



When Recognition Matters



EXAM PREPARATION GUIDE

PECB Certified ISO 22301 Lead Implementer

The objective of the “Certified ISO 22301 Lead Implementer” examination is to ensure that the candidate has the knowledge and the skills to support an organization in implementing and managing a Business Continuity Management System (BCMS) based on ISO 22301:2012.

The target population for this examination is:

- Project managers or consultants wanting to prepare and to support an organization in the implementation of a Business Continuity Management System (BCMS)
- Business Continuity auditors who wish to fully understand the implementation of a Business Continuity Management System
- Persons responsible for the business continuity or conformity in an organization
- Members of a Business Continuity team
- Expert advisors in Business Continuity
- Member of an organization that want to prepare for a business continuity function or for a BCMS project management function

The exam content covers the following domains:

- Domain 1: Fundamental Principles and Concepts in Business Continuity (BC)
- Domain 2: Business Continuity Best Practices based on ISO 22301
- Domain 3: Planning a BCMS based on ISO 22301
- Domain 4: Implementing a BCMS based on ISO 22301
- Domain 5: Performance Evaluation, Monitoring and Measurement of a BCMS based on ISO 22301
- Domain 6: Continual Improvement of a BCMS based on ISO 22301
- Domain 7: Preparation for a BCMS Certification Audit

The content of the exam is divided as follows:

Domain 1: Fundamental Principles and Concepts In Business Continuity

Main objective: To ensure that the ISO 22301 Lead Implementer candidate can understand, interpret and illustrate the main Business Continuity concepts related to a Business Continuity Management System (BCMS).

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Understand and explain the operations of the ISO organization and the development of Business Continuity standards. 2. Ability to identify, analyze and evaluate the Business Continuity compliance requirements for an organization. 3. Ability to explain and illustrate the main concepts in Business Continuity and Business Continuity risk management. 4. Ability to distinguish and explain the difference between information asset, data and record. 5. Understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls. 	<ol style="list-style-type: none"> 1. Knowledge of the application of the eight ISO management principles to Business Continuity. 2. Knowledge of the main standards in Business Continuity. 3. Knowledge of the different sources of Business Continuity requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies. 4. Knowledge of the main Business Continuity concepts and terminology as described in ISO 22301. 5. Knowledge of the concept of risk and its application in Business Continuity. 6. Knowledge of the relationship between the concepts of asset, vulnerability, threat, impact and controls. 7. Knowledge of the difference between preventive, detective and corrective controls and their characteristics.

Domain 2: Business Continuity Best Practice based on ISO 22301

Main objective: To ensure that the ISO 22301 Lead Implementer candidate can understand, interpret and provide guidance on how to implement and manage Business Continuity requirements based on best practices of ISO 22301.

Competencies	Knowledge statements
1. Ability to identify, understand, classify and explain the clauses with requirements from ISO 22301.	1. Knowledge of operational planning and control.
2. Ability to detail and illustrate the requirements and best practices by concrete examples.	2. Knowledge of business impact analysis and risk assessment.
3. Ability to compare possible solutions to a business continuity issue of an organization and identify/analyze the strength and weakness of each solution.	3. Knowledge of business continuity strategy.
4. Ability to select and demonstrate the best business continuity solution in order to address Business Continuity objectives stated by the organization.	4. Knowledge of establishing and implementing business continuity procedures.
5. Ability to create and justify an action plan to implement a business continuity by listing the activities related.	5. Knowledge of exercising and testing.
6. Ability to analyze, evaluate and validate action plans to implement a specific requirement.	6. Knowledge of Business Continuity Incident Management Controls Best Practices.
	7. Knowledge of Business Continuity Management Best Practices.

Domain 3: Planning a BCMS based on ISO 22301

Main objective: To ensure that the ISO 22301 Lead Implementer candidate can plan the implementation of a BCMS in preparation for an ISO 22301 certification.

Competencies

1. Ability to manage a BCMS implementation project following project management best practices.
2. Ability to gather, analyze and interpret the necessary information to plan the BCMS implementation.
3. Ability to observe, analyze and interpret the external and internal environment of an organization.
4. Ability to perform a gap analysis and clarify the Business Continuity objectives of an organization.
5. Ability to state and justify an BCMS scope adapted to the security objectives of a specific organization.
6. Ability to select and justify the selected approach and methodology adapted to the needs of the organization.
7. Ability to perform the different steps of the risk assessment and risk treatment phases

Knowledge statements

1. Knowledge of the main project management concepts, terminology, process and best practice as described in ISO 10006.
2. Knowledge of the principal approaches and methodology frameworks to implement a BCMS.
3. Knowledge of the main concepts and terminology related to organizations
4. Knowledge of an organization's external and internal environment.
5. Knowledge of the main interested parties related to an organization and their characteristics.
6. Knowledge of techniques to gather information on an organization and to perform a gap analysis of a management system.
7. Knowledge of the characteristics of an BCMS scope in terms of organizational, technological and physical boundaries.
8. Knowledge of the different approaches and main methodology characteristics to perform a risk assessment.
9. Knowledge of the main activities of the risk identification, estimation, evaluation related to the assets included in the BCMS of an organization.

