



EXCELLENCE.  
COMPETENCE.  
RECOGNITION.



**ISO 22301**

SOCIETAL SECURITY  
BUSINESS CONTINUITY  
MANAGEMENT SYSTEMS

# Whitepaper

---



Societal security  
Business continuity management systems

---

[www.pecb.org/iso22301](http://www.pecb.org/iso22301)

## PRINCIPAL AUTHORS

René St-GERMAIN, PECB (France)  
Faton ALIU, PECB (Canada)  
Eric LACHAPELLE, PECB (Canada)  
Pierre DEWEZ, Devoteam (Belgium)

## CONTRIBUTORS

Ian BELL (UK)  
Yannick BERNERON, Egyde (Canada)  
Daniela CATALIN, IT Academy (Romania)  
Goran CHAMUROVSKI, INTEGRA Solution (Macedonia)  
Jacques CHENEVIÈRE, Devoteam (France)  
Marcelo CORREA, Behaviour (Brasil)  
Karsten M. DECKER, Decker Consulting (Switzerland)  
Jérôme FERRU, Devoteam (France)  
Karim HAMD AOUI, LMPS Consulting (Morocco)  
Emile KOK, TSTC (Netherlands)  
Mathieu LACHAINE, Kereon (Canada)  
Jan MAES, Devoteam (Belgium)  
Simona MOSTEANU (Belgium)  
Graeme PARKER, Parker Solutions (UK)  
Dirk PAUWELS, Devoteam (Belgium)  
Joaquim PEREIRA, Behaviour (Portugal)  
Sébastien RABAUD, SCASSI (France)  
Itzhak SHARON, GSECTRA (Israel)  
François TÊTE, Devoteam (France)  
Gilles TROUÉSSIN, SCASSI (France)  
Alexandrine VILLE, SEKOIA (France)  
Richard G. WILSHER, Zygma (USA)

# CONTENTS

Introduction.....	4
An overview of ISO 22301:2012.....	5
Key clauses of ISO 22301:2012.....	5
Link between ISO 22301 and other standards.....	9
Link with other business continuity standards.....	9
Link with ISO 27001.....	10
Integration with other management systems.....	11
Business Continuity Management - The Business Benefits.....	12
Implementation of a BCMS with IMS2 methodology.....	13
Certification of organizations.....	15
Training and certifications of professionals .....	16

## || INTRODUCTION

Recent natural disasters, environmental accidents, technology mishaps and man-made crises have demonstrated that severe incidents can and will happen, impacting the public and private sectors alike. The challenge goes beyond providing an emergency response plan or using disaster management strategies that were previously used.

Organizations of all sizes and types should now engage in a comprehensive and systematic process of prevention, protection, preparedness, mitigation, response for business continuity and recovery. It is no longer enough to draft a response plan that anticipates and minimizes the consequences of naturally, accidentally, or intentionally caused disruptions, but rather organizations must also take adaptive and proactive measures to reduce the likelihood of a disruption. Today's threats require the creation of an on-going, managed process that ensures the survival and sustainability of an organization's core activities before, during, and after a disruptive event.

The ability of an organization to recover from a disaster is directly related to the degree of business continuity planning that has taken place BEFORE the disaster. Studies show that two out of five businesses that experience a disaster will go out of business within five years of the event.

Business continuity plans are critical to the continuous operation of all types of businesses. More importantly, these plans are assuming increased importance as companies become increasingly reliant on technology to do business.

Despite this clear message that downtime is disastrous, Gartner research shows that less than 30 percent of Fortune 2000 companies have invested in a full business continuity plan. The reason for this oversight may simply be that the technical challenges seem to be too daunting. Or perhaps the cost of implementation is perceived as too great. All of these are viable concerns, but they can be addressed with business continuity solutions.

ISO 22301, the world's first international standard for Business Continuity Management (BCM), has been developed to help organizations minimize the risk of such disruptions. ISO has officially launched ISO 22301, "Societal security - Business continuity management systems – Requirements", the new international standard for Business Continuity Management System (BCMS). This standard will replace the current British standard BS 25999.

*According to research by the META Group, the potential financial loss due to downtime is staggering. For an online retailer, the hourly loss is over one million dollars, on average. For a financial institution, the average hourly loss is closer to \$1.5 million. And for utility companies such as telecommunications and energy, the potential loss can reach as high as \$2.8 million per hour. That's over \$67 million in a day. Or, \$24.5 billion per year.*

## || AN OVERVIEW OF ISO 22301:2012

ISO 22301 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise.

The requirements specified in ISO 22301 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.

### **Business continuity standardization evolves with ISO 22301 by adding:**

- ⦿ Greater emphasis on setting the objectives, monitoring performance and metrics;
- ⦿ Clearer expectations on management;
- ⦿ More careful planning for and preparing the resources needed for ensuring business continuity;

### **ISO 22301 applies to all types and sizes of organizations that wish to:**

1. establish, implement, maintain and improve a BCMS;
2. assure conformity with the organization's stated business continuity policy;
3. demonstrate conformity to others;
4. seek certification/registration of its BCMS by an accredited third party certification body; or
5. make a self-determination and self-declaration of conformity with this International Standard.

