PECB

BEYOND RECOGNITION

ISO/IEC 27001
LEAD AUDITOR

Candidate Handbook

PECB

Table of Contents

PECB

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education[1], certification, and certificate programs for individuals on a wide range of disciplines.

Through our presence in more than 150 countries, we help professionals demonstrate their competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

Our key objectives are:

1. Establishing the minimum requirements necessary to certify professionals and to grant designations
2. Reviewing and verifying the qualifications of individuals to ensure they are eligible for certification
3. Maintaining and continually improving the evaluation process for certifying individuals
4. Certifying qualified individuals, granting designations and maintaining respective directories
5. Establishing requirements for the periodic renewal of certifications and ensuring that the certified individuals are complying with those requirements
6. Ascertaining that PECB professionals meet ethical standards in their professional practice
7. Representing our stakeholders in matters of common interest
8. Promoting the benefits of certification and certificate programs to professionals, businesses, governments, and the public

Our mission

Provide our clients with comprehensive examination, certification, and certificate program services that inspire trust and benefit the society as a whole.

Our vision

Become the global benchmark for the provision of professional certification services and certificate programs.

Our values

Integrity, Professionalism, Fairness

[1] Education refers to training courses developed by PECB and offered globally through our partners.

The Value of PECB Certification

Global recognition
PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is an associate member of The Independent Association of Accredited Registrars (IAAR), a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO certification. For more detailed information, click here.

High-quality products and services
We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

Compliance with standards
Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

Customer-oriented service
We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

Flexibility and convenience
Online learning opportunities make your professional journey more convenient as you can schedule your learning sessions according to your lifestyle. Such flexibility gives you more free time, offers more career advancement opportunities, and reduces costs.

PECB Code of Ethics

The Code of Ethics represents the highest values and ethics that PECB is fully committed to follow, as it recognizes the importance of them when providing services and attracting clients.

The Compliance Division makes sure that PECB employees, trainers, examiners, invigilators, partners, distributors, members of different advisory boards and committees, certified individuals, and certificate holders (hereinafter "PECB professionals") adhere to this Code of Ethics. In addition, the Compliance Division consistently emphasizes the need to behave professionally and with full responsibility, competence, and fairness in service provision with internal and external stakeholders, such as applicants, candidates, certified individuals, certificate holders, accreditation authorities, and government authorities.

It is PECB's belief that to achieve organizational success, it has to fully understand the clients and stakeholders' needs and expectations. To do this, PECB fosters a culture based on the highest levels of integrity, professionalism, and fairness, which are also its values. These values are integral to the organization, and have characterized the global presence and growth over the years and established the reputation that PECB enjoys today.

PECB believes that strong ethical values are essential in having healthy and strong relationships. Therefore, it is PECB's primary responsibility to ensure that PECB professionals are displaying behavior that is in full compliance with PECB principles and values.

PECB professionals are responsible for:

1. Displaying professional behavior in service provision with honesty, accuracy, fairness, and independence
2. Acting at all times in their service provision solely in the best interest of their employer, clients, the public, and the profession in accordance with this Code of Ethics and other professional standards
3. Demonstrating and developing competence in their respective fields and striving to continually improve their skills and knowledge
4. Providing services only for those that they are qualified and competent and adequately informing clients and customers about the nature of proposed services, including any relevant concerns or risks
5. Informing their employer or client of any business interests or affiliations which might influence or impair their judgment
6. Preserving the confidentiality of information of any present or former employer or client during service provision
7. Complying with all the applicable laws and regulations of the jurisdictions in the country where the service provisions were conducted
8. Respecting the intellectual property and contributions of others
9. Not communicating intentionally false or falsified information that may compromise the integrity of the evaluation process of a candidate for a PECB certification or a PECB certificate program
10. Not falsely or wrongly presenting themselves as PECB representatives without a proper license or misusing PECB logo, certifications or certificates
11. Not acting in ways that could damage PECB's reputation, certifications or certificate programs
12. Cooperating in a full manner on the inquiry following a claimed infringement of this Code of Ethics

To read the complete version of PECB's Code of Ethics, go to Code of Ethics | PECB.

Introduction to ISO/IEC 27001 Lead Auditor

As both consumers and organizations are facing an increasing number of threats and attacks against their personal and financial data, information security has become more and more important for all the organizations regardless of their size and complexity. Also, both consumers and legislators are expecting additional protection of information from the organizations they deal with. The need for information security is greater than ever and is expected to constantly increase.

To answer these issues, the International Organization for Standardization (ISO) jointly with the International Electro technical Commission (IEC) has developed the ISO/IEC 27001:2013 standard for information security. ISO/IEC 27001:2013 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).

Since 2005, when the first ISO/IEC 27001 certification for an organization was granted, there is a lack of available qualified and certified ISMS professionals. