

Exam Preparation Guide

ISO 22301 Lead Auditor

GENERAL

The objective of the “PECB Certified ISO 22301 Lead Auditor” exam is to ensure that the candidate has acquired the necessary knowledge to perform a business continuity management system (BCMS) audit in compliance with the requirements of ISO 22301 and manage an audit team by applying widely recognized audit principles, procedures, and techniques. Furthermore, the exam seeks to determine a candidate’s competence to plan and conduct internal and external audits in accordance with the recommendations of ISO 19011 and the requirements of ISO/IEC 17021-1.

The ISO 22301 Lead Auditor exam is intended for:

- Auditors seeking to perform and lead business continuity management system (BCMS) audits
- Managers or consultants wishing to master the BCMS audit process
- Individuals responsible for maintaining conformity with the ISO 22301 and BCMS requirements in an organization
- Members of business continuity teams
- Internal auditors
- Individuals tasked with improving their organization’s business continuity effectiveness
- Technical experts seeking to prepare for a BCMS audit
- Experts in business continuity management

The exam covers the following competency domains:

- **Domain 1:** Fundamental principles and concepts of business continuity management system (BCMS)
- **Domain 2:** Business continuity management system (BCMS)
- **Domain 3:** Fundamental audit concepts and principles
- **Domain 4:** Preparing for an ISO 22301 audit
- **Domain 5:** Conducting an ISO 22301 audit
- **Domain 6:** Closing an ISO 22301 audit
- **Domain 7:** Managing an ISO 22301 internal audit program

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts of business continuity management system (BCMS)

Main objective: Ensure that the candidate understands and is able to interpret the ISO 22301 principles and concepts

Competencies	Knowledge statements
<ol style="list-style-type: none">1. Ability to explain what ISO does and the key principles in standard development2. Ability to distinguish between various ISO management system standards3. Ability to explain what an integrated management system is and how it can help an organization4. Ability to evaluate the applicability of ISO 22301 requirements to an organization5. Ability to explain the advantages of implementing a BCMS based on ISO 223016. Ability to describe the management system certification process7. Ability to explain and illustrate the main terms and definitions of ISO 223018. Ability to illustrate the correlation between the Plan-Do-Check-Act (PDCA) cycle and the main clauses of ISO 22301	<ol style="list-style-type: none">1. Knowledge of management system standards and integrated management systems2. Knowledge of various standards that are part of the ISO 22301 family of standards3. Knowledge of the scope of ISO 223014. Knowledge of the benefits of implementing a BCMS based on ISO 223015. Knowledge of management system certification process for an organization, from the implementation phase to the obtainment of the certification6. Knowledge of the main terms and definitions of ISO 223017. Knowledge of the business continuity performance approach, as described in ISO 223018. Knowledge of the Plan-Do-Check-Act (PDCA) cycle and its application in ISO 22301

Domain 2: Business continuity management system (BCMS)

Main objective: Ensure that the candidate is aware of the main ISO 22301 requirements for a BCMS, as described in clauses 4 to 10

Competencies	Knowledge statements
<ol style="list-style-type: none">1. Ability to interpret the requirements of ISO 22301 in the specific context of an organization2. Ability to interpret the standard's requirements for the top management of the organization, and their role and engagement before, during, and after the establishment of the BCMS3. Ability to describe the process and requirements for setting strategy objectives and establishing guiding principles4. Ability to explain the standard's requirements relating to the resources that need to be provided and the BCMS documented information that must be maintained5. Ability to describe the standard's requirements for planning, implementing, and controlling the processes needed to achieve business continuity objectives6. Ability to interpret the standard's requirements on evaluating the effectiveness of the BCMS	<ol style="list-style-type: none">1. Knowledge of the requirements of ISO 22301 for establishing, implementing, maintaining, and continually improving a BCMS2. Thorough knowledge of the ISO 22301 requirements – clauses 4 to 10

Domain 3: Fundamental audit concepts and principles

Main objective: Ensure that the candidate understands and adheres to the fundamental concepts and principles of management system auditing