ISO 22301 is the first standard to be fully compliant with the new guidelines from ISO/Guide 83 ("High level structure and identical text for management system standards and common core management system terms and definitions"). It has been developed in response to standards users' critics that, while current standards have many common components, they are not sufficiently aligned, making it difficult for organizations to rationalize their systems and to interface and integrate them.

This means that ISO 22301 will be the first standard to fully integrate a high-level structure and common text that will make it totally aligned with all other management systems once the related standards have also adopted the ISO Guide 83 guidelines.

### *What is Business Continuity Management?*

*BCM is a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities*

## Key clauses of ISO 22301:2012

### **Following the new structure of the ISO Guide 83, ISO 22301 is organized into the following main clauses:**

- Clause 4: Context of the organization
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement

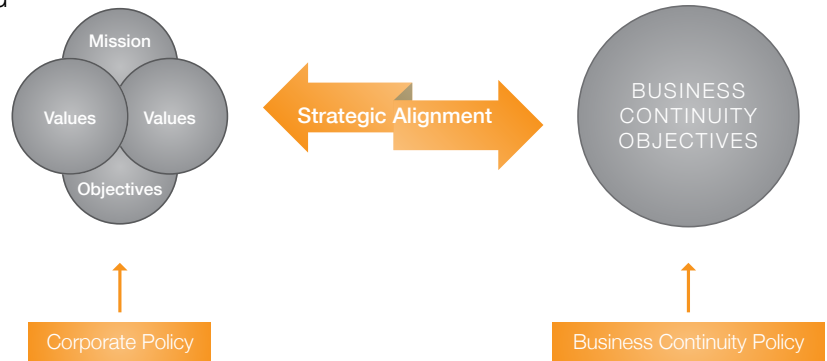
Each of these key activities is listed below.



## || CLAUSE 4: CONTEXT OF THE ORGANIZATION

Determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the expected outcomes of its BCMS such as:

- the organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident;
- links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy;
- the organization's risk appetite;
- the needs and expectations of relevant interested parties;
- applicable legal, regulatory and other requirements to which the organization subscribes.



Identifying the scope of the BCMS, taking into account the organization's strategic objectives, key products and services, risk tolerance, and any regulatory, contractual or stakeholder obligations is also part of this clause.

## || CLAUSE 5: LEADERSHIP

Top management needs to demonstrate an ongoing commitment to the BCMS. Through its leadership and actions, management can create an environment in which different actors are fully involved and in which the management system can operate effectively in synergy with the objectives of the organization. They are responsible for:

- ensuring the BCMS is compatible with the strategic direction of the organization;
- integrating the BCMS requirements into the organization's business processes;
- providing the necessary resources for the BCMS;
- communicating the importance of effective business continuity management;
- ensuring that the BCMS achieves its expected outcomes;
- directing and supporting continual improvement;
- establish and communicate a business continuity policy;
- ensuring that BCMS objectives and plans are established;
- ensuring that the responsibilities and authorities for relevant roles are assigned.

## || CLAUSE 6: PLANNING

This is a critical stage as it relates to establishing strategic objectives and guiding principles for the BCMS as a whole. The objectives of a BCMS are the expression of the intent of the organization to treat the risks identified and/or to comply with requirements of organizational needs. The business continuity objectives must:

- be consistent with the business continuity policy;
- take into account the minimum level of products and services that is acceptable to the organization to achieve its objectives;
- be measurable;
- take into account applicable requirements;
- be monitored and updated as appropriate.

## || CLAUSE 7: SUPPORT

The day-to-day management of an effective business continuity management system relies on using the appropriate resources for each task. These include competent staff with relevant (and demonstrable) training and supporting services, awareness and communication. This must be supported by properly managed documented information.

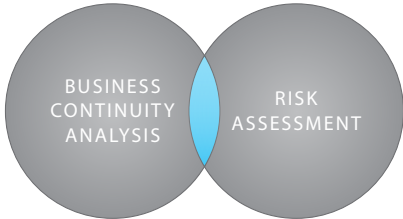
Both internal and external communications of the organization must be considered in this area, including the format, the content and the proper timing of such communications.

The requirements on the creation, update and control of documented information are also specified in this clause.

