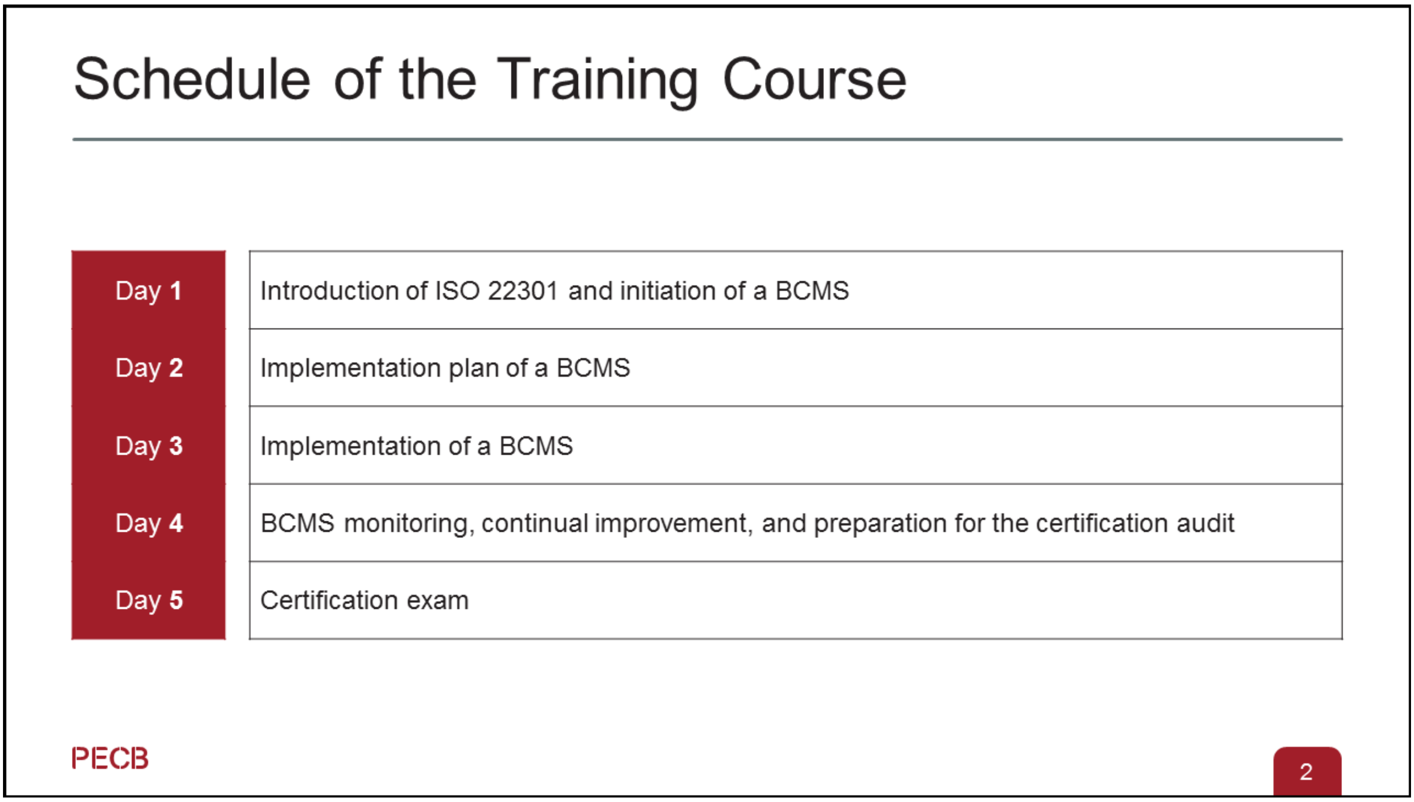
DAY 1

Certified ISO 22301 Lead Implementer

Version 4.4

Document number: BCMSLID1V4.4



## Schedule of the Training Course

| | |
|---|---|
| Day **1** | Introduction of ISO 22301 and initiation of a BCMS |
| Day **2** | Implementation plan of a BCMS |
| Day **3** | Implementation of a BCMS |
| Day **4** | BCMS monitoring, continual improvement, and preparation for the certification audit |
| Day **5** | Certification exam |

### Day 1: Introduction of ISO 22301 and initiation of a BCMS

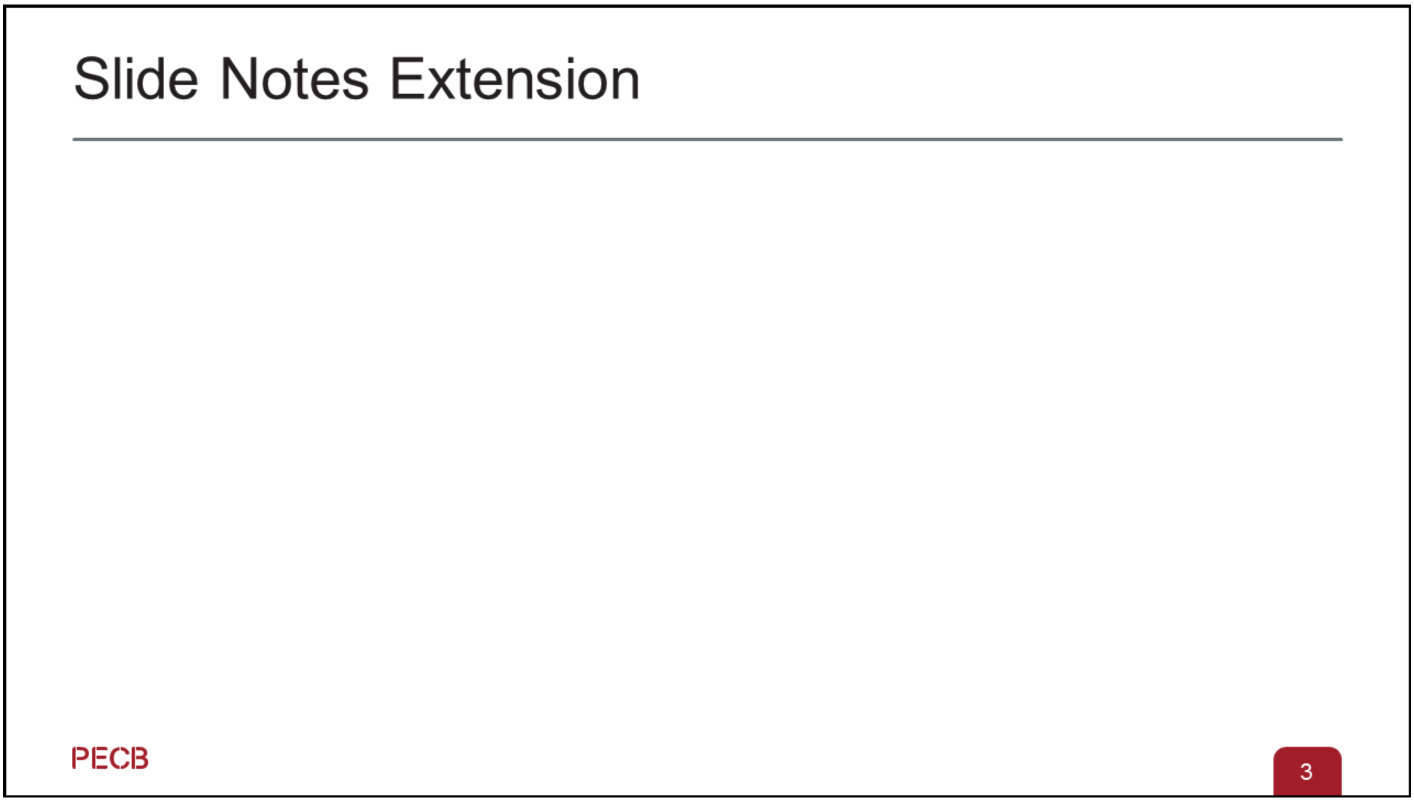
- Section 1: Training course objectives and structure
- Section 2: Standards and regulatory frameworks
- Section 3: Business continuity management system
- Section 4: Fundamental business continuity principles and concepts
- Section 5: Initiation of the BCMS implementation
- Section 6: The organization and its context
- Section 7: BCMS scope

### Day 2: Implementation plan of a BCMS

- Section 8: Leadership and commitment
- Section 9: Business continuity policy
- Section 10: Risks, opportunities, and business continuity objectives
- Section 11: Support for the BCMS
- Section 12: Business impact analysis

### Day 3: Implementation of a BCMS

- Section 13: Risk assessment
- Section 14: Business continuity strategies and solutions
- Section 15: Business continuity plans and procedures
- Section 16: Incident response and emergency response
- Section 17: Crisis management



## Slide Notes Extension

PECB

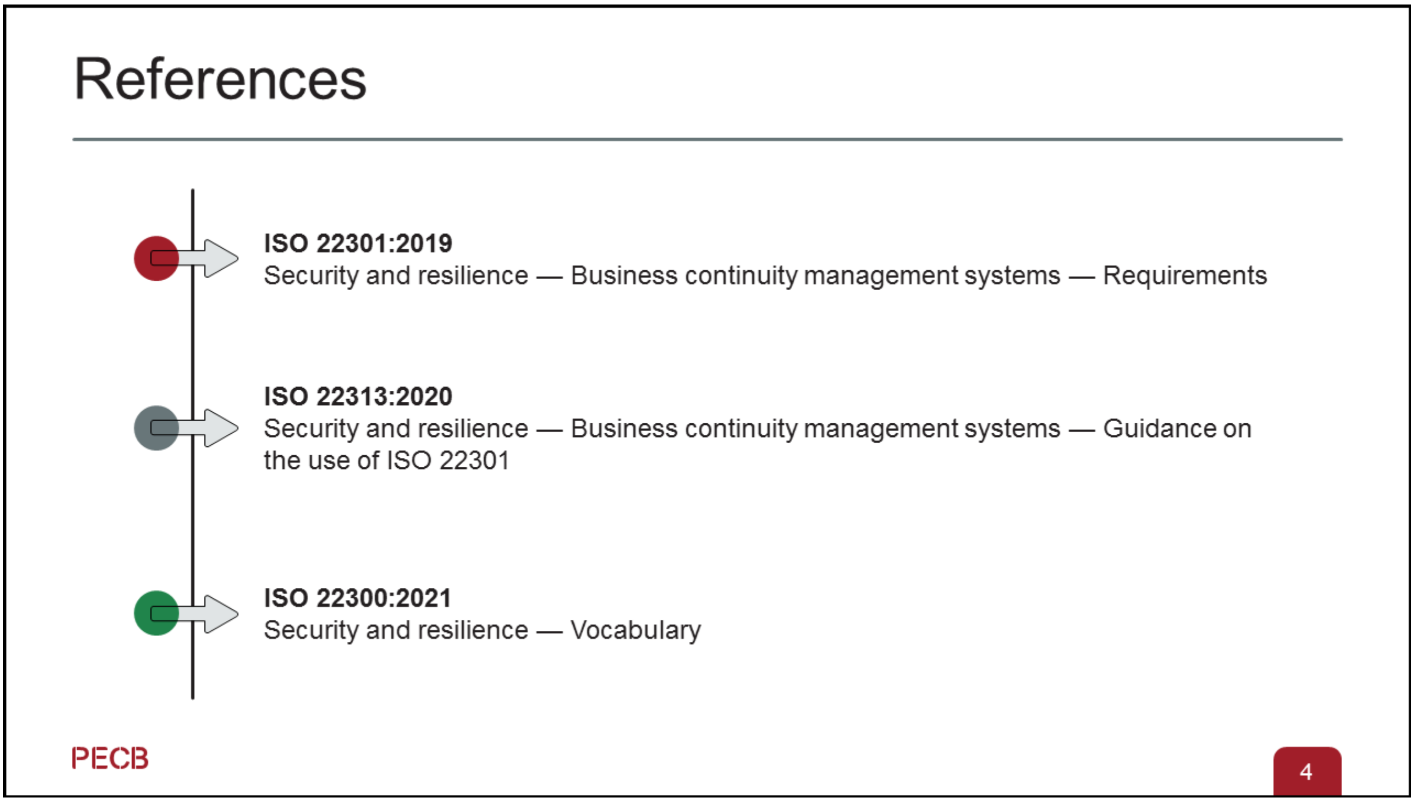
3

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

- Section 18: Exercise programs
- Section 19: Monitoring, measurement, analysis, and evaluation
- Section 20: Internal audit
- Section 21: Management review
- Section 22: Treatment of nonconformities
- Section 23: Continual improvement
- Section 24: Preparation for the certification audit
- Section 25: 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.



# References

**ISO 22301:2019**
Security and resilience — Business continuity management systems — Requirements

**ISO 22313:2020**
Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

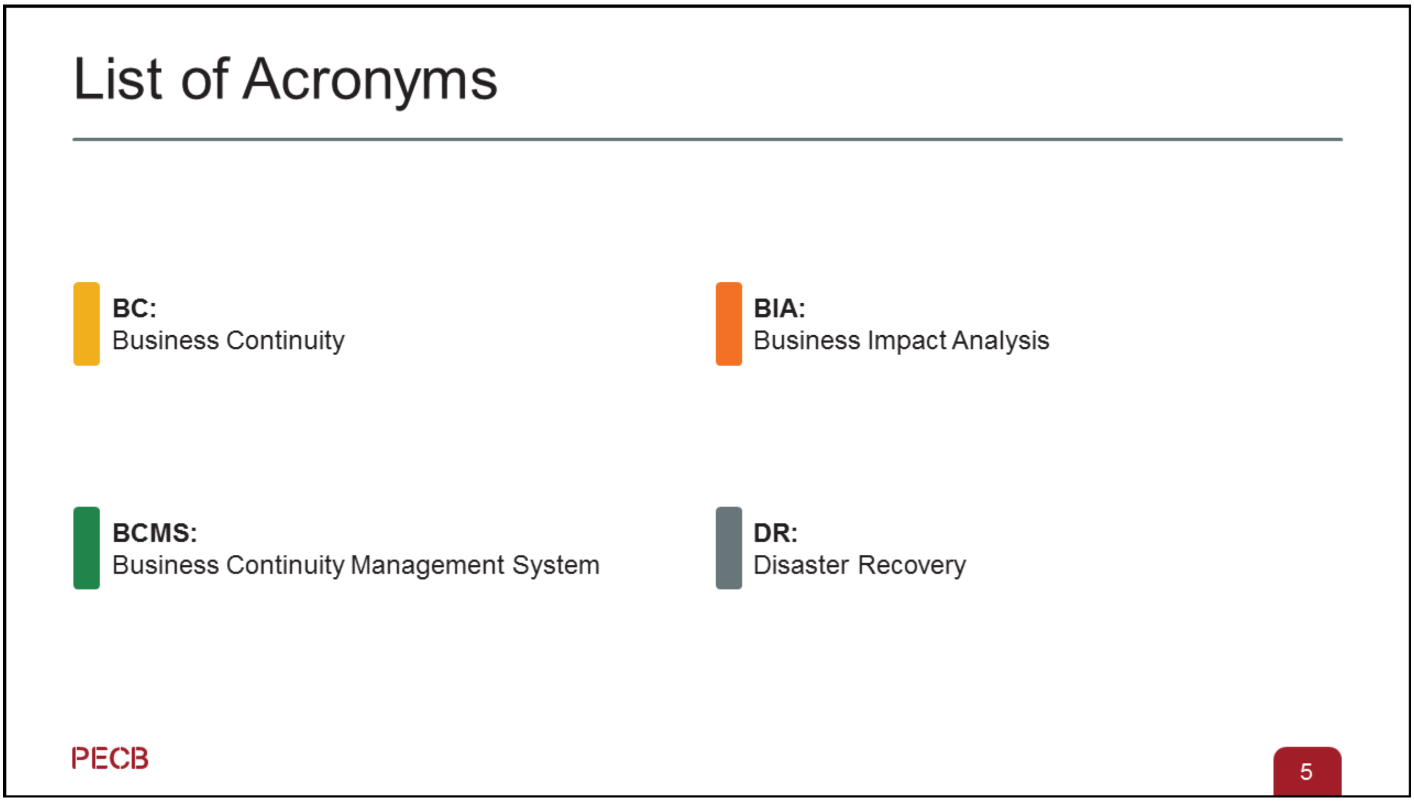
**ISO 22300:2021**
Security and resilience — Vocabulary

PECB

4

**Other references cited in this training course:**

- ISO/TS 22317:2015, Societal security — Business continuity management systems — Guidelines for Business Impact Analysis (BIA)
- ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
- ISO 19011:2018, Guidelines for auditing management systems
- ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
- ISO/IEC 17024:2012, Conformity assessment — General requirements for bodies operating certification of persons
- ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services
- ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements
- ISO 55000:2014, Asset management — Overview, principles and terminology
- NIST 800-34 Rev 1.:2010, Contingency Planning Guide for Federal Information Systems
- ISO 10015:2019, Quality management — Guidelines for competence management and people development
- ISO 31000:2018, Risk management — Guidelines
- IEC 31010:2019, Risk management — Risk assessment techniques
- ISO/IEC Directives, Part 1:2019, Procedures for the technical work



## List of Acronyms

**BC:**
Business Continuity

**BIA:**
Business Impact Analysis

**BCMS:**
Business Continuity Management System

**DR:**
Disaster Recovery

PECB

5

**Other acronyms used throughout this training course:**

**BCC:** Business Continuity Coordinator

**BCM:** Business Continuity Management

**BCP:** Business Continuity Plan

**CERT:** Computer Emergency Response Team

**CMS:** Content Management System

**CPD:** Continuing Professional Development

**EDMS:** Electronic Document Management System

**EMV:** Expected Monetary Value

**EOC:** Emergency Operations Center

**HVAC:** Heating, Ventilation, and Air Conditioning

**IAS:** International Accreditation Service

**ISO:** International Organization for Standardization

**KPI:** Key Performance Indicator

**LA:** Lead Auditor

**LI:** Lead Implementer

**MAO:** Maximum Acceptable Outage

**MBCO:** Minimum Business Continuity Objective

**MoU:** Memorandum of Understanding

**MTPD:** Maximum Tolerable Period of Disruption

**NIST:** National Institute of Standards and Technology

**PDCA:** Plan, Do, Check, and Act

**PDM:** Product Data Management

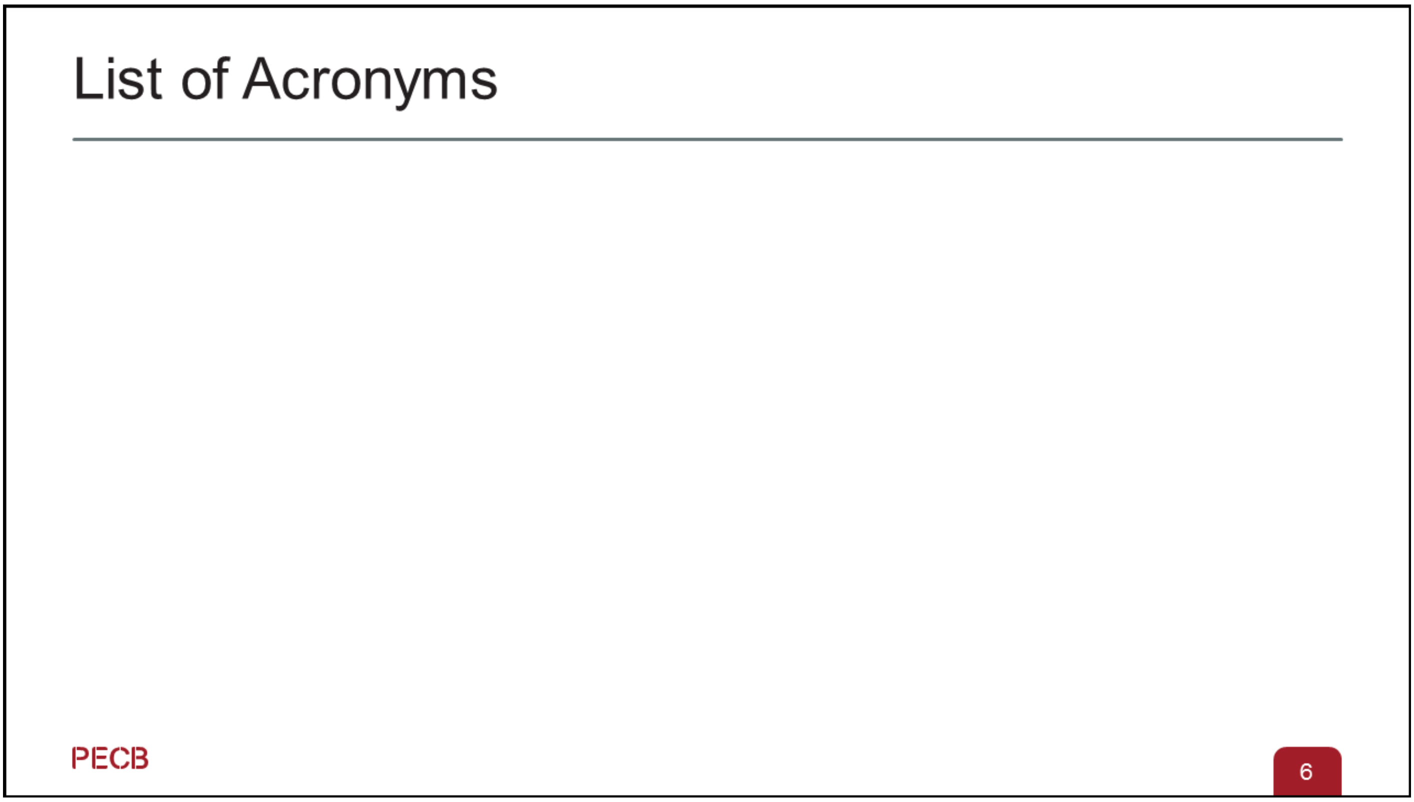
**PECB:** Professional Evaluation and Certification Board

