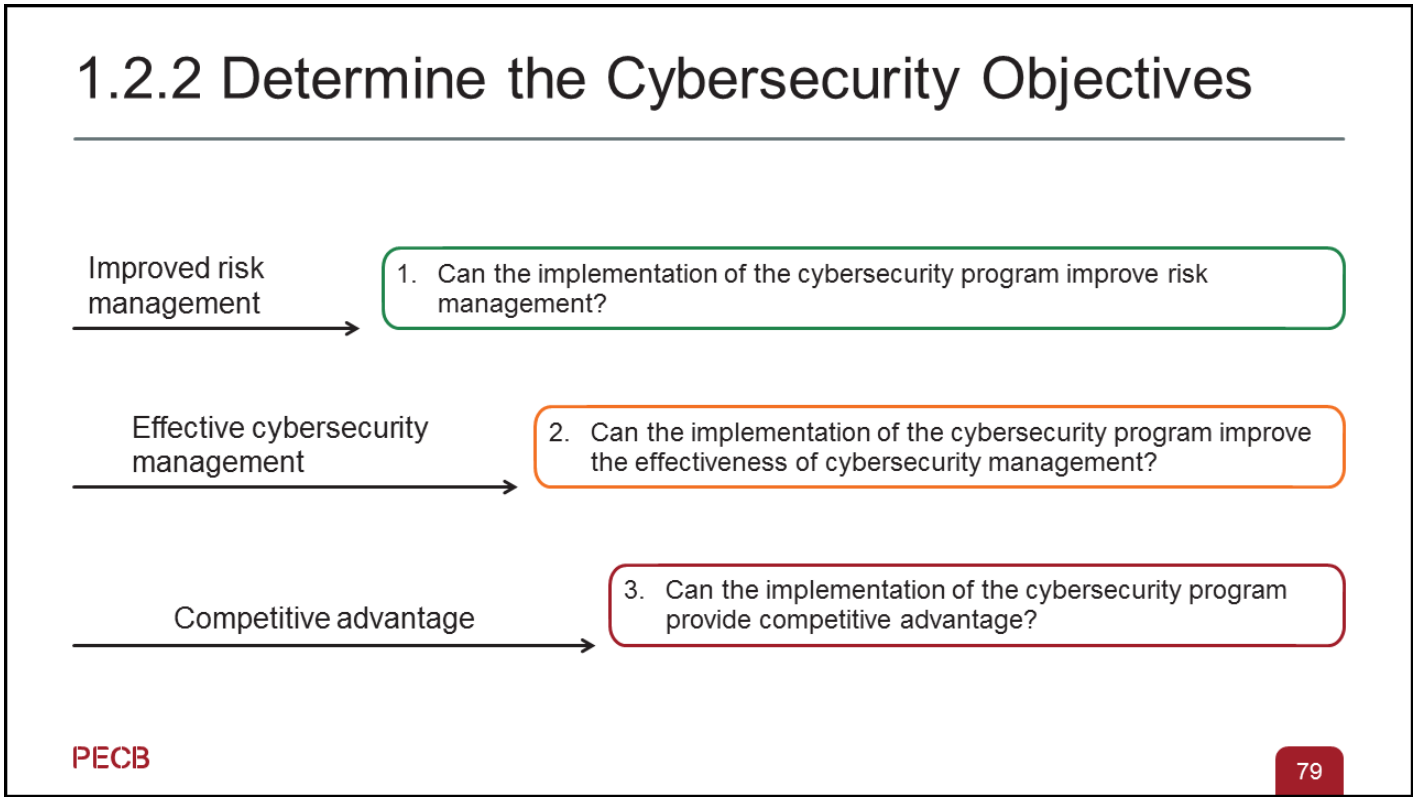
Implications for cybersecurity program: The values of the organization influence the choices made by professionals in cybersecurity program. For example, values can influence the priorities and policies in terms of evaluating cybersecurity risks.

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

Implications for cybersecurity program: As for strategy, the cybersecurity program must be aligned with the organization's objectives in order to achieve the ultimate objective and ensure that cybersecurity is achieved.

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

Implications for cybersecurity program: The choice and results of actions will also depend on the cybersecurity strategy defined by the organization.



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

The cybersecurity objectives must be validated at the highest level of the organization. Objectives can be modified as the implementation progresses, particularly after the completion of risk analysis. Objectives must be documented properly.

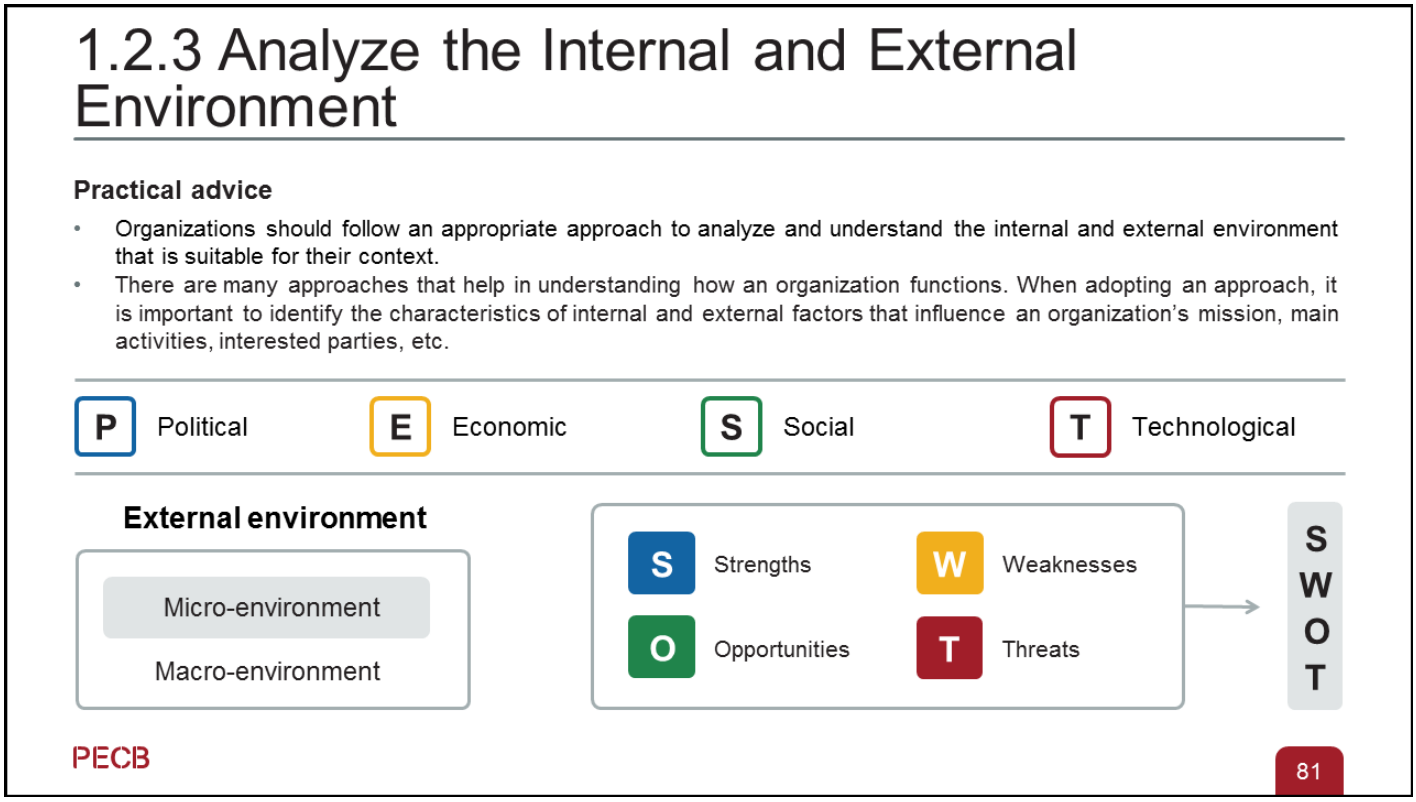
When determining the objectives, the following should be taken into account:

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

Examples of Cybersecurity Objectives

Examples of objectives related to the cybersecurity program implementation include, but are not limited to:

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



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

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

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

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

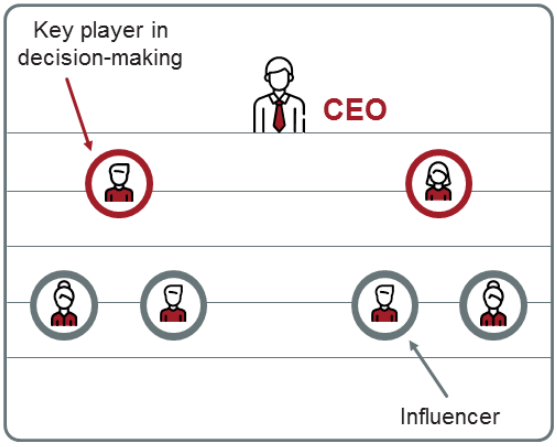
Porter's Five Forces analysis: Porter's Five Forces analysis examines the competitiveness level of an organization by employing the five factors that influence the business environment within an industry. These five forces consist of the intensity of rivalry among competitors, the bargaining power of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

Analyze the Internal and External Environment

Organizational structure and key players

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

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



PECB

82

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

The structure of an organization may be of different types:

1. **The divisional structure:** Each division is under the authority of a division director responsible for the strategic, administrative, and operational decisions within that unit.
2. **The functional structure:** The functional authority is exercised over proceedings, including planning and decision-making.

Notes:

- A division within the organization can be organized into functions and vice versa.
- An organization can have a matrix structure where the entire organization is based on the two structure types (divisional and functional).
- Whatever the structure, the following levels are distinguished:
    1. The strategic level (responsible for policies and the strategies)
    2. The steering level (responsible for the coordination and management of activities)
    3. The operational level (responsible for operations and other support activities)

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

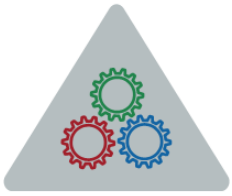
1.2.4 Identify the Key Processes and Activities

Assets

What are the key assets of the organization?

Organization's activities

What are the products and services offered by the organization?



Business processes

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

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

PECB

83

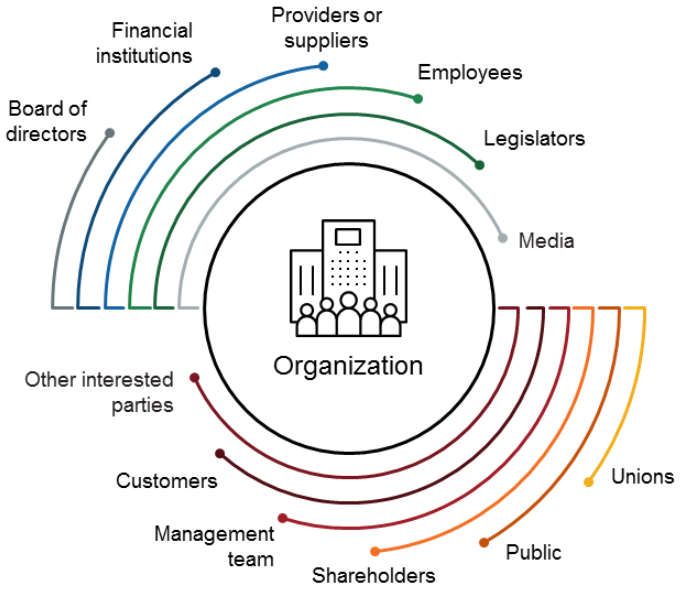
It is essential that the cybersecurity program manager is familiar with the organization's activities that affect cybersecurity. The type of products and services offered by the organization will certainly have a major impact on its business model. These products and services may also expose the organization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

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

The identification of the organization's assets is crucial when establishing a cybersecurity program. The increasingly complex technical management environments tend to enhance the rate of difficulty of protecting assets since such assets are subject to constant advancement. Thus, the cybersecurity program managers have to pay particular attention when they:

- Identify the owners of the assets
- Increase the owners' awareness of the value of the assets for which they are responsible
- Define a complete set of related security requirements for each asset
- Describe, unequivocally, where assets are stored, moved, and used
- Determine the value that the organization attaches to the evaluated assets that can be absolute (e.g., a purchase price or replacement) or relative (direct cost or indirect loss caused by this asset)

1.2.5 Identify and Analyze the Interested Parties



PECB

84

ISO 9000, clause 3.2.3 Interested party *(Stakeholder)*

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

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

ISO 9000, clause 3.2.4 Customer

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

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

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

ISO 9000, clause 3.2.5 Provider *(Supplier)*

Organization that provides a product or a service

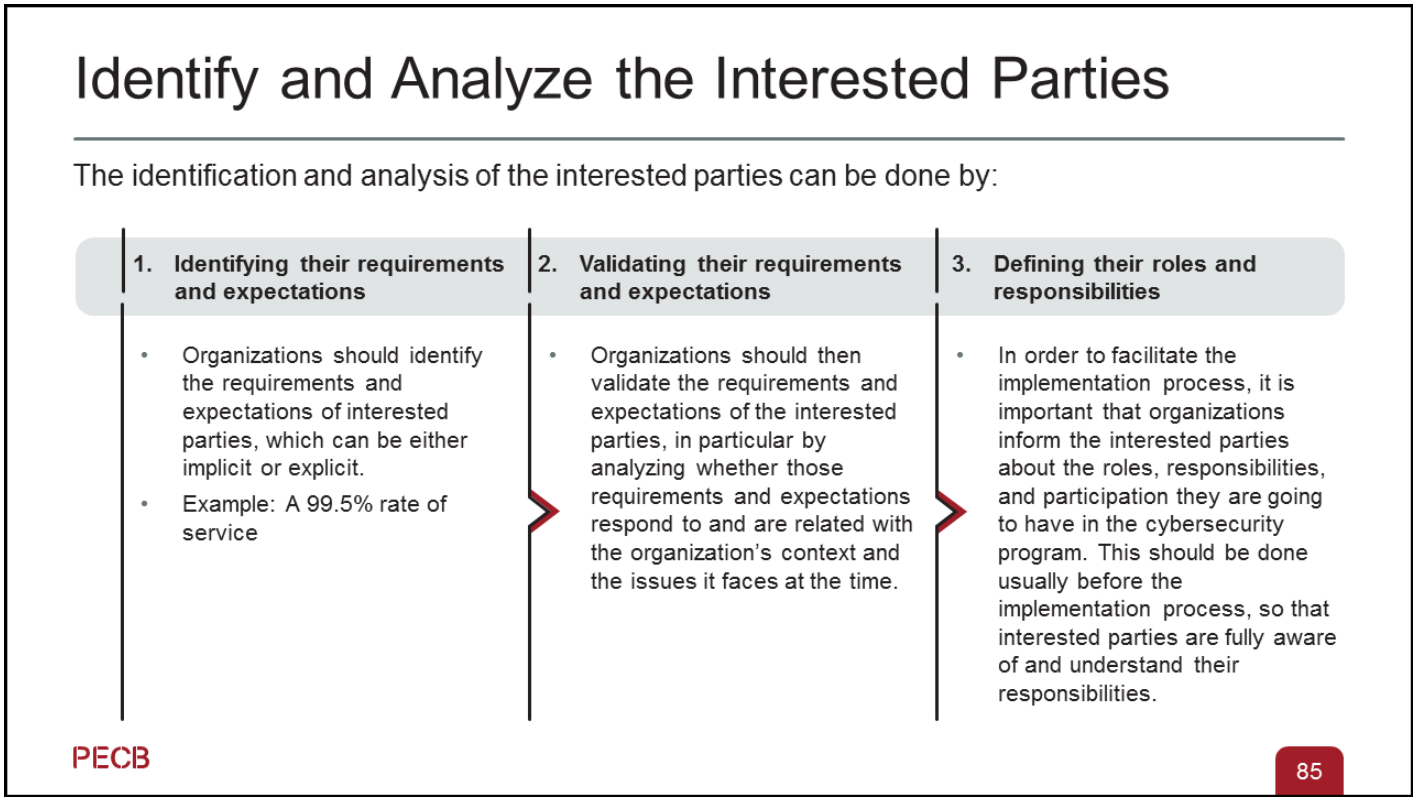
EXAMPLE Producer, distributor, retailer or vendor of a product or a service.