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to understand, explain, and illustrate the application of audit principles in a BCMS audit 2. Ability to identify and judge situations that would discredit the professionalism of the auditor and violate the PECB Code of Ethics 3. Ability to identify and judge ethical issues considering the obligations related to the audit client, auditee, law enforcement, and regulatory authorities 4. Ability to explain, illustrate, and apply the audit evidence approach in the BCMS audit 5. Ability to explain and compare evidence types and their characteristics 6. Ability to determine and justify the choice and amount of evidence required in the BCMS audit 7. Ability to determine and evaluate the level of materiality and apply the risk-based approach during the different stages of the BCMS audit 8. Ability to judge the appropriate level of reasonable assurance needed for verification of compliance 	<ol style="list-style-type: none"> 1. Knowledge of the main audit concepts and terminology as described in ISO 19011 2. Knowledge of the differences between first, second, and third party audits 3. Knowledge of auditing principles: integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach 4. Knowledge of an auditor's responsibilities 5. Knowledge of the requirements originating from the PECB Code of Ethics 6. Knowledge of the different types of audit evidence: physical, mathematical, confirmative, technical, analytical, documentary, and verbal 7. Knowledge of the quality of audit evidence and the factors that influence it 8. Knowledge of the risk-based approach to an audit and the different types of risks related to audit activities such as inherent risk, control risk, and detection risk 9. Knowledge of the concept of materiality and its application on audits 10. Knowledge of the concept of reasonable assurance and its application on a BCMS audit

Domain 4: Preparing for an ISO 22301 audit

Main objective: Ensure that the candidate is able to prepare a business continuity management system audit

Competencies	Knowledge statements
<ol style="list-style-type: none">1. Ability to understand the activities needed for the preparations of a BCMS audit considering the specific context of the auditee2. Ability to understand and explain the roles and responsibilities of the audit team leader, audit team members, and technical experts3. Ability to determine, evaluate, and confirm the objectives, the criteria, and the scope of the BCMS audit4. Ability to conduct a feasibility study5. Ability to explain, illustrate, and define the characteristics of the terms of the audit engagement and apply the best practices to establish the initial contact with an auditee6. Ability to develop audit working papers and elaborate appropriate audit test plans in the BCMS audit	<ol style="list-style-type: none">1. Knowledge of the main responsibilities of the audit team leader and other members of the audit team2. Knowledge of the roles and responsibilities of technical experts3. Knowledge of the audit objectives, audit scope, and audit criteria4. Knowledge of the difference between the BCMS scope and the audit scope5. Knowledge of the elements to review during the feasibility study of an audit6. Knowledge of the cultural aspects to consider in an audit7. Knowledge of the characteristics of terms of the audit engagement and the best practices to establish the initial contact with an auditee8. Knowledge of the audit plan preparation procedure9. Knowledge of the preparation and development of audit working papers10. Knowledge of the advantages and disadvantages of using audit checklists11. Knowledge of the best practices for the creation of audit test plans

Domain 5: Conducting an ISO 22301 audit

Main objective: Ensure that the candidate can efficiently conduct a BCMS audit

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to organize and conduct an opening meeting 2. Ability to conduct the stage 1 audit, taking into account the criteria for documented information review 3. Ability to conduct the stage 2 audit by appropriately following the procedures that this stage entails 4. Ability to apply the best practices of communication to collect the appropriate audit evidence 5. Ability to consider the roles and responsibilities of all the interested parties involved 6. Ability to explain, illustrate, and apply statistical techniques and audit sampling methods 7. Ability to gather appropriate evidence from the available information during an audit and evaluate it objectively 	<ol style="list-style-type: none"> 1. Knowledge of the objectives and the topics covered in a opening meeting in an audit 2. Knowledge of the difference between stage 1 audit and stage 2 audit 3. Knowledge of stage 1 audit requirements, steps, and activities 4. Knowledge of the criteria for documented information review 5. Knowledge of stage 2 audit requirements, steps, and activities 6. Knowledge of the best communication practices during an audit 7. Knowledge of the roles and responsibilities of guides and observers during an audit 8. Knowledge of different conflict resolution techniques 9. Knowledge of evidence collection procedures such as observation, documented information review, interviewing, analysis, sampling, and technical verification 10. Knowledge of the evidence analysis procedures: corroboration and evaluation 11. Knowledge of the main concepts, principles, and statistical techniques used in an audit 12. Knowledge of the main audit sampling methods and their characteristics