**RM:** Risk Management

**RMA:** Records Management Application

**RPO:** Recovery Point Objective

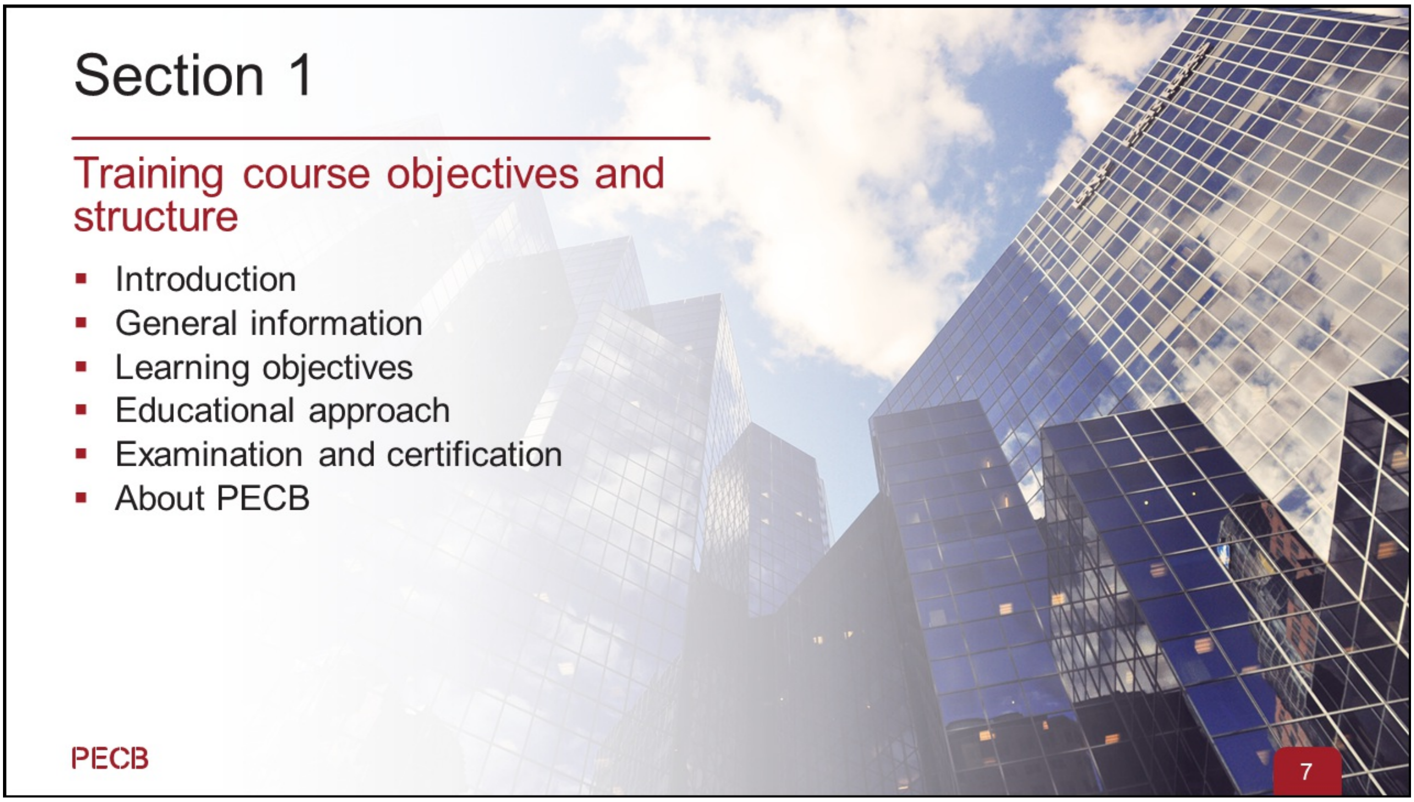
**RTO:** Recovery Time Objective



# List of Acronyms

**WBS:** Work Breakdown Structure

**WHO:** World Health Organization



# Section 1

## Training course objectives and structure

- Introduction
- General information
- Learning objectives
- Educational approach
- Examination and certification
- About PECB

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

# Introduction

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

- Name
- Current position
- Knowledge and experience regarding business continuity management
- Knowledge and experience regarding ISO 22301 and other related standards (ISO/IEC 27031, ISO 22315, ISO/TS 22317, etc.)
- Knowledge and experience regarding other management systems (ISO 9001, ISO 14001, ISO/IEC 27001, etc.)
- Training course expectations

## General Information

Use of smartphones and computers and access to the internet

Interactive and engaging sessions

Schedule and absences

Meals and breaks

Customer Service

Safety instructions

PECB

9

- 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**

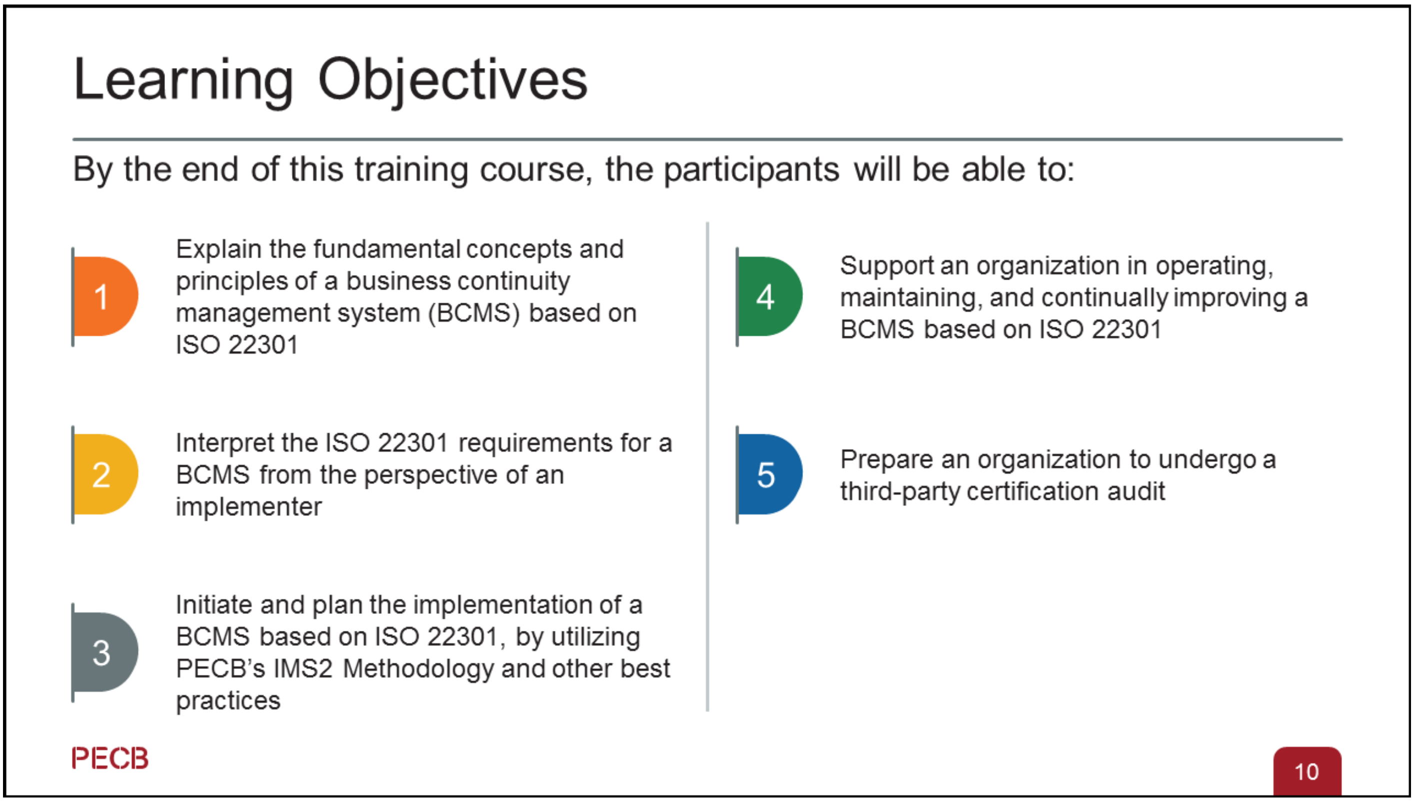
To ensure customer satisfaction and continual improvement, PECB Customer Service has established a support ticket system for handling complaints.

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).



## Learning Objectives

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

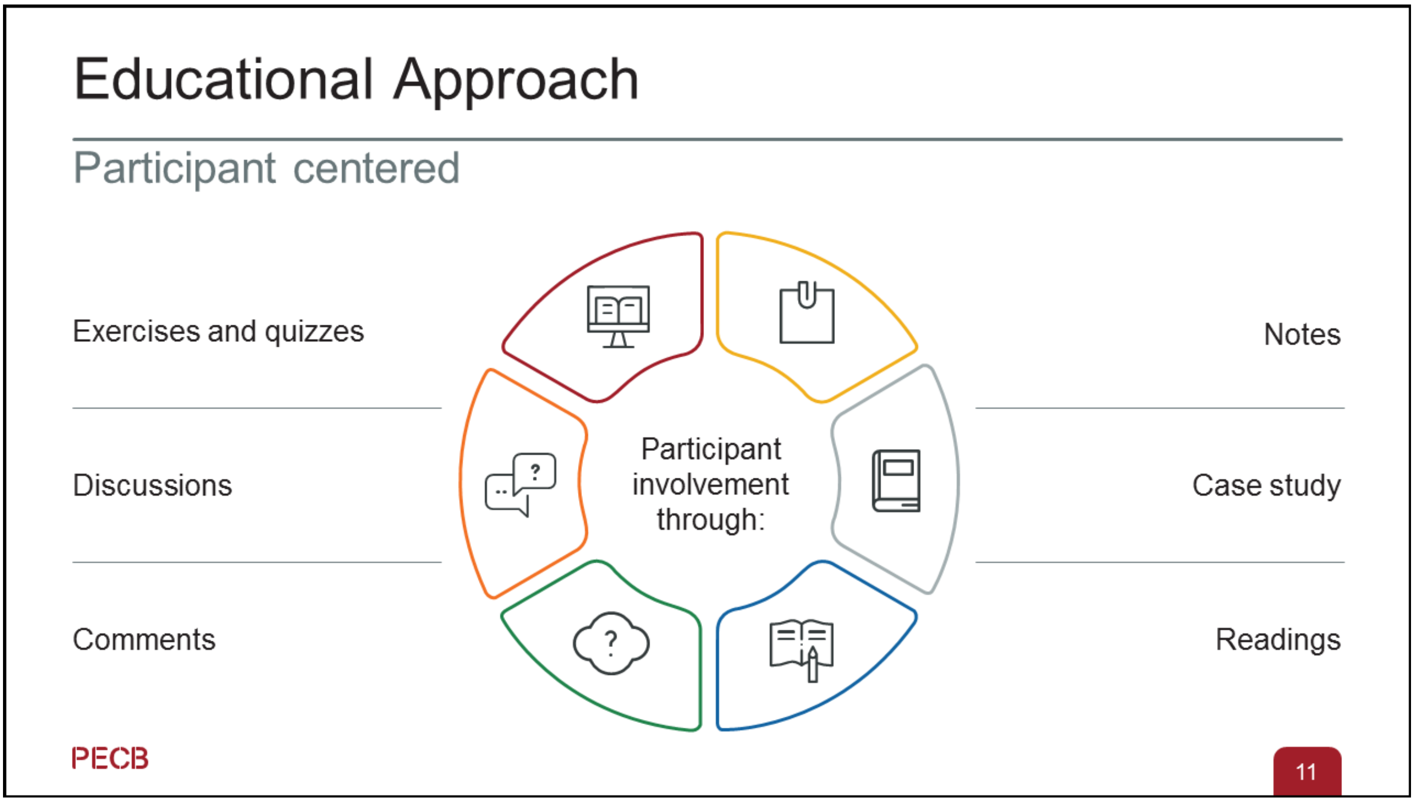
1. Explain the fundamental concepts and principles of a business continuity management system (BCMS) based on ISO 22301
2. Interpret the ISO 22301 requirements for a BCMS from the perspective of an implementer
3. Initiate and plan the implementation of a BCMS based on ISO 22301, by utilizing PECB's IMS2 Methodology and other best practices
4. Support an organization in operating, maintaining, and continually improving a BCMS based on ISO 22301
5. Prepare an organization to undergo a third-party certification audit

The training course is intended to help participants develop their competences to participate in the implementation of a business continuity management system (BCMS). 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 BCMS based on the ISO 22301 requirements, not merely a list of the ISO 22301 requirements. Therefore, general knowledge of the business continuity concepts is required for the successful completion of the training course.

If participants wish to obtain more in-depth knowledge of a BCMS audit process, including the audit principles, techniques, and best practices, we recommend them to take the PECB Certified ISO 22301 Lead Auditor training course.



# Educational Approach

## Participant centered

Participant involvement through:

Exercises and quizzes

Discussions

Comments

Notes

Case study

Readings

PECB

11

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

- Trainer instructions
- Participant involvement

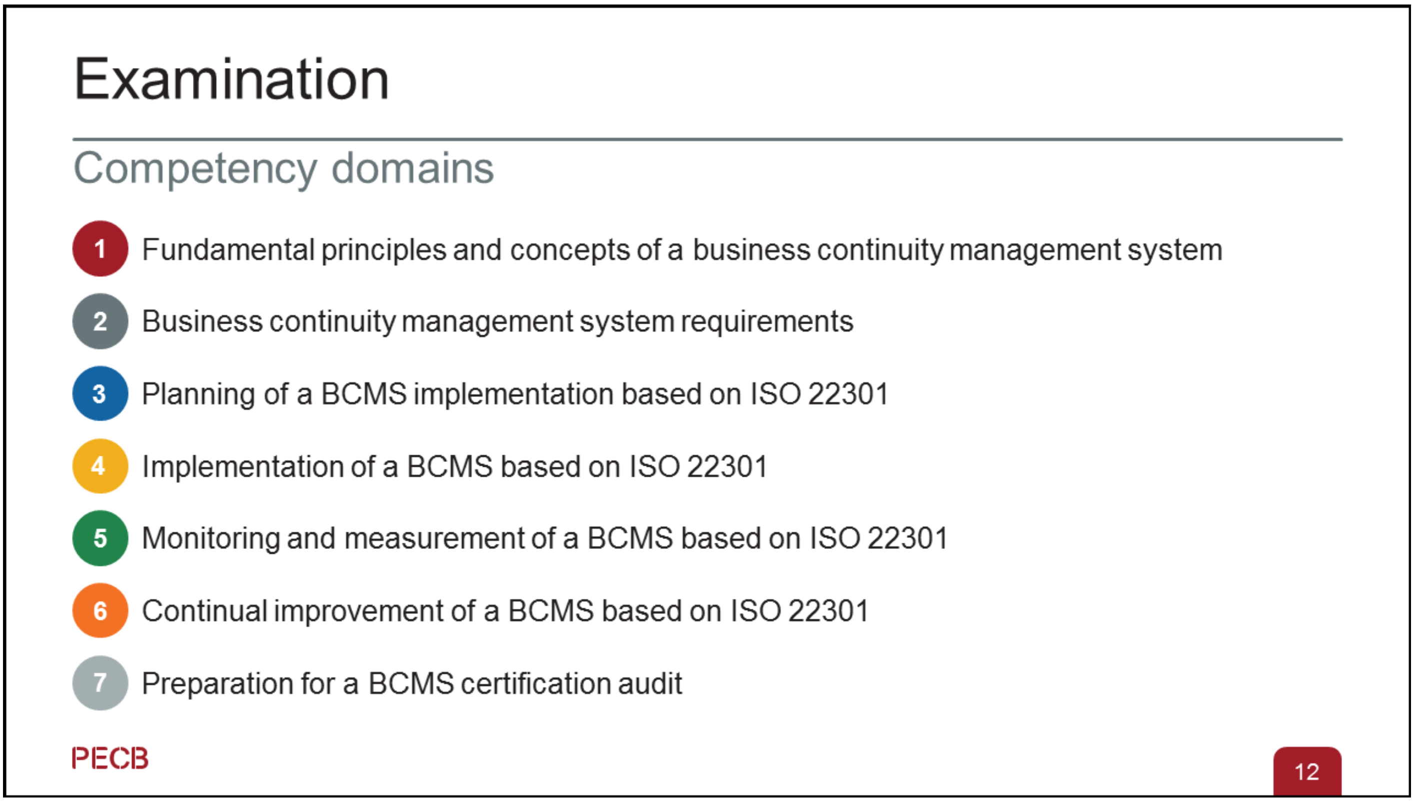
Interaction by means of questions and suggestions is highly encouraged. Participants can best contribute to the training course by partaking in exercises, quizzes, case studies, and discussions. Participants are also advised to take personal notes.

Exercises and 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



# Examination

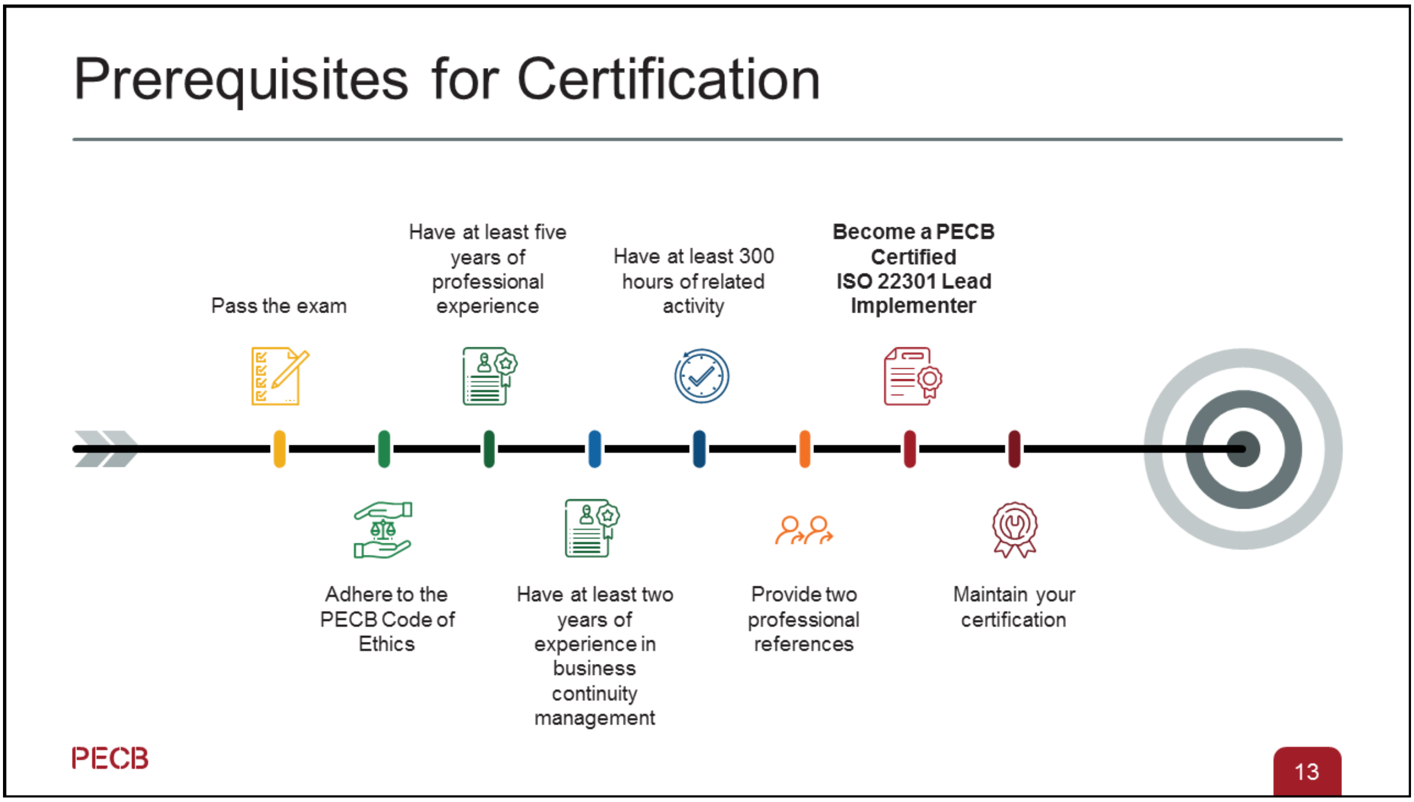
## Competency domains

1. Fundamental principles and concepts of a business continuity management system
2. Business continuity management system requirements
3. Planning of a BCMS implementation based on ISO 22301
4. Implementation of a BCMS based on ISO 22301
5. Monitoring and measurement of a BCMS based on ISO 22301
6. Continual improvement of a BCMS based on ISO 22301
7. Preparation for a BCMS certification audit

The purpose of the certification exam is to evaluate whether candidates have mastered the business continuity management concepts, methods, and techniques so that they are able to participate in and lead BCMS implementation projects.