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

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

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

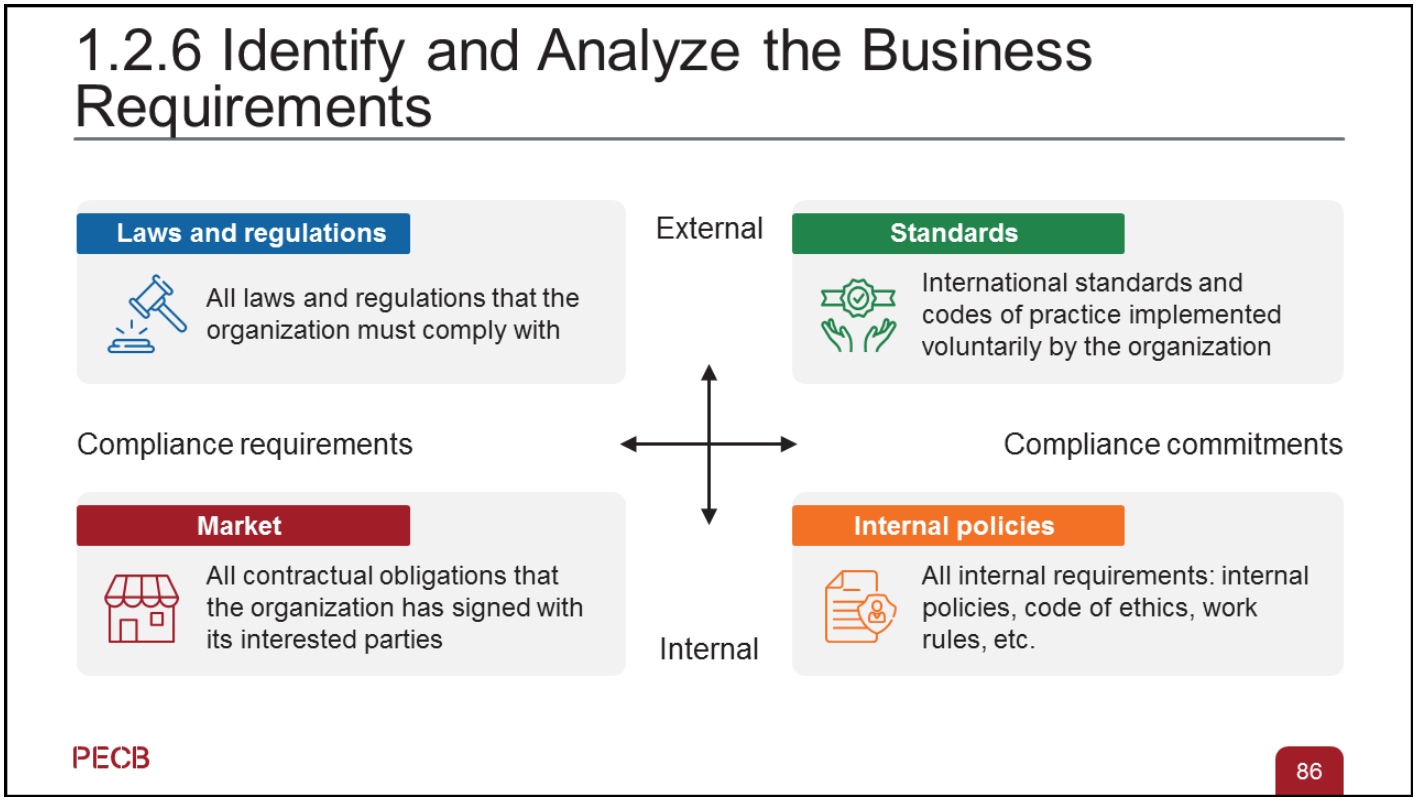
- How to approach the interested parties and how to manage them in the long term
- How to balance the different opinions and needs of interested parties
- How to categorize the interested parties when there are no clear boundaries between them, when multiple interested parties groups exist, or when there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



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

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

Organizations should inform all the interested parties of the actions taken regarding the cybersecurity program and of the impact and responsibilities they have in it.



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

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

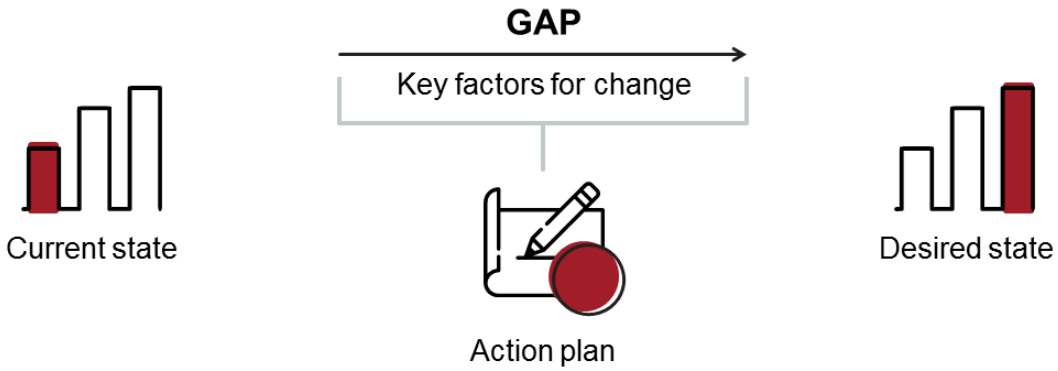
The cybersecurity requirements for all organizations are mainly derived from four sources:

1. **Laws and regulations:** This will be discussed in the following section.
2. **Standards:** Organizations must comply with a set of international standards and codes of practice related to their industry sector. Although the implementation of regulatory frameworks is a voluntary choice, from the cybersecurity management point of view, they become obligations to comply with (the risk of losing certification in case of serious failure).
3. **Market:** Market requirements include all contractual obligations that the organization has signed with its interested parties. A breach of contractual obligations may result in penalties (when stated in the contracts) or civil suits for damages. Market requirements are all implicit rules that an organization should fulfill in order to perform their businesses. For example, although the organization has no contractual obligation to deliver its products as planned, it goes without saying that this is a commercial policy basis to meet the scheduled delivery times. Failing to do so will lead to a loss of market share, customer trust, profits, etc.
4. **Internal policies:** Internal policies are principles, rules, and guidelines that include all the requirements defined within the organization: internal policies (human resources, food safety management, supply chain, etc.), ethical codes, and work rules. It is worth noting that not complying with internal policies does not necessarily involve any legal implications.

2.1.7 Conduct a Gap Analysis

Understanding gap analysis

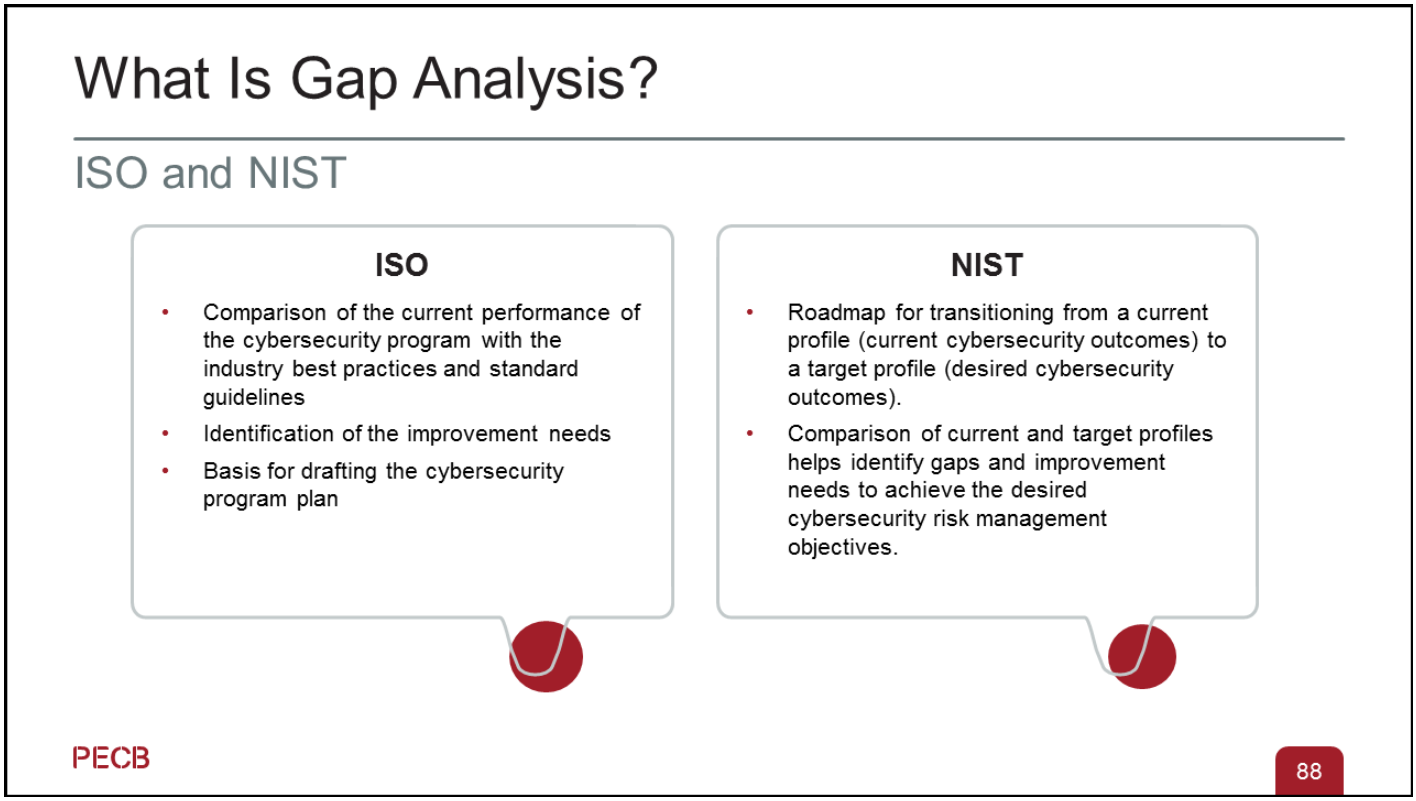
Gap analysis is a technique used to determine the steps to move from a current state to a desired state.



