PECB

Whitepaper

ISO 22301 TRANSITION

Table of contents

PRINCIPAL AUTHOR

- Eric LACHAPELLE, PECB
- Faton ALIU, PECB
- Albana ISENI, PECB

CONTRIBUTORS

- Taulanta Kryeziu, PECB
- Jetë Spahiu, PECB
- Ahmed Sayed Aly, Egypt, Trusted Security Solutions
- Ahmed Abdel Raouf, Egypt, Trusted Security Solutions
- Hermann Amonzame, France, AB Conseils
- Mohammad Nawaz, Saudi Arabia, Petro Rabigh
- Issam Mellah, Tunisia, Skills Net company
- Adrian Sanchez, Mexico, Pink Elephant
- Miguel Roca, Spain, Nunsys
- Brian Reid, Barbados, iRisk Consulting Group
- Dayla Rivera Fernández, Freelancer, Costa Rica
- Yiannos Gregoriou, Cyta, Cyprus
- Thomas Schuermann, Freelancer, Germany
- Henri Haenni, Switzerland, Abilene Advisors
- Daniel De Giorgio, Argentina, Sinergia Learning Center
- Daniel Charlong, Canada, Standards Council of Canada
- Silvana Tomic Rotim, Croatia, ZIH d.o.o.
- Roberto Carlos Alvarez Valencia, Bolsa Mexicana de Valores, Mexico
- Betty Kildow, United States, Kildow Consulting
- Alexandrine Ville, France, Valor Consultants

Introduction

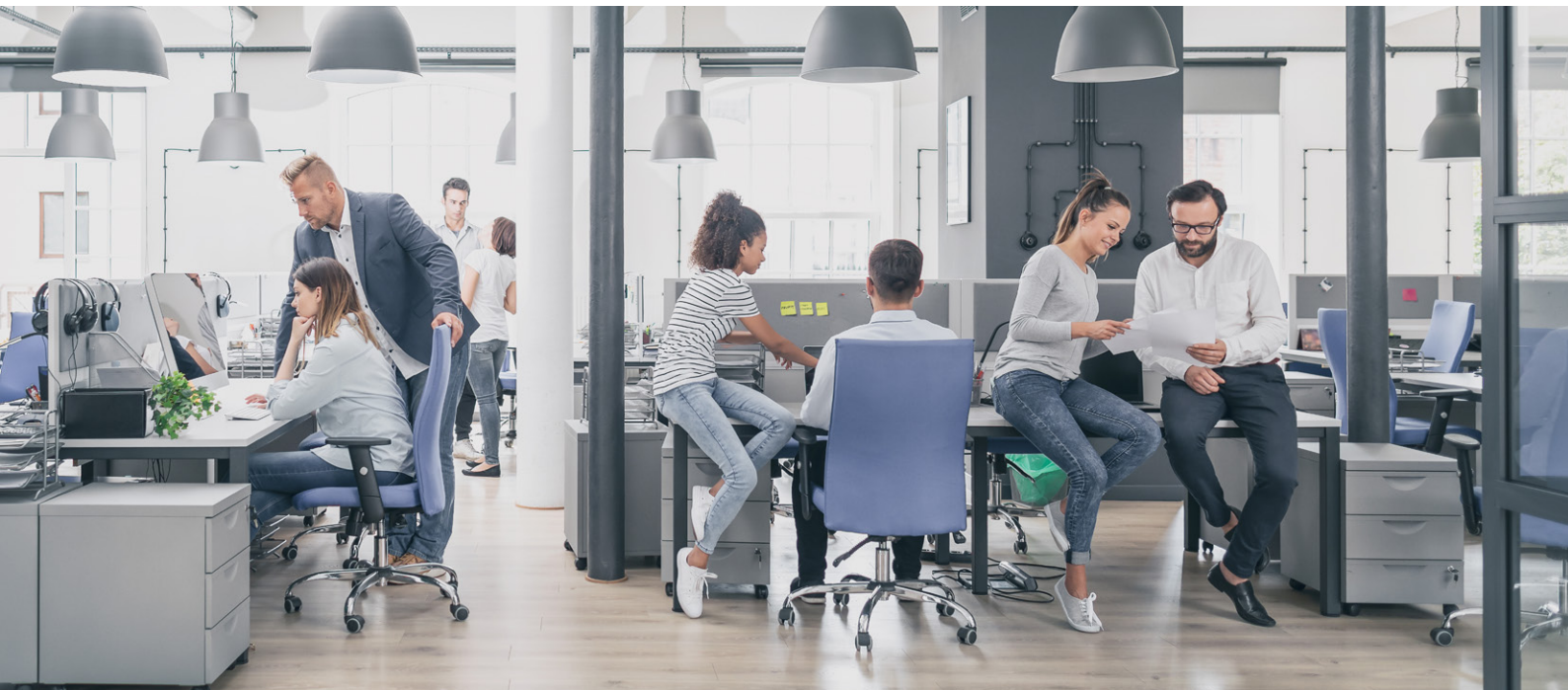
In an increasingly competitive business environment, competitive edge is the ultimate goal. On their attempts to reach this goal, organizations implement innovative strategies and technologies. In addition, organization should ensure the achievement of business objectives (especially in any case of disruption or incident) as well as maintain a steady state and continuous operations in order to protect the organization's reputation and customer trust. Those aspects are covered by the business continuity practice, and one of the most accepted frameworks is the business continuity management system (BCMS).

The implementation of a BCMS helps an organization to enhance its capability to continue the delivery of products and services within an acceptable time frame at predefined capacity during a disruption. To be more precise, the BCMS life cycle includes the best practices to prepare for, respond to, and recover from disruptions in a timely manner, regardless of whether they are natural, technological, or human-made. The BCMS life cycle is managed through different stages such as top management approval, planning, understanding of the context, setting of objectives, risk evaluation, business impact analysis, business continuity strategy and solutions, business continuity plans and procedures, exercise programs, maintenance, performance evaluation, and continual improvement.

The benefits of implementing a BCMS based on ISO 22301 are manifold: it helps in identifying threats, vulnerabilities, and risks that could potentially affect the critical operations, thus contributing to enhancing organizational resilience.

ISO 22301 emphasizes the importance of:

- Understanding the necessity for business continuity policies and objectives
- Establishing and maintaining processes, capabilities, and response structures to ensure that the organization is capable of surviving disruptions
- Monitoring and reviewing the performance and effectiveness of the BCMS
- Ensuring the continual improvement of the BCMS



ISO 22301:2019 Overview

Similar to other management systems, a BCMS is a set of interrelated elements used to establish policies, objectives, and processes which pave the way for the continual delivery of products and services even in the event of a disruption.

ISO 22301 as the international benchmark for business continuity management systems specifies the requirements to implement, manage, and improve a BCMS. It is important to note that the extent to which these requirements will be implemented will depend on the operating environment and complexity of the organization. The new edition of ISO 22301 published in 2019 replaces the first edition which was published in 2012.

Figure 1 outlines the clauses of ISO 22301:2019. It does not represent any structural hierarchy or authority level as there is no standard requirement regarding the structure that should be applied to the BCMS. That being said, organizations can choose terms that suit their operations.

The new edition of the standard shares a high-level structure (identical core text, terms, and definitions) with other ISO management system standards, which facilitates their integration. ISO 22301:2019 is applicable to any organization that intends to:

- Establish, implement, and maintain a BCMS to continuously deliver its products and services on the face of a disruption
- Improve its organizational resilience
- Ensure conformity to standard requirements and the enactment of the business continuity policy
- Create competitive advantage

The effective implementation of a BCMS based on ISO 22301 helps an organization to identify the existing and potential risks that have a high probability of impact. Furthermore, the implementation of the BCMS enables ongoing visibility, control of operations, and continual improvement, leading to a greater overall efficiency. Compliance with the requirements of ISO 22301 leads to enhanced service-providing capabilities.