Domain 4: Implementing a BCMS based on ISO 22301

Main objective: To ensure that the ISO 22301 Lead Implementer candidate can implement the processes and security controls of a BCMS required for an ISO 22301 certification.

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of a BCMS. 2. Ability to define the document and record management processes needed to support the implementation and the operations of a BCMS. 3. Ability to define and design security controls & processes and document them. 4. Ability to define and write BCMS policies & procedures. 5. Ability to implement the required processes and security controls of an BCMS. 6. Ability to define and implement appropriate Business Continuity training, awareness and communication plans. 7. Ability to define and implement an incident management process based on Business Continuity best practices. 8. Ability to transfer a BCMS project to operations and manage the change management process. 	<ol style="list-style-type: none"> 1. Knowledge of the roles and responsibilities of the key actors during the implementation of a BCMS and in its operation after the end of the implementation project. 2. Knowledge of the main organizational structures applicable for an organization to manage Business Continuity. 3. Knowledge of the best practices on document and record management processes and the document management life cycle. 4. Knowledge of the characteristics and the differences between the different documents related to BCMS: policy, procedure, guideline, standard, baseline, worksheet, etc. 5. Knowledge of model-building controls and processes techniques and best practices. 6. Knowledge of controls and processes deployment techniques and best practices. 7. Knowledge of techniques and best practices to write Business Continuity policies, procedures and others types of documents include in a BCMS. 8. Knowledge of the characteristics and the best practices to implement Business Continuity training, awareness and communication plans 9. Knowledge of the characteristics and main processes of an information management incident management process based on best practices. 10. Knowledge of change management techniques best practices.

Domain 5: Performance Evaluation, Monitoring and Measurement of a BCMS based on ISO 22301

Main objective: To ensure that the ISO 22301 Lead Implementer candidate can evaluate, monitor and measure the performance of a BCMS in the context of an ISO 22301 certification.

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of a BCMS in operation.	1. Knowledge of the techniques and best practices to monitor the effectiveness of a BCMS.
2. Ability to verify the extent to which identified security requirements have been met.	2. Knowledge of the main concepts and components related to a Business Continuity Measurement Programme: measures, attributes, indicators, dashboard, etc.
3. Ability to define and implemented an internal audit program for ISO 22301.	3. Knowledge of the characteristics and the differences between an operational, tactical and strategic Business Continuity indicators and dashboard.
4. Ability to perform regular and methodical reviews regarding the suitability, adequacy, effectiveness and efficiency of a BCMS with policies and objectives of an organization.	4. Knowledge of the techniques and methods to define and document adequate and reliable indicators.
5. Ability to define and implement a management review process and counsel management on it.	5. Knowledge of the main concepts and components related to the implementation and operation of a BCMS internal audit program.
	6. Knowledge of the differences between the concepts of major nonconformity, minor nonconformity, anomaly and observation.
	7. Knowledge of the guidelines and best practices to write nonconformity report.
	8. Knowledge of the best practices on how to perform management reviews.

Domain 6: Continual Improvement of a BCMS based on ISO 22301

Main objective: To ensure that the ISO 22301 Lead Implementer candidate can provide guidance on the continual improvement of a BCMS in the context of ISO 22301.

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to understand the principle and concepts related to continual improvement. 2. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of a BCMS. 3. Ability to implement BCMS continual improvement processes in an organization. 4. Ability to determine the appropriate business improvement tools to support continual improvement processes of a specific organization. 5. Ability to identify, analyze the root-causes of nonconformities and proposed action plans to treat them. 6. Ability to identify, analyze the root-cause of potential nonconformities and proposed action plans to treat them. 	<ol style="list-style-type: none"> 1. Knowledge of the main concepts related to continual improvement. 2. Knowledge of the characteristics and the difference between the concept of effectiveness and the efficiency. 3. Knowledge of the concept and techniques to perform a benchmarking. 4. Knowledge of the main processes, tools and techniques used by professionals to identify the root-causes of nonconformities. 5. Knowledge of the characteristics and the difference between corrective actions and preventive actions. 6. Knowledge of the main processes, tools and techniques used by professionals to develop and proposed the best corrective and preventive action plans.

Domain 7: Preparation for a BCMS Certification Audit

Main objective: To ensure that the ISO 22301 Lead Implementer candidate can prepare and assist an organization for the certification of a BCMS against the ISO 22301 standard.