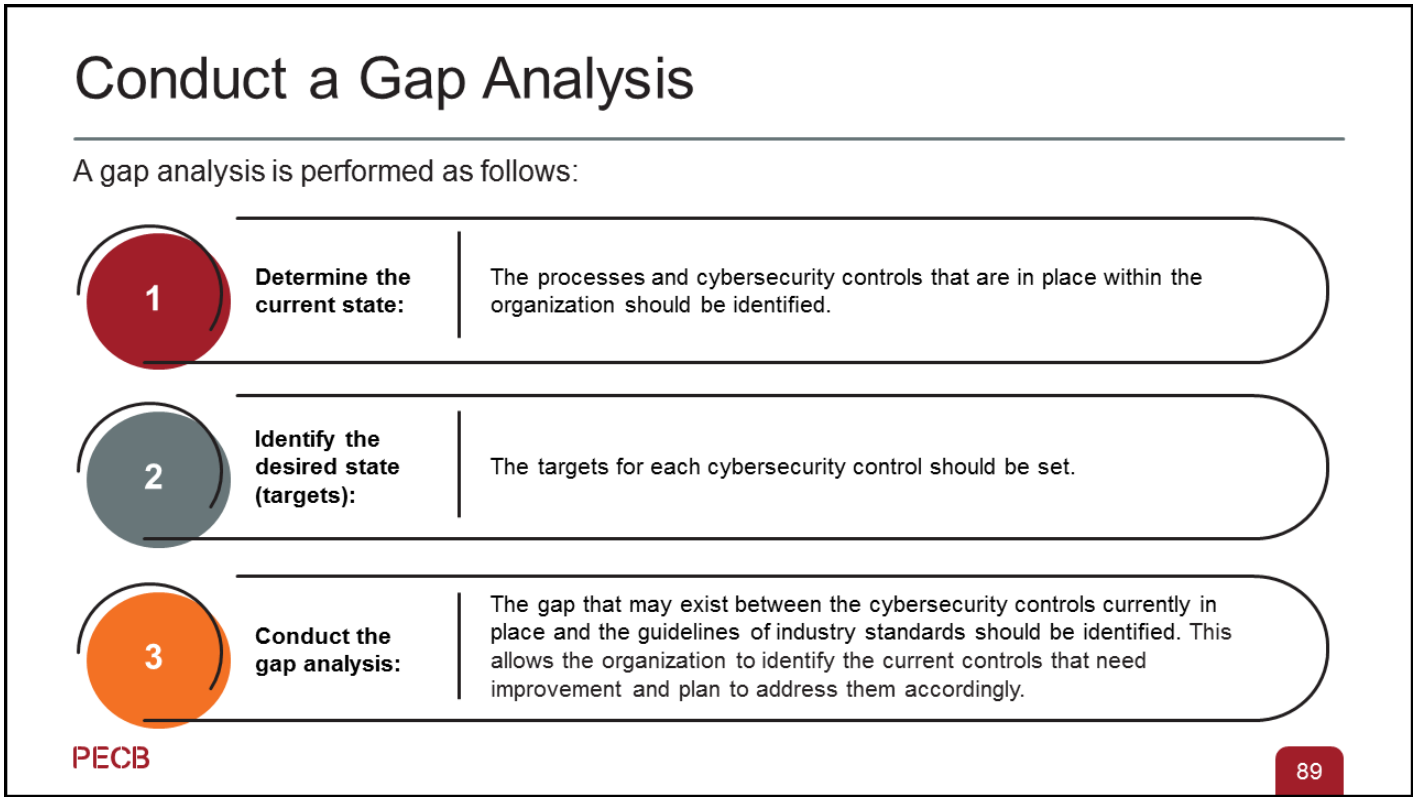
PECB

87

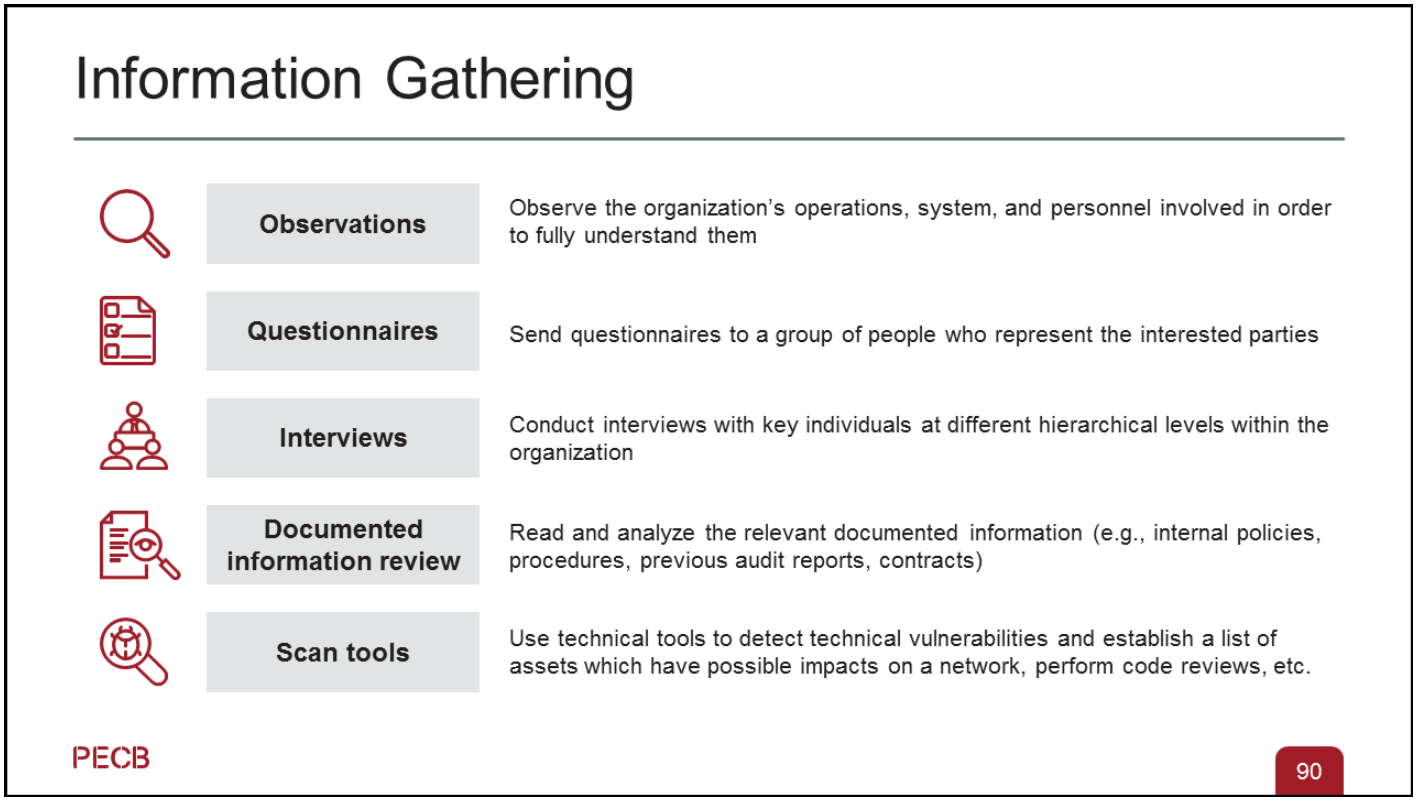
Gap analysis is conducted to determine the current state, the desired state, and the difference between the two.



The gap analysis technique, a shared element between the ISO and NIST cybersecurity frameworks, involves comparing the current state of cybersecurity practices against established standards and objectives to identify gaps and areas for enhancement. The difference lies in terminology and specific details of how they implement this process within their respective frameworks.



Gap analysis helps identifying and measuring investments in time, money, human, and other resources to effectively implement the cybersecurity program.



The cybersecurity program manager, in cooperation with the program team, should collect information from multiple interested parties in order to have an understanding of the existing cybersecurity program.

When determining the state of the existing cybersecurity program, the program manager should take into account many factors, such as the data collection method used, the individuals to be interviewed, their skills and knowledge, the availability of resources (e.g., budget, time), etc.

The following actions can be helpful in collecting information about an organization:

- Observe the organization's on-site physical security controls
- Conduct interviews with the individuals responsible for cybersecurity management and those responsible for the daily operations of the cybersecurity program
- Examine the documented information on cybersecurity processes, procedures, description of security controls, reports, etc.

Conduct Interviews

Recommendations when conducting interviews:

- Use open-ended questions and avoid close-ended or guiding questions
- Ensure that all subjects are covered in the predefined time for the interview
- Take notes during the interview
- Ask additional questions to clarify a response or situation

PECB

91

Preparation is one of the key elements of a productive interview. An effective strategy can be to create checklists that ensure a systematic conduct of interviews and obtainment of relevant information from them. Checklists should have a section for answers, comments, and observations, as well as references to the related standards, where applicable.

During the interview, it may be useful to clarify the specialized terminology related to security architecture using a language that is more comprehensible for the interviewees.

The interview can be recorded only if the interviewee agrees to it. However, the most common practice is to simply take notes. Recording the interview can be intimidating to the interviewee and could have a negative impact on the outcomes of the interview.

The interview notes should contain the following:

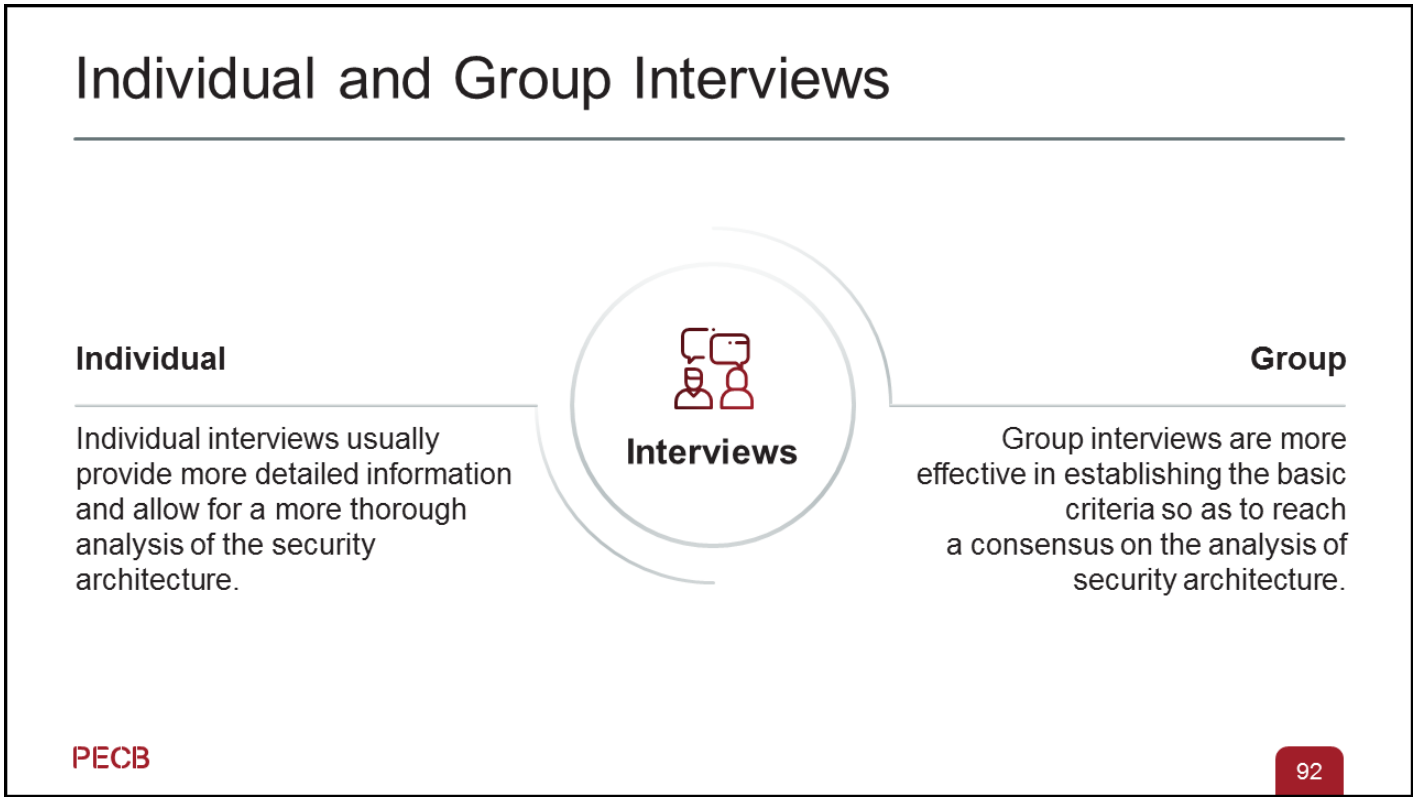
Function of the interviewee and date (due to the principle of confidentiality, the name of the interviewee is not included in the interview notes, unless the interview is a member of the management)

Example: Discussion with an employee from the IT Department, February 20, 2021

Interview objectives

Example: Validating whether the organization has conducted trainings in accordance with its policy

Summary of the collected evidence (The documented information should be collected in a clear, concise, and accurate language; only facts, not judgments, should be included; any weaknesses should be identified and reported in the gap analysis; the reference to the related standard should be listed with the clause number.)



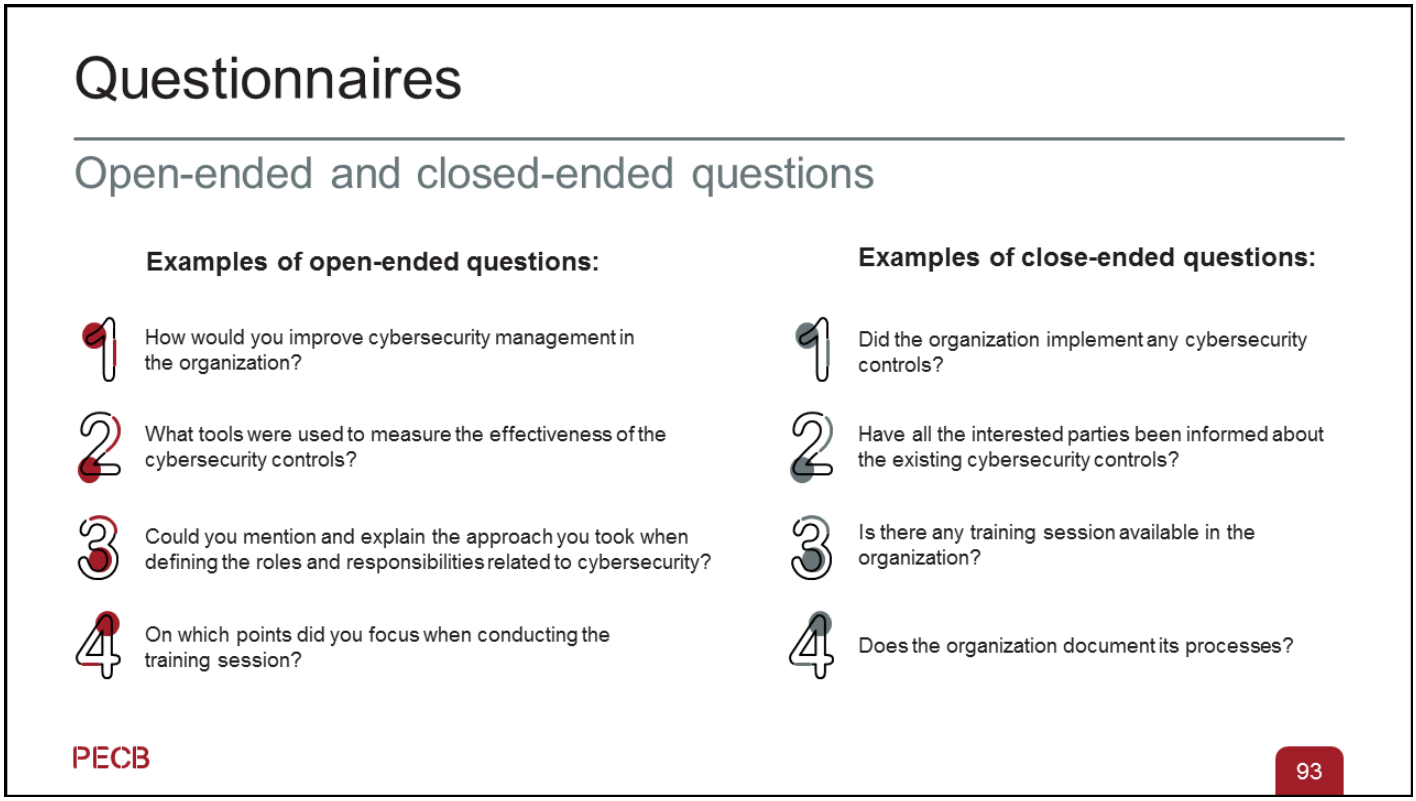
All interested parties' members, be them experts or not, should be interviewed regarding their activities and tasks in order to obtain information regarding cybersecurity risks in their field. Individuals responsible for business processes will provide a much more "business" oriented view on risks, e.g., the public relations officer will indicate concerns about a risk in the organization's reputation.

Individual interviews:

The most significant advantage of individual interviews is that interviewing only one person at a time allows the interviewer to obtain more detailed information about the security architecture. In this way, the interviewer will be able to get a more comprehensive understanding of the organization and its security architecture. The interviewer is able to read the body language of the interviewee and can ask for further explanation of responses. However, the interview length can be time-consuming if there are a lot of people to be interviewed.

Group interviews:

Group interviews are helpful when there is little time to conduct individual interviews or when the interviewer wants to examine the interaction between the group members. However, group interviews can produce unnatural responses, since a dominant member of the group may influence the response of others, known otherwise as the "bandwagon effect."



The current state of the cybersecurity can be determined by the project team or outsourced to external consultants. External consultants may generate more neutral reports from the organization than the project team. In most cases, the current state of the cybersecurity controls is determined by the reports received from questionnaires that, depending on the choice or context, will be sent in writing or electronically.

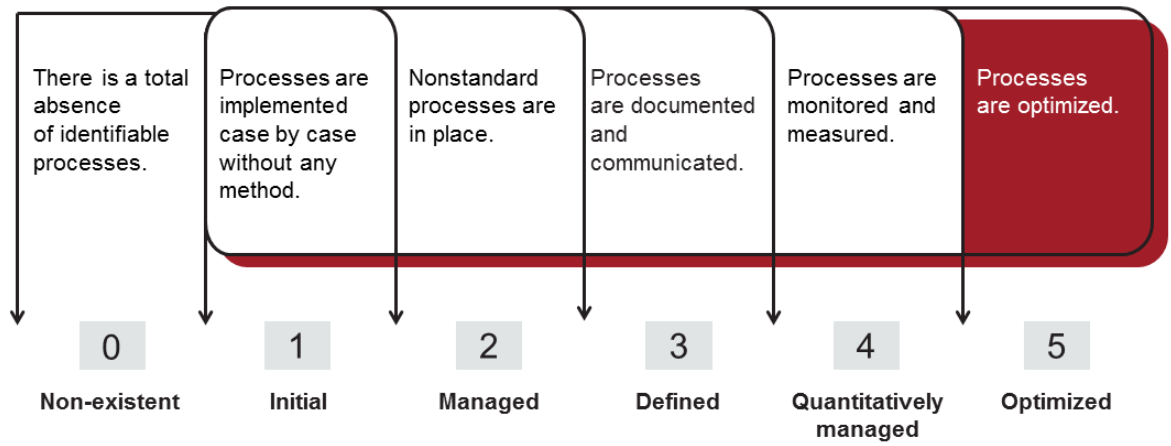
When using questionnaires, questions can be:

- **Open-ended:** This type of questionnaire generates answers that are detailed and clarified. Interviewers obtain more valuable and complete information about the security architecture. However, these answers can sometimes be difficult to analyze due to the length of the content or response rate.
- **Closed-ended:** This type of questionnaire generates answers easier and faster. This type is useful for gaining general opinions about the security architecture. However, interviewers will lack the information or reasoning behind the answers.

Establish Maturity Targets

Gap analysis and the level of maturity

Targets for processes and cybersecurity controls can be set based on target maturity levels:



PECB

94

0.Nonexistent: The organization is not aware that there is a total absence of the identifiable process.