Business Continuity Management System (BCMS)

CONTEXT OF THE ORGANIZATION

Understanding the organization and its context / Understanding the needs and expectations of interested parties / Determining the scope of the business continuity management system / Business continuity management system

LEADERSHIP

Leadership and commitment / Policy / Roles, responsibilities and authorities

PLANNING

Actions to address risks and opportunities / Business continuity objectives and planning to achieve them / Planning changes to the business continuity management system

SUPPORT

Resources / Competence / Awareness / Communication / Documented information

OPERATION

Operational planning and control / Business impact analysis and risk assessment / Business continuity strategies and solutions / Business continuity plans and procedures Exercise programme / Evaluation of business continuity documentation and capabilities

PERFORMANCE EVALUATION

Monitoring, measurement, analysis and evaluation / Internal audit / Management review

IMPROVEMENT

Nonconformity and corrective action / Continual improvement

Figure 1: Clauses of the ISO 22301:2019 international standard

The Key Changes in ISO 22301:2019

The update of ISO 22301 is linked to an increasing need to deal with various disruptive events, such as IT breakdowns, cyberattacks, incidents, and natural disasters, which threaten the smooth running of operations. The new edition of the standard aims to reflect the changing trends in the business continuity world and helps organizations to prepare for, respond to, and recover from disruptions in an effective and timely manner. This translates into reduced costs of disruptions, greater customer confidence, and protection of the organization's image and reputation. ISO 22301:2019 brings greater flexibility for organizations to achieve the desired results through less prescriptive requirements and more streamlined clauses.

The following is a summary of the key changes in ISO 22301:2019:

- The document is now shorter and easier to read and adopt. Redundant wording has been removed. Clauses have been merged, divided, or renamed.
- The PDCA cycle graph has been removed, although clauses 4 to 10 still cover the components of the PDCA.
- A new clause (6.3), which requires organizations to make changes to the BCMS in a planned manner, has been introduced.
- Clause 3 Terms and definitions is simplified and is now more consistent: several terms have been modified, removed, and others added.
- Risk appetite references have been removed from the standard.
- The standard now has less documentation requirements, for instance, it is no longer mandatory to document the business impact analysis and risk assessment processes (although it is a good practice to do so).
- The standard now has clearer requirements
- The new edition puts greater emphasis on setting objectives, monitoring performance and metrics, and aligning business continuity to strategic objectives.
- Some requirements are less prescriptive, which means that organizations now have more freedom to adopt approaches that best fit their needs.
- The new edition of the standard helps organizations to maximize the benefits of the BCMS implementation and at the same time minimize the costs associated with such an implementation project.

Being renamed from "Business continuity strategy" to "Business continuity strategies and solutions," clause 8.3 now requires organizations to not only develop high-level strategies for business continuity, but also to define solutions to handle specific risks and impacts. Subclause 8.3.5 is new to the standard. Organizations must implement and maintain business continuity solutions to be activated when needed. This is the most significant change for the top management, because the identification and allocation of resources are now related to solutions, not strategies. Defining resources based on the selected solutions in particular affects the budget of the BCMS implementation project.

The disadvantage of defininining resources based on strategy is that it may limit solutions, for instance due to poorly planned budget or investments, the organization's budget is compromised.

The Fundamental Elements of a BCMS

The three fundamental elements of a business continuity management system are the business continuity (BC) policy, the business impact analysis (BIA), and the risk assessment (RA).

INPUT		OUTPUT
Organization's purpose, BC framework, top management support	BC policy	BC structure, roles and responsibilities, communication. and commitment to business continuity
Critical operations criteria, classification, available resources, and the BIA methodology	BIA	MTPD, RTO, prioritization, dependencies, and required resources
The identified risks, threats, and vulnerabilities, and risk treatment criteria	RA	Likelihood of highly impact events, and countermeasures

Figure 2: The inputs and outputs of the BC policy, BIA, and RA to the BCMS
Note: MTPD (Maximum tolerable period of disruption) and RTO (Recovery time objective)

A well-defined business continuity policy is the cornerstone of the BCMS implementation and maintenance. The policy aims to establish preparedness, resilience, and capabilities to continue the delivery of services and products in the event of a disruption.

Although the new edition of ISO 22301 does not require organizations to maintain documented information on the BIA process or methodology, it is helpful to set and formalize the criteria for the execution of the BIA in the organization. A BIA establishes a set of steps to identify the critical functions in the organization, in order to estimate the potential impacts of a business disruption. In this process, the BIA executors (either internal or external) gather information, evaluate the potential impacts, and define the time objectives, dependencies, and resources needed to resume the critical functions quickly and without any major losses. The findings, outcomes, and recommendations are usually documented in a BIA report that is presented to the top management for approval.

The risk assessment process establishes a set of steps in order to identify the likelihood of highly impact events and their countermeasures as well as the required resources for the countermeasures. Subsequently, the risk treatment criteria should be applied, and an action plan (remove, share, or retain the risk) should be established.

In conjunction, the BIA and RA help to determine the BCMS requirements, while the BC policy supports the BCMS life cycle and lays down the foundations for an organizational resilience culture.

The BCMS Implementation Process

In order to successfully implement a business continuity management system, the organization should follow the steps outlined below:

1. BCM project planning and management	**2. Understanding the organization's business context**	**3. Identification of strategies and solutions**
4. BC plans and procedures *(including the BC structure and BC response)*	**5. Exercise and evaluation of documentation and capabilities**	**6. Performance evaluation and improvement** *(including monitoring, internal audit, and management review)*

- **Stage 1:** The BCMS scope is defined, the top management approval is obtained, appropriate project management mechanisms to manage the BCMS life cycle are established, and the BC policy is implemented.

NOTES:

a. *Depending on the BCMS scope, size, and complexity, it is worthy to consider the creating of a Department of Disaster Resilience, responsible for the whole life cycle and with the authority to interact and participate in projects impacting the scope and performance of the BCMS in the organization.*

b. *For those organizations already having a BCMS based on ISO 22301:2012, a Resilience Office could be an alternative for transition to ISO 22301:2019, since most of the changes were focused on streamlined text and reduced prescriptive requirements, to be more pragmatic in the BCMS life cycle, aligning with other management system standards.*

- **Stage 2:** This stage entails understanding the organization's context, to determine the BCMS requirements, which is obtained through the BIA and RA.
- **Stage 3:** With the BCMS requirements approved, the next step is the identification of BC strategies and solutions in order to select those that best fit the organization's needs..
- **Stage 4:** This stage consists in developing BC plans and procedures, while ensuring consistency between them. The stage includes defining the BC structure and the BC response plan.
- **Stage 5:** This stage considers the establishment of an exercise program and the evaluation of BCMS documentation and capabilities, both focused on verifying that the necessary resources are allocated to the BCMS project.
- **Stage 6:** This stage involves the performance evaluation of the BCMS and its continual improvement through mechanisms like monitoring performance indicators, internal audits, management reviews, and communication with relevant interested parties.

PECB Training and Certification

The need for career advancement and success in the workplace have resulted in an increased popularity of certification. A person's achievement of certification proves their skills and knowledge to perform job-related responsibilities. It also allows organizations to make sound decisions regarding the selection of employees.

PECB offers a wide range of training courses that help individuals obtain certifications that can boost their career. PECB training courses are offered globally through a network of authorized training providers. They are available in several languages and include introduction, foundation, implementer, and auditor training courses. The table below provides a short description of PECB's training courses for business continuity management based on ISO 22301.

Training title	Short description of the training	Who should attend?
ISO 22301 Introduction	› One-day training course › Introduction to the fundamental concepts of business continuity management › Not intended for certification purposes	› Individuals interested in business continuity management › Individuals seeking to gain knowledge about the main processes of a business continuity management system (BCMS)
ISO 22301 Foundation	› Two-day training course › Become acquired with the fundamental BC methodologies, framework, and management approach › One-hour exam	› Individuals involved in business continuity management › Individuals seeking to gain knowledge about the main processes of a business continuity management system (BCMS) › Individuals interested in pursuing a career in business continuity management
ISO 22301 Lead Implementer	› Five-day training course › Master the concepts, approaches, methods, and techniques used for the implementation, management, maintenance, and continual improvement of a BCMS › Three-hour exam	› Managers and consultants involved in business continuity management › Expert advisors seeking to master the implementation of a business continuity management system (BCMS) › Individuals responsible for implementing the BCMS in an organization based on the requirements of ISO 22301
ISO 22301 Lead Auditor	› Five-day training course › Master the audit techniques and become competent to manage a BCMS audit program and lead a team of auditors › Three-hour exam	› Auditors seeking to perform and lead BCMS certification audits › Managers or consultants seeking to master the BCMS audit process › Individuals responsible for maintaining conformance with ISO 22301 requirements › Expert advisors in business continuity