## || CLAUSE 8: OPERATION

After planning the BCMS, an organization must put it in operation. This clause includes:

- >> **Business Impact Analysis (BIA):** This activity enables an organization to identify the critical processes that support its key products and services, the interdependencies between processes and the resources required to operate the processes at a minimally-acceptable level.
  - >> **Risk assessment:** ISO 22301 proposes to refer to the ISO 31000 standard to implement that process. The goal of this requirement is to establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyzes, and evaluates the risk of disruptive incidents to the organization.
- Process of analysing business functions and the effect that the business disruption might have upon them



Overall process of risk identification, risk analysis and risk evaluation
- >> **Business continuity strategy:** After requirements have been established through the BIA and the risk assessment, strategies can be developed to identify arrangements that will enable the organization to protect and recover critical activities based on organizational risk tolerance and within defined recovery time objectives. Experience and good practice clearly indicate that the early provision of an overall organizational BCM strategy will ensure BCM activities are aligned with and support the organization's overall business strategy. The business continuity strategy should be an integral component of an institution's corporate strategy.
  - >> **Business continuity procedures:** The organization shall document procedures (including necessary arrangements) to ensure continuity of activities and management of a disruptive incident. The procedures have to:
    - o establish an appropriate internal and external communications protocol;
    - o be specific regarding the immediate steps that are to be taken during a disruption;
    - o be flexible to respond to unanticipated threats and changing internal and external conditions;
    - o focus on the impact of events that could potentially disrupt operations;
    - o be developed based on stated assumptions and an analysis of interdependencies; and;
    - o be effective in minimizing consequences through implementation of appropriate mitigation strategies.
  - >> **Exercising and testing:** To ensure that business continuity procedures are consistent with its business continuity objectives, an organization will have to test them regularly. Exercising and testing are the processes of validating business continuity plans and procedures to ensure the selected strategies are capable of providing response and recovery results within the timeframes agreed to by management.

## || CLAUSE 9: PERFORMANCE EVALUATION

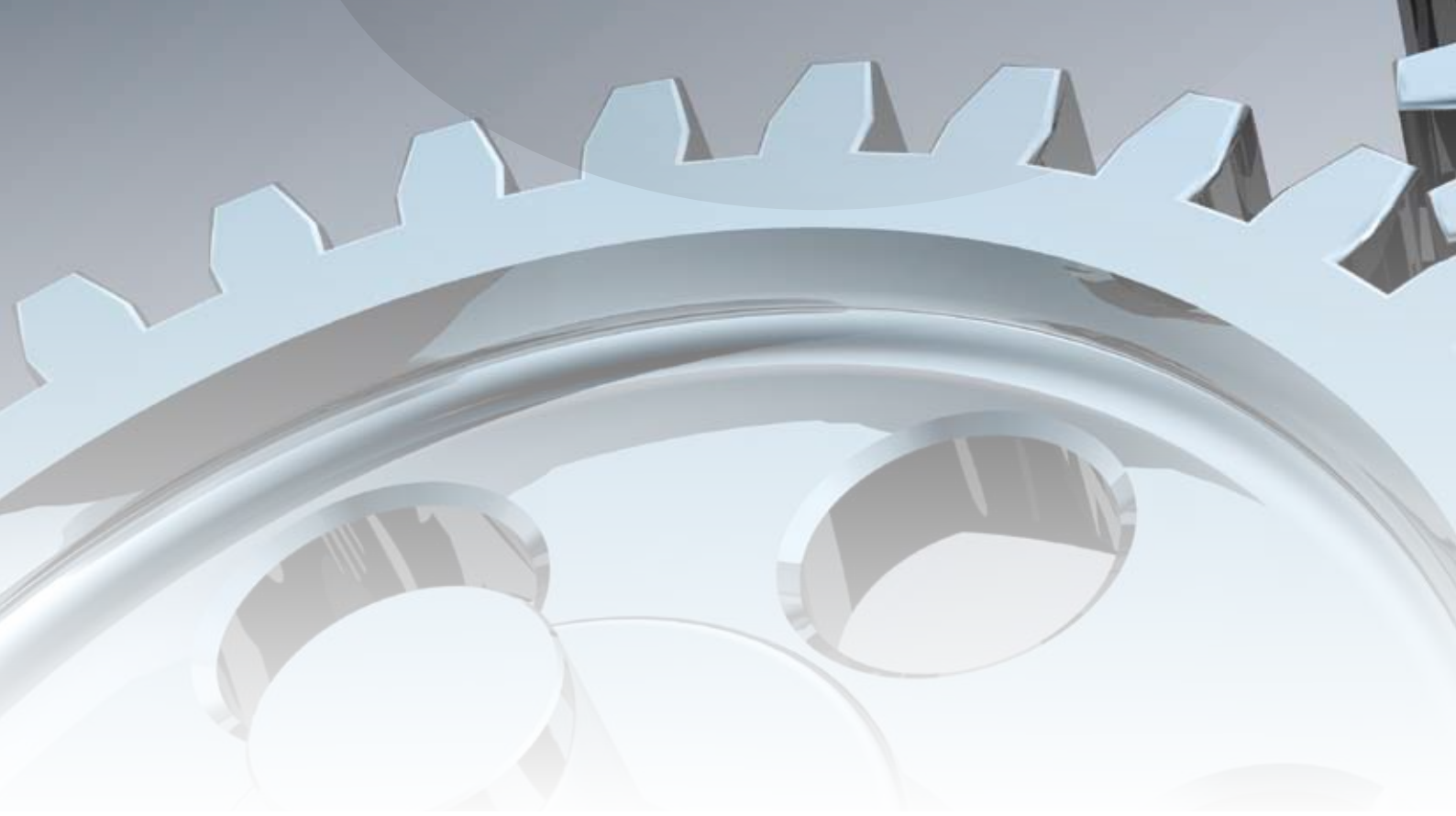
Once the BCMS is implemented, ISO 22301 requires permanent monitoring of the system as well as periodic reviews to improve its operation:

- monitoring the extent to which the organization's business continuity policy, objectives and targets are met;
- measuring the performance of the processes, procedures and functions that protect its prioritized activities;
- monitoring compliance with this standard
- and the business continuity objectives;
- monitoring historical evidence of deficient BCMS' performance
- conducting internal audits at planned intervals; and
- evaluating all this in the management review at planned intervals.