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

Pass the exam

Adhere to the PECB Code of Ethics

Have at least five years of professional experience

Have at least two years of experience in business continuity management

Have at least 300 hours of related activity

Provide two professional references

**Become a PECB Certified ISO 22301 Lead Implementer**

Maintain your certification

PECB

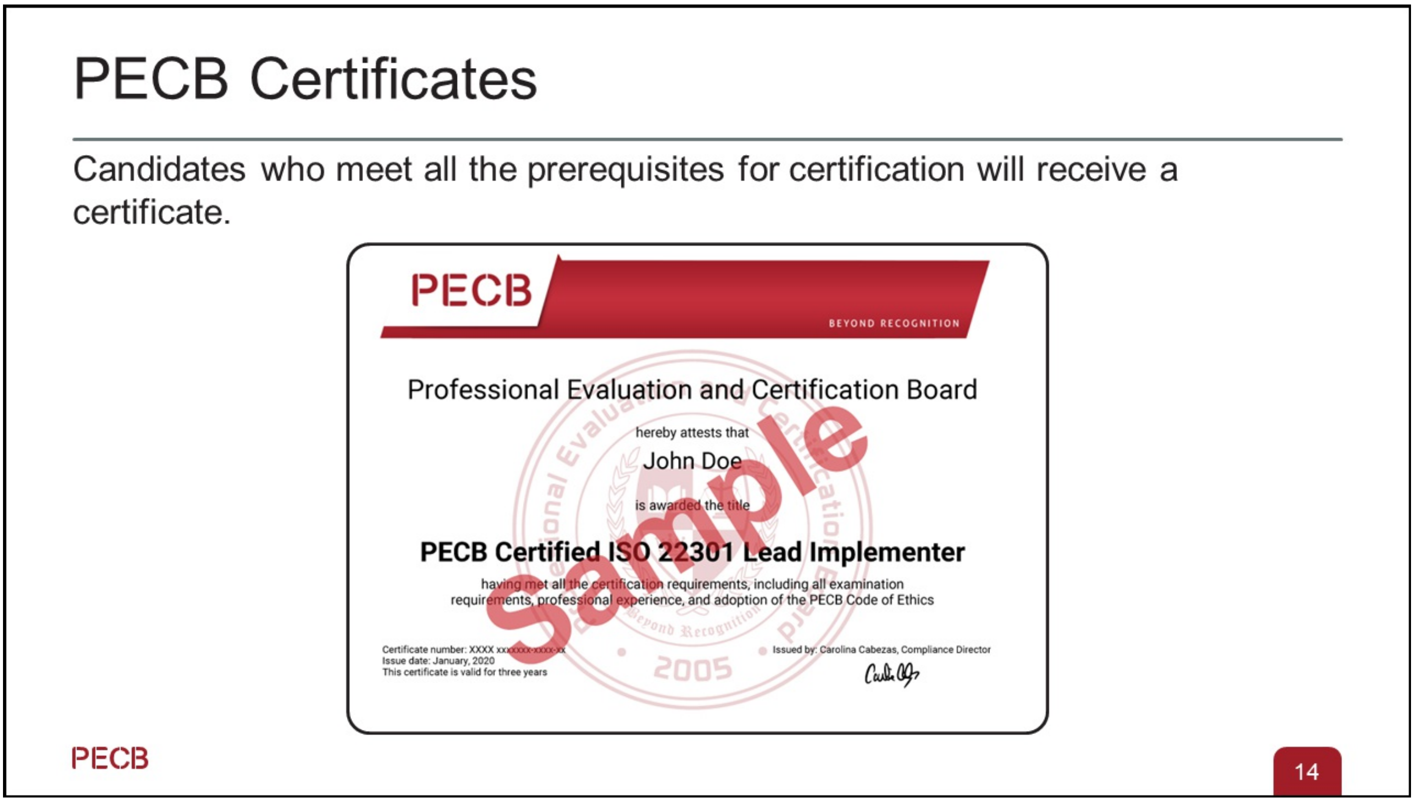
13

Individuals who do not meet all the prerequisites for certification cannot claim to be PECB ISO 22301 Lead Implementer-certified.

A less experienced candidate can apply for the “PECB Certified ISO 22301 Implementer” credential or “PECB Certified ISO 22301 Provisional Implementer” credential.

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

The certification process will be explained in detail on the last day of this training course.



# PECB Certificates

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

PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

John Doe

is awarded the title

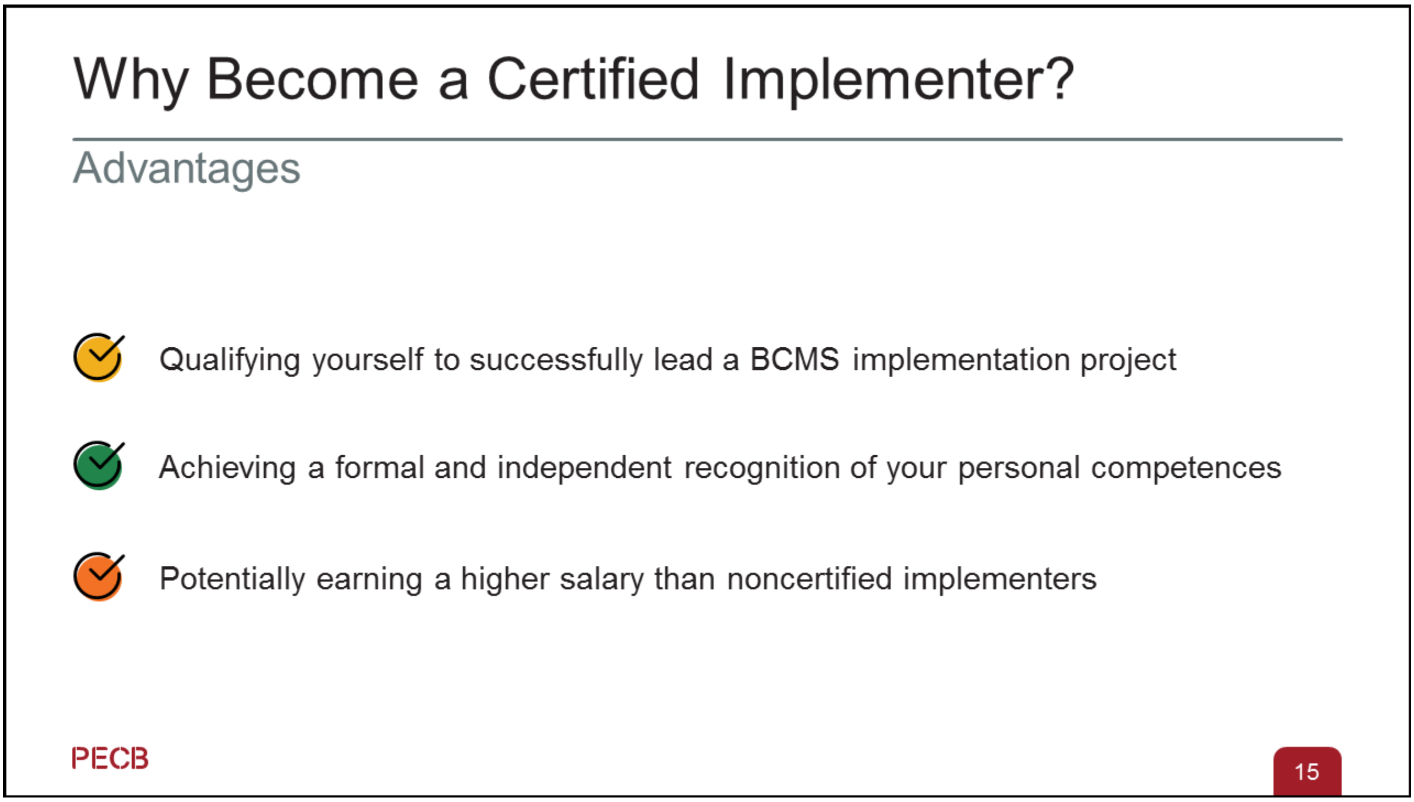
**PECB Certified ISO 22301 Lead Implementer**

having met all the certification requirements, including all examination requirements, professional experience, and adoption of the PECB Code of Ethics

Certificate number: XXXX xxxxxxx-xxxx-xx
Issue date: January, 2020
This certificate is valid for three years

Issued by: Carolina Cabezas, Compliance Director

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



# Why Become a Certified Implementer?

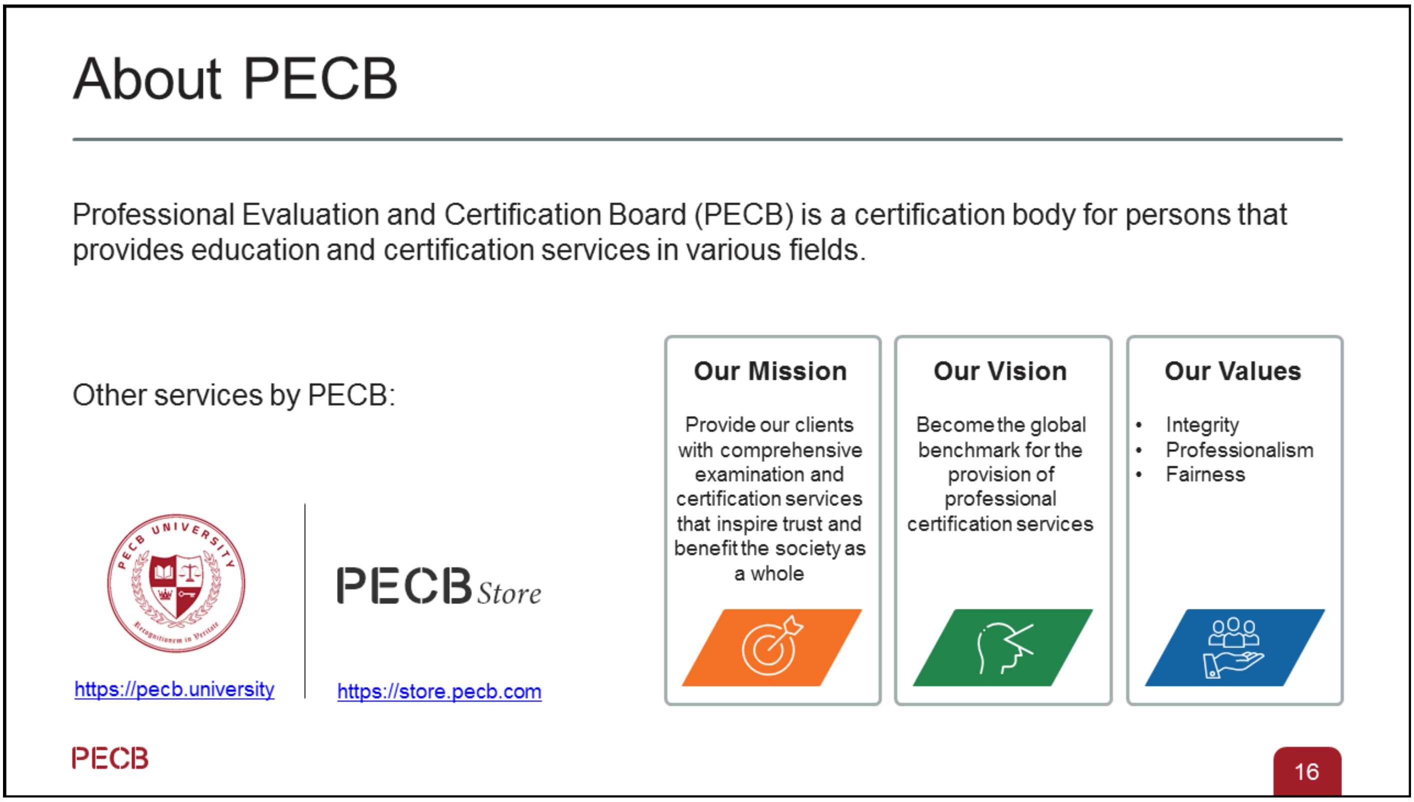
## Advantages

- ✓ Qualifying yourself to successfully lead a BCMS implementation project
- ✓ Achieving a formal and independent recognition of your personal competences
- ✓ Potentially earning a higher salary than noncertified implementers

PECB

15

- Certification is a formal recognition of your professional competence to perform job-related responsibilities.
- An internationally recognized certification can help you maximize your career potential and reach your professional goals.
- Research shows that certified implementers earn considerably higher average salaries than noncertified implementers.



# About PECB

Professional Evaluation and Certification Board (PECB) is a certification body for persons that provides education and certification services in various fields.

Other services by PECB:

https://pecb.university

https://store.pecb.com

**Our Mission**

Provide our clients with comprehensive examination and certification services that inspire trust and benefit the society as a whole

**Our Vision**

Become the global benchmark for the provision of professional certification services

**Our Values**

- Integrity
- Professionalism
- Fairness

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

## Questions?

# Section 2

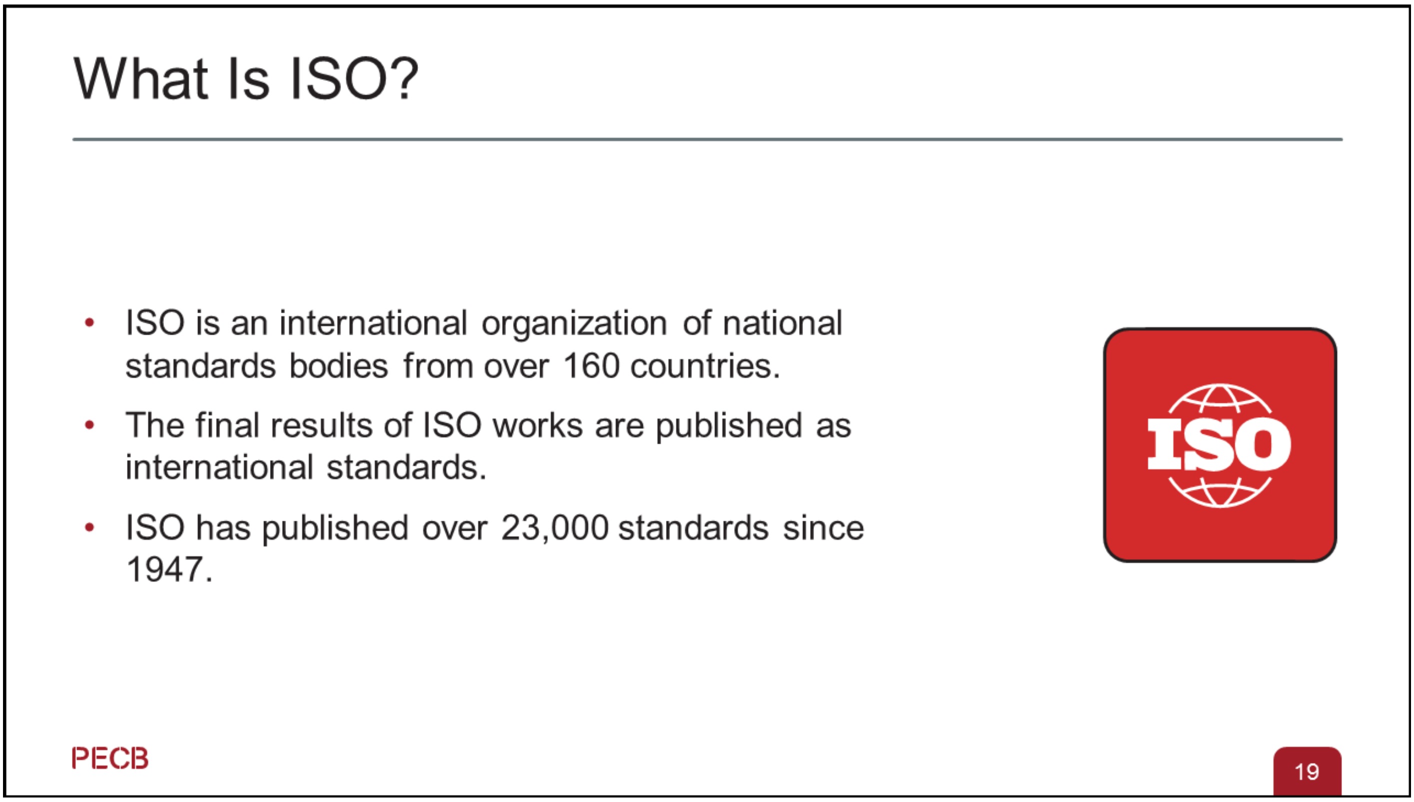
## Standards and regulatory frameworks

- What is ISO?
- The ISO 22300 family of standards
- Benefits of ISO 22301

PECB

18

This section introduces the International Organization for Standardization (ISO) and ISO 22300 family of standards. ISO 22301 and its benefits are also discussed.



## What Is ISO?

- ISO is an international organization of national standards bodies from over 160 countries.
- The final results of ISO works are published as international standards.
- ISO has published over 23,000 standards since 1947.

PECB

19

**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.

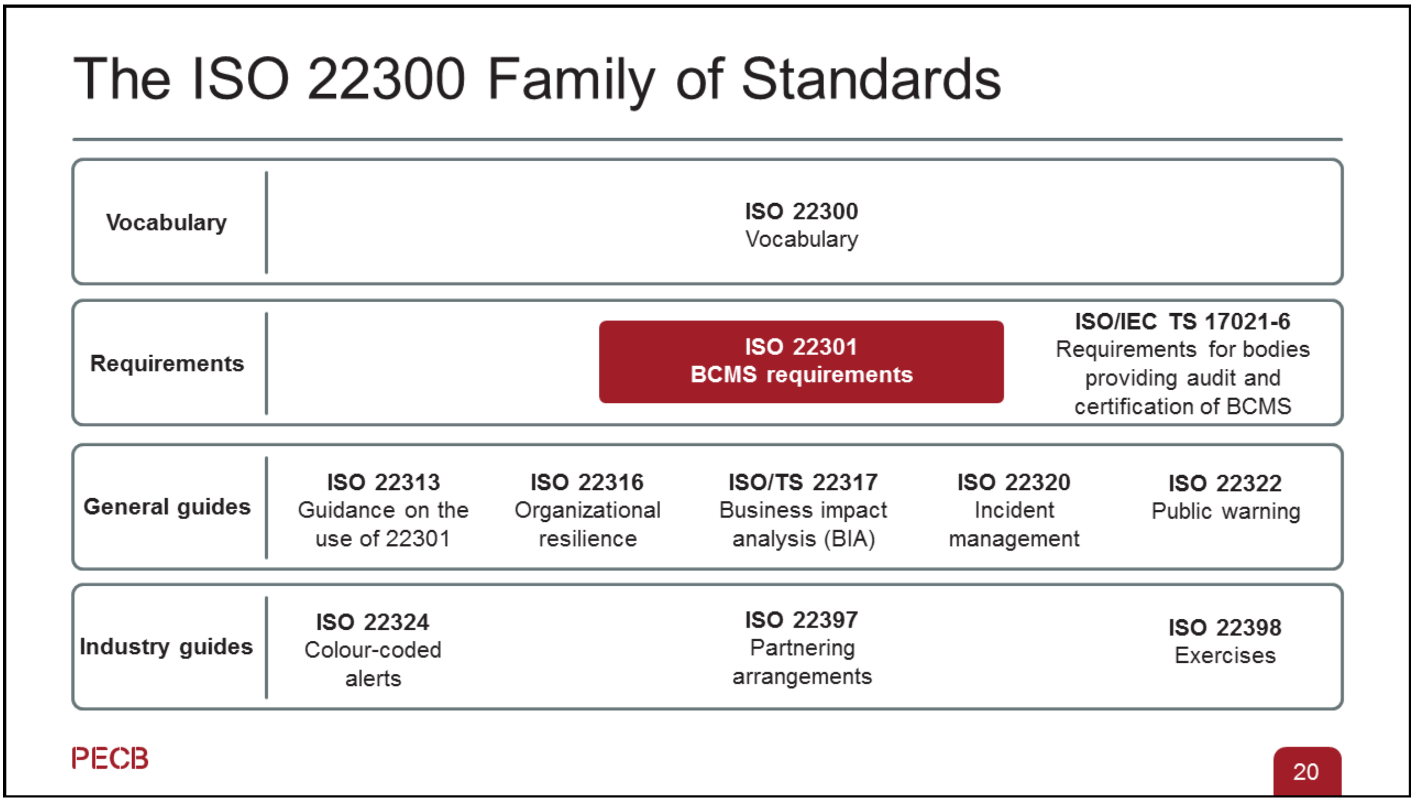
**3.ISO standards are developed through a multi-stakeholder process.**

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 22300 Family of Standards

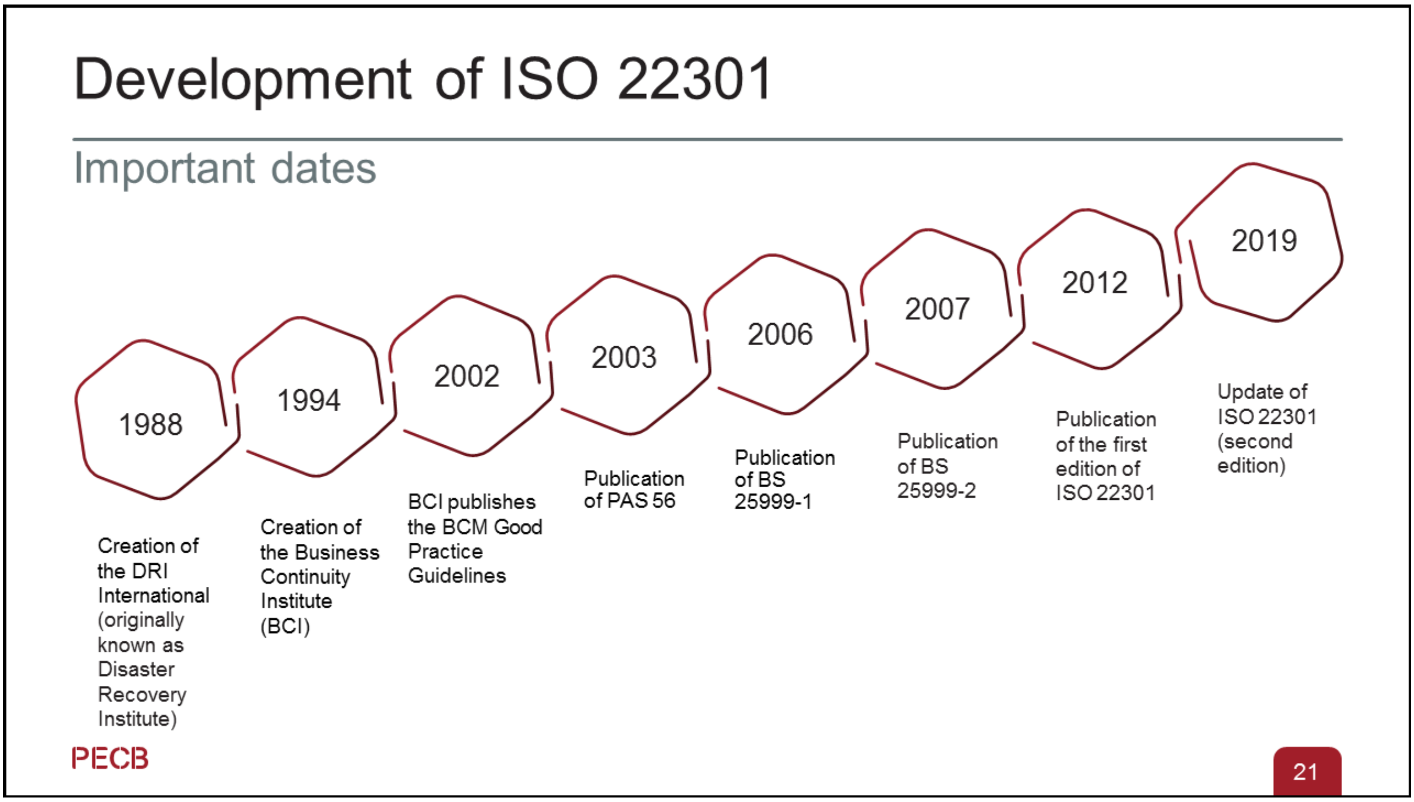
| | | | | | |
|---|---|---|---|---|---|
| Vocabulary | ISO 22300<br>Vocabulary | | | | |
| Requirements | | | ISO 22301<br>BCMS requirements | | ISO/IEC TS 17021-6<br>Requirements for bodies providing audit and certification of BCMS |
| General guides | ISO 22313<br>Guidance on the use of 22301 | ISO 22316<br>Organizational resilience | ISO/TS 22317<br>Business impact analysis (BIA) | ISO 22320<br>Incident management | ISO 22322<br>Public warning |
| Industry guides | ISO 22324<br>Colour-coded alerts | | ISO 22397<br>Partnering arrangements | | ISO 22398<br>Exercises |

PECB

20

The ISO 22300 family includes the following standards:

- **ISO 22300** presents the basic concepts and vocabulary used in security and resilience standards.
- **ISO 22301** defines the requirements to implement, maintain, and improve a business continuity management systems (BCMS) with the aim of preparing, responding, and recovering from disruptive incidents.
- **ISO/IEC TS 17021-6** includes specific competence requirements for personnel involved in the certification process for business continuity management systems.
- **ISO 22313** provides guidance for applying the requirements of ISO 22301.
- **ISO 22316** provides guidance to enhance organizational resilience.
- **ISO/TS 22317** provides guidelines for organizations to establish, implement, and manage a formal and documented business impact analysis (BIA) process.
- **ISO 22320** provides guidelines for incident management.
- **ISO 22322** provides guidelines for developing, handling, and implementing public warning before, during, and after incidents.
- **ISO 22324** provides guidelines for the use of color codes to inform people at risk as well as first response personnel about danger.
- **ISO 22397** provides guidelines for organizations to establish partnering arrangements among each other.
- **ISO 22398** provides guidelines for an organization to plan, conduct, and improve an exercise program.



## Development of ISO 22301

### Important dates

1988
Creation of the DRI International (originally known as Disaster Recovery Institute)

1994
Creation of the Business Continuity Institute (BCI)

2002
BCI publishes the BCM Good Practice Guidelines

2003
Publication of PAS 56

2006
Publication of BS 25999-1

2007
Publication of BS 25999-2

2012
Publication of the first edition of ISO 22301

2019
Update of ISO 22301 (second edition)

PECB

21

The two main associations of business continuity management experts were created in the 80s-90s:

1. The DRI International (originally known as Disaster Recovery Institute)
2. The Business Continuity Institute (BCI)

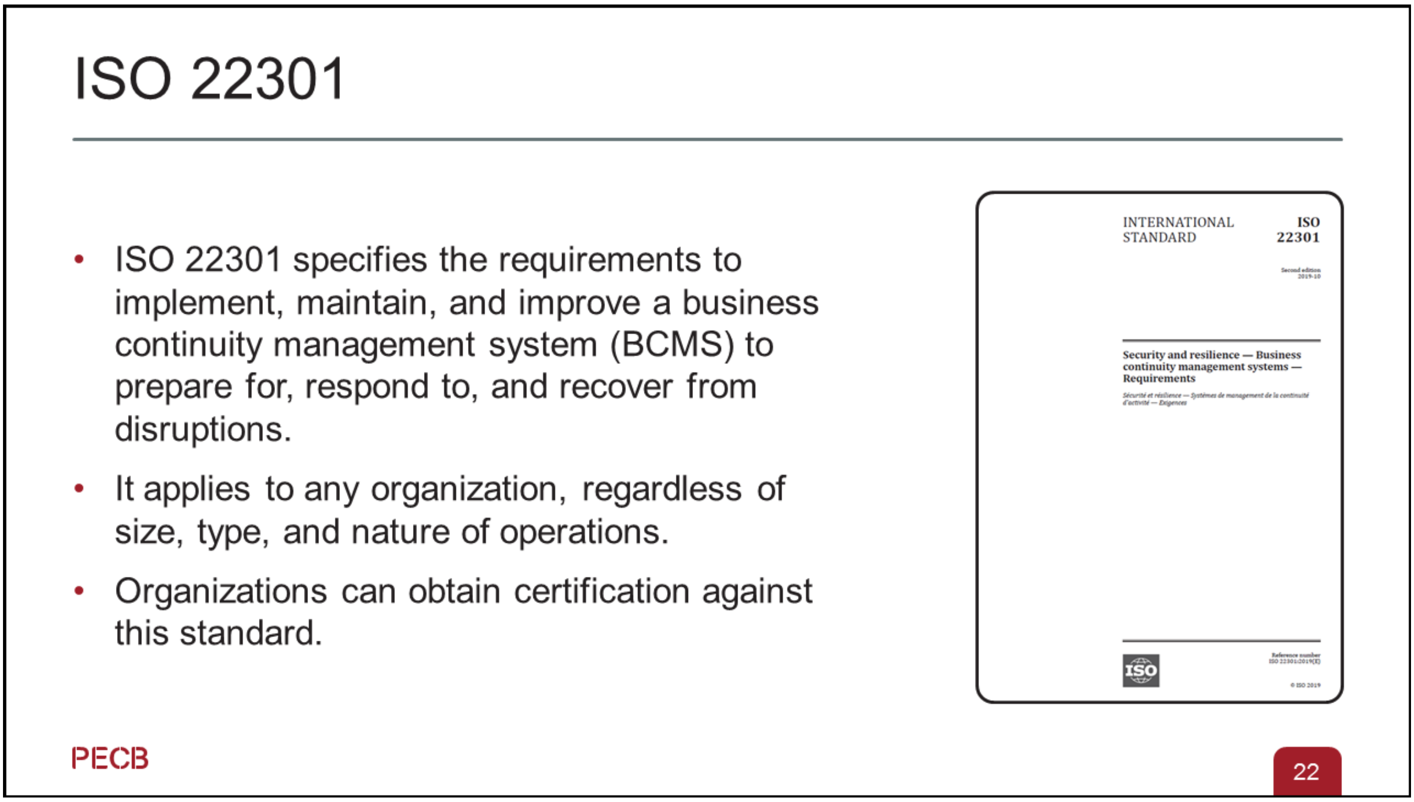
The British Standards Institution (BSI), in conjunction with the Business Continuity Institute (BCI), published PAS 56 in 2003. This was later replaced by BS 25999.

The ISO Technical Committee 223, often referred to as “TC 223 Societal security,” examined the existing standards and created a framework for a global BCM standard. To create the new business continuity standard, ISO adapted content from some of its existing standards, such as ISO 9000 and ISO 14000.

However, the proliferation of business continuity standards released between 2000 and 2010 made the development of a global standard more difficult for officials. Most of the European Commission members adopted an existing BCM standard, typically BS 25999, while nations such as Japan and India turned existing banking and finance standards into national standards.

BS 25999-2 was withdrawn in November 2012, having been replaced by the international standard ISO 22301. BS 25999-1 was withdrawn in early 2013, having been replaced by ISO 22313.

**In 2019, the second edition of ISO 22301 was published.** This version replaced the 2012 version.



## ISO 22301

- ISO 22301 specifies the requirements to implement, maintain, and improve a business continuity management system (BCMS) to prepare for, respond to, and recover from disruptions.
- It applies to any organization, regardless of size, type, and nature of operations.
- Organizations can obtain certification against this standard.

INTERNATIONAL STANDARD
ISO 22301
Second edition 2019-10
Security and resilience — Business continuity management systems — Requirements
Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences
ISO
Reference number ISO 22301:2019(E)
© ISO 2019
PECB
22

***ISO 22301, clause 1 Scope***

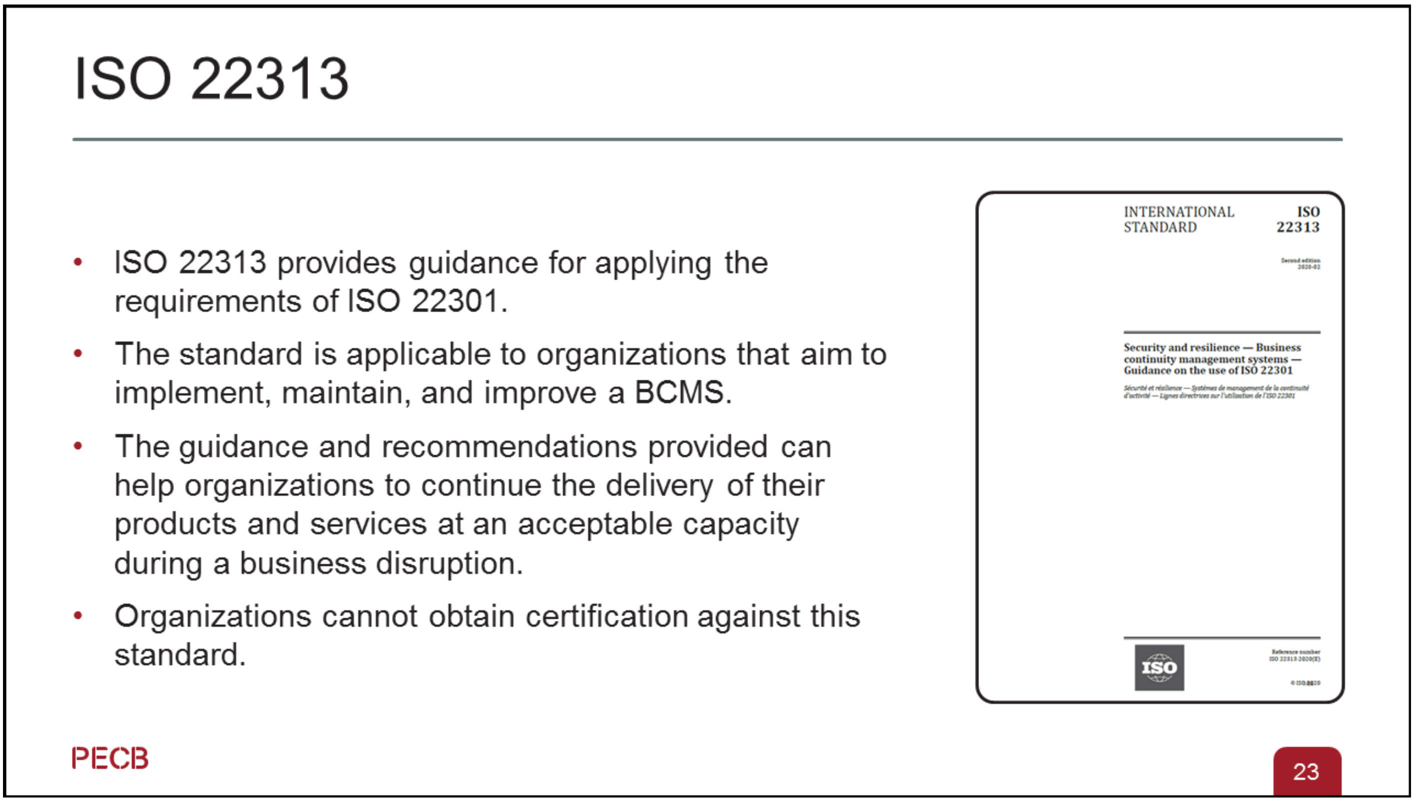
*This document specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise.*

*The requirements specified in this document are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.*

*This document is applicable to all types and sizes of organizations that:*

a. *implement, maintain and improve a BCMS;*
b. *seek to ensure conformity with stated business continuity policy;*
c. *need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;*
d. *seek to enhance their resilience through the effective application of the BCMS.*

*This document can be used to assess an organization's ability to meet its own business continuity needs and obligations.*



# ISO 22313

- ISO 22313 provides guidance for applying the requirements of ISO 22301.
- The standard is applicable to organizations that aim to implement, maintain, and improve a BCMS.
- The guidance and recommendations provided can help organizations to continue the delivery of their products and services at an acceptable capacity during a business disruption.
- Organizations cannot obtain certification against this standard.

INTERNATIONAL STANDARD

ISO 22313

Second edition
2020-02

**Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301**

*Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices sur l'utilisation de l'ISO 22301*

Reference number
ISO 22313:2020(E)

© ISO 2020

PECB

23

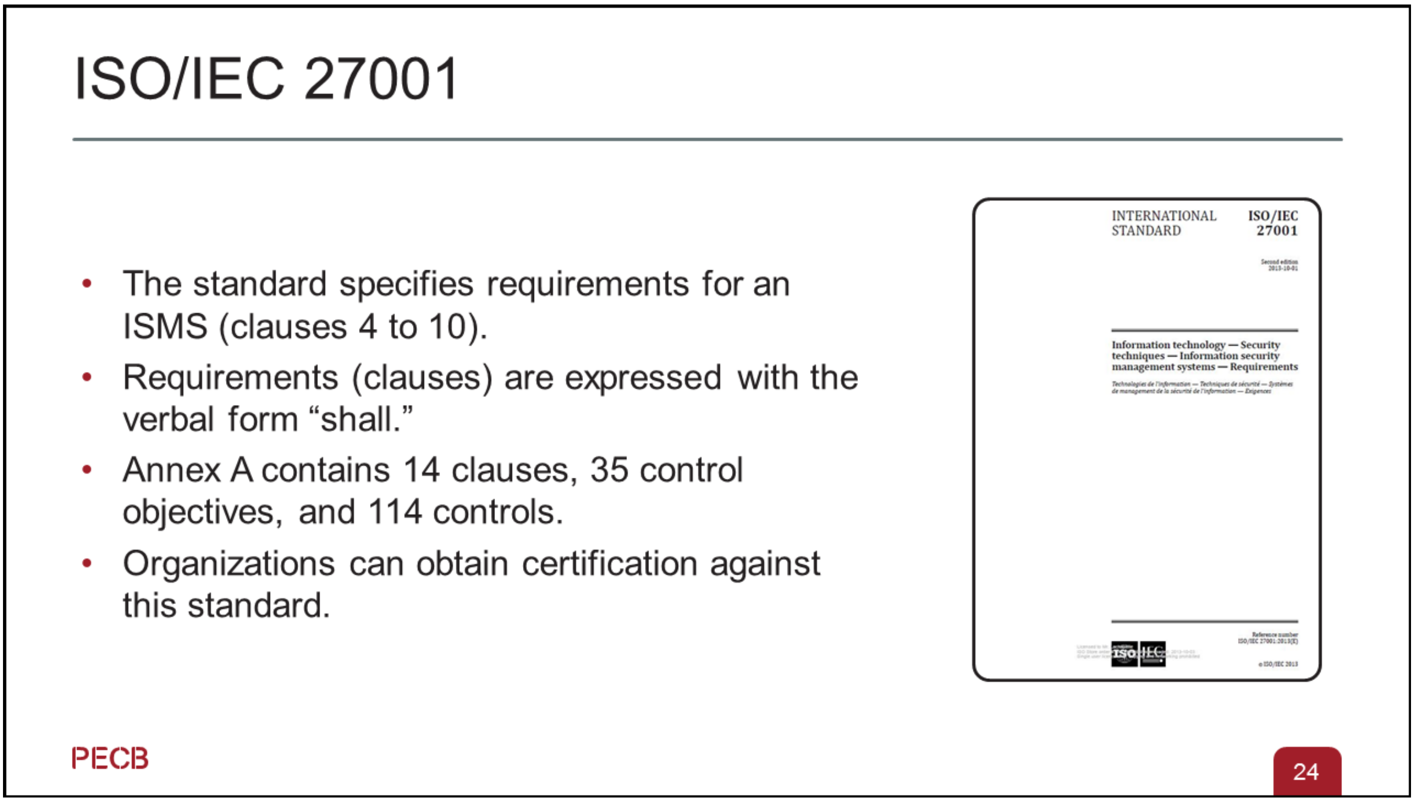
***ISO 22313, clause 1 Scope***

*This document gives guidance and recommendations for applying the requirements of the business continuity management system (BCMS) given in ISO 22301. The guidance and recommendations are based on good international practice.*

*This document is applicable to organizations that:*

a. *implement, maintain and improve a BCMS;*
b. *seek to ensure conformity with stated business continuity policy;*
c. *need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;*
d. *seek to enhance their resilience through the effective application of the BCMS.*

*The guidance and recommendations are applicable to all sizes and types of organizations, including large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors. The approach adopted depends on the organization's operating environment and complexity.*



## ISO/IEC 27001

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

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition 2013-10-01

**Information technology — Security techniques — Information security management systems — Requirements**

*Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

Reference number ISO/IEC 27001:2013(E)