Domain 6: Closing an ISO 22301 audit

Main objective: Ensure that the candidate is able to conclude a BCMS audit and conduct audit follow-up activities

Competencies	Knowledge statements
<ol style="list-style-type: none"> 1. Ability to explain and follow the evidence evaluation process: drafting audit findings and preparing audit conclusions 2. Ability to understand, explain, and illustrate the different levels of conformity and the concept of the benefit of the doubt in audit 3. Ability to report appropriate audit observations in order to help an organization improve the BCMS with respect to audit rules and principles 4. Ability to complete audit work documents and conduct quality reviews 5. Ability to draft the audit conclusions and present them to the auditee's management 6. Ability to organize and conduct a closing meeting 7. Ability to draft an ISO 22301 audit report and provide and justify a recommendation for certification 8. Ability to conduct the activities following an initial audit, including the evaluation of action plans, follow-up, and surveillance during the different stages of the BCMS audit 	<ol style="list-style-type: none"> 1. Knowledge of the evidence evaluation process: to draft audit findings and to prepare audit conclusions 2. Knowledge of the characteristics and differences between the concepts of conformity, minor nonconformity, major nonconformity, anomaly, and observation 3. Knowledge of the guidelines and best practices to draft nonconformity reports 4. Knowledge of the guidelines and best practices to draft and report audit observations 5. Knowledge of the benefit of the doubt principle and its application in a BCMS audit 6. Knowledge of the guidelines and best practices to complete audit work documents and perform a quality review 7. Knowledge of the guidelines and best practices to present audit findings and conclusions to the management of the auditee 8. Knowledge of the possible recommendations that an auditor can issue during the certification audit 9. Knowledge of the guidelines and best practices to evaluate action plans 10. Knowledge of audit follow-ups, surveillance audits, and recertification audit requirements, steps, and activities 11. Knowledge of the conditions for the modification, extension, suspension, or withdrawal of an organization's certification

Domain 7: Managing an ISO 22301 internal audit program

Main objective: Ensure that the candidate is able to establish and manage a BCMS internal audit program based on the recommendations of ISO 19011 and in adherence to the requirements of ISO 22301

Competencies	Knowledge statements
<ol style="list-style-type: none">1. Ability to establish an internal audit program based on the recommendations of ISO 190112. Ability to describe the application of the PDCA cycle on an internal audit program3. Ability to explain the roles and responsibilities of the internal audit function4. Ability to describe the main internal audit services and activities5. Ability to ensure the access and independence of the internal audit function6. Ability to develop short- and long-term planning of internal audit activities7. Ability to determine the need for resources for the internal audit program8. Ability to manage internal audit program records9. Ability to decide when an internal audit program needs to be improved or modified	<ol style="list-style-type: none">1. Knowledge of the ISO 19011 definition and recommendations on the internal audit program2. Knowledge of the correlation between the PDCA cycle and the internal audit program3. Knowledge of the roles and responsibilities of individuals managing an internal audit program, as described in ISO 190114. Knowledge of the main internal audit services and activities5. Knowledge of the principles and main considerations for the independence of the internal audit function6. Knowledge of the ISO 19011 recommendations with regard to determining audit program resources7. Knowledge of the typical records generated from the internal audit program8. Knowledge of the factors that can indicate the need to modify the internal audit program

Based on the above-mentioned domains and their relevance, 12 questions are included in the exam, as summarized below:

				Level of understanding (cognitive/taxonomy) required		% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
				Questions that measure synthesis and evaluation	Number of questions per competency domain			
Points per question	Questions that measure comprehension, application, and analysis			Questions that measure synthesis and evaluation	Number of questions per competency domain	% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Fundamental principles and concepts of the business continuity management system (BCMS)	5	X		1	8.33	5	6.67
	Business continuity management system (BCMS)	10		X	1	8.33	10	13.34
	Fundamental audit concepts and principles	5	X		3	24.99	15	20.01
		5		X				
		5		X				
	Preparing the ISO 22301 audit	5	X		1	8.33	5	6.67
	Conducting the ISO 22301 audit	5		X	4	33.32	25	33.35
		5	X					
		5	X					
		10	X					
Closing the ISO 22301 audit	10		X	1	8.33	10	13.34	
Managing the ISO 22301 internal audit program	5		X	1	8.33	5	6.67	
Total points	75							
Number of questions per level of understanding			6	6				
% of the exam devoted to each level of understanding (cognitive/taxonomy)			50.00	50.00				

The passing score is 70%.