Exercise Type	What is it?	Benefit	Disadvantages
Checklist	Distribute plans for review	Ensures plan addresses all activities	Does not address effectiveness
Structured Walkthrough	Thorough look at each step of the BCP	Ensures planned activities are accurately described in the BCP	Low value in proving response capabilities
Simulation	Scenario to enact recovery procedures	Practice session	When subsets are very different
Parallel	Full test, but primary processing does not stop	Ensures high level of reliability without interrupting normal operations	Expensive as all personnel is involved
Full Interruption	Disaster is replicated to the point of ceasing normal operations	Most reliable test of BCP	Risky

## || CLAUSE 10: IMPROVEMENT

Continual improvement can be defined as all the actions taken throughout the organization to increase effectiveness (reaching objectives) and efficiency (an optimal cost/benefit ratio) of security processes and controls to bring increased benefits to the organization and its stakeholders. An organization can continually improve the effectiveness of its management system through the use of the business continuity policy, objectives, audit results, analysis of monitored events, indicators, corrective and preventive actions and management review.



## Link between ISO 22301 and other standards

ISO 22301 can be easily linked with other Business Continuity and Information Security standards, like the recent ISO/IEC 27031:2011 - Guidelines for information and communication technology readiness for business continuity. Published in March 2011 and superseding BS 25777, this international standard describes the concepts and principles of ICT readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects for improving an organization's ICT readiness to ensure business continuity.

Similarly, the BCMS will also be achieved in practice thanks to ISO/IEC 24762:2008 - Guidelines for information and communications technology disaster recovery services.

In this section, we present some standards that ISO 22301 can be in relation with to create an integrated management system.

## Link with other business continuity standards

In addition to ISO 22301 business continuity standard, several other well-known standards include:

- ⦿ British Standards Institute: BS 25999, Parts 1 and 2
- ⦿ National Fire Protection Association: NFPA 1600:2010
- ⦿ ASIS International: ASIS SPC.1-2009
- ⦿ Australia/New Zealand Standard AS/NZS 5050
- ⦿ Singapore Standard SS540
- ⦿ Canadian Standard: CSA Z1600
- ⦿ Government of Japan BCP Guideline
- ⦿ Japanese Corporate Code – BCP
- ⦿ National Association of Stock Dealers: NASD 3510/3520
- ⦿ National Institute of Standards and Technology: NIST SP 800-34
- ⦿ New York Stock Exchange: NYSE Rule 446



In the table below, the first column lists the usual components that more or less all BCM standards propose. Other columns describe for each standard where the information for each category can be found. This table doesn't indicate the usefulness of content of each of these standards, only the fact that the information can be found within the standard.

BCM Element	ISO 22301	ASIS/BSI BCM.01-2010 ASIS	SPC.1:2009 BS	BS 25999:2	NFPA 1600:2010
Understanding the organization	Section 4.1	N/A	N/A	Section 4.1	N/A
Needs and expectations of interested parties	Section 4.1	N/A	N/A	Section 4.1	Chapter 4.5
Scope	Section 4.3	Section 1	Section 1	Section 3.2.1	Chapter 5.3
BCMS	Section 4.4	Section 4	Section 4	Section 3	Annex D
Management commitment	Section 5.2	Not explicit	Not explicit	Not explicit	Chapter 4.1
Policy	Section 5.3	Section 4.3	Section 4.2.1	Section 3.2.2	Chapter 4
Roles and Responsibilities	Section 5.4	Section 4.5.2	Section 4.4.1	Section 3.2.4	Chapter 6.6
Planning	Section 6	Section 4.4	Section 4.3	Section 3	Chapter 5
Resources	Section 7.1	Section 4.5.1	Section 4.4.1	Section 4.3	Chapter 6.1
Competence	Section 7.2	Section 4.5.3	Section 4.4.2	Section 3.2.4	Chapter 6.11
Awareness	Section 7.3	Section 4.5.3	Section 4.4.2	Section 3.2.4	Chapter 6.11
Communication	Section 7.4	Section 4.5.7	Section 4.4.3	Section 4.3.3	Chapter 6.8
Documented information	Section 7.5	Section 4.6.4	Section 4.5.4	Section 3.4.2	Chapter 4.8
Business Impact Analysis	Section 8.2.2	Section 4.4.1.1	Section 4.3.1	Section 4.4.1	Chapter 5.5
Risk Analysis	Section 8.2.3	Section 4.4.1.2	Section 4.3.1	Section 4.1.2	Chapter 5.4
BC Strategies	Section 8.3	Section 4.3	Section 4.2	Section 4.2	Chapter 5
Business continuity procedures	Section 8.4	Section 4.5.6.2	Section 4.3	Section 4.3.3	Chapter 6.7
Testing and Exercising	Section 8.5	Section 4.6.2.2	Section 4.5.2.2	Section 4.4	Chapter 7
Monitoring and Measurement	Section 9.1	Section 4.6.1	Section 4.5.1	Section 4.4	Chapter 7.1
Internal audit	Section 9.2	Section 4.6.5	Section 4.5.5	Section 5.1	Chapter 8.1
Management review	Section 9.3	Section 4.7.4	Section 4.6.5	Section 5.2	N/A
Improvement	Section 10	Section 4.7.4	Section 4.6.5	Section 6.2	Chapter 8
Auditing	Section 9.2	Section 4.6.5	Section 4.5.5	Section 5.1	Chapter 8.1
Continuous Improvement	Section 10.2	Section 4.7.4	Section 4.6.5	Section 6.2	Chapter 8