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to understand the main steps processes and activities related to an ISO 22301 certification audit. 2. Ability to understand, explain and illustrate the audit evidence approach in the context of an ISO 22301 audit. 3. Ability to counsel an organization to identify and select a certification body that meets their needs. 4. Ability to review the readiness of an organization for an ISO 22301 certification audit. 5. Ability to coach and prepare the personnel of an organization for an ISO 22301 certification audit. 6. Ability to argue and challenge the audit findings and conclusions with external auditors. 	<ol style="list-style-type: none"> 1. Knowledge of the Knowledge of evidence based approach in an audit. 2. Knowledge of the different types of evidences: physical, mathematical, confirmative, technical, analytical, documentary and verbal. 3. Knowledge of the difference of the stage 1 audit and the stage 2 audit. 4. Knowledge of stage 1 audit requirements, steps and activities. 5. Knowledge of the documentation review criteria. 6. Knowledge of stage 2 audit requirements, steps and activities. 7. Knowledge of follow-up audit requirements, steps and activities. 8. Knowledge of surveillance audits and recertification audit requirements, steps and activities. 9. Knowledge of the requirements, guidelines and best practices to develop action plans following an ISO 22301 certification audit.

Based on these seven domains and their relevance, thirteen questions are included in the exam, as summarized in the following table:

		Points per Question	Level of Understanding (Cognitive/Taxonomy) Required		Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points competency domain
			Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation				
Competency Domains	Fundamental principles and concepts of BC	5	x		2	15.38	10	13.33
		5	x					
	BC Best Practice based on ISO 22301	5		x	2	15.38	10	13.33
		5	x					
	Planning a BCMS based on ISO 22301	5	x		1	7.69	5	6.67
		10	x					
	Implementing a BCMS based on ISO 22301	5	x		3	23.08	20	26.67
		5	x					
		5	x					
	Performance evaluation, monitoring and measurement of a BCMS based on ISO 22301	5		x	3	23.08	20	26.67
		5		x				
		10		x				
	Continual improvement of a BCMS based on ISO 22301	5		x	1	7.69	5	6.67
	5		x					
Preparation for an BCMS certification audit	5		x	1	7.69	5	6.67	
Total points		75						
Number of Questions per level of understanding			7	6				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			53.85	46.15				

The passing score is established at **70%**.

After successfully passing the exam, candidates will be able to apply for the credentials of Certified ISO 22301 Lead Implementer, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the proctor and the exam confirmation letter.

The exam duration is three (3) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be “open book” and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are “open book”; candidates are authorized to use the following reference materials:

- A copy of the ISO 22301:2012 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com.

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limitation on how many times a candidate can retake the same exam. However, there are some limitations in terms of allowed time-frame in between exams.

When candidates fail the examination, they are only allowed to retake the examination once within 12 months after the first attempt. If second examination is unsuccessful, candidates will be allowed to retake the exam only after 1 year (12 months). Retake fee applies.

Only candidates, who have completed a full PECB training but fail the written exam, are eligible to retake the exam for free, under one condition:

“A candidate can only retake the exam once and this retake must occur within 12 months from the initial exam's date.”

When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. Mitigation measures

For the following scenario of the BIA, select and define at least two mitigation measures to reduce or avoid this disruption.

Possible answers:

Scenarios	Impact	Probability	RTO	RPO	Strategy	Mitigation measures
Total damage and loss of the Storage Area Network (SAN)	<p>Dissatisfaction of client requirements</p> <p>Financial losses aroused from unfulfilled orders</p> <p>Negative publicity</p>	<p>Negative publicity would most certainly occur if customers could not obtain products due to their unavailability</p> <p>The loss of clients may occur due to issues, however if these repeated issues will continue to happen would increase the probability of occurrence</p>	4 Hours	1 Hour	Arrangement of the service based on the best practices by a specific IT service provider who could set up the SAN quickly and restore data from backups within the RTO.	<p>Implementation of failover controls (e.g. disk mirroring, failover components, control path failover, data path failover and load balancing).</p> <p>Implementing controls at the facility where the SAN is held including, power failure controls, fire suppressant systems and physical security</p>

2. Action plans to verify compliance with clauses

For each of the following clauses of the ISO 22301 standard, please provide an action plan with at least two concrete actions that would be acceptable to verify compliance with the clause and meet the requirements.

8.4.4 Business continuity plans

Possible answers:

- Business continuity plans (BCP) reviewed and updated.
- BCP test reports
- BCP project team and their responsibilities

7.5.3 Control of documented information

Controls for documented information shall include as applicable:

e) control of changes (e.g. version control);

Possible answers:

- Elaborate a documented procedure for controlling documented information, that includes control of changes
- Add a revision history at the end of documents that includes the version, change description and date

3. Development of metrics

Please provide metrics that allow measuring the effectiveness of clause 10.1d: 10.1 Non-conformity and corrective action

Possible answers:

- Number of non-conformities identified vs. non-conformities corrected
- Number of re-occurrences of non-conformities
- Average length of time taken to correct non-conformities by category
- Frequency of re-occurring non-conformities

4. Corrective action plans

You have received a corrective action plan to review. Please evaluate the effectiveness of the corrective actions that are proposed. If you agree with these corrective actions, explain why. If you do not agree, explain why, and propose what would be minimal adequate corrective action.

- **A nonconformity has been observed because the organization did not define the necessary competencies that each employee needs to hold.**
- **Corrective action: Purchase a series of job description templates (Timeframe: immediately).**

Possible answers:

Not acceptable. The organization needs to define its own competency needs, not just take generic ones. The generic templates could be used as a start.