1.Initial: The organization has some processes that are implemented but there is no standardized procedure to do this.

2.Managed: The organization has some processes that are implemented using the same procedure, but there are no training and communication sessions performed with regard to these procedures. People implementing these processes rely on personal knowledge, where the probability of error is high.

3.Defined: The organization has standardized, documented, and communicated the procedure in the training sessions. However, there is still a margin for error since these procedures are used only on individual initiatives.

4.Quantitatively managed: The organization is able to monitor and measure whether these processes are implemented as required and take action when procedures are not fully functional. The organization constantly improves these processes but there is limited or partial use of automation and tools.

5.Optimized: The organization's processes have reached a top-quality level following continual improvement and compliance with best practices. Computers are being used to automate integrated workflow in order to improve quality and efficiency and allow the organization to quickly adapt to new situations.

Establish Maturity Targets and Analysis

Example 2: Gap analysis in the context of NIST Cybersecurity Framework

Clause	Requirement	Description of the actual situation	Current maturity	Target maturity	Gap analysis	Responsible
ID.AM-6	*Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established*	The formal document stating the cybersecurity roles and responsibilities in the organization has existed for more than six months but it has not been formally reviewed by the management yet. Currently, there is no scheduled review.	2	5	The management is responsible for reviewing and approving the document. However, there is no scheduled review and employees do not have a formal job responsibilities document.	Robert Johnson, CISO

PECB

95

The list of controls of NIST Cybersecurity Framework can be used for the identification of existing and planned cybersecurity controls in an organization. This helps to get an overview of the existing status in relation to security best practices.

Present the Gap Analysis Report

Example of the content of a gap analysis report

- Introduction
  - Report objective
  - Methodology
- Baseline of the current cybersecurity controls
  - Available tools and processes
  - Challenges with the available tools, processes, and resources
- Cybersecurity focused decision-making framework
  - Identify and select a project
  - Predict the outcomes of the cybersecurity controls
  - Implement the cybersecurity program
- Identification and analysis of gap(s)
- Suggested bridging options
- Summary and next steps to be taken

Section Summary:

- In accordance with NIST recommendations, understanding an organization's mission, objectives, stakeholders, and activities shapes cybersecurity roles, responsibilities, and risk management decisions.
- To determine cybersecurity objectives, organizations should evaluate whether the program implementation enhances risk management, improves the effectiveness of cybersecurity management, and provides a potential competitive advantage.
- Different methods assist in understanding how organizations operate; when choosing one, it is important to recognize the traits of both internal and external factors that affect an organization's mission, activities, and stakeholders.
- The cybersecurity requirements for all organizations derive from laws and regulations, markets, internal policies, and standards.
- Gap analysis is conducted in order to define the steps to move from a current to a desired state.
- There are six maturity levels that are helpful in setting targets for security controls: nonexistent, initial, managed, defined, quantitatively managed, and optimized.

Questions?

Quiz 4

PECB

97

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

This section provides information that will help participants understand the critical role of cybersecurity governance and regulatory compliance, as well as the use of established cybersecurity frameworks. Additionally, this section provides information on different types of policies, policy models, and the importance of a cybersecurity policy, including specific security policies.

Cybersecurity Program Framework

1. CYBERSECURITY PROGRAM AND GOVERNANCE	2. SECURITY OPERATIONS AND INCIDENT RESPONSE	3. TESTING, MONITORING, AND IMPROVEMENT
1.1 Cybersecurity program	2.1 Attack mechanisms	3.1 Testing in cybersecurity
1.2 The organization and its context	2.2 Cybersecurity controls	3.2 Measuring and reporting cybersecurity performance and metrics
1.3 Cybersecurity governance	2.3 Cybersecurity communication	3.3 Continual improvement
1.4 Cybersecurity roles and responsibilities	2.4 Awareness and training	
1.5 Asset management	2.5 ICT readiness in business continuity	
1.6 Risk management	2.6 Cybersecurity incident management	

PECB

Cybersecurity Governance

- Cybersecurity governance is the set of policies, processes, and procedures that guide the approach of the organization to manage cybersecurity. It should be incorporated into an organization's operations and aims to protect against cyber threats.
- There are five main principles of cybersecurity governance:
  - Define roles and responsibilities
  - Develop, implement, and improve a comprehensive cyber strategy
  - Integrate cybersecurity into the existing risk management process
  - Encourage a culture of cyber resilience
  - Plan for cybersecurity incidents

PECB

100

Define roles and responsibilities: The process of defining roles and responsibilities is a crucial element in building a strong defense against cyber threats. Ensuring clear and comprehensive reporting to the board, which includes effective communication with management and updates on emerging trends, plays a vital role in the board's assessment of the organization's cyber resilience.

Develop, implement, and improve a comprehensive cyber strategy: By actively overseeing a cyber strategy, the board can potentially support business expansion by identifying opportunities for the organization to enhance its ability to withstand cyber threats.

Integrate cybersecurity into existing risk management procedures: Cyber risk falls under the category of operational risk and aligns with the organization's existing approach to risk management. It is essential for the board to periodically assess the effectiveness of cyber controls to adapt to evolving threats, technological advancements, and the organization's capabilities.

Encourage a culture of cyber resilience: Consistent, interactive, and relevant training is an important method for fostering a cybersecurity culture.

Plan for cybersecurity incidents: Maintaining transparent and open channels of communication with key interested parties during a significant cyber attack is crucial for minimizing the damage to organization's reputation and facilitating a successful recovery.

Source: Australian Institute of Company Directors. "Cyber Security Governance Principles." Last Modified October, 2022. https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf

Cybersecurity Regulatory Compliance

- Regulatory compliance refers to a collection of guidelines that organizations must follow in order to safeguard sensitive information and ensure human safety.
- Cybersecurity compliance evaluates potential risks by following security standards and regulations and helps to maintain the confidentiality of data.
- The procedure entails taking preventive measures to avoid security breaches, creating protocols to mitigate them, and developing a contingency plan in case a breach occurs, which also includes providing support to impacted individuals.

PECB

101

Sources:

BusinessCloud. “Cybersecurity Compliance: What, Why, and How?” Last modified March 21, 2022. https://businesscloud.co.uk/news/cybersecurity-compliance-what-why-and-how/

Proofpoint. “What Is Regulatory Compliance?” Last accessed April 13, 2023. https://www.proofpoint.com/us/threat-reference/regulatory-compliance

Benefits of Cybersecurity Compliance

- Prevent penalties and fines resulting from noncompliance
- Establish customer confidence and promote brand reputation
- Strengthen data management practices
- Enhance security measures
- Improve access controls and accountability

PECB

102

Source: Ciufo Brian, “Check Out Five Cybersecurity Compliance Benefits.” NetComLearning. Last modified March 06, 2023. https://www.netcomlearning.com/blogs/502/check-out-five-cybersecurity-compliance-benefits.html

1.3 Cybersecurity Governance

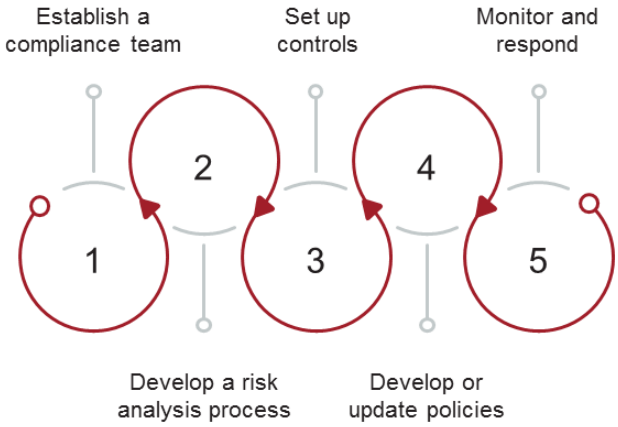
List of activities

1.3.1 Develop the cybersecurity compliance program

1.3.2 Develop the cybersecurity policy

1.3.1 Develop the Cybersecurity Compliance Program

Steps for developing a compliance plan



PECB

104

1. **Establish a compliance team:** The organization should establish a team responsible for evaluating and overseeing cybersecurity. This team should be established as a cross-functional capacity to guarantee that their actions are in line with the organization's business and IT requirements and procedures.
2. **Develop a risk analysis process:** In addition to determining the legal obligations for protecting its assets, the organization must also identify all of the information resources, systems, data, and networks that are essential for its operations.
3. **Set up controls:** The organization should establish controls to adhere to cybersecurity standards. Such controls typically include firewalls, encryption, password policies, and so on.
4. **Develop or update policies:** Having policies for updating documentation simplifies the process of meeting regulatory requirements for information on the organization's cybersecurity programs.
5. **Monitor and respond:** Continuous monitoring is crucial for detecting emerging threats, and an effective compliance program should aim to respond to these threats promptly to prevent data breaches.

Sources:

Baja, Sanjay, and Mark Weston. “The A-Z of Cybersecurity Compliance Frameworks.” Birlasoft. Last modified Jun 08, 2021. https://www.birlasoft.com/articles/the-a-z-of-cybersecurity-compliance-frameworks

Walsh Karen. “Cybersecurity Compliance 101.” Zeguro. Last modified November 24, 2020. https://www.zeguro.com/blog/cybersecurity-compliance-101

Cybersecurity Frameworks

The following are some guidelines on cybersecurity that organizations can use to meet industry standards:

PECB

105

- ISO has developed several standards on cybersecurity covering the baseline security practices that organizations need to ensure the security of their assets in the cyberspace. For example, ISO/IEC TS 27110 provides guidelines for developing a cybersecurity framework.
- NIST Cybersecurity Framework has been published as a response to the need to establish a set of voluntary cybersecurity standards for critical infrastructure organizations. The framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management process.
- COBIT is a framework issued by ISACA and is mostly used in Europe. It provides a framework focused on information governance and risk management by presenting activities in a manageable and logical structure. COBIT is strongly focused on control rather than execution.

ISO/IEC TS 27110 Framework

ISO/IEC TS 27110

The standard provides a set of concepts that should be included in a cybersecurity framework: Identify, Protect, Detect, Respond, and Recover. These concepts serve as foundational pillars for structuring and developing a cybersecurity framework.

The cybersecurity framework can include standards, guidelines, and practices to promote effective cybersecurity risk management.

PECB

106

- **Identify concept:** Focuses on developing the cybersecurity ecosystem under consideration
- **Protect concept:** Establishes safeguards to protect an organization's cyber persona, ensuring the effectiveness of preventative controls, and maintaining readiness to deliver critical services while safeguarding operations and information security
- **Detect concept:** Involves developing activities to detect cybersecurity events effectively
- **Respond concept:** Focuses on developing activities related to responding to cybersecurity events
- **Recover concept:** Involves developing the restoration and communication activities after a cybersecurity event

Although a cybersecurity framework is not mandatory for implementing an ISMS based on ISO/IEC 27001, the two approaches can be complementary. Combining a cybersecurity framework with an ISMS allows for effective implementation and communication of information security and cybersecurity activities.

NIST Cybersecurity Framework

- NIST Cybersecurity Framework helps organizations reduce and manage cybersecurity risks.
- The framework provides mechanisms to describe the current cybersecurity state and the target state, identify and prioritize opportunities for improvement, assess progress toward the target state, and communicate cybersecurity risks with stakeholders.

PECB

107

NIST Cybersecurity Framework does not introduce new standards or concepts. Instead, it leverages and integrates industry-leading cybersecurity practices. The framework aims to improve cybersecurity risk management in critical infrastructure and comprises a risk-based compilation of guidelines that help organizations identify, implement, and improve cybersecurity practices by also creating a common language for internal and external communication of cybersecurity risks.

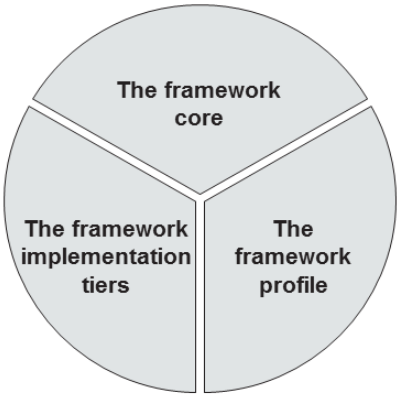
Organizations can use NIST Cybersecurity Framework in their current processes to determine gaps in their cybersecurity risk approach.

NIST Cybersecurity Framework

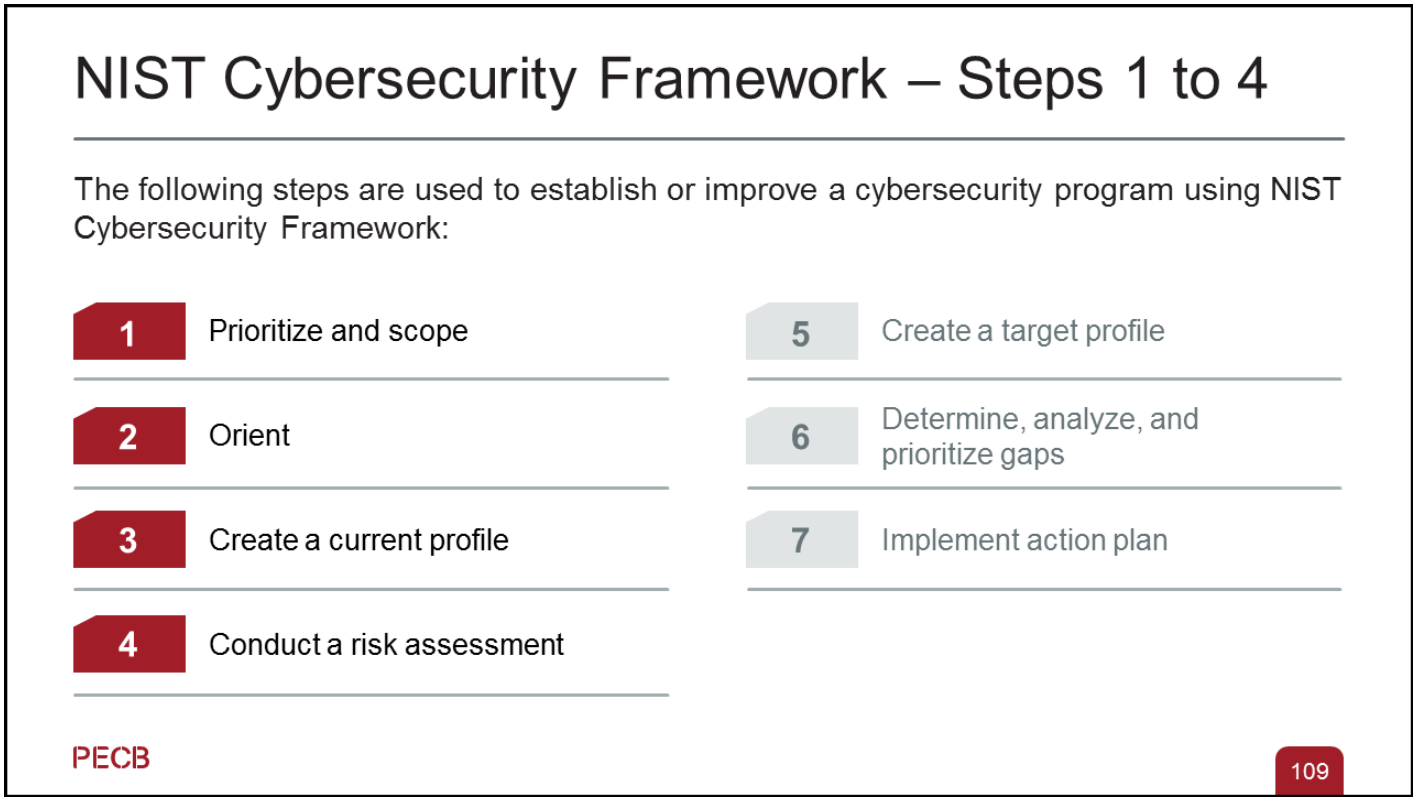
Overview of the framework

The framework core includes common cybersecurity activities, desired outcomes, and references in the critical infrastructure sectors. It provides an overall view of the management of cybersecurity risk life cycle in an organization using its five functions. The framework core functions are: identify, protect, detect, respond, and recover.