All of these business continuity standards conform to the common outline as stated in the above table. Does this mean that they are all the same? It doesn't, but it means that they all, starting with ISO 22301, address the commonly faced issues for each kind of business continuity management. This is why this newly published management system will quickly become a matter of corporate preference, and maybe the ultimate standard as dictated by industry regulations.





## Link with ISO 27001

ISO 22301 is obviously useful as part of a certification process to ISO/IEC 27001:2005. ISO 22301 can be used to directly comply with the objective of clause A.14 - Business continuity management. Additionally, regarding the implementation and execution of a risk assessment in the context of ISMS compliance, an organization could always refer to ISO/IEC 27005:2011 or, in a broader context, to ISO 31000:2009 - Risk management - Principles and guidelines or, to execute the assessment itself, to ISO 31010:2009 - Risk management - Risk assessment techniques.

### A.14.1 Information security aspects of business continuity management

**Objective:** To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A.14.1.1	Including information security in the business continuity management process	<i>Control</i> A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
A.14.1.2	Business continuity and risk assessment	<i>Control</i> Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
A.14.1.3	Developing and implementing continuity plans including information security	<i>Controls</i> Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
A.14.1.4	Business continuity planning framework	<i>Control</i> A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and identify priorities for testing and maintenance.
A.14.1.5	Testing, maintaining and reassessing Business continuity plans	<i>Control</i> Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

## ISO 22301 requirements

4.4

Business continuity management system

8.2

BIA and Risk assessment

8.4

Business continuity procedures

6

Planning the BCMS

8.5

Exercising and testing

## Integration with other management systems

General requirements presented in the table below are commonly stated in any management system and relate to determining objectives, applying them according to the organization's habits and needs, keeping them alive based on a strong management commitment, monitoring and reviewing, supporting the management system by good documentation, regular 'health-checks' via internal or external audits and to gain benefits through continual improvement as achieved by a regular management review.

The table below shows how a BCMS can be considered jointly with other management systems. This will authorize the organization to envision "combined audits" in order to achieve their compliance goals with adequate effort and budget.

Requirements	ISO 9001:2008	ISO 14001:2004	ISO 20000:2011	ISO 22301:2012	ISO 27001:2005
Objectives of the management system	5.4.1	4.3.3	4.5.2	6.2	4.2.1
Policy of the management system	5.3	4.2	4.1.2	5.3	4.2.1
Management commitment	5.1	4.4.1	4.1	5.2	5
Documentation requirements	4.2	4.4	4.3	7.5	4.3
Internal audit	8.2.2	4.5.5	4.5.4.2	9.2	5
Continual improvement	8.5.1	4.5.3	4.5.5	10	8
improvement	5.6	4.6	4.5.4.3	9.3	7





## Business Continuity Management - The Business Benefits

As with all major undertakings within an organization, it is essential to gain the backing and sponsorship of executive management. By far the best way to achieve this, rather than through highlighting the negative aspects of not having business continuity management, is to illustrate the positive gains of having an effective business continuity management process in place.

Today good business continuity management is not about being forced into taking action to address external pressures. It is about recognizing the positive value of Business Continuity good practice being embedded throughout your organization.

Predictable and effective response to crises	Protection of people	Maintenance of vital activities of the organization	Better understanding of the organization
Cost reduction	Respect of the interested parties	Protection of the reputation and brand	Confidence of clients
Competitive advantage	Legal compliance	Regulatory compliance	Contract compliance

**The adoption of an effective business continuity management process within an organization will have benefits in a number of areas, examples of which include:**

1. Protection of shareholder value
2. Improved understanding of the business as gained through risk identification and analysis
3. Operational resilience which results from implementing risk reduction
4. Downtime that is reduced when alternative processes and workarounds are identified
5. Compliance issues that can be identified and managed for alternative processes
6. Vital records that can be maintained and protected
7. The implications for health & safety legislation and duties of care can be correctly considered.
8. Improved operational effectiveness through a forced programme of business process re-engineering
9. Protection of both the physical and knowledge assets of the business
10. Preservation of markets by ensuring continuity of supply
11. Improved overall security
12. Avoidance of liability actions