After successfully passing the exam, candidates will be able to apply for the “PECB Certified ISO 22301 Lead Auditor” credential, depending on their level of experience.

TAKE THE EXAM

Candidates will be required to arrive at least 30 minutes before the exam starts. Candidates arriving late will not be given additional time to compensate for the late arrival and may even be denied entry to the exam.

All candidates are required to present a valid identity card such as a national ID card, driver's license, or passport to the invigilator.

The duration of the exam is three hours. Non-native speakers will receive an additional 30 minutes.

The exam contains essay type questions: This type of format was selected as a means of determining whether a candidate can clearly answer training course-related questions, by assessing problem-solving techniques and formulating arguments that are supported with reasoning and evidence. The exam is set to be "open book" and does not measure the recall of data or information. The exam evaluates candidates' comprehension, application, and analytical skills. Therefore, candidates will have to justify their answers by providing concrete explanations to demonstrate that they have been capable of understanding the training course concepts. At the end of this document, you will find samples of exam questions and possible answers.

Since the exam is "open book," candidates are authorized to use:

- A copy of the ISO 22301 standard
- Course notes from the Participant Handout
- Any personal notes made by the candidate during the training course
- A hard copy dictionary

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

All attempts to copy, collude, or otherwise cheat during the exam will automatically lead to the failure of the exam.

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 via email within a period of six to eight weeks from the exam date. The candidate will be provided with only two possible exam results: pass or fail, rather than an exact grade.

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

In case of exam failure, the results will be accompanied with the list of domains in which the candidate failed to fully answer the question(s). This can help the candidate better prepare for a retake exam.

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

Exam Retake Policy

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of the allowed time frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, the candidate must wait 15 days (from the initial date of the exam) for the next attempt (first retake). The retake fee applies.

Note: Candidates who have completed the full training course but failed the written exam are eligible to retake the exam once for free within a 12-month period from the initial date of the exam.

- If a candidate does not pass the exam on the second attempt, the candidate must wait three months (from the initial date of the exam) for the next attempt (second retake). The retake fee applies.
- If a candidate does not pass the exam on the third attempt, the candidate must wait six months (from the initial date of the exam) for the next attempt (third retake). The retake fee applies.
- After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for the candidate to retake the same exam. The regular fee applies.

For the candidates that fail the exam in the second retake, PECB recommends to attend an official training course in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, costs), the candidate needs to contact the PECB partner who has initially organized the training course session.

Closing A Case

If a candidate does not apply for the certificate within three years, their case will be closed. Even though the certification period expires, the candidate has the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, candidate handbook, or exam preparation guide that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing and pay the required fees.

Exam Security

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certificate holders and applicants to maintain the security and confidentiality of PECB exams. If candidates or someone who hold PECB credentials reveal information about PECB exam 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

Question 1:

List at least five pieces of evidence that an organization can provide in order to demonstrate conformity with clause 8.2 *Business impact analysis and risk assessment* of ISO 22301.

Possible answer:

To prove conformity to the requirements of clause 8.2 of ISO 22301, an organization must provide the following evidence:

- *The identified impact types and criteria relevant to the specific context of the organization*
- *The identified activities that are critical to the provision of products and services*
- *Documented evaluation process for determining continuity and recovery priorities, objectives, and targets*
- *Business impact analysis (BIA) report*
- *Risk assessment results*

Question 2:

Provide at least two pieces of evidence that would be sufficient to verify an organization's conformity to the following clauses of ISO 22301.

Possible answer:

Clause 6.1.2 Addressing risks and opportunities

- *Planned actions on how to address the identified risks and opportunities*
- *Evaluation reports of the actions taken*

Address:

Head Quarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.

T: +1-844-426-7322
F: +1-844-329-7322

PECB Help Center

Visit our [Help Center](#) to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system. Visit Help Center here: www.pecb.com/help

Emails:

Examination: examination@pecb.com
Certification: certification@pecb.com
Customer Care: customer@pecb.com

Copyright © 2019 PECB. Reproduction or storage in any form for any purpose is not permitted without a PECB prior written permission.

www.pecb.com