The framework implementation tiers uses four tiers to present the organization's cybersecurity risk and processes to manage this risk. The fours tiers are Tier 1: Partial, Tier 2: Risk Informed, Tier 3: Repeatable, and Tier 4: Adaptive.



The framework profile is used to identify opportunities for improvement and is based on the business needs of an organization. It is the alignment of standards, guidelines, and practices of the framework core.



NIST, Framework for Improving Critical Infrastructure Cybersecurity, clause 3.2 Establishing or Improving a Cybersecurity Program

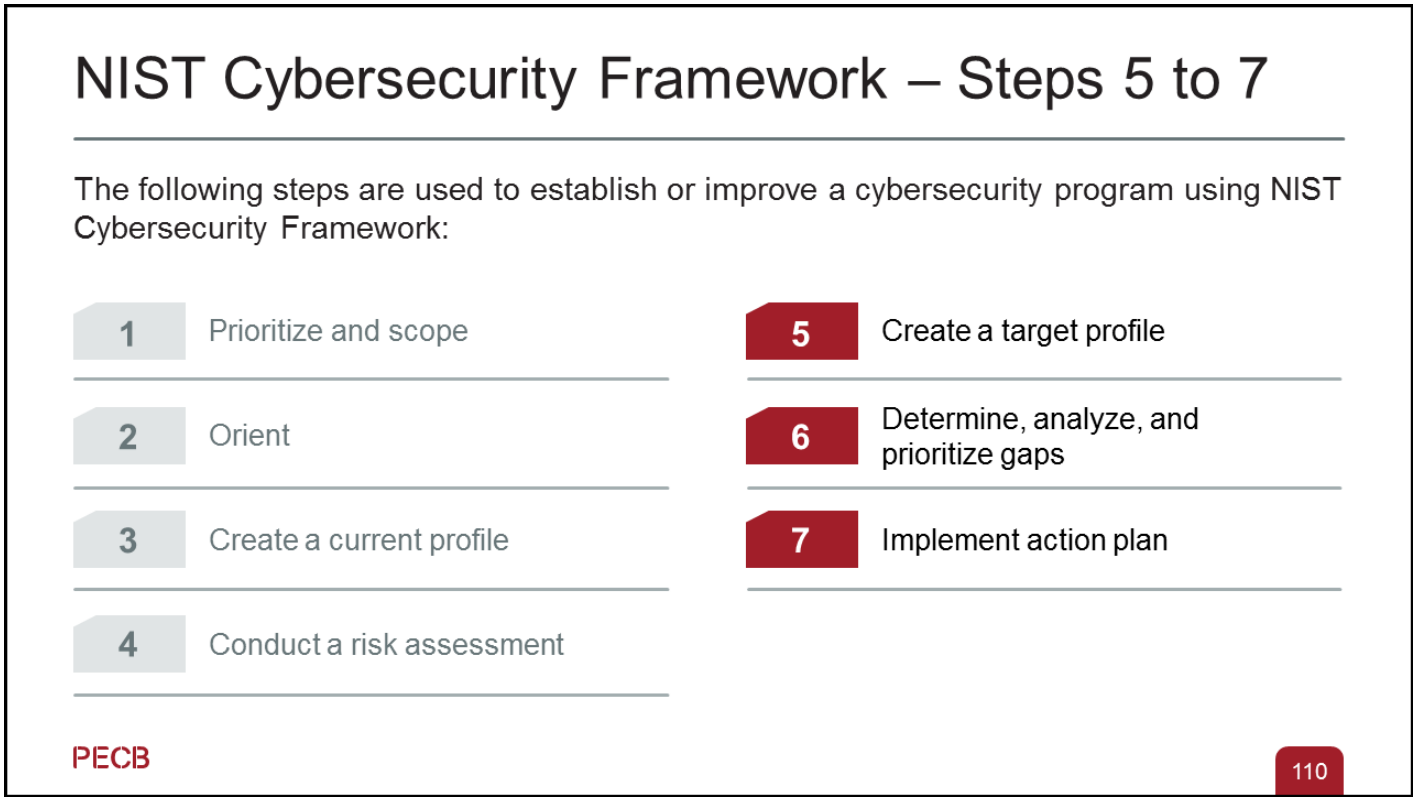
The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. *The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.*

Step 2: Orient. *Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.*

Step 3: Create a Current Profile. *The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.*

Step 4: Conduct a Risk Assessment. *This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.*



***Step 5: Create a Target Profile**. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.*

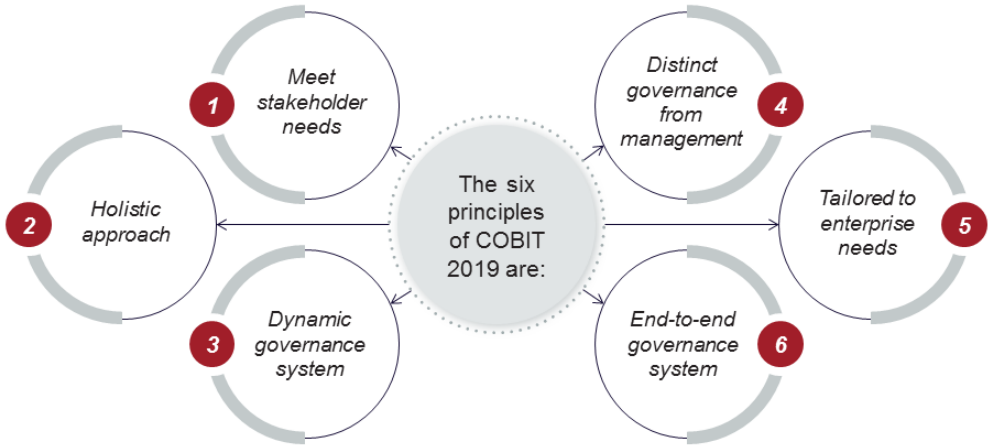
***Step 6: Determine, Analyze, and Prioritize Gaps**. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.*

***Step 7: Implement Action Plan**. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.*

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

Control Objectives for Information and Related Technologies (COBIT)

COBIT 2019, the latest version of the COBIT Framework, is both comprehensive and adaptable. Compared to COBIT 5, which had five governing principles, COBIT 2019 has six. Furthermore, the framework now supports 40 processes to aid in achieving management objectives and governance, an increase from the previous 37 processes.



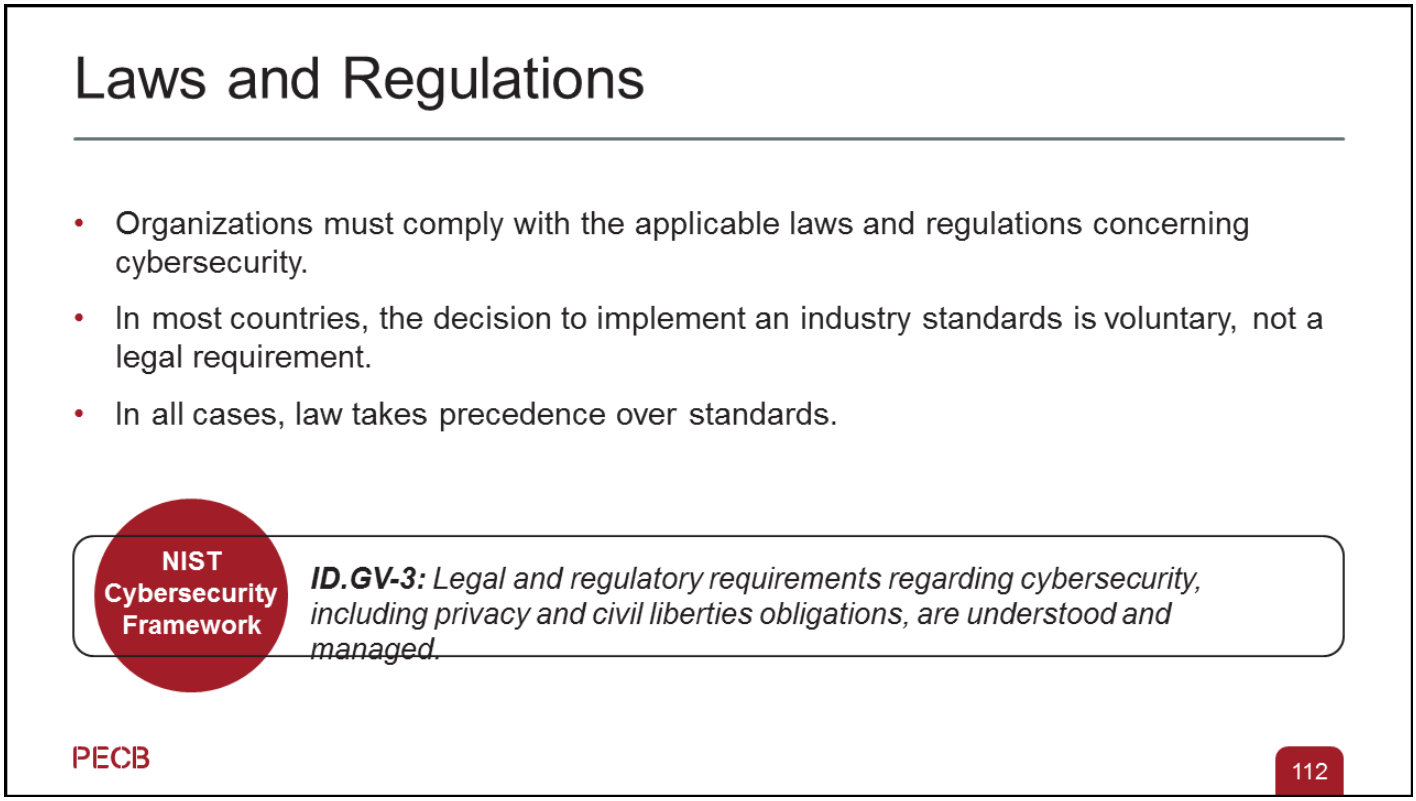
PECB

111

COBIT serves as a valuable resource for managers, enabling them to effectively distinguish technical challenges, business risks, and control demands.

In essence, COBIT guarantees the high standard, governance, and trustworthiness of information systems within an organization.

Source: Simplilearn. "What Is COBIT? Understanding the OCBIT Framework." Last modified February 21, 2023. https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article



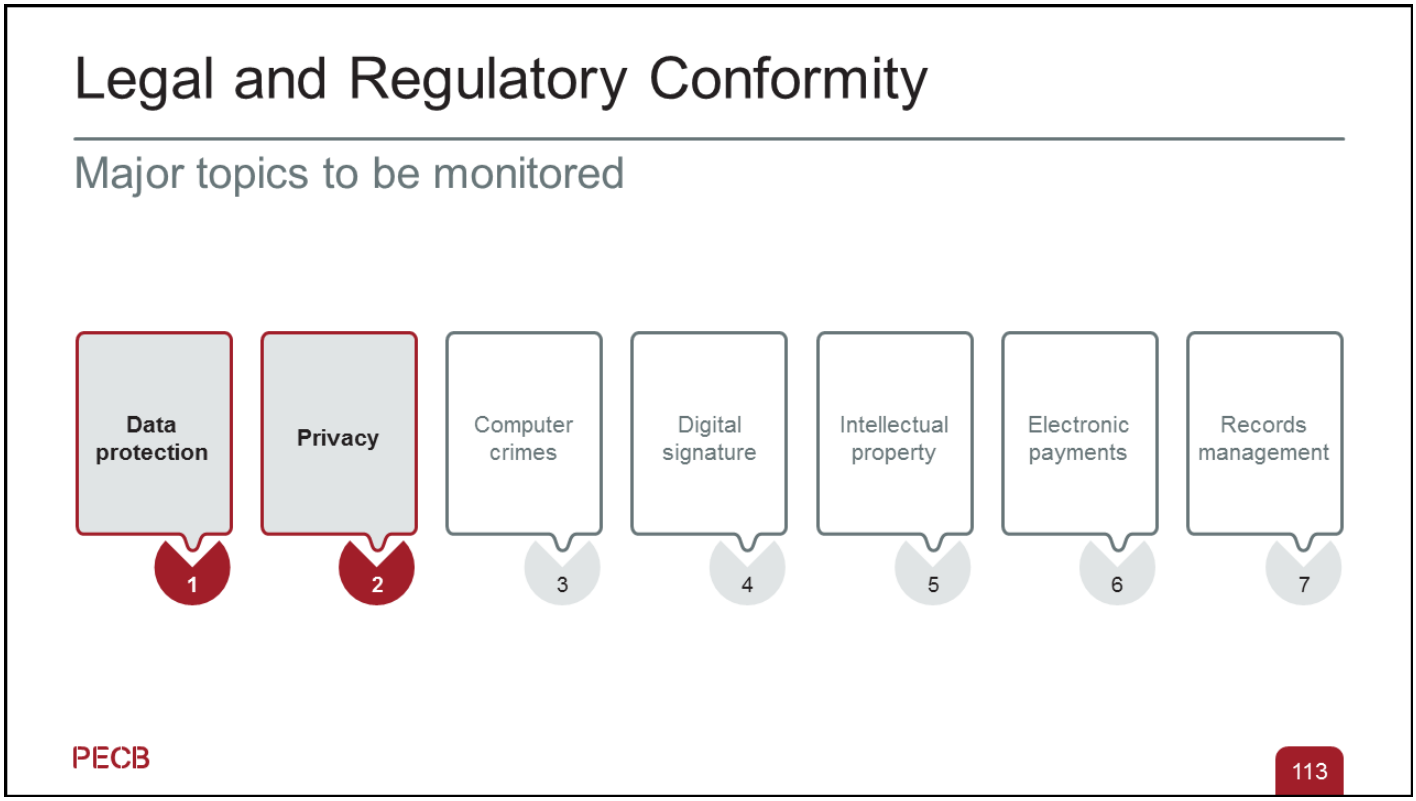
ISO/IEC 27002, clause 5.31 Legal, statutory, regulatory and contractual requirements

Guidance

General

External requirements including legal, statutory, regulatory or contractual requirements should be taken into consideration when:

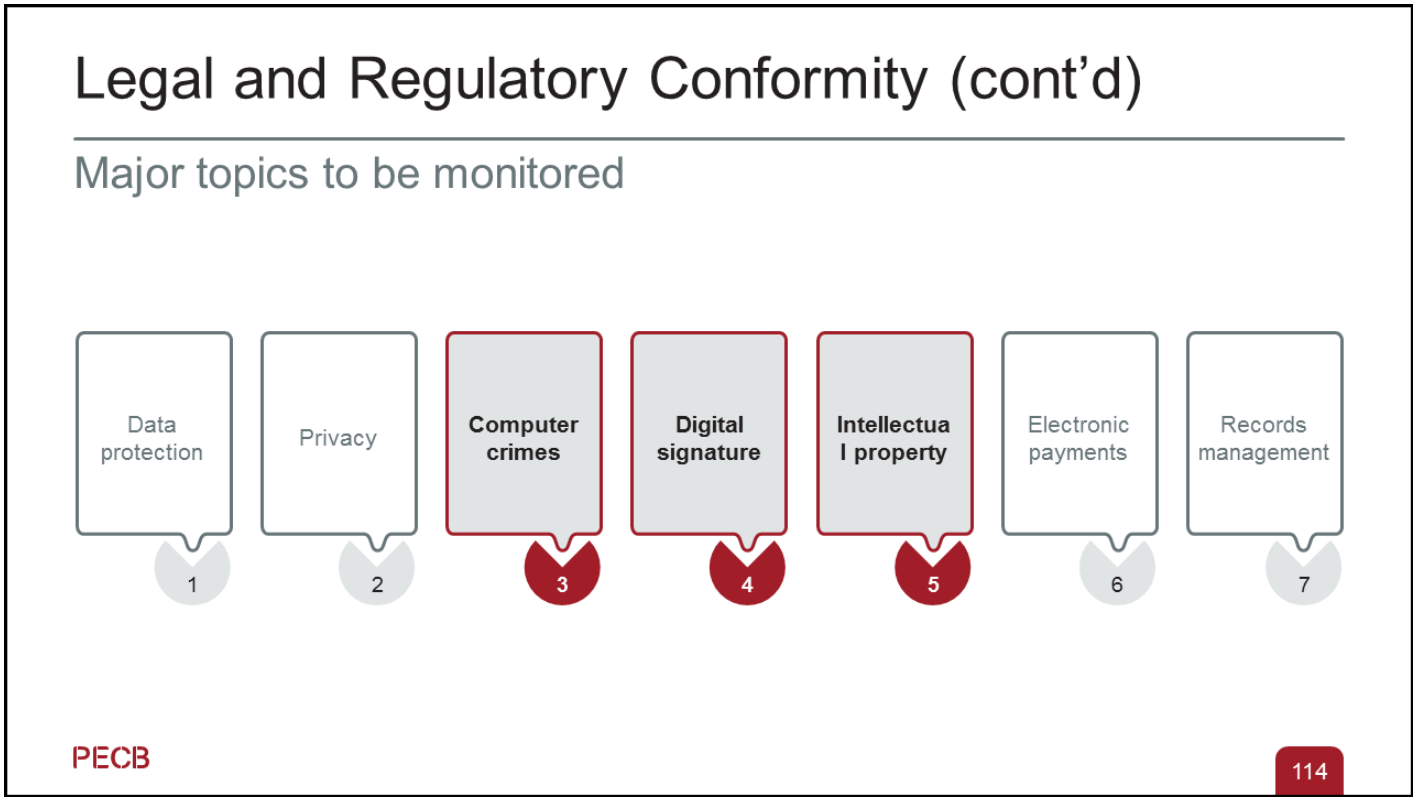
a. *developing information security policies and procedures;*
b. *designing, implementing or changing information security controls;*
c. *classifying information and other associated assets as part of the process for setting information security requirements for internal needs or for supplier agreements;*
d. *performing information security risk assessments and determining information security risk treatment activities;*
e. *determining processes along with related roles and responsibilities relating to information security;*
f. *determining suppliers' contractual requirements relevant to the organization and the scope of supply of products and services.*



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

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

1. **Data protection**
    - In several countries, specific laws cover the safeguarding of confidentiality and data integrity, often limited to the control of personal data, for example, the General Data Protection Regulation (GDPR) in Europe. In the same way that security incidents must be related to the individuals who caused it, personal information should be subject to management and adequate recording. A structured approach for incident management related to cybersecurity should, therefore, manage the most appropriate measures to protect the privacy and personal data of individuals.
2. **Privacy**
    - In compliance with applicable laws, many organizations choose to establish a policy for the protection of privacy, often designed to achieve the following objectives:
        - Increase awareness of regulatory, legal, and business requirements regarding the handling and protection of personal information
        - Establish a clear and complete policy for the treatment of personal information
        - Define the responsibilities of all persons dealing with personal information
        - Enable the organization to meet its commercial liability and legal and regulatory obligations with regard to personal information



3.Computer crimes

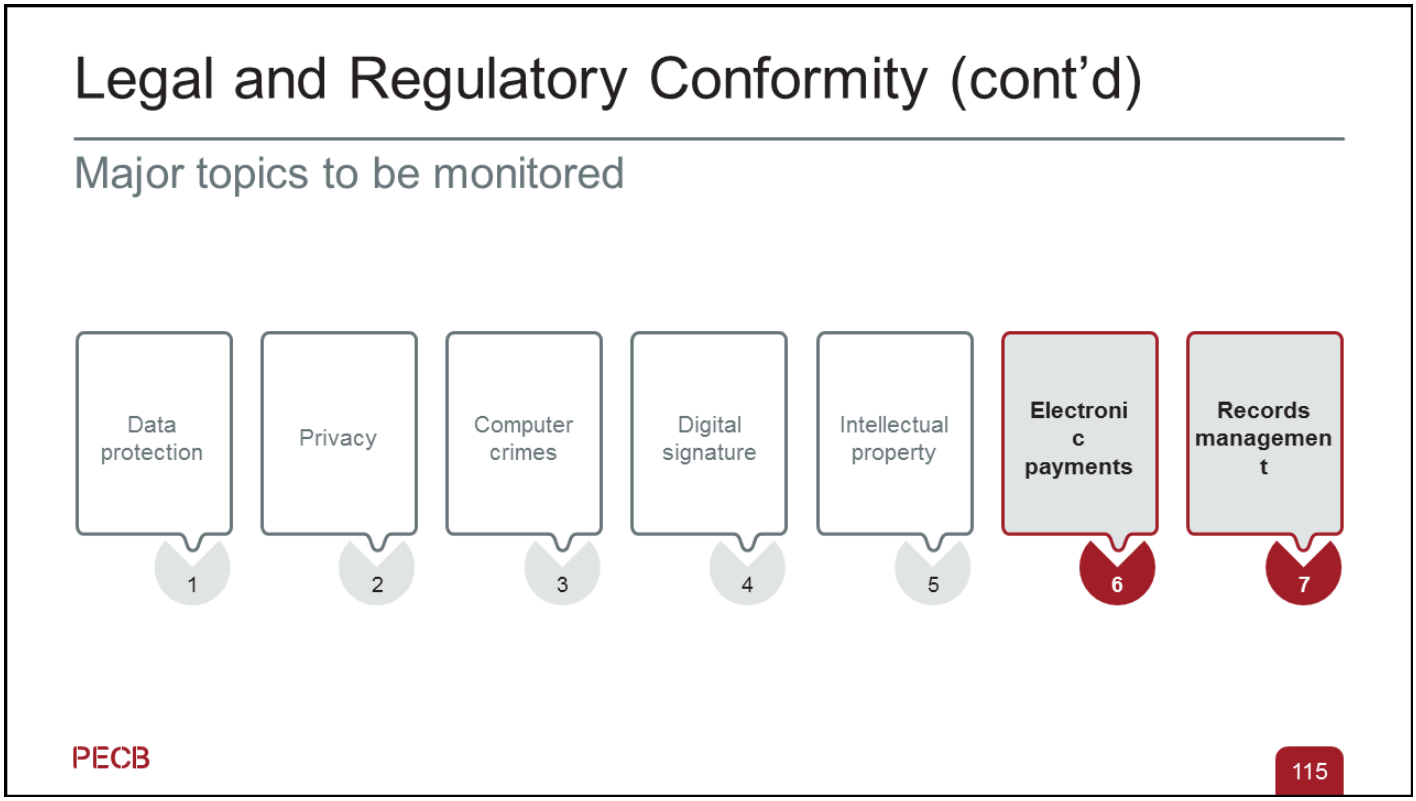
- They encompass any illegal activity that is performed through a computer and network and that is intended to cause harm to organizations' systems and gain unauthorized access to data. Targeted organizations might experience, among others, financial and reputational damages. In order to prevent and respond to these activities, organizations should establish adequate procedures and measures.

4. Digital signature

- It is an electronic signature that enables organizations to verify the authenticity of a message or document by verifying who the author of a document is and if the content has been modified. As a result, an electronic document that is digitally signed has the same legal validity as a hard copy document signed in handwriting, as long as there are regulations that give full legal value to it. In some countries, electronic records must ensure the preservation of "traces" as evidence of integrity and safety procedures developed on the basis of recognized standards for electronic records, e.g., the NF Z42-013 standard, or ISO 14721, which provides the reference model for an open archival information system (OAIS).

5.Intellectual property

- The result of intellectual effort is often recognized by national and international conventions as an intellectual property right to protect certain intangible assets. For small and medium organizations, the efficient use of human intellectual property can help compete with bigger organizations. Intellectual property has a great potential in terms of legal protection, information technology, and competitive advantage. The goal here is to strengthen the competitive position of the organization.



6.Electronic payments

- From a legal standpoint, in most countries, it is quite essential to prove in court that a customer bought the product or service sold by the organization. It should also be possible to satisfy the tax authority to demonstrate the time in which the individual transactions took place. The big difference between electronic commerce and trade by paper is the medium in which transactions are stored. With proof on paper, a physical change is difficult, while a change to an electronic file is easier. Another aspect is the possibility that a competitor may offer the same products from a server located in a tax haven. Finally, when a customer buys a product on a website, it is not always easy to determine which national law applies.

7.Records management

- Some national laws require that organizations maintain updated records regarding their activities and review them through a process of annual audit. Similar requirements exist at the governmental level. In some countries, organizations are obliged by law to issue such reports or to provide records for legal purposes (for example, in a case that could be the result of an offense involving penetration into a sensitive government system).

1.3.2 Develop the Cybersecurity Policy

- The purpose of a cybersecurity policy is to clearly express the objectives and boundaries of cybersecurity.
- The cybersecurity policy should:
  - Define the cybersecurity scope within the information security policy
  - Conform to legal requirements and ensure the privacy and integrity of the data
  - Encourage the use of best cybersecurity practices
  - Promote awareness against cybersecurity threats
- The cybersecurity policy may be a cross-reference to other security-related policies such as business continuity, risk management, etc.

PECB

116

The cybersecurity policy should define the specific roles and responsibilities related to cybersecurity. The cybersecurity-related activities should be clearly distinguished from other activities within the organization.

NIST Recommendation

NIST Cybersecurity Framework

Governance (ID.GV):	***ID.GV-1:***
The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	*Organizational cybersecurity policy is established and communicated*

NIST Recommendation

NIST Cybersecurity Framework

Information Protection Processes and Procedures (PR.IP): *Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.*

PR.IP-5: *Policy and regulations regarding the physical operating environment for organizational assets are met*

PR.IP-6: *Data is destroyed according to policy*

Protective Technology (PR.PT): *Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.*

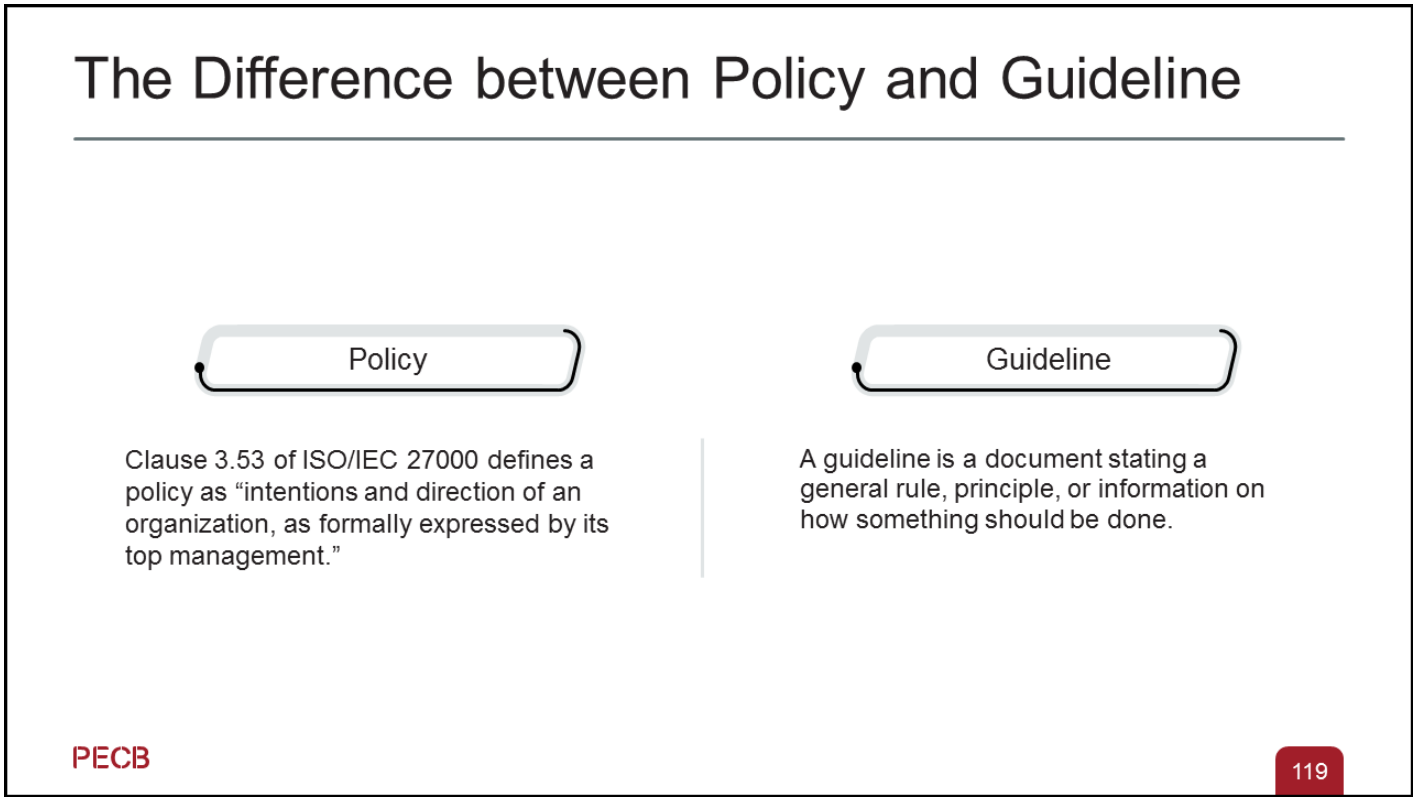
PR.PT-1: *Audit/log records are determined, documented, implemented, and reviewed in accordance with policy*

PR.PT-2: *Removable media is protected and its use restricted according to policy*