## Implementation of a BCMS with IMS2 methodology

Making the decision to implement a business continuity management System based on ISO 22301 is often a very simple one, as the benefits are well documented. Most companies now realize that it is not sufficient to implement a generic, “one size fits all” business continuity plan. For an effective response, with respect to maintaining operational continuity, such a plan must be customized to specific risks and catastrophic scenarios which could range from major building loss to local system failure [As it is written earlier, a good plan goes beyond the reactive model]. A more difficult task is the compilation of an implementation plan that balances the requirements of the standard, the business needs and the deadline to become certified.

There is no single blueprint for implementing ISO 22301 that will work for every company, but there are some common steps that will allow you to balance the often conflicting requirements and prepare you for a successful certification audit.

PECB has developed a methodology for implementing a management system. It is called “Integrated Implementation Methodology for Management Systems and Standards (IMS2)” and is based on applicable best practices. This methodology is based on the guidelines of ISO standards and also meets the requirements of ISO 22301.

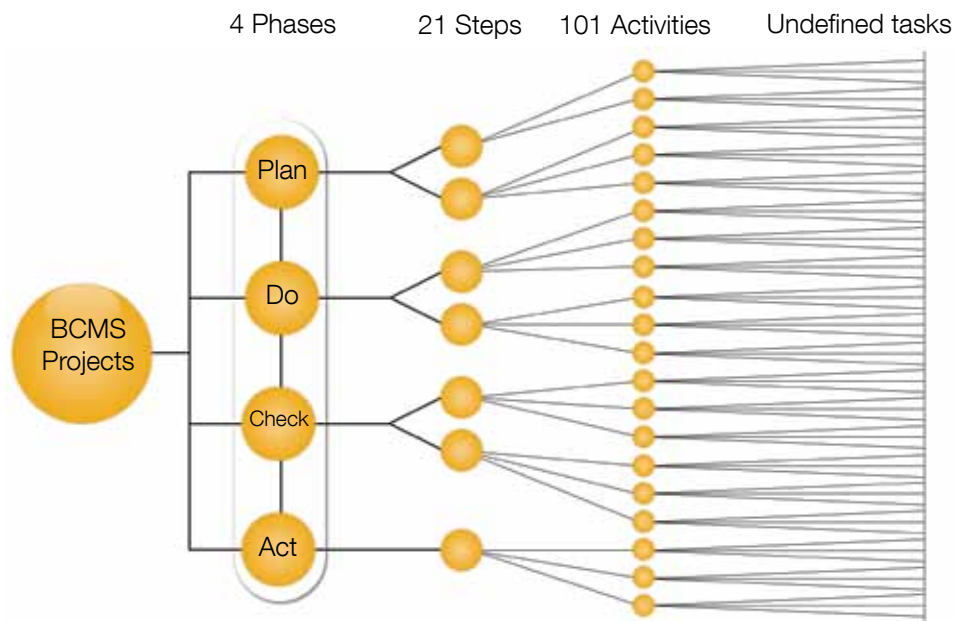


IMS2 is based on the PDCA cycle divided into four phases: Plan, Do, Check and Act. Each phase has between 2 and 8 steps for a total of 21 steps. In turn, these steps are divided into 101 activities and tasks. This ‘Practical Guide’ considers the key phases in your implementation project from start to finish and suggests the appropriate ‘best practice’ for each one, while directing you to further helpful resources as you embark on your ISO 22301 journey.



By following a structured and effective methodology, an organization can be sure it covers all minimum requirements for the implementation of a management system. Whatever methodology used, the organization must adapt it to its particular context (requirements, size of the organization, scope, objectives, etc...) and not apply it like a cookbook.

The sequence of steps can be changed (inversion, merge). For example, the implementation of the management procedure for documented information can be done before the understanding of the organization. Many processes are iterative because of the need for progressive development throughout the implementation project; for example, communication and training.



By following a structured and effective methodology, an organization can be sure it covers all minimum requirements for the implementation of a management system. Whatever methodology used, the organization must adapt it to its particular context (requirements, size of the organization, scope, objectives, etc...) and not apply it like a cookbook.

The sequence of steps can be changed (inversion, merge). For example, the implementation of the management procedure for documented information can be done before the understanding of the organization. Many processes are iterative because of the need for progressive development throughout the implementation project; for example, communication and training.

