When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO 22301 Lead Auditor

The objective of the “Certified ISO 22301 Lead Auditor” examination is to ensure that the candidate has the knowledge and the skills to audit a Business Continuity Management System (BCMS) as specified in ISO 22301:2012 and to manage a team of auditors by applying widely recognized audit principles, procedures and techniques, to master audit principles and techniques, and to manage (or be part of) audit teams and audit programs.

The target population for this examination is:

- Internal auditors
- Auditors wanting to perform and lead Business Continuity Management System (BCMS) certification audits
- Project managers or consultants wanting to master the Business Continuity Management System audit process
- Persons responsible for the Business continuity or conformity in an organization
- Members of an business continuity team
- Expert advisors in information technology
- Technical experts wanting to prepare for an Business continuity audit function

The exam content covers the following domains:

- Domain 1: Fundamental Principles and Concepts of Business Continuity
- Domain 2: Business Continuity Management System (BCMS)
- Domain 3: Fundamental Audit Concepts and Principles
- Domain 4: Preparation of an ISO 22301 Audit
- Domain 5: Conducting of an ISO 22301 Audit
- Domain 6: Closing an ISO 22301 Audit
- Domain 7: Managing an ISO 22301 Audit Program

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 Auditor candidate can understand, interpret and illustrate the main Business Continuity concepts related to a Business Continuity Management System (BCMS).

Competencies	Knowledge statements
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. Understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls.	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 and characteristics of security objectives and controls. 8. Knowledge of the difference between preventive, detective and corrective controls and their characteristics.

Domain 2: Business Continuity Management System (BCMS)

Main objective: To ensure that the ISO 22301 Lead Auditor candidate can understand, interpret and illustrate the main concepts and components of an Business Continuity Management System based on ISO 22301.

Competencies	Knowledge statements
1. Understand and explain the components of an Business Continuity Management System based on ISO 22301 and its principal processes.	1. Knowledge of the concepts, principles and terminology related to management systems and the "Plan-Do-Check-Act" (PDCA) model.
2. Ability to interpret and analyze ISO 22301 requirements.	2. Knowledge of the principal characteristics of an integrated management system.
3. Understand, explain and illustrate the main steps to establish, implement, operate, monitor, review, maintain and improve an organization's BCMS.	3. Knowledge of the main advantages of a certification for an organization.
	4. Knowledge of the ISO 22301 requirements presented in the clauses 4 to 10.
	5. Knowledge of the main steps to establish the BCMS and security policies, security objectives, processes and procedures relevant to managing risk and improving Business Continuity to deliver results in accordance with an organization’s overall policies and objectives (Awareness level).
	6. Knowledge of the concept of continual improvement and its application to a BCMS.

Domain 3: Fundamental Audit Concepts and Principles

Main objective: To ensure that the ISO 22301 Lead Auditor candidate can understand, interpret and apply the main concepts and principles related to a BCMS audit in the context of ISO 22301.

Competencies	Knowledge statements
1. Understand, explain and illustrate the application of the audit principles in the context of an ISO 22301 audit. 2. Ability to identify and judge situations that would discredit the professionalism of the auditor and the PECB code of ethics. 3. Ability to identify and evaluate ethical problems taking into account the obligations related to sponsors, auditee and law enforcement or regulatory authorities. 4. Ability to explain, illustrate and apply the audit evidence approach in the context of an ISO 22301 audit. 5. Ability to explain and compare the types and characteristics of evidence. 6. Ability to determine and justify what type of evidence and how much evidence will be required in the context of a specific BCMS audit mission. 7. Ability to determine and evaluate the level of materiality and apply the risk based approach during the different phases of an ISO 22301 audit. 8. Ability to judge the appropriate level of reasonable assurance needed for a specific ISO 22301 audit mission.	1. Knowledge of the main audit concepts and terminology as described in ISO 19011. 2. Knowledge of the differences between first party, second party and third party audit. 3. Knowledge of the following audit principles: integrity, fair presentation, due professional care, professional judgment, professional skepticism, confidentiality and independence. 4. Knowledge of professional responsibility of an auditor and the PECB code of ethics. 5. Knowledge of evidence based approach in an audit. 6. Knowledge of the different types of evidences: physical, mathematical, confirmative, technical, analytical, documentary and verbal. 7. Knowledge of quality of audit evidences (competent, appropriate, reliable and sufficient) and the factors that will influence them. 8. Knowledge of the risk based approach in an audit and the different types of risk related to audit activities. 9. Knowledge of the concept of materiality and its application in an audit. 10. Knowledge of the concept of reasonable assurance and its applicable in an audit.

Domain 4: Preparation of an ISO 22301 Audit

Main objective: To ensure that the ISO 22301 Lead Auditor candidate can prepare appropriately a BCMS audit in the context of ISO 22301.