PECB

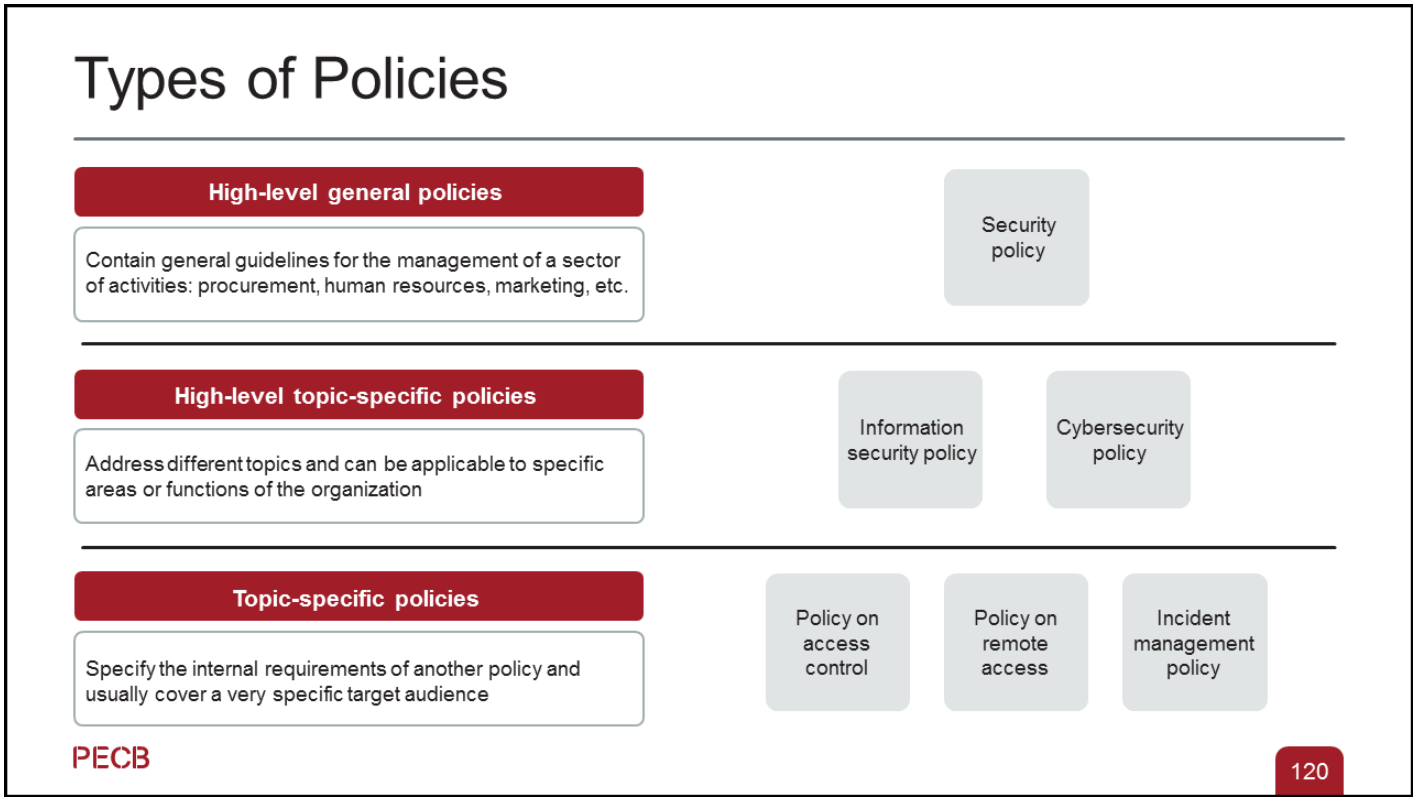
118

Depending on the size of the organization and its existing security-related policies, the cybersecurity policy may be cross-referenced with other policies. Some of the policies that can be referenced include access control policy, data classification policy, physical security policy, network security policy, removable media policy, password policy, social media policy, and web access policy.



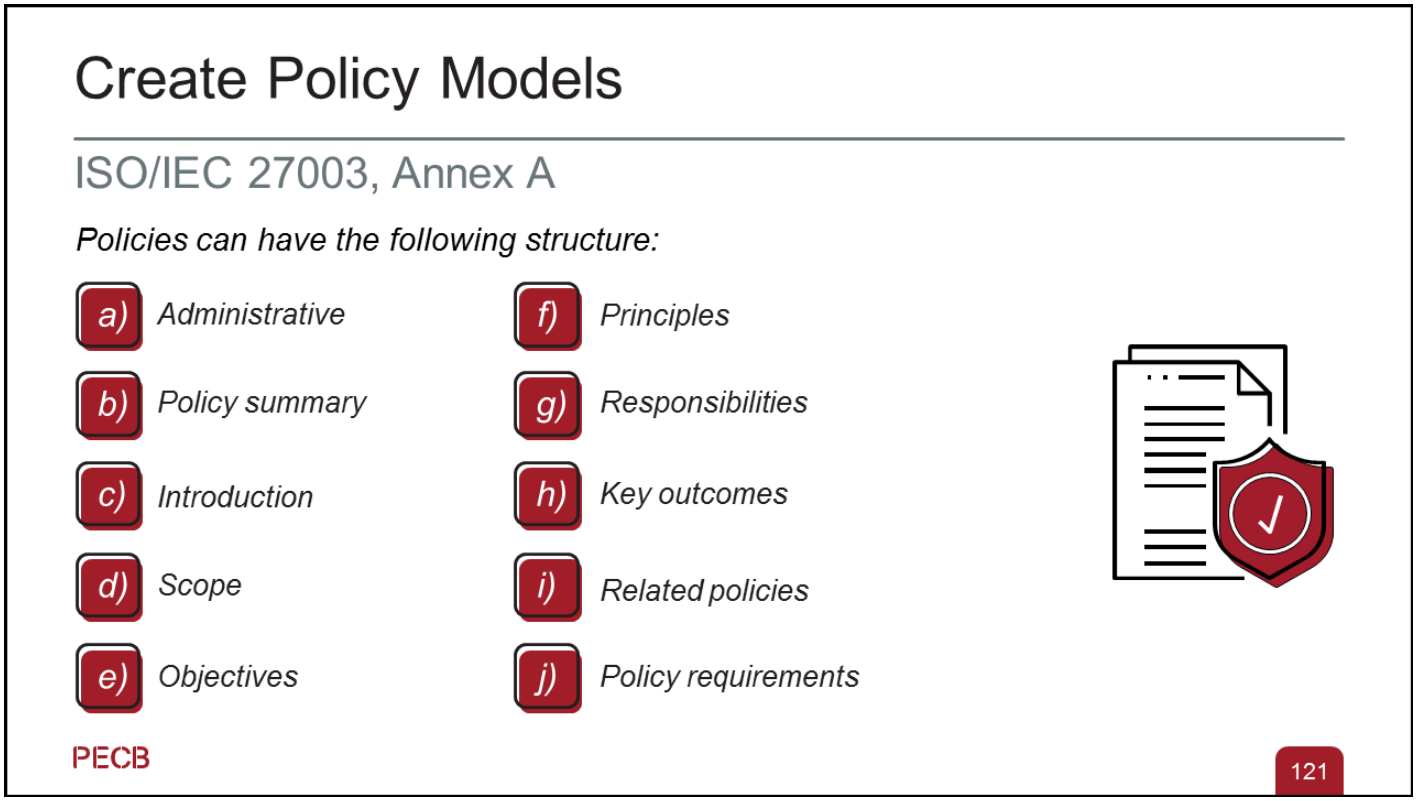
Note on terminology:

It is important to not confuse “policy” with a direction, procedure, guideline, or other types of documented information. The main goal of a policy is to provide guidance on a particular topic.



There are generally three levels of policies within an organization:

1. **High-level general policies** define a general framework within which the cybersecurity will be provided and the general objectives to ensure business continuity and to limit or prevent the potential damage of assets to an acceptable level and consequently limit the potential consequences of security incidents.
2. **High-level specific policies** define a subset of rules and practices still fairly general but that are related to a specific area. They are mostly subordinate to the high-level general policies.
    - **Note:** Both types of policies are usually subject to a review process because of their sensitive nature with regard to the functional strategy of the organization they are supposed to support.
3. **Topic-specific policies** are policies that support the high-level specific policies. These policies determine how to proceed in order to ensure security in specific application areas. Examples include security policy for access rights to information and technology infrastructure, policy on internet use, policy on P2P file sharing, etc.



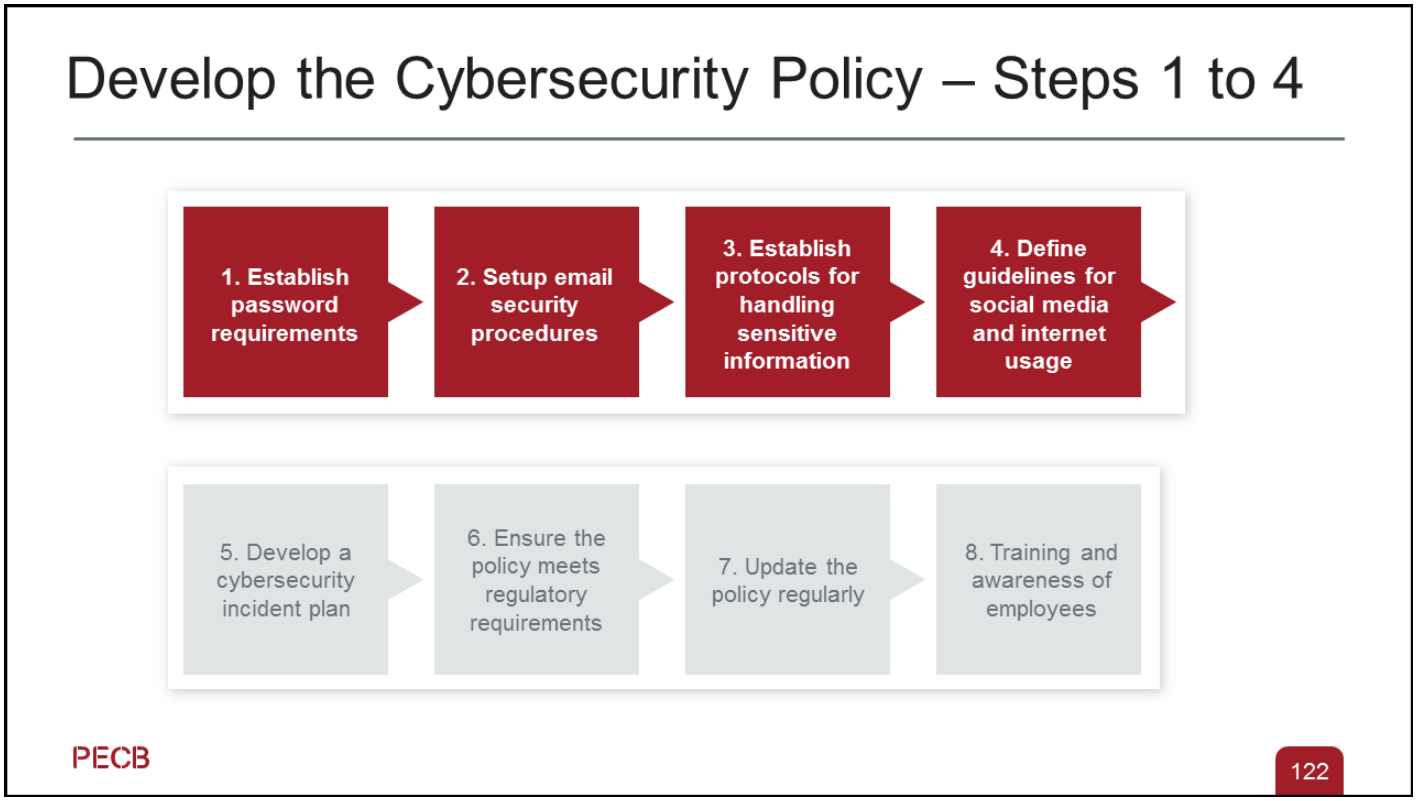
ISO/IEC 27003, Annex A Policy framework (cont'd)

Policies can have the following structure:

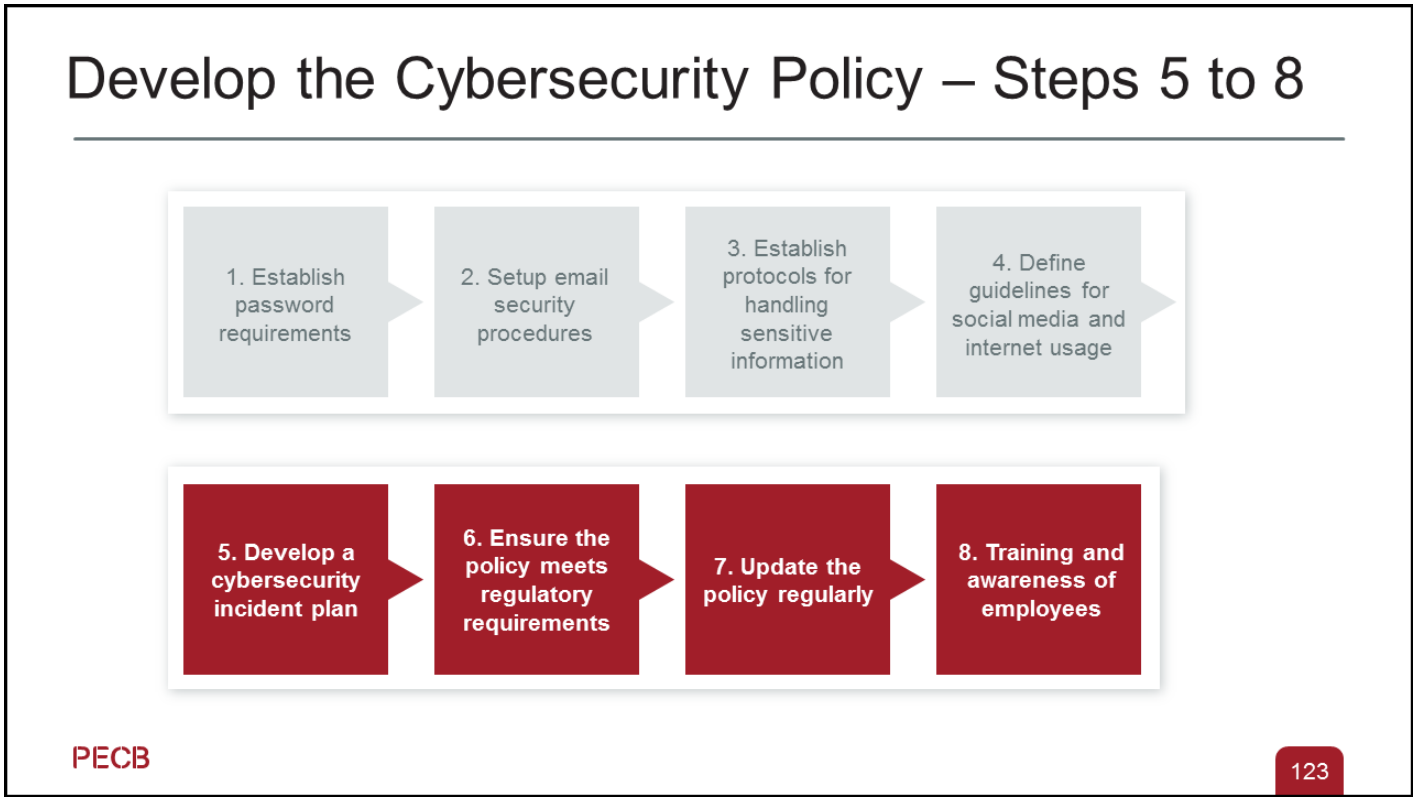
a. *Administrative – policy title, version, publication/validity dates, change history, owner(s) and approver(s), classification, intended audience etc.;*
b. *Policy summary – a one or two sentence overview. (This can sometimes be merged with the introduction.);*
c. *Introduction – a brief explanation of the topic of the policy;*
d. *Scope – describes those parts or activities of an organization that are affected by the policy. If relevant, the scope clause lists other policies that are supported by the policy;*
e. *Objectives – describes the intent of the policy;*
f. *Principles – describes the rules concerning actions and decisions for achieving the objectives. In some cases, it can be useful to identify the key processes associated with the topic of the policy and then the rules for operating the processes;*
g. *Responsibilities – describes who is responsible for actions to meet the requirements of the policy. In some cases, this can include a description of organizational arrangements as well as the responsibilities and authority of persons with designated roles;*
h. *Key outcomes – describes the business outcomes if the objectives are met. In some cases, this can be merged with the objectives;*
i. *Related policies – describes other policies relevant to the achievement of the objectives, usually by providing additional detail concerning specific topics; and*
j. *Policy requirements – describes the detailed requirements of the policy.*

Other subjects may be added to the model of the policy of an organization, such as:

- **Definitions** contains a list of terms and definitions used in the policy that may be unclear to the reader.
- **Penalties** contains a description of the list of possible sanctions if a user violates a policy (e.g., any user who violates this policy is subject to disciplinary action up to and including dismissal, including criminal prosecution).