## Certification of organizations

The usual path for an organization that wishes to be certified against ISO 22301 is the following:

- 1. Implementation of the management system:** Before being audited, a management system must be in operation for some time. Usually, the minimum time required by the certification bodies is 3 months.
- 2. Internal audit and review by top management:** Before a management system can be certified, it must have had at least one internal audit report and one management review.
- 3. Selection of the certification body (registrar):** Each organization can select the certification body (registrar) of its choice.
- 4. Pre-assessment audit (optional):** An organization can choose to do a pre-audit to identify any possible gap between its current management system and the requirements of the standard.
- 5. Stage 1 audit:** A conformity review of the design of the management system. The main objective is to verify that the management system is designed to meet the requirements of the standard(s) and the objectives of the organization. It is recommended that at least some portion of the Stage 1 audit be performed on-site at the organization's premises.
- 6. Stage 2 audit (On-site visit):** The Stage 2 audit objective is to evaluate whether the declared management system conforms to all requirements of the standard, is actually being implemented in the organization and can support the organization in achieving its objectives. Stage 2 takes place at the site(s) of the organization's sites(s) where the management system is implemented.
- 7. Follow-up audit (optional):** If the auditee has non-conformities that require additional audit before being certified, the auditor will perform a follow-up visit to validate only the action plans linked to the non-conformities (usually one day).
- 8. Confirmation of registration:** If the organization is compliant with the conditions of the standard, the Registrar confirms the registration and publishes the certificate.
- 9. Continual improvement and surveillance audits:** Once an organization is registered, surveillance activities are conducted by the Certification Body to ensure that the management system still complies with the standard. The surveillance activities must include on-site visits (at least 1/year) that allow verifying the conformity of the certified client's management system and can also include: investigations following a complaint, review of a website, a written request for follow-up, etc.



## Training and certifications of professionals

PECB has created a recommended training roadmap and personnel certification schemes for implementers and auditors of an organization that wishes to get certified against ISO 22301. Whereas certification of organizations is a vital component of the business continuity field as it provides evidence that organizations developed standardized processes based on best practices, certification of individuals serves also as documented evidence of professional competencies and experience for/ of those individuals that attended one of the related courses and exams.

It serves to demonstrate that the certified professional holds defined competencies based on best practices. It also allows organizations to make an informed selection of employees or services based on the competencies that are represented by the certification designation. Finally, it provides incentives to the professional to constantly improve his/her skills and knowledge and serves as a tool for employers to ensure that training and awareness have been effective.

PECB training courses are offered globally through a network of authorized training providers and they're available in several languages and include introduction, foundation, implementer and auditor courses. The table below gives a short description about PECB's official training courses for Business continuity management system based on ISO 22301.

Training title	Short description	Who should attend
<b>ISO 22301 Introduction</b>	<ul style="list-style-type: none"> <li>• One day training</li> <li>• Introduction to concepts management and implementation of a BCMS</li> <li>• Do not lead to certification</li> </ul>	<ul style="list-style-type: none"> <li>• IT Professionals</li> <li>• Staff involved in the implementation of BCMS</li> <li>• IT Expert advisors</li> <li>• Managers responsible for implementing a BCMS</li> <li>• Auditors</li> </ul>
<b>ISO 22301 Foundation</b>	<ul style="list-style-type: none"> <li>• A two days training</li> <li>• Become familiar with best practices for implementation and management of BCMS</li> <li>• One hour exam</li> </ul>	<ul style="list-style-type: none"> <li>• Members of an business continuity team</li> <li>• IT Professionals</li> <li>• Staff involved in BCMS</li> <li>• Technicians</li> <li>• Auditors</li> </ul>
<b>ISO 22301 Lead Implementer</b>	<ul style="list-style-type: none"> <li>• A five days training</li> <li>• Manage the implementation and a management of a BCMS</li> <li>• Three hours exam</li> </ul>	<ul style="list-style-type: none"> <li>• Project managers and/or consultants</li> <li>• Business continuity auditors</li> <li>• Members of an business continuity team</li> <li>• Technical experts</li> </ul>
<b>ISO 22301 Lead Auditor</b>	<ul style="list-style-type: none"> <li>• A five days training</li> <li>• Manage the audit of a BCMS</li> <li>• Three hours exam</li> </ul>	<ul style="list-style-type: none"> <li>• Internal auditors</li> <li>• Auditors</li> <li>• Project managers and/or consultants</li> <li>• Members of an business continuity team</li> <li>• Technical experts</li> </ul>

Although no specified set of courses or curriculum of study is required as part of the certification process, the completion of a recognized PECB course or program of study will significantly enhance your chance of passing a PECB certification examination. You can verify the list of approved organization that offers PECB official training sessions on our website at [www.pecb.org/en/eventlist](http://www.pecb.org/en/eventlist)



## || CHOOSING THE RIGHT CERTIFICATION:

The ISO 22301 Foundation certification is a professional certification for professionals needing to have an overall understanding of the ISO 22301 standard and its requirements.

The ISO 22301 Implementer certifications are professional certifications for professionals needing to implement a BCMS and, in case of the ISO 22301 Lead Implementer Certification, needing to manage an implementation project.

The ISO 22301 Auditor certifications are credentials for professionals needing to audit a BCMS and, in case of the “ISO 22301 Lead Auditor” Certification, needing to manage a team of auditors.

The ISO 22301 Master certification is a professional certification for professionals needing to implement a BCMS and to master the audit techniques and manage (or be part of) audit teams and audit program.