© ISO/IEC 2013

PECB

24

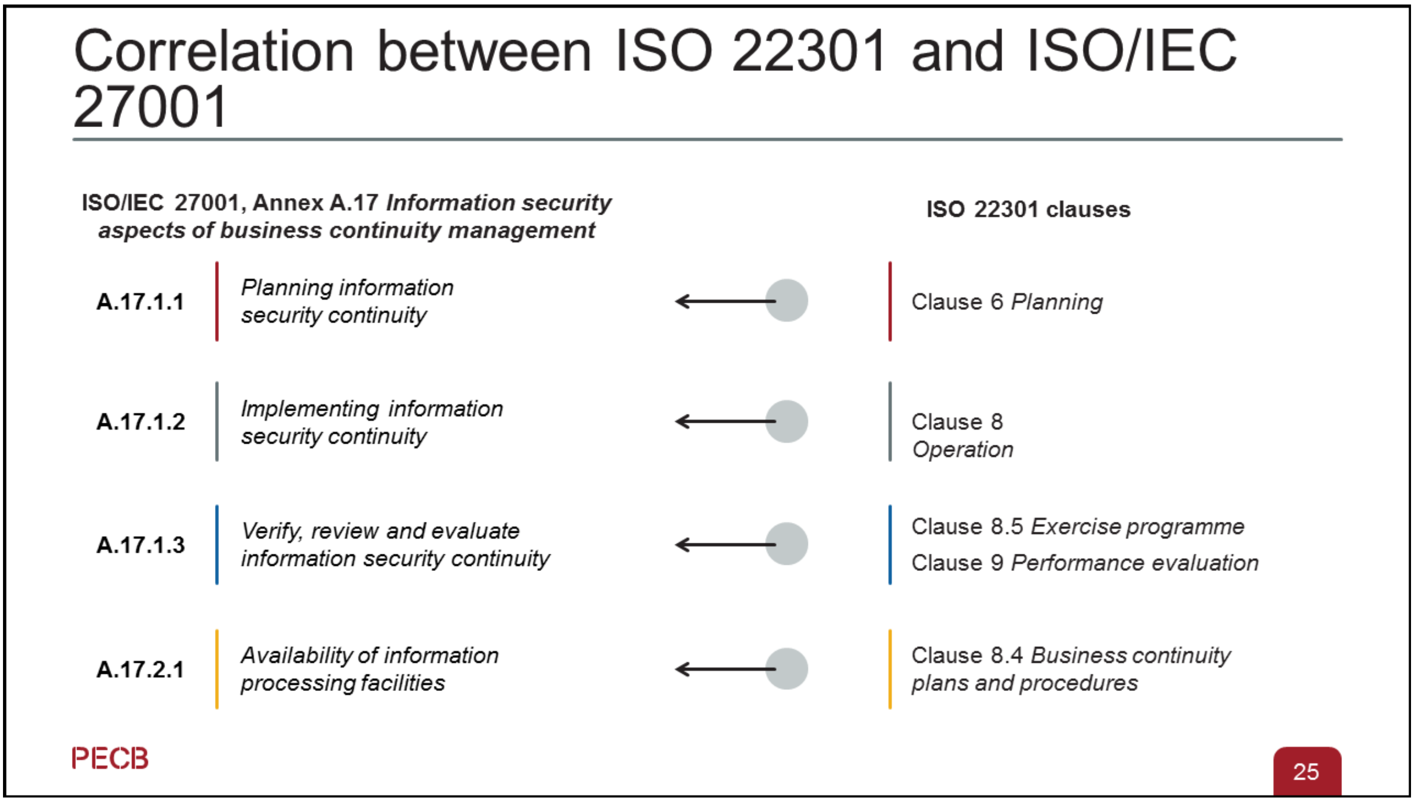
***ISO/IEC 27001, clause 0.1 General***

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

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

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

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



# Correlation between ISO 22301 and ISO/IEC 27001

| **ISO/IEC 27001, Annex A.17** ***Information security aspects of business continuity management*** | | **ISO 22301 clauses** |
|---|---|---|
| **A.17.1.1** | *Planning information security continuity* | Clause 6 *Planning* |
| **A.17.1.2** | *Implementing information security continuity* | Clause 8<br>*Operation* |
| **A.17.1.3** | *Verify, review and evaluate information security continuity* | Clause 8.5 *Exercise programme*<br>Clause 9 *Performance evaluation* |
| **A.17.2.1** | *Availability of information processing facilities* | Clause 8.4 *Business continuity plans and procedures* |

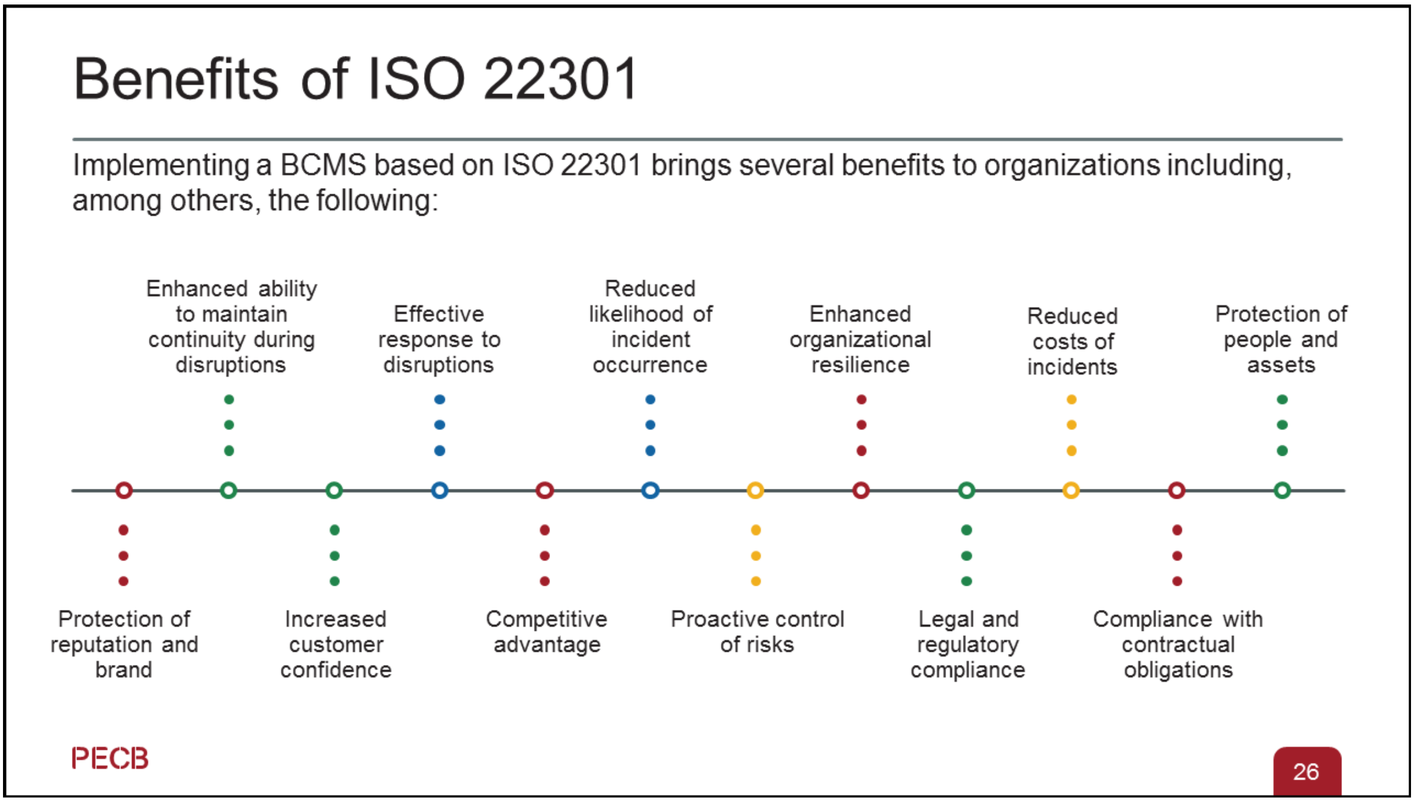
PECB

25

We can easily match the controls of ISO/IEC 27001 with the requirements of ISO 22301.

If the ISO/IEC 27001 certification has been obtained, the right management framework is in place and ISO 22301 implementation is already on the right track.

Reciprocally, if ISO 22301 certification has been obtained, the part of Annex A.17 of ISO/IEC 27001 implementation can be considered as covered.



## Benefits of ISO 22301

Implementing a BCMS based on ISO 22301 brings several benefits to organizations including, among others, the following:

- Protection of reputation and brand
- Enhanced ability to maintain continuity during disruptions
- Increased customer confidence
- Effective response to disruptions
- Competitive advantage
- Reduced likelihood of incident occurrence
- Proactive control of risks
- Enhanced organizational resilience
- Legal and regulatory compliance
- Reduced costs of incidents
- Compliance with contractual obligations
- Protection of people and assets

PECB

26

***ISO 22301, clause 0.2 Benefits of a business continuity management system***

*The purpose of a BCMS is to prepare for, provide and maintain controls and capabilities for managing an organization's overall ability to continue to operate during disruptions. In achieving this, the organization is:*

a. *from a business perspective:*
   1. *supporting its strategic objectives;*
   2. *creating a competitive advantage;*
   3. *protecting and enhancing its reputation and credibility;*
   4. *contributing to organizational resilience;*

b. *from a financial perspective:*
   1. *reducing legal and financial exposure;*
   2. *reducing direct and indirect costs of disruptions;*

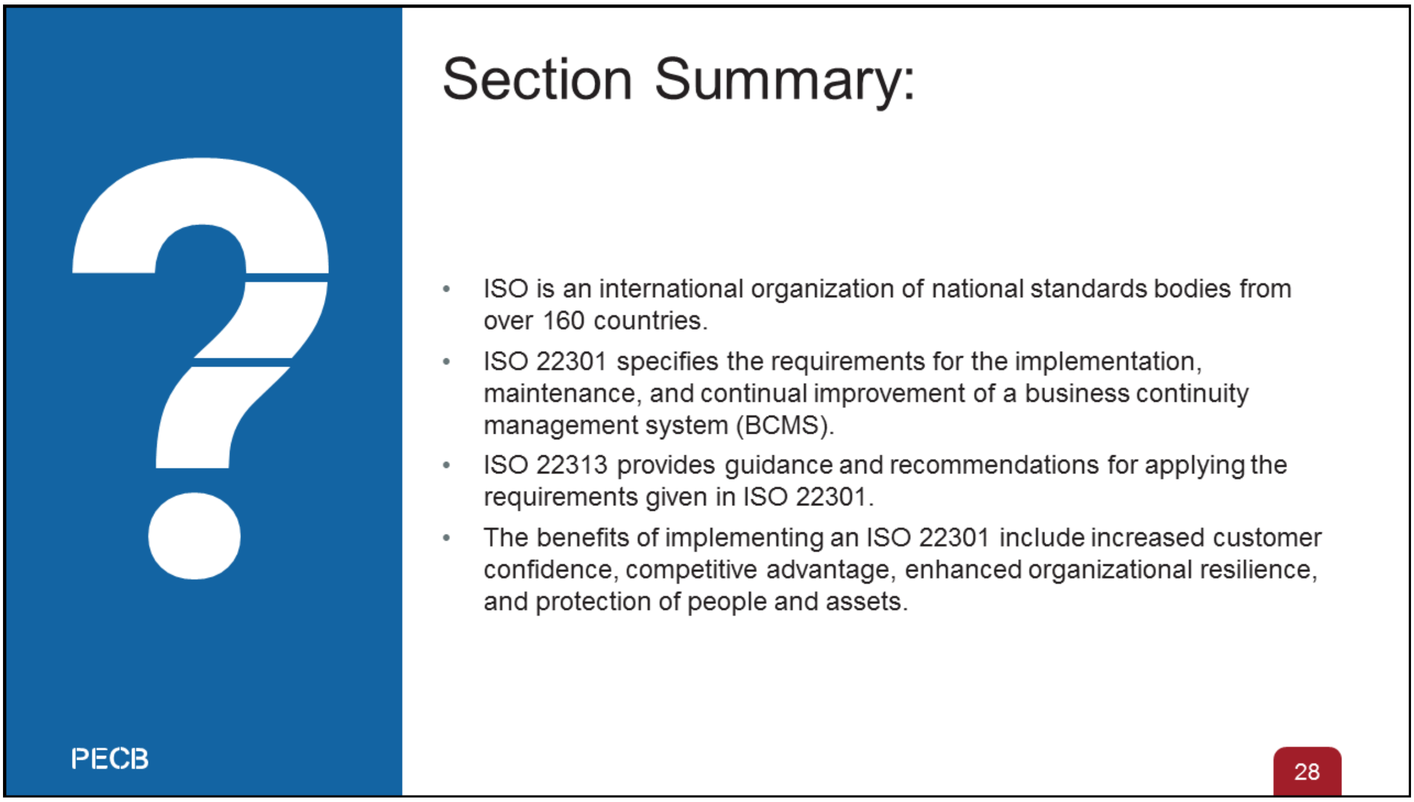
c. *from the perspective of interested parties:*
   1. *protecting life, property and the environment;*
   2. *considering the expectations of interested parties;*
   3. *providing confidence in the organization's ability to succeed;*

d. *from an internal processes perspective:*
   1. *improving its capability to remain effective during disruptions;*
   2. *demonstrating proactive control of risks effectively and efficiently;*
   3. *addressing operational vulnerabilities.*

Quiz 1

**Quiz 1: Standards and regulatory frameworks**

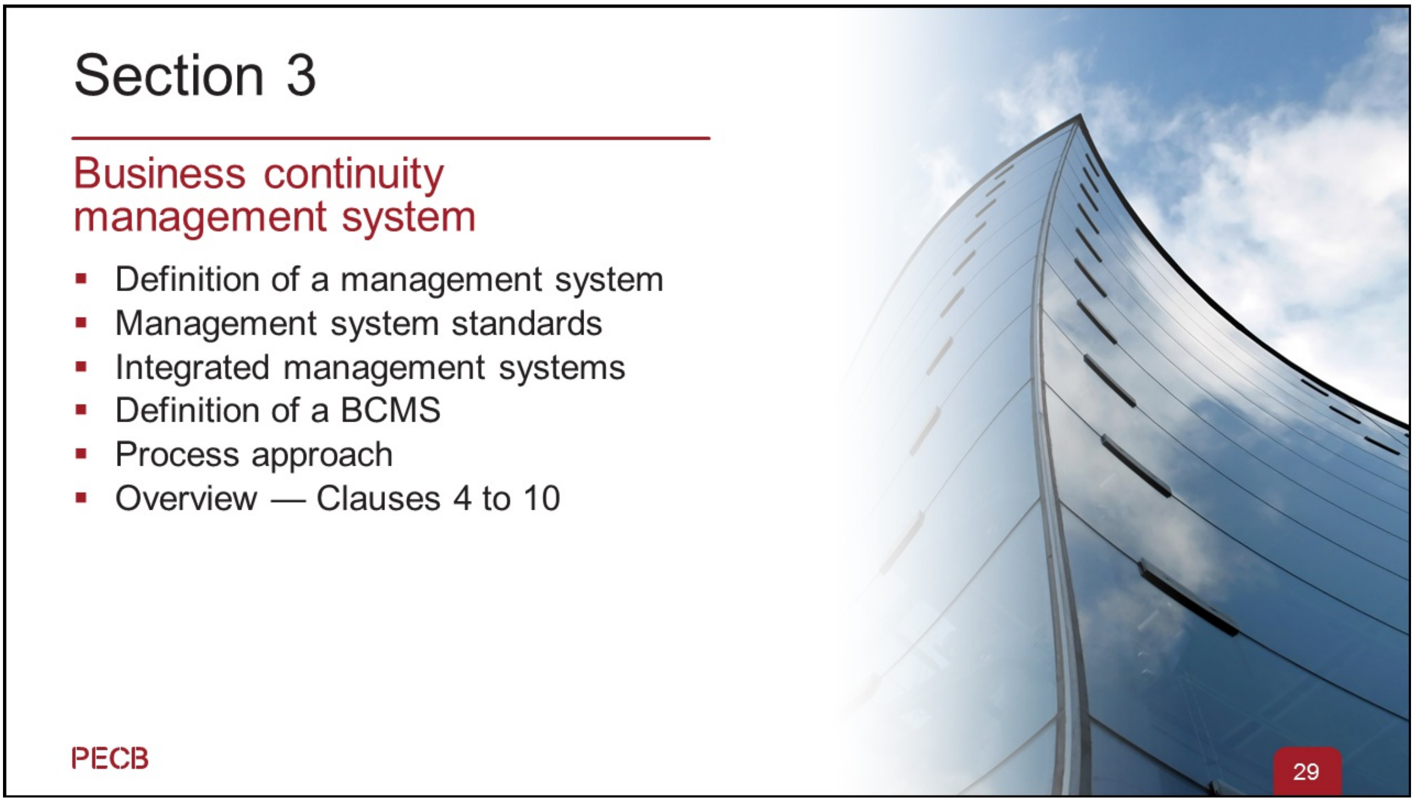
1. **ISO 22301 provides guidelines on how to implement, maintain, and improve a business continuity management system (BCMS).**
    A. True
    B. False
2. **Which controls of ISO/IEC 27001's annex are considered similar to some clauses of ISO 22301?**
    A. Annex A.14
    B. Annex A.17
    C. Annex A.11
3. **Which benefit can be gained from the implementation of a BCMS?**
    A. Increased flexibility
    B. Increased access to advanced technologies
    C. Increased customer confidence
4. **Being ISO/IEC 27001 certified lays the foundation for an easier and more effective implementation of BCMS.**
    A. True
    B. False
5. **Organizations cannot obtain certification against _______________ standard.**
    A. ISO 22313
    B. ISO 22301
    C. ISO/IEC 27001



# Section Summary:

- ISO is an international organization of national standards bodies from over 160 countries.
- ISO 22301 specifies the requirements for the implementation, maintenance, and continual improvement of a business continuity management system (BCMS).
- ISO 22313 provides guidance and recommendations for applying the requirements given in ISO 22301.
- The benefits of implementing an ISO 22301 include increased customer confidence, competitive advantage, enhanced organizational resilience, and protection of people and assets.

PECB

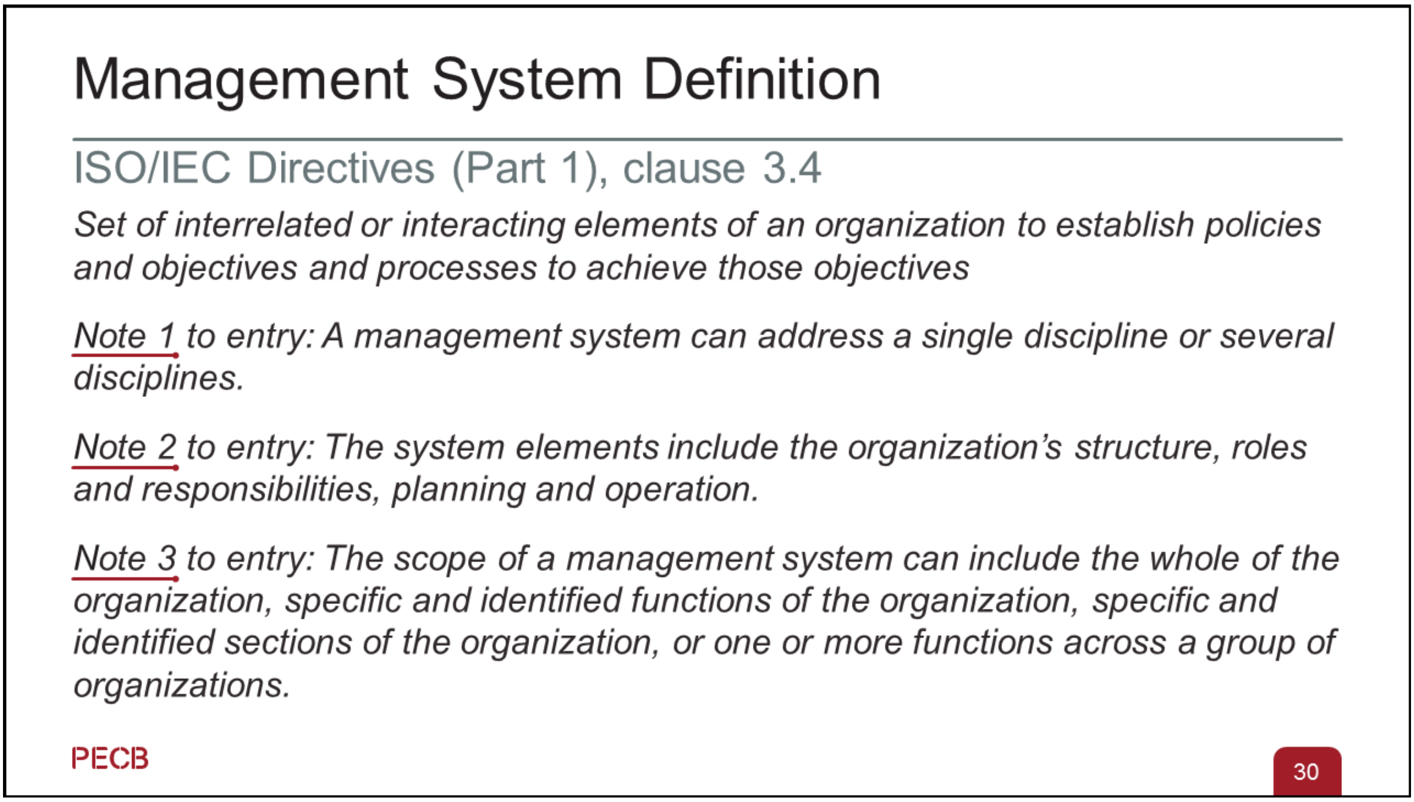


# Section 3

## Business continuity management system

- Definition of a management system
- Management system standards
- Integrated management systems
- Definition of a BCMS
- Process approach
- Overview — Clauses 4 to 10

This section provides information that will help participants gain knowledge on the definition of a management system and a BCMS, process approach, and the structure of ISO 22301, including an overview of clauses 4 to 10.



## Management System Definition

### ISO/IEC Directives (Part 1), clause 3.4

*Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives*

*Note 1 to entry: A management system can address a single discipline or several disciplines.*

*Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.*

*Note 3 to entry: The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.*

30

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

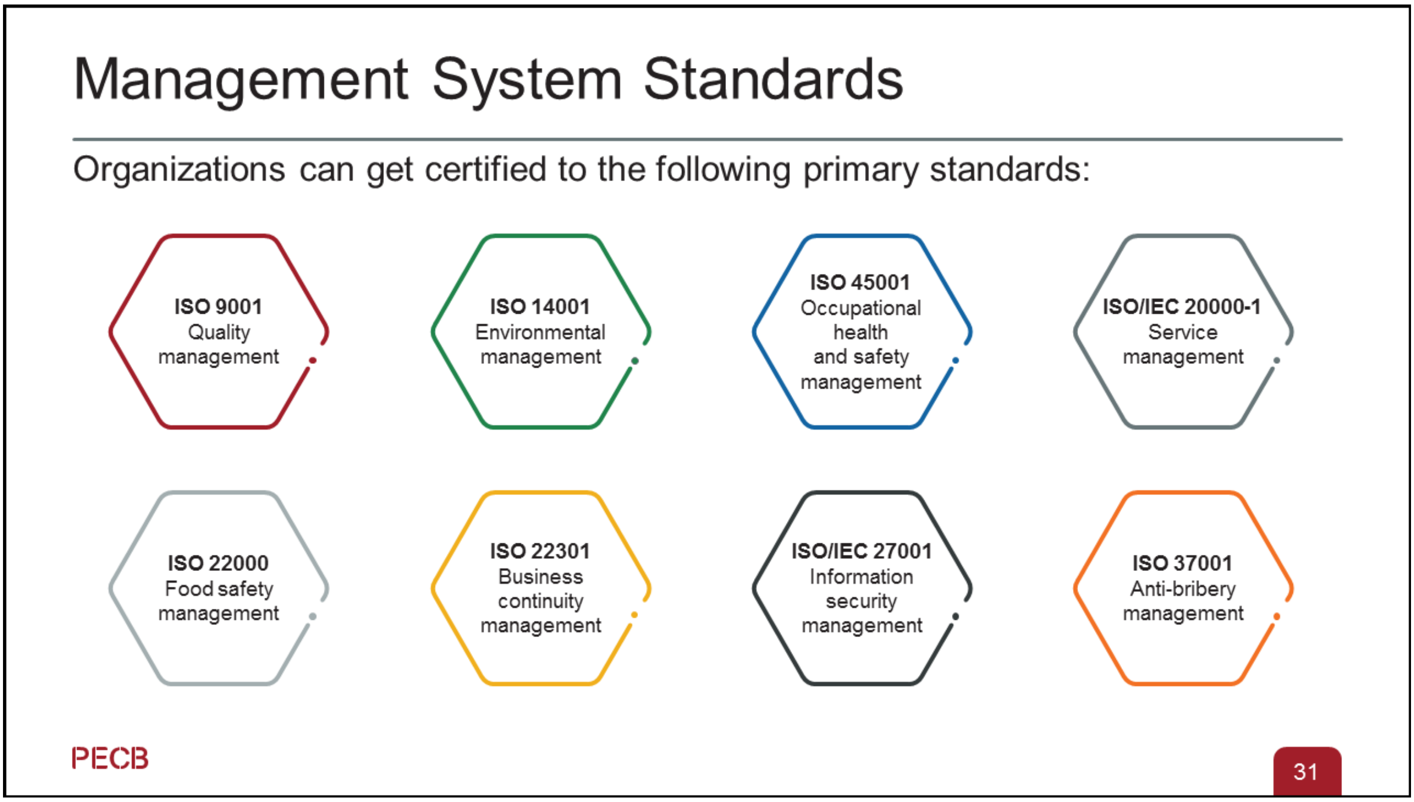
**Note: What is implemented must be controlled and measured, and what is controlled and measured must be managed.** The "Performance evaluation" clause is an essential component of any management system because without the evaluation of the effectiveness of processes and controls in place, it is impossible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

***ISO/IEC Directives (Part 1), Annex L.2.2 Management system standard***

***MSS***

*Standard for management systems*

*Note 1 to entry: For the purposes of this document, this definition also applies to other ISO and IEC deliverables (e.g. TS, PAS).*



## Management System Standards

Organizations can get certified to the following primary standards:

**ISO 9001**
Quality management

**ISO 14001**
Environmental management

**ISO 45001**
Occupational health and safety management

**ISO/IEC 20000-1**
Service management

**ISO 22000**
Food safety management

**ISO 22301**
Business continuity management

**ISO/IEC 27001**
Information security management

**ISO 37001**
Anti-bribery management

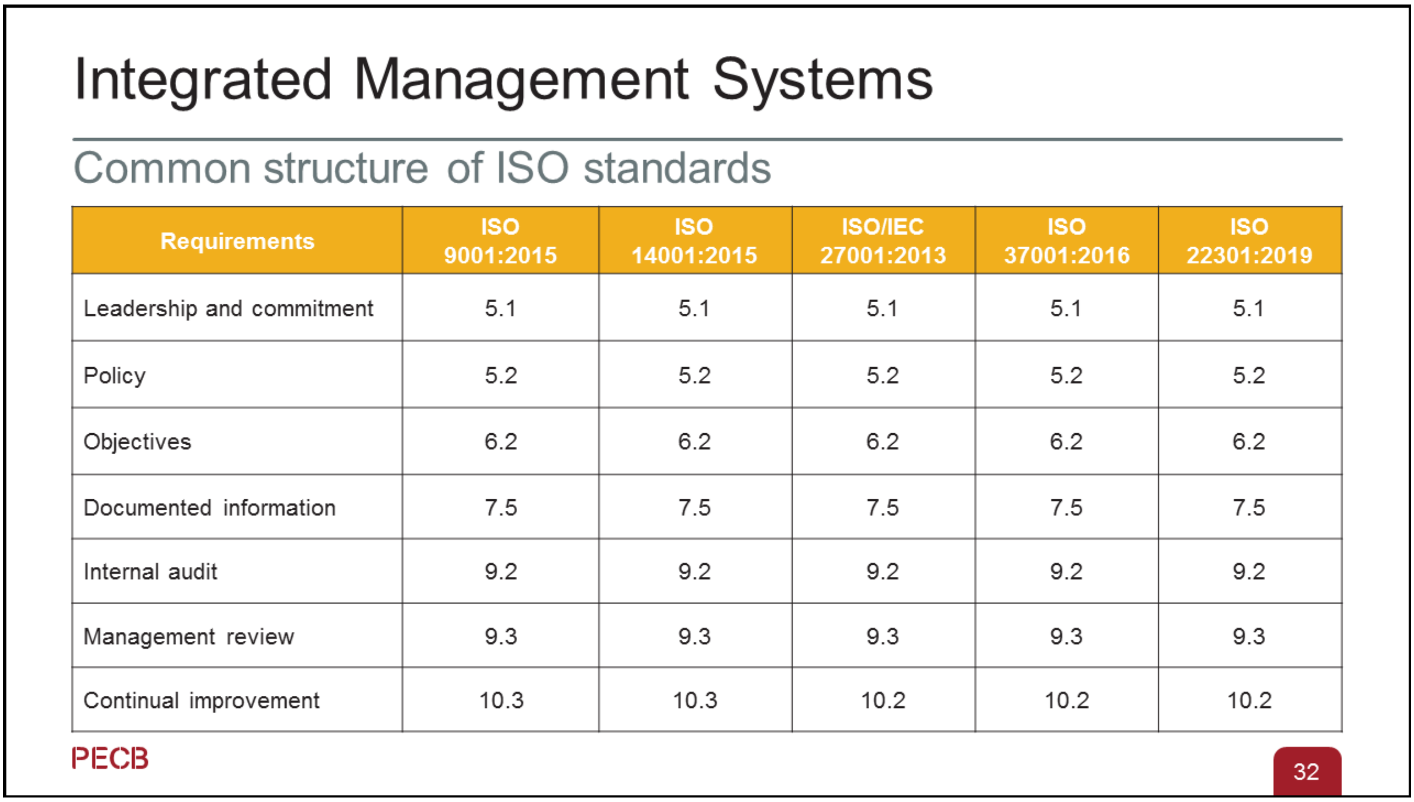
PECB

31

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

ISO 9000 and ISO 14000 families of standards are among the best known. ISO 9001 has become an international reference with regard to quality. ISO 14001, on the other hand, helps organizations enhance their environmental performance. Both standards are generic and applicable to any organization, regardless of size or complexity of processes.

For detailed information on each standard, please visit https://pecb.com or https://www.iso.org.



# Integrated Management Systems

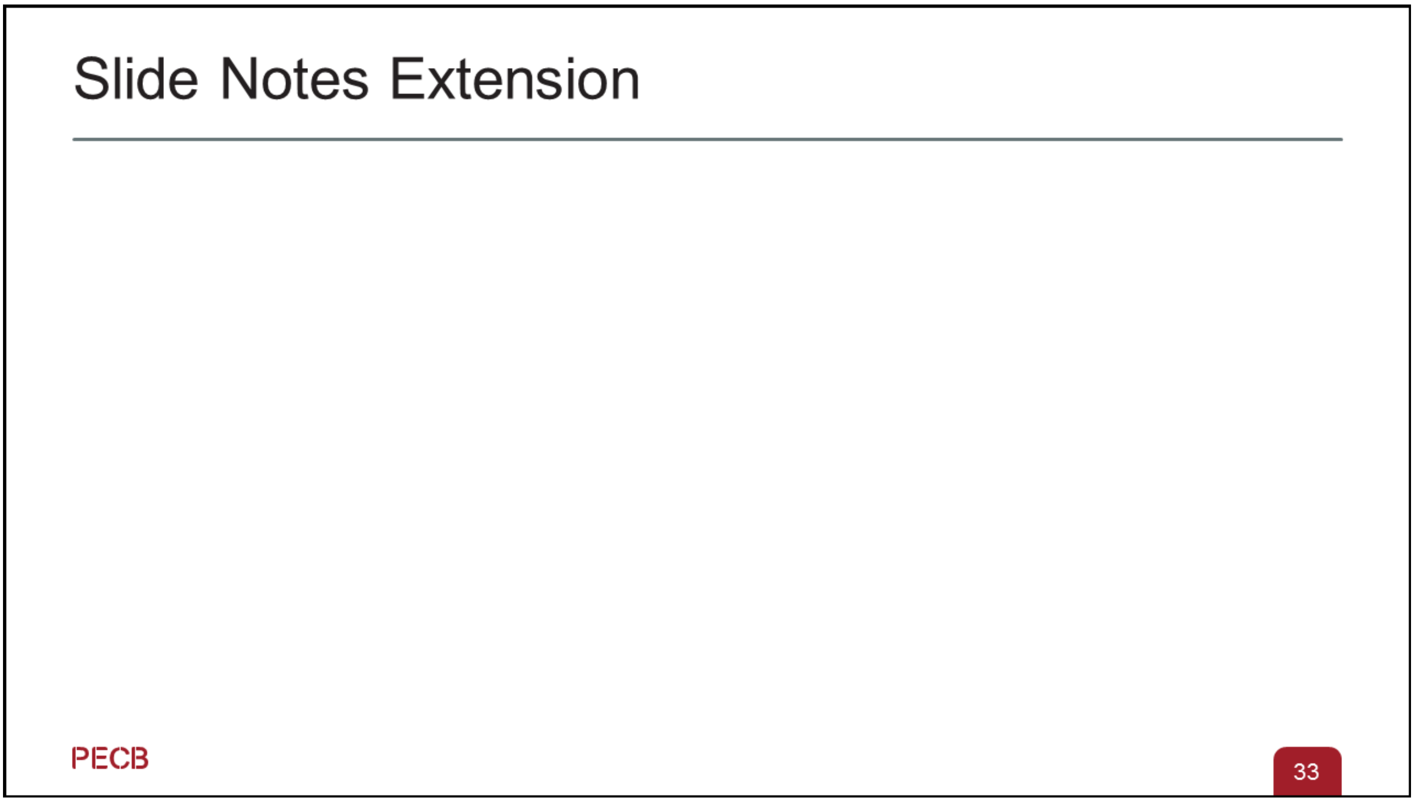
## Common structure of ISO standards

| Requirements | ISO 9001:2015 | ISO 14001:2015 | ISO/IEC 27001:2013 | ISO 37001:2016 | ISO 22301:2019 |
|---|---|---|---|---|---|
| Leadership and commitment | 5.1 | 5.1 | 5.1 | 5.1 | 5.1 |
| Policy | 5.2 | 5.2 | 5.2 | 5.2 | 5.2 |
| Objectives | 6.2 | 6.2 | 6.2 | 6.2 | 6.2 |
| Documented information | 7.5 | 7.5 | 7.5 | 7.5 | 7.5 |
| Internal audit | 9.2 | 9.2 | 9.2 | 9.2 | 9.2 |
| Management review | 9.3 | 9.3 | 9.3 | 9.3 | 9.3 |
| Continual improvement | 10.3 | 10.3 | 10.2 | 10.2 | 10.2 |

As organizations manage several compliance frameworks simultaneously, it is recommended to implement an integrated management system (IMS). An IMS is a management system which integrates all the components of a business into a coherent system so as to enable the achievement of its purpose and mission. The table on the slide presents the requirements that are common to all management systems which allow for integration.

There are several good reasons for integration, including to:

- Harmonize and optimize practices
- Formalize informal systems
- Reduce duplication and therefore costs
- Reduce risks and increase profitability
- Shift focus toward achieving business goals
- Create and maintain consistency
- Improve communication



# Slide Notes Extension

PECB

33

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

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

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

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

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

*Each general principle should be given due consideration and, ideally, when preparing the JS, the proposer should provide a general rationale for each principle, prior to answering the questions associated with the principle.*

*The principles to which the proposer of the MSS should pay due attention when preparing the justification study are:*

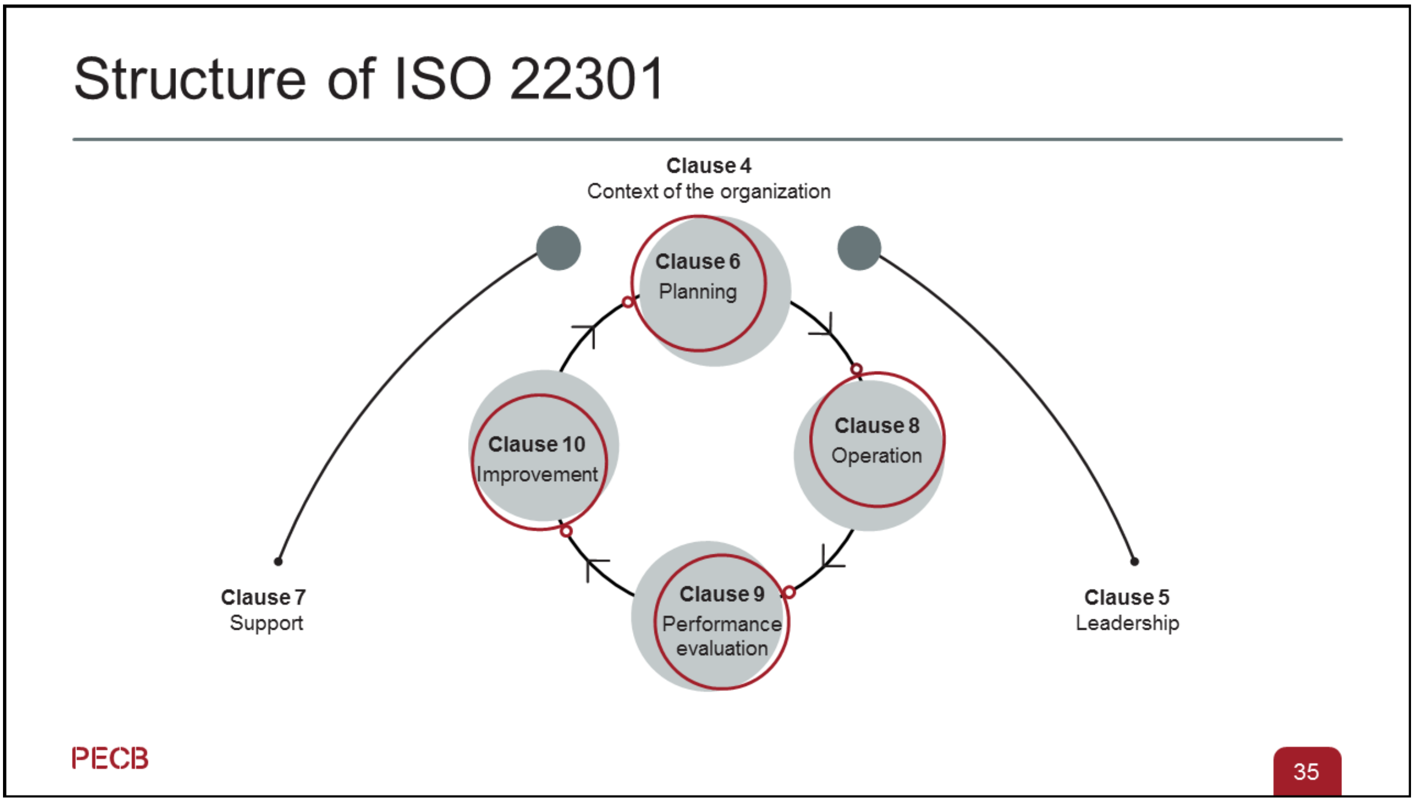
1. *Market relevance*
2. *Compatibility*
3. *Topic coverage*
4. *Flexibility*
5. *Free trade*
6. *Applicability of conformity assessment*
7. *Exclusions*

# Definition of BCMS

## ISO 22300, clause 3.1.21

*Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity*

***Note 1*** *to entry: The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.*



# Structure of ISO 22301

Clause 4
Context of the organization

Clause 6
Planning

Clause 8
Operation

Clause 9
Performance evaluation

Clause 10
Improvement

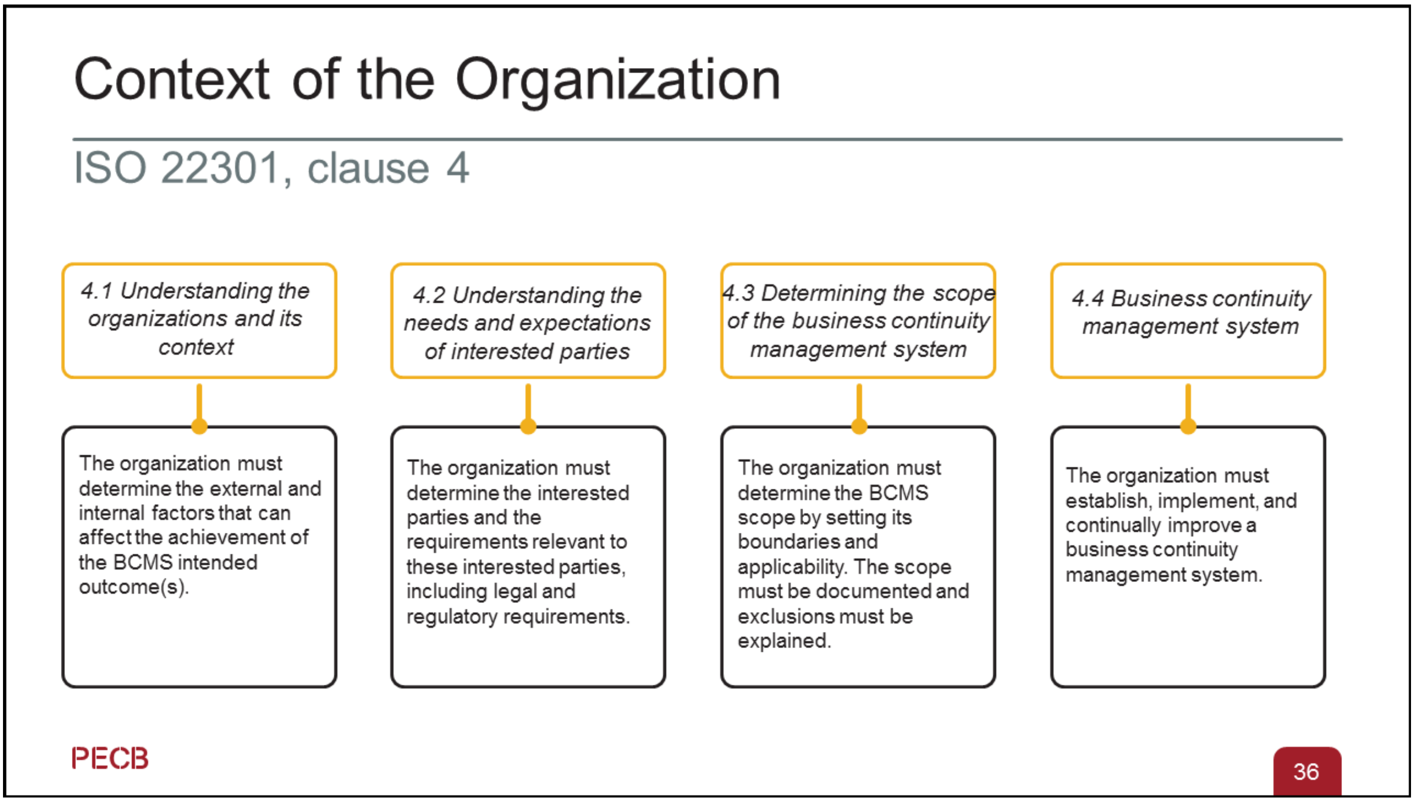
Clause 7
Support

Clause 5
Leadership

PECB

35

An organization seeking certification against ISO 22301 must comply with requirements set out in clauses 4 to 10 of the standard.



# Context of the Organization

## ISO 22301, clause 4

*4.1 Understanding the organizations and its context*

The organization must determine the external and internal factors that can affect the achievement of the BCMS intended outcome(s).

*4.2 Understanding the needs and expectations of interested parties*

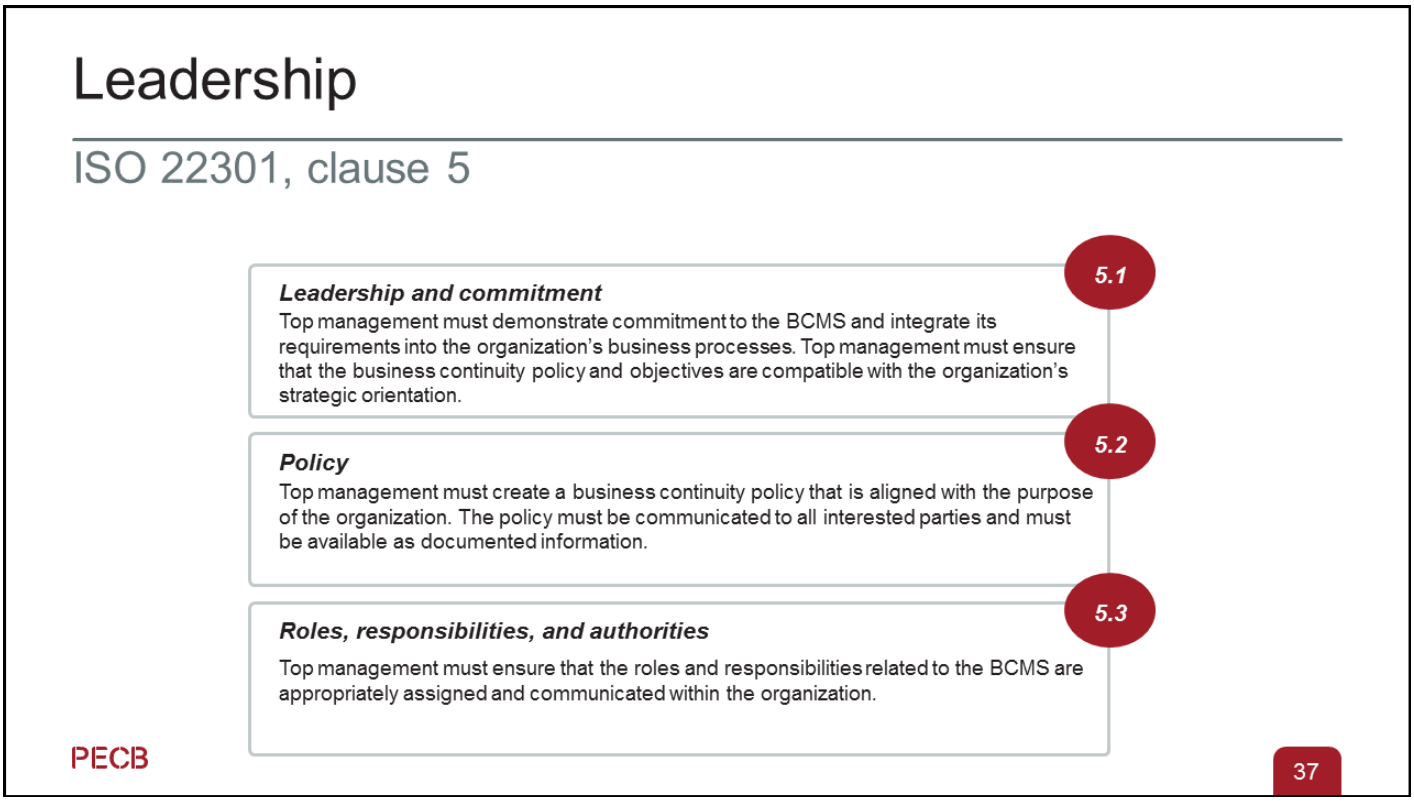
The organization must determine the interested parties and the requirements relevant to these interested parties, including legal and regulatory requirements.

*4.3 Determining the scope of the business continuity management system*

The organization must determine the BCMS scope by setting its boundaries and applicability. The scope must be documented and exclusions must be explained.

*4.4 Business continuity management system*

The organization must establish, implement, and continually improve a business continuity management system.



# Leadership

## ISO 22301, clause 5

5.1

***Leadership and commitment***

Top management must demonstrate commitment to the BCMS and integrate its requirements into the organization's business processes. Top management must ensure that the business continuity policy and objectives are compatible with the organization's strategic orientation.

5.2

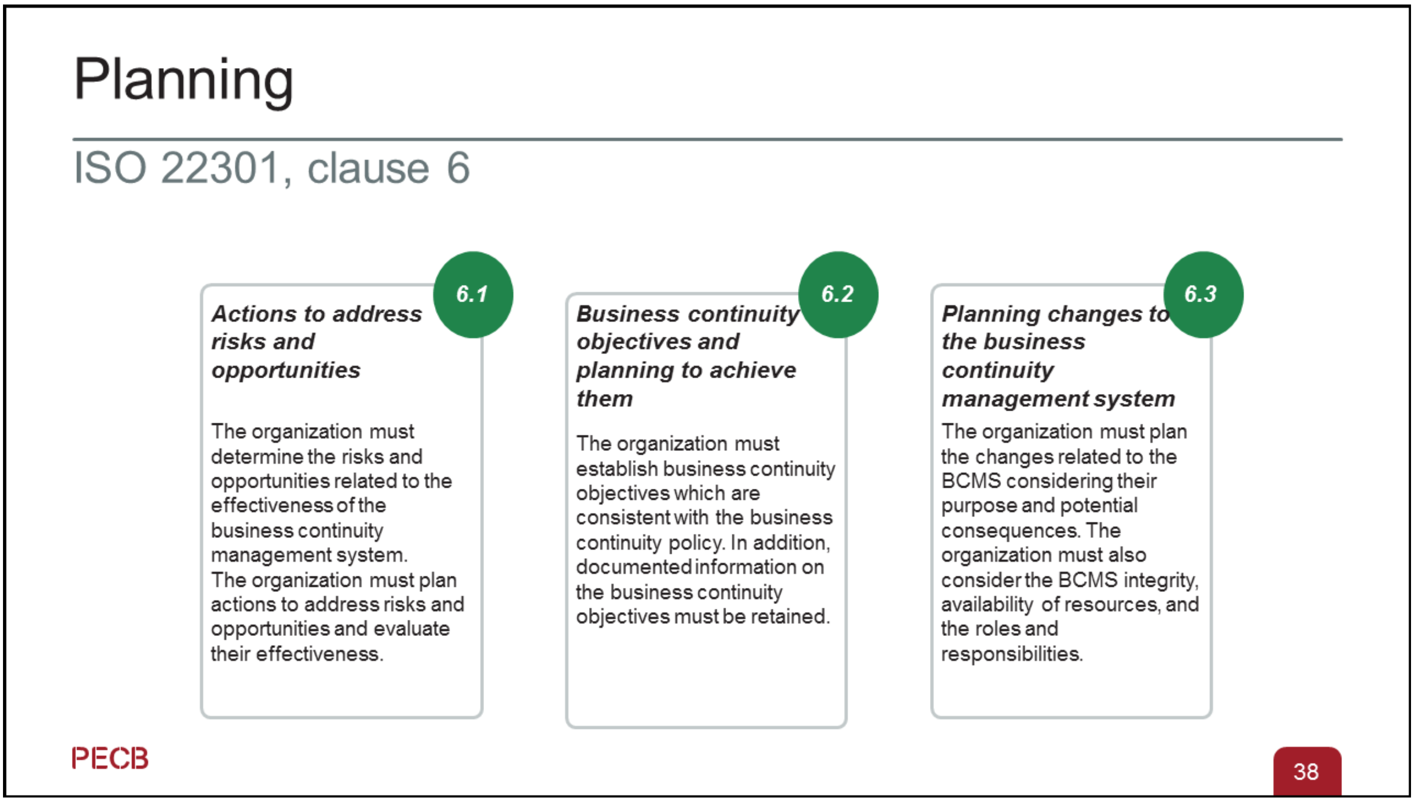
***Policy***

Top management must create a business continuity policy that is aligned with the purpose of the organization. The policy must be communicated to all interested parties and must be available as documented information.

5.3

***Roles, responsibilities, and authorities***

Top management must ensure that the roles and responsibilities related to the BCMS are appropriately assigned and communicated within the organization.



# Planning

## ISO 22301, clause 6

**6.1**

***Actions to address risks and opportunities***

The organization must determine the risks and opportunities related to the effectiveness of the business continuity management system.

The organization must plan actions to address risks and opportunities and evaluate their effectiveness.

**6.2**

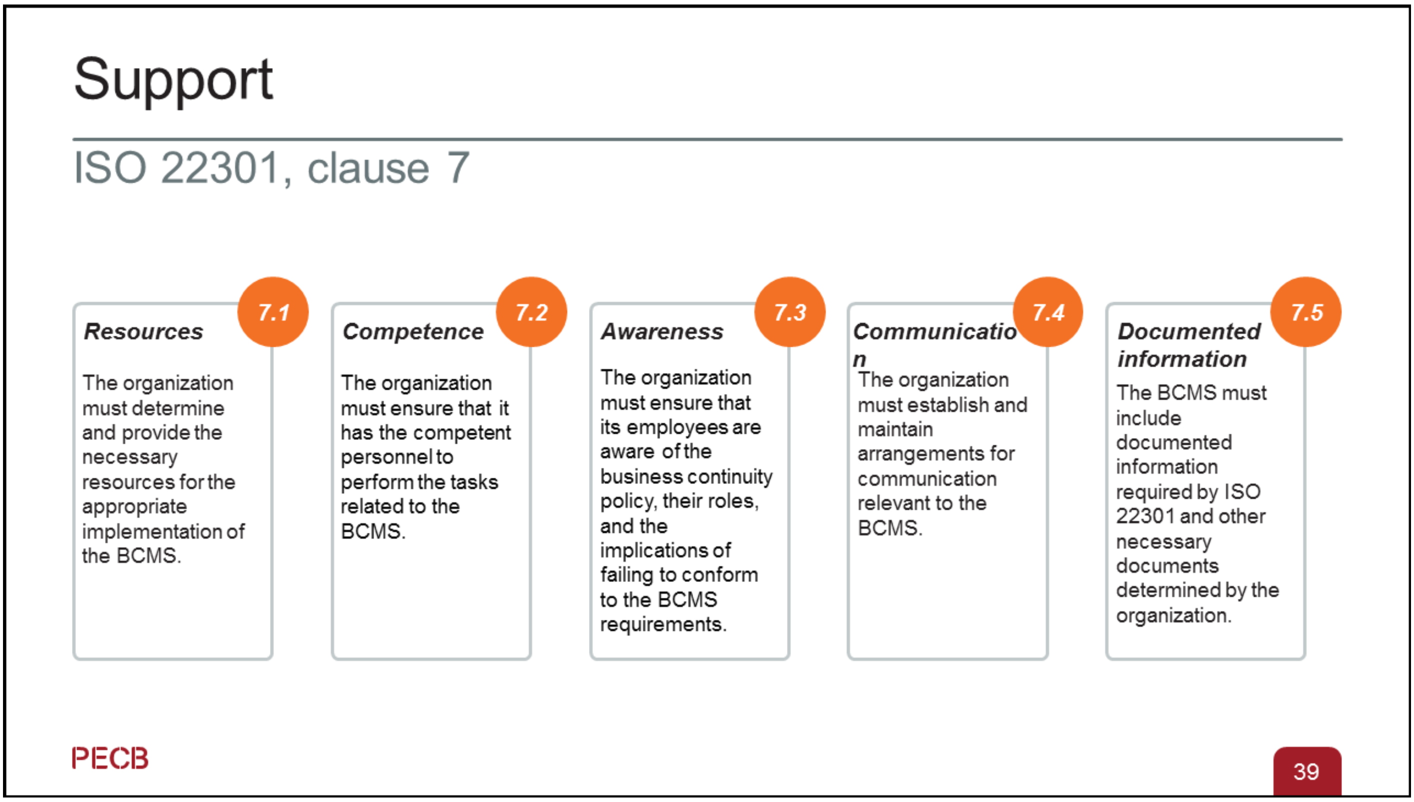
***Business continuity objectives and planning to achieve them***

The organization must establish business continuity objectives which are consistent with the business continuity policy. In addition, documented information on the business continuity objectives must be retained.

**6.3**

***Planning changes to the business continuity management system***

The organization must plan the changes related to the BCMS considering their purpose and potential consequences. The organization must also consider the BCMS integrity, availability of resources, and the roles and responsibilities.



# Support

## ISO 22301, clause 7

**7.1** ***Resources***

The organization must determine and provide the necessary resources for the appropriate implementation of the BCMS.

**7.2** ***Competence***

The organization must ensure that it has the competent personnel to perform the tasks related to the BCMS.

**7.3** ***Awareness***

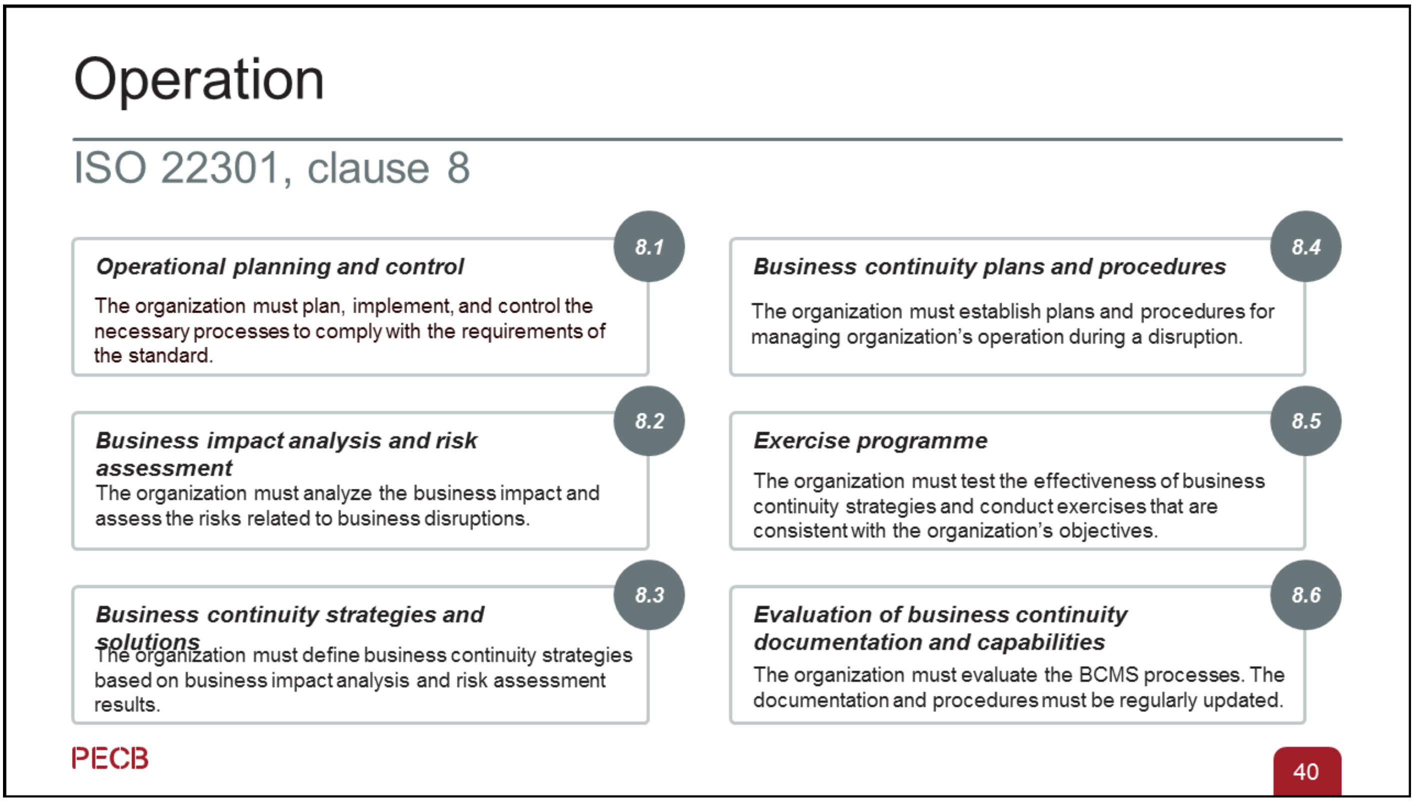
The organization must ensure that its employees are aware of the business continuity policy, their roles, and the implications of failing to conform to the BCMS requirements.

**7.4** ***Communication***

The organization must establish and maintain arrangements for communication relevant to the BCMS.

**7.5** ***Documented information***

The BCMS must include documented information required by ISO 22301 and other necessary documents determined by the organization.



# Operation

## ISO 22301, clause 8

**8.1** ***Operational planning and control***

The organization must plan, implement, and control the necessary processes to comply with the requirements of the standard.

**8.2** ***Business impact analysis and risk assessment***

The organization must analyze the business impact and assess the risks related to business disruptions.

**8.3** ***Business continuity strategies and solutions***

The organization must define business continuity strategies based on business impact analysis and risk assessment results.

**8.4** ***Business continuity plans and procedures***

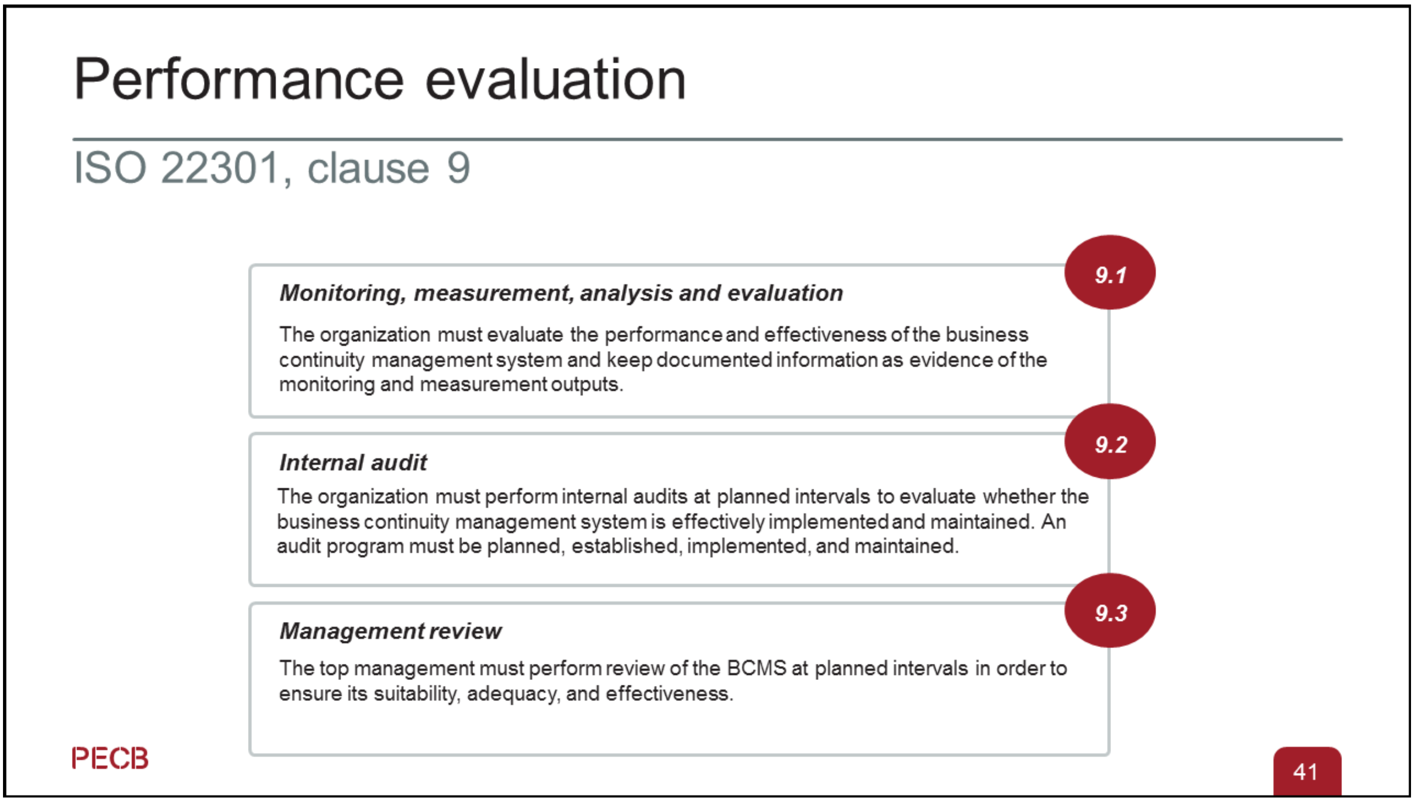
The organization must establish plans and procedures for managing organization's operation during a disruption.

**8.5** ***Exercise programme***

The organization must test the effectiveness of business continuity strategies and conduct exercises that are consistent with the organization's objectives.

**8.6** ***Evaluation of business continuity documentation and capabilities***

The organization must evaluate the BCMS processes. The documentation and procedures must be regularly updated.



# Performance evaluation

## ISO 22301, clause 9

9.1

***Monitoring, measurement, analysis and evaluation***

The organization must evaluate the performance and effectiveness of the business continuity management system and keep documented information as evidence of the monitoring and measurement outputs.

9.2

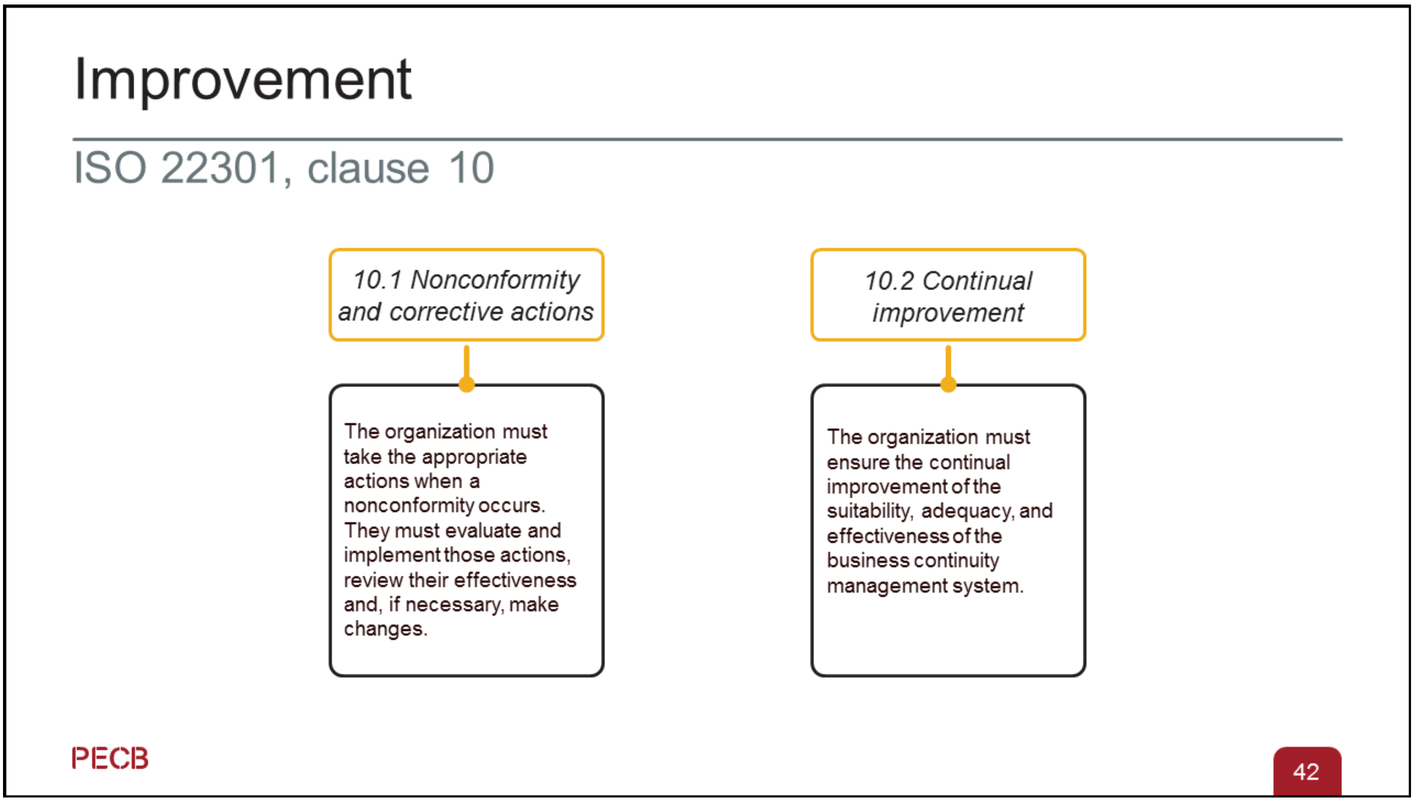
***Internal audit***

The organization must perform internal audits at planned intervals to evaluate whether the business continuity management system is effectively implemented and maintained. An audit program must be planned, established, implemented, and maintained.

9.3

***Management review***

The top management must perform review of the BCMS at planned intervals in order to ensure its suitability, adequacy, and effectiveness.



# Improvement

## ISO 22301, clause 10

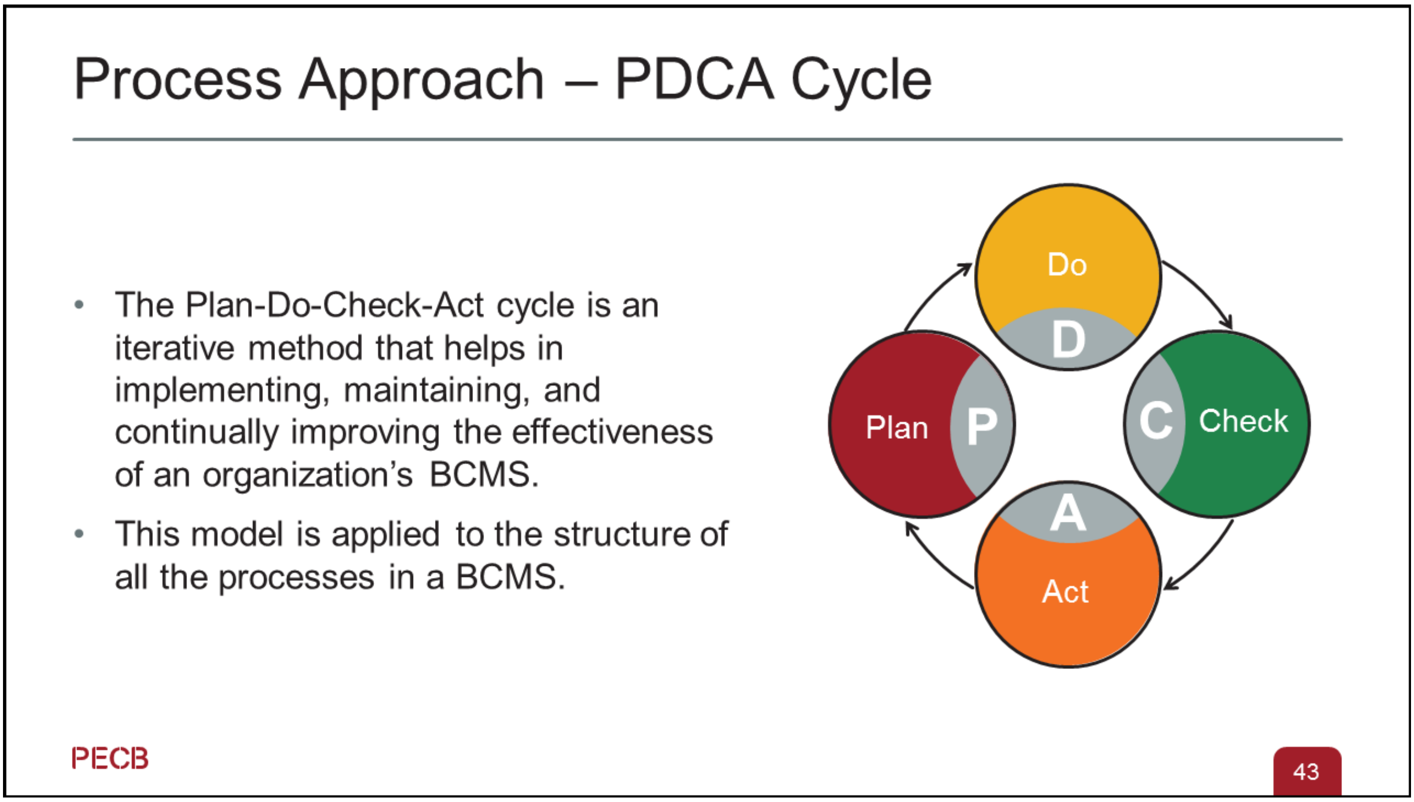
*10.1 Nonconformity and corrective actions*

The organization must take the appropriate actions when a nonconformity occurs. They must evaluate and implement those actions, review their effectiveness and, if necessary, make changes.

*10.2 Continual improvement*

The organization must ensure the continual improvement of the suitability, adequacy, and effectiveness of the business continuity management system.

PECB



## Process Approach – PDCA Cycle

- The Plan-Do-Check-Act cycle is an iterative method that helps in implementing, maintaining, and continually improving the effectiveness of an organization's BCMS.
- This model is applied to the structure of all the processes in a BCMS.

PECB

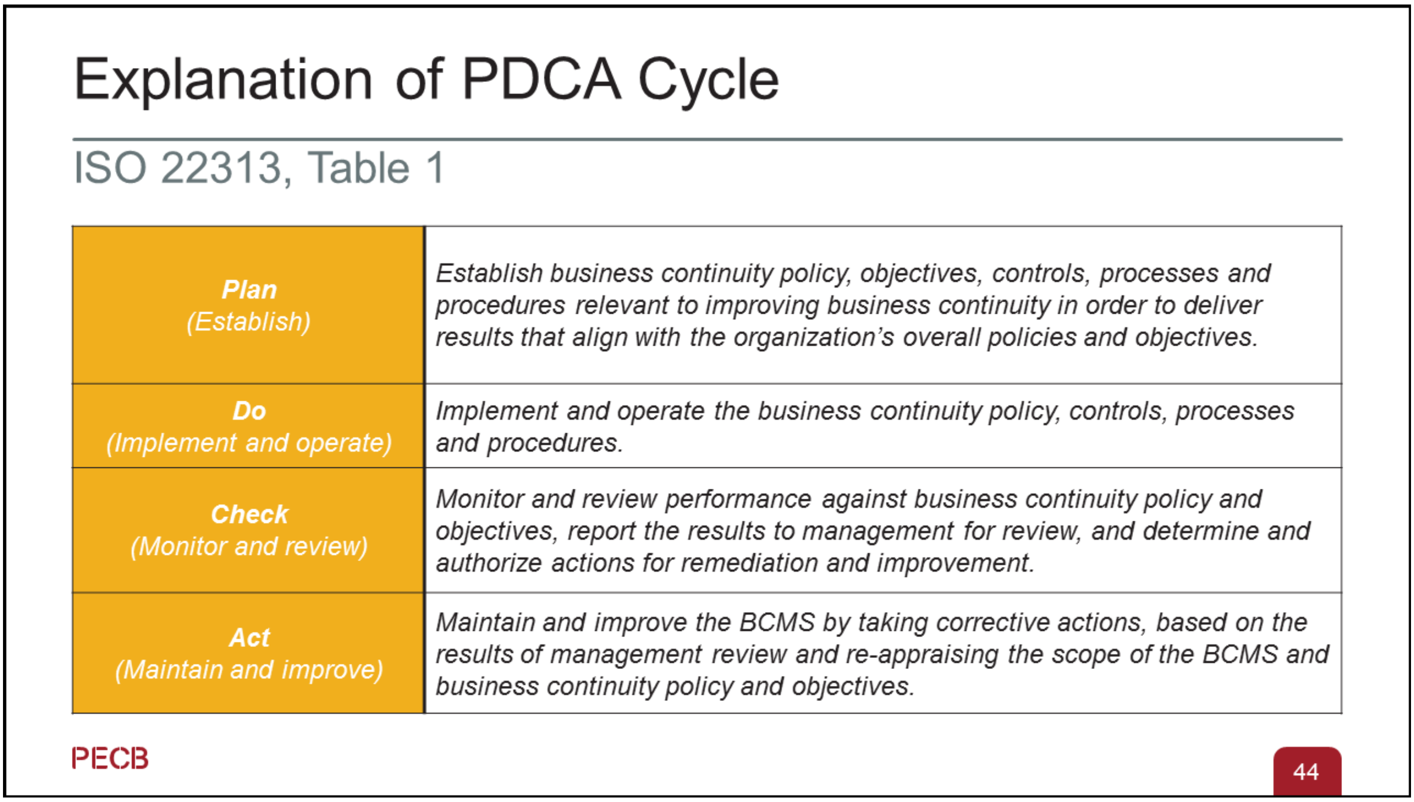
***ISO 22301, clause 0.3 Plan-Do-Check-Act (PDCA) cycle***

*This document applies the Plan (establish), Do (implement and operate), Check (monitor and review) and Act (maintain and improve) (PDCA) cycle to implement, maintain and continually improve the effectiveness of an organization's BCMS.*

*This ensures a degree of consistency with other management systems standards, such as ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 and ISO 28000, thereby supporting consistent and integrated implementation and operation with related management systems.*

*In accordance with the PDCA cycle, Clauses 4 to 10 cover the following components.*

- *Clause 4 introduces the requirements necessary to establish the context of the BCMS applicable to the organization, as well as needs, requirements and scope.*
- *Clause 5 summarizes the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations to the organization via a policy statement.*
- *Clause 6 describes the requirements for establishing strategic objectives and guiding principles for the BCMS as a whole.*
- *Clause 7 supports BCMS operations related to establishing competence and communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documented information.*
- *Clause 8 defines business continuity needs, determines how to address them and develops procedures to manage the organization during a disruption.*
- *Clause 9 summarizes the requirements necessary to measure business continuity performance, BCMS conformity with this document, and to conduct management review.*
- *Clause 10 identifies and acts on BCMS nonconformity and continual improvement through corrective action.*



# Explanation of PDCA Cycle

## ISO 22313, Table 1

| | |
|---|---|
| ***Plan***<br>*(Establish)* | *Establish business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.* |
| ***Do***<br>*(Implement and operate)* | *Implement and operate the business continuity policy, controls, processes and procedures.* |
| ***Check***<br>*(Monitor and review)* | *Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.* |
| ***Act***<br>*(Maintain and improve)* | *Maintain and improve the BCMS by taking corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.* |

# Quiz 2

PECB

45

## Quiz 2: Business continuity management system

1. **An organization, wishing to get certified against ISO 22301, must demonstrate compliance with requirements outlined in clauses:**
   A. 3-7
   B. 1-10
   C. 4-10
2. **What, among others, does ISO 223001 require in relation to understanding the context of the organization?**
   A. Identification of the external and internal factors
   B. Management reviews of the BCMS
   C. Competence and awareness of employees
3. **Which statement regarding management systems is correct?**
   A. The scope of a management system can only include parts of an organization
   B. A management system facilitates achievement of objectives in one or more disciplines
   C. An organization cannot have more than one management system at the same time
4. **___________ is an iterative method that helps implementing, maintaining, and systematically improving a BCMS.**
   A. The Plan-Act-Review-Check cycle
   B. The Plan-Do-Rehearse-Act cycle
   C. The Plan-Do-Check-Act cycle

Quiz 2

**5.Organizations are encouraged to implement a/an ____________________ if they have to manage several compliance frameworks.**

A. Integrated management system
B. Inclusive management system
C. BCMS

Exercise 1

47

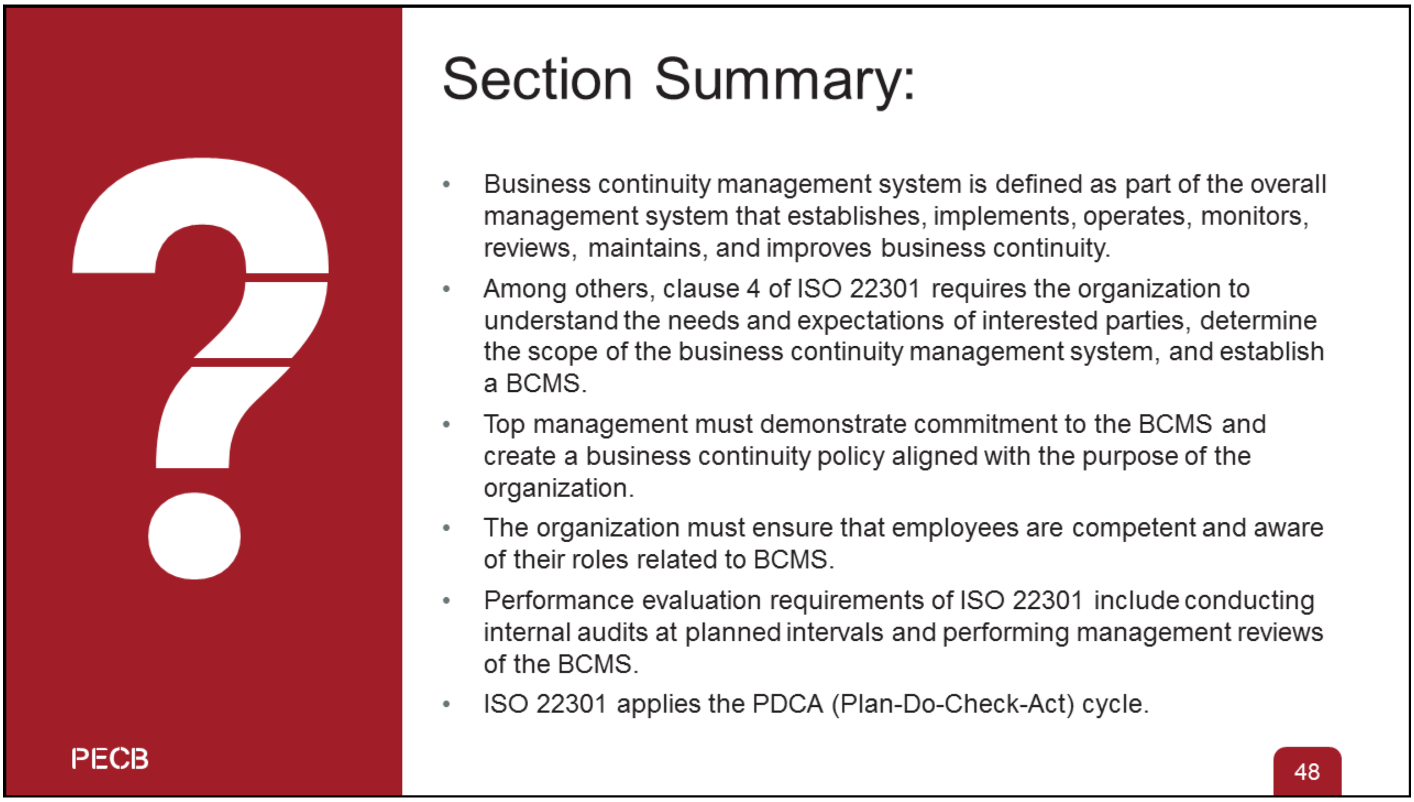
**Exercise 1: Business continuity — Myths and realities**

Do you agree with the following statements? Justify your answer with arguments.

1. Every organization should prioritize their readiness and response capabilities to natural disasters.
2. We have a business continuity plan, so we are prepared.
3. The IT Department is responsible for developing and exercising the business continuity plan.
4. A business continuity plan is not necessary because my employees know what to do.
5. Business continuity plans and disaster recovery plans are the same thing.
6. One disaster recovery plan meets the requirements of all possible scenarios.

Duration of the exercise: 35 minutes

Comments: 30 minutes



## Section Summary:

- Business continuity management system is defined as part of the overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity.
- Among others, clause 4 of ISO 22301 requires the organization to understand the needs and expectations of interested parties, determine the scope of the business continuity management system, and establish a BCMS.
- Top management must demonstrate commitment to the BCMS and create a business continuity policy aligned with the purpose of the organization.
- The organization must ensure that employees are competent and aware of their roles related to BCMS.
- Performance evaluation requirements of ISO 22301 include conducting internal audits at planned intervals and performing management reviews of the BCMS.
- ISO 22301 applies the PDCA (Plan-Do-Check-Act) cycle.