1. **Establish password requirements:** Weak passwords increase the likelihood of employees being targeted by cybercriminals. Hence, it is crucial to incorporate password management policies into the IT security policy, including guidelines for:
    - Creating strong passphrases
    - Storing and updating passwords
    - Using unique passwords for different logins
2. **Setup email security procedures:** To ensure email security across all departments, cybersecurity policies and procedures must include designated measures. This involves adhering to guidelines for:
    - Sharing work email addresses
    - Only opening email attachments from trusted business contacts
    - Deleting and reporting spam emails
    - Preventing phishing
3. **Establish protocols for handling sensitive information:** A cybersecurity policy must clearly define sensitive data and how to handle it. The policy should specify sharing permissions and data masking techniques during threats, and guidelines for storing physical files with sensitive data.
4. **Define guidelines for social media and internet usage:** Standard operating procedures for handling technology are crucial for remote teams in cybersecurity. The cybersecurity policy should set guidelines for:
    - Accessing devices when not physically at work
    - Shutting down and storing unused devices
    - Reporting lost work devices
    - Safeguarding data on secondary storage or removable devices
    - Updating personal computers
    - Scanning and protecting data
    - Locking device screens when not in use.



5.Develop cybersecurity incident plan: A cybersecurity policy must outline the necessary steps for each user to take in the case of a cyber-attack. This includes procedures, response actions, and incident handling.

6.Ensure the policy meets regulatory requirements: Cybersecurity project managers must consider the regulatory requirements to ensure compliance with federal government standards.

7.Update the policy regularly: Organizations should regularly review their cybersecurity policy in accordance with the lasted developments.

8.Training and awareness of employees: Updating the policy is essential to avoid new threats, but it is equally important pay attention to employee training. Since employees operate new security technologies and methodologies, regular training is necessary.

Sources:

Australian Government Business. “Create a Cyber Security Policy.” Last modified March 7, 2023. https://business.gov.au/online/cyber-security/create-a-cyber-security-policy

Babu. Sabdeeo “What Is a Cybersecurity Policy and How to Create One?” Small Business Trends. Last modified August 30, 2022. https://smallbiztrends.com/2022/08/cybersecurity-policy.html

Cybersecurity Policy

Model

Summary of the cybersecurity policy	The cybersecurity policy aims to ensure an adequate protection level of the information assets of the organization against all cybersecurity threats. The cybersecurity program establishes, implements, operates, monitors, reviews, maintains, and improves processes and controls related to cybersecurity following on a risk-based approach.
Introduction	The organization must ensure the confidentiality, integrity, and availability of the organization's information. The organization must ensure the protection of its information assets against internal or external and accidental or deliberate cybersecurity threats.
Cybersecurity policy scope	This policy applies to all activities of the organization and its employees and interested parties who have access to information assets and systems.
Cybersecurity policy objectives	The objectives are to ensure continuity of critical business activities; ensure that all information processed, stored, traded, or released by the organization is of absolute integrity; ensure that all information is monitored and stored according to the procedures for maintaining confidentiality; provide choice of appropriate security controls to protect the assets and give confidence to interested parties; and ensure effective management and efficient cybersecurity management.
Principles of the cybersecurity policy	The organization must establish, implement, operate, monitor, review, maintain, and improve the cybersecurity program based on a documented approach to risk activity and guidance of ISO/IEC 27032 and NIST Cybersecurity Framework. The organization should take into account all legal, regulatory, and contractual requirements. The legal and regulatory requirements will be met in priority, even if they are inconsistent with the policy described here. This policy has been approved by the top management and is subject to an annual review.

PECB

124

The cybersecurity policy includes:

- A framework that allows to define objectives and policy guidelines for the management of cybersecurity
- A consideration of legal and regulatory obligations imposed on the organization as well as other commitments
- Alignment of the cybersecurity risk management with the strategic objectives of the organization
- A list of criteria to evaluate cybersecurity risks
- Formal approval by the management for the abovementioned measures

Although the cybersecurity policy model presented on the slide is applicable to most organizations, it should, however, be adapted to the specific conditions of each organization.

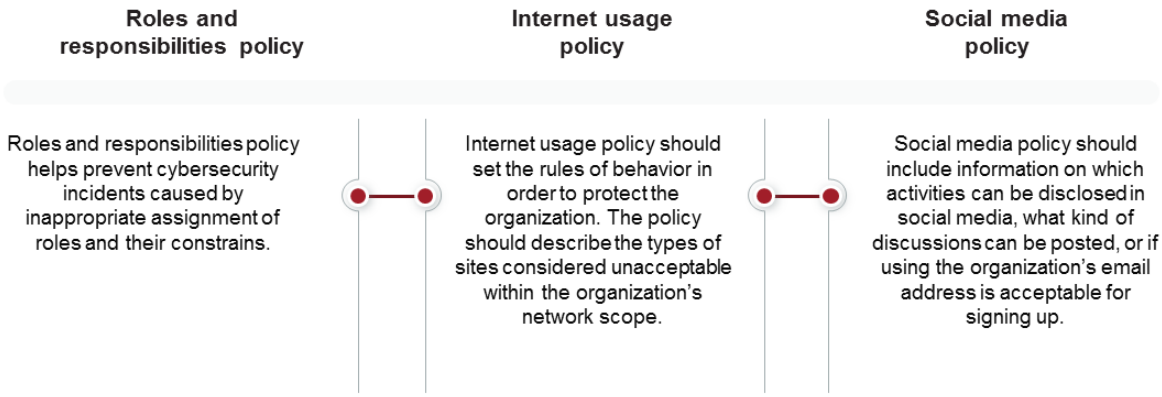
Cybersecurity Policy (Cont'd)

Model

Responsibilities	The management is responsible for ensuring that the objectives and plans for the cybersecurity program are established and reviewed annually in management review meetings, the roles and responsibilities regarding cybersecurity are defined, awareness programs are conducted, and the necessary resources to maintain and improve the cybersecurity program are provided. The CISO is responsible for intervening on all aspects of the organization's cybersecurity. The CISO decides on, in general, all the requirements for the effective operation of the cybersecurity program by means of administrative directives, previously submitted to the top management. Each executive has the responsibility of ensuring that persons working under their control will protect information in accordance with the policies of the organization. All users (management, employees, contractors, and third party users) should be aware of the risks to cybersecurity, their responsibilities, and the need to respect the policies to ensure the adequate protection of information.
Expected results	Appropriate and proportionate cybersecurity controls will be implemented to protect assets and give confidence to interested parties. Decisions on matters of cybersecurity will be based on an evaluation of risks faced by the organization. The legal, regulatory, and contractual requirements related to cybersecurity will be met.
Related policies	The access control policy, the change management policy, the information security policy, the incident response policy, etc.

Specific Security Policies

- Other security policies should be consistent with the cybersecurity policy, reviewed on a regular basis, and adapted to the changed business needs.
- The following is a list of important security policies needed to protect sensitive information, business data, and the reputation of an organization.



PECB

126

Source: Federal Communications Commission. "*Cyber Security Planning Guide."* Last accessed May 16, 2023. https://www.fcc.gov/sites/default/files/cyberplanner.pdf

Access Control Policy

Example

Policy summary	For every system, network, and application, formal user access controls need to be implemented and enforced in order to grant access to the authorized users and prevent unauthorized access.
Introduction	The access control policy is used to define the access rights of users in a system, network, or application and prevent unauthorized access.
Scope	The access control policy applies to all employees, members of management, and contracted personnel having access to information assets and systems of the organization.
Access control objectives	The objective is to prevent unauthorized access to a system, network, and application of the organization arising from improper allocation of system and application access control and poor administration of user accounts.

PECB

Access Control Policy (Cont'd)

Example

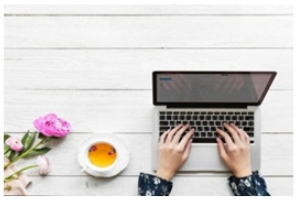
Access control principles	• **Defense in depth:** The security of information should not depend on a single control only. • **Least privilege:** Users, applications, and processes should have only the bare minimum privileges required to perform their function. • **Need to know:** Access is given only for the information and resources that are needed to fulfill a function.
Responsibilities	It is the responsibility of the cybersecurity team, in cooperation with the information security team, to ensure compliance with this policy and take steps to enforce it. Each user must know this policy and respect it.
Key outcomes	The outcomes are: decrease of unauthorized use, user accounts that have more access than their role requires, and user accounts with misallocations of roles.
Related policies	Cybersecurity policy, information security policy, password policy, etc.

Ensure Management Approval

- The cybersecurity policy shall:
  - Demonstrate the commitment of the management
  - Be approved by the management
- The policy must be signed by an individual (often the CEO) but the approval process may belong to:
  - Board of directors
  - Management board
  - Security governance committee

Publish the Policy

Main modes of communication



Intranet

Meeting

Distribution of hard copies

Employee onboarding

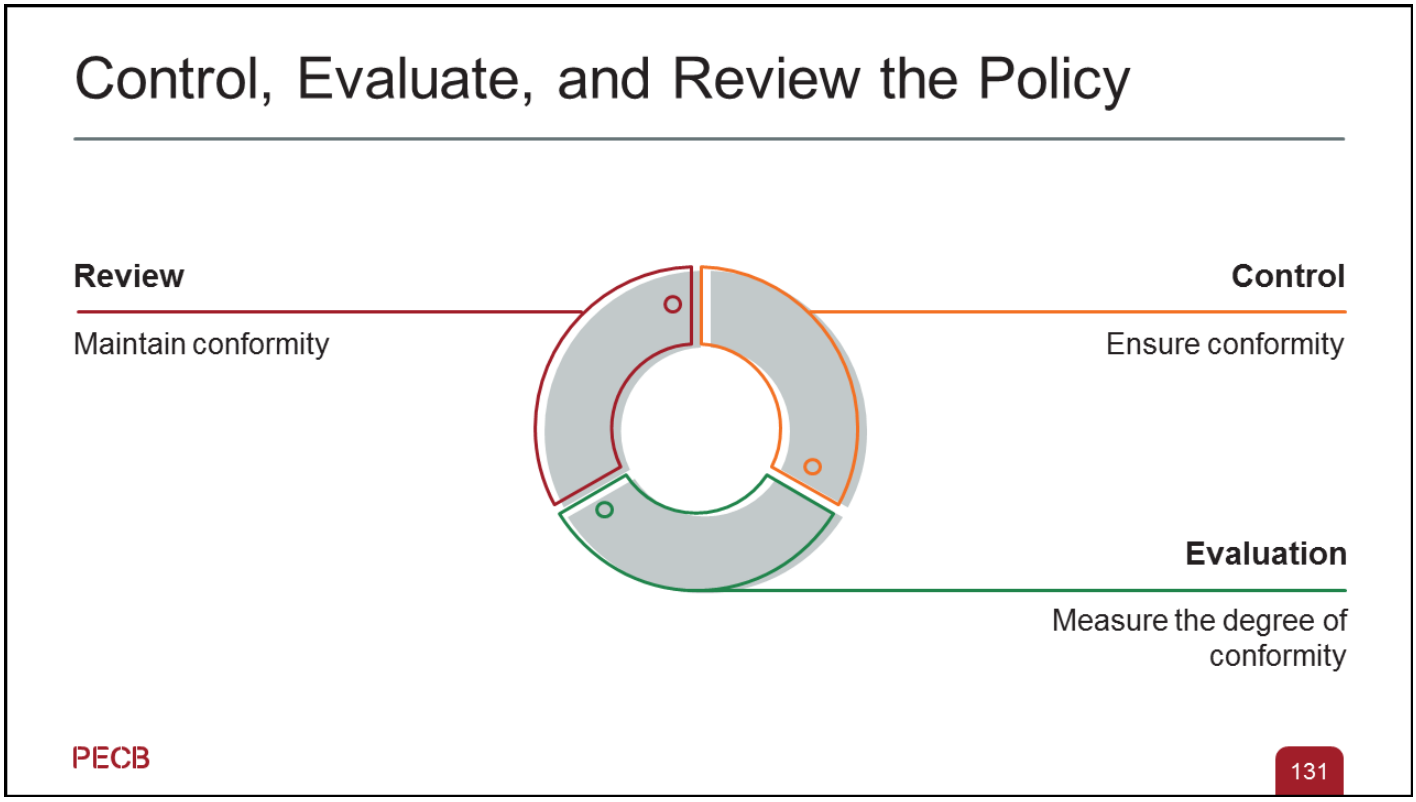
PECB

130

During the initial publication of the cybersecurity policy, it is good practice (but not required) to have this policy signed by all employees of the organization, including the management team. The original signed form should be kept by the Human Resources Department staff or any other body that is responsible.

For new employees, making them aware of organizational policies and having them agree is usually a step included in the process of employee onboarding.

If the signing of the policy is not done, the organization should be able to demonstrate that members of the organization understand and respect the policy. For example, this can be achieved by participating in a training session.



The control, evaluation, and review of the cybersecurity policy facilitate the initiation of a continual improvement process. By regularly reviewing the cybersecurity policy, the organization ensures consistency with business requirements and legal constraints.

Control: The management must ensure that the cybersecurity policy is respected in day-to-day operations in the organization. In addition, the management must provide a formal disciplinary process for employees who violate the policy. The formal disciplinary process ensures a correct and fair treatment of employees suspected of violating the policy. The formal disciplinary process should provide for a gradual response that takes into consideration factors such as the nature and severity of the breach and its impact on the business (ISO/IEC 27002, clause 7.2.3 *Disciplinary process*).

Evaluation: The organization must implement mechanisms for evaluating the effectiveness and enforcement of its cybersecurity policy.

Review: To ensure the relevance, adequacy, and effectiveness of the cybersecurity policy, the policy should be reviewed at planned intervals or when major changes occur. The emergence of new threats and vulnerabilities and the constantly changing technological environment are non-exhaustive examples of events that may affect, partly or in all, the operational nature of a cybersecurity policy.

Section Summary:

- Cybersecurity governance is a comprehensive approach to cybersecurity that aims to safeguard against cyber threats or attacks that may disrupt the activities of an organization.
- Some commonly used cybersecurity frameworks are the NIST Cybersecurity Framework, ISO/IEC TS 27110 Framework, and COBIT.
- There are generally three levels of policies within an organization: high-level general policies, high-level specific policies, and topic-specific policies.
- The process of drafting a policy consists of assigning a competent person, defining the policy components, drafting the policy sections, validating the contents and the format of the policy, and validating the policy with the interested parties.
- By regularly reviewing the information security policy, the organization guarantees consistency with business requirements and legal constraints.

Questions?

Quiz 5

PECB

132

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

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

Summary of Day 1

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

- The ISO/IEC 27000 family of standards
- NIST Cybersecurity Framework
- Cybersecurity, cyberspace, and cybercrime
- Information security
- Confidentiality, integrity, and availability
- Vulnerabilities and threats
- Information security risk
- Security controls
- Gap analysis
- Cybersecurity program
- Cybersecurity governance
- Cybersecurity regulatory compliance
- Cybersecurity policy

PECB