Based on your overall professional experience and your acquired qualifications, you will get granted one or more of these certifications based on projects or audits activities you have been performing by the past or which you are currently working on.

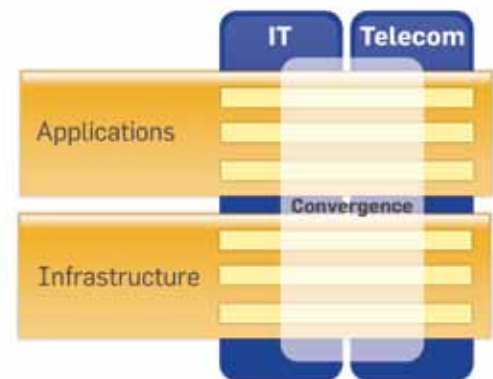
Certification	Exam	Professional experience	Audit experience	Project experience
Provisional Implementer	Lead Implementer Exam	None	None	None
Implementer	Lead Implementer Exam	Two years One year of work experience in the field of certification	None	Project activities totaling 200 hours
Lead Implementer	Lead Implementer Exam	Five years Two years of work experience in the field of certification	None	Project activities totaling 300 hours
Provisional Auditor	Lead Auditor Exam	None	None	None
Auditor	Lead Auditor Exam	Two years One year of work experience in the field of certification	Audit activities totaling 200 hours	None
Lead Auditor	Lead Auditor Exam	Five years Two years of work experience in the field of certification	Audit activities totaling 300 hours	None
Master	Lead Auditor Exam Lead Implementer exam	Ten years Two years of work experience in the field of certification	Audit activities totaling 500 hours	Project activities totaling 500 hours



## About DEVOTEAM

Devoteam NV/SA is a leading ICT service company with a very solid knowledge base of more than 260 highly skilled experts in Belgium and an international network of more than 4500 colleagues in the Devoteam Group.

Thanks to its genes, **Devoteam NV/SA has a very strong background in IT, Telecommunication and Media realizations.** Devoteam offers **solutions** and **services** covering IT and Telecom in the two specific domains of applications and infrastructure.



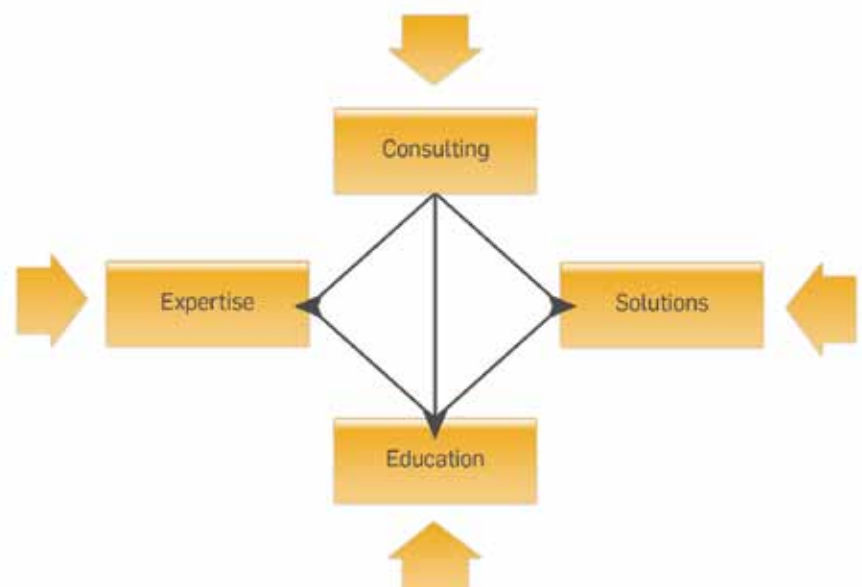
### Applications:

- Enterprise Content Management
- Applications for Digital Television
- Business Application Integration

### Infrastructure:

- IT Service Management
- Advanced Infrastructure Services
- Risk & Security Management

Depending on customer's needs, Devoteam NV/SA in Belgium can offer its experience through **consultancy, expertise, education** as well as by providing complete **solutions**. Devoteam NV/SA has a long experience in doing projects and quality assurance. Devoteam has several Prince2 certified project managers and an ISO 9001:2008 certificate.







Excellence. Competence. Recognition

EXCELLENCE.  
COMPETENCE.  
RECOGNITION.



**PECB** – Professional Evaluation and Certification Board

7275 Sherbrooke East, Suite 32  
CP 49060, Montreal, QC  
H1N 1H0, CANADA

80 Broad Street, 5th Floor  
New York City, NY  
10004, USA

**Email:**

**General inquiries:** [info@pecb.org](mailto:info@pecb.org)  
**Certification:** [certification@pecb.org](mailto:certification@pecb.org)  
**Examination:** [examination@pecb.org](mailto:examination@pecb.org)  
**Training:** [training@pecb.org](mailto:training@pecb.org)  
**Technical support:** [support@pecb.org](mailto:support@pecb.org)

**Tel:** 1-514-562-5464  
**Fax:** (202) 618-6264

[www.pecb.org](http://www.pecb.org)