Competencies	Knowledge statements
1. Understand and explain the steps and activities to do to prepare a BCMS audit taking in consideration the specific context and conditions of the mission.	1. Knowledge of the main responsibilities of the audit team leader and audit team members.
2. Understand and explain the roles and responsibilities of the audit team leader, audit team members and technical experts.	2. Knowledge of the roles and responsibilities of technical experts used for an audit.
3. Ability to determine, evaluate and confirm the audit objectives, the audit criteria and the audit scope for a specific ISO 22301 audit mission.	3. Knowledge of the definition of audit objectives, audit scope and audit criteria.
4. Ability to do a feasibility study of an audit in the context of a specific ISO 22301 audit mission.	4. Knowledge of the difference between the BCMS scope and the audit scope.
5. Ability to explain, illustrate and define the characteristics of the audit terms of engagement and apply the best practices to establish a first contact with an auditee in the context of a specific ISO 22301 audit mission.	5. Knowledge of the elements to review during the feasibility study of an audit.
6. Ability to develop audit working papers and to elaborate appropriate audit test plans in the context of a specific ISO 22301 audit mission	6. Knowledge of the cultural aspects to consider in an audit.
	7. Knowledge of the characteristics of audit terms of engagement and the best practices to establish a first contact with an auditee.
	8. Knowledge of the preparation of an audit plan
	9. Knowledge of the preparation and development of audit working paper.
	10. Knowledge of advantages and disadvantages of using audit checklists.
	11. Knowledge of the best practices for creation of audit test plans.

Domain 5: Conduct of an ISO 22301 Audit

Main objective: To ensure that the ISO 22301 Lead Auditor candidate can conduct efficiently a BCMS audit in the context of ISO 22301.

Competencies	Knowledge statements
1. Ability to organize and conduct the opening meeting in the context of a specific ISO 22301 audit mission. 2. Ability to conduct a stage 1 audit in the context of a specific ISO 22301 audit mission and taking into account the documentation review conditions and criteria. 3. Ability to conduct a stage 2 audit in the context of a specific ISO 22301 audit mission by applying the best practices of communication to collect the appropriate evidence and taking into account the roles and responsibilities of all people involved. 4. Ability to explain, illustrate and apply statistical techniques and main audit sampling methods. 5. Ability to gather appropriate evidences objectively from the available information in an audit and to evaluate them objectively.	1. Knowledge of the objectives and the content of the opening meeting of an audit. 2. Knowledge of the difference of the stage 1 audit and the stage 2 audit. 3. Knowledge of stage 1 audit requirements, steps and activities. 4. Knowledge of the documentation review criteria 5. Knowledge of the documentation requirements stated in ISO 22301. 6. Knowledge of stage 2 audit requirements, steps and activities. 7. Knowledge of best practices of communication during an audit. 8. Knowledge of the roles and responsibilities of guides and observers during an audit. 9. Knowledge of the conflict resolution techniques. 10. Knowledge of evidence collection procedures: observation, documentation review, interviews, analysis and technical verification. 11. Knowledge of evidence analysis procedures: corroboration and evaluation. 12. Knowledge of main concepts, principles and statistical techniques used in an audit. 13. Knowledge of the main audit sampling methods and their characteristics.

Domain 6: Conclusion and Follow-up of an ISO 22301 Audit

Main objective: To ensure that the ISO 22301 Lead Auditor candidate can conclude a BCMS audit and conduct follow-up activities in the context of ISO 22301.

Competencies	Knowledge statements
1. Ability to explain and apply the evaluation process of evidences to draft audit findings and prepare audit conclusions. 2. Understand, explain and illustrate the different levels of conformity and the concept of benefits of doubt. 3. Ability to report appropriate audit observations in order to help an organization to improve a BCMS in respect of audit rules and principles. 4. Ability to complete audit working documents and do a quality review of an ISO 22301 audit. 5. Ability to draft audit conclusions and present these to the management of the audited organization. 6. Ability to organize and conduct an audit closing meeting. 7. Ability to write an ISO 22301 audit report and justify a certification recommendation. 8. Ability to conduct the activities following an initial audit including the evaluation of action plans, follow up audits, surveillance audits and recertification audits.	1. Knowledge of the evaluation process of evidences to draft audit findings and prepare audit conclusions. 2. Knowledge of the differences and the characteristics between the concepts of conformity, minor nonconformity, major nonconformity, anomaly and observation. 3. Knowledge of the guidelines and best practices to write nonconformity report. 4. Knowledge of the guidelines and best practices to draft and report audit observation. 5. Knowledge of the principle of benefits of doubt and his application in the context of an audit. 6. Knowledge of the guidelines and best practices to complete audit working documents and do a quality review of an audit. 7. Knowledge of the guidelines and best practices to present audit findings and conclusions to management of an audited organization. 8. Knowledge of the possible recommendations that an auditor can issue in the context of a certification audit and the certification decision process. 9. Knowledge of the guidelines and best practices to evaluate action plans. 10. Knowledge of follow-up audit, surveillance audits and recertification audit requirements, steps and activities. 11. Knowledge of the conditions for modification, extension, suspension or withdrawal of a certification for an organization.

Domain 7: Management of an ISO 22301 Audit Program

Main objective: To ensure that the ISO 22301 Lead Auditor understands how to establish and manage a BCMS audit program.

Competencies	Knowledge statements
1. Understand and explain the establishment of an audit program and the application of the PDCA model.	1. Knowledge of the application of the PDCA model in the management of an audit program.
2. Understand and explain the implementation of an ISO 22301 audit program (first party, second party and third party).	2. Knowledge of requirements, guidelines and best practices regarding audit resources, procedures and policies.
3. Understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records.	3. Knowledge of the types of tools used by professional auditors.
4. Understand the requirements related to the components of the management system of an audit program as quality management, record management, and complaint management.	4. Knowledge of requirements, guidelines and best practices regarding the management of audit records.
5. Understand the evaluation of the efficiency of the audit program by monitoring the performance of each auditor, each team and the entire certification body.	5. Knowledge of the application of the concept of continual improvement to the management of an audit program.
6. Understand and explain the way combined audits are handled in an audit program.	6. Knowledge of the particularities to implement and manage a first, second or third party audit program.
7. Ability to demonstrate the application of the personal attributes and behaviors associated to professional auditors	7. Knowledge of the management of combined audit activities.
	8. Knowledge of the concept of competency and its application to auditors.
	9. Knowledge of the personal attributes and behavior of a professional auditor.

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

			Level of Understanding (Cognitive/Taxonomy) Required					
		Points per Question	Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points competency domain
Competency Domains	Fundamental principles and concepts in BC	5	x		2	16.67	15	20.00
		10	x					
	BCMS	5	x		1	8.33	5	6.67
	Fundamental audit concepts and principles	5	x		2	16.67	10	13.33
		5	x					
	Preparation of an ISO 22301 audit	5	x		1	8.33	5	6.67
	Conduct of an ISO 22301 audit	5	x		1	8.33	5	6.67
	Conclusion and follow-up of an ISO 22301 audit	10		x	3	25.00	25	33.33
		5		x				
		10		x				
	Management of an ISO 22301 audit program	5		x	2	16.67	10	13.33
		5		x				
Total points		75						
Number of Questions per level of understanding			7	5				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			58.33	41.67				

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 Auditor, 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. Identification and management of risk scenarios

Determine the threats, vulnerabilities and impacts associated with the following situations. Complete the matrix and propose at least two mitigation measures to treat (accept, reduce, transfer or avoid) the risks.

Possible answers:

Statements	Vulnerabilities	Threats	Potential Impacts	Mitigation measures
Example: Many employees of the organization work remotely from their home.	Large number of unverified/unevaluated service providers	Service failure	Loss of productivity due to unavailability Deterioration of the network Data loss	▪ Assess service providers. ▪ Create list of authorized remote service providers. ▪ Develop emergency procedures in case of unavailability of service.

2. Evidence in an audit

For each of the following clauses of the ISO 22301 standard, please provide at least two different evidences that would be acceptable to verify the existence and effectiveness of the control.

7.5.3 Control of documented information - For the control of documented information, the organization shall address the following activities, as applicable

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

Possible answers:

Review a sample of documents to ensure that these are adequately identified, versioned and if any of those documents had changes to verify the identification of changes.

3. Writing of a test plan

In certain cases, there are several applicable and appropriate audit procedures to validate a control measure. Please prepare a test plan by selecting 5 different suitable, applicable and appropriate procedures to validate clause 7.5.3 Control of Documented Information

Possible answers:

Control of Documented Information (clause 7.5.3). When establishing control of documented information, the organization shall ensure that there is adequate protection for the documented information (e.g. protection against compromise, unauthorized modification or deletion).	
Observation	Observe how employees ensure the protection of documented information and whether those actions are consistent with the policies and procedures of the organization
Document	Policy on documented information management and procedures on information lifecycle management: their identification, storage, backup, protection, accessibility and conservation
Interview	Member of management (to confirm policies and the organization's needs related to documented information) and the personnel responsible for information management and archiving (to obtain the documented information management details)
Technical verification	Validate the electronic structure for classifying and storing of documented information, verify the protection mechanisms of them, observe the compilation of the automated journals report
Analysis	Select documented information samples and verify if they respect the documentation structure and policy criteria on documented information

4. Evaluation of corrective actions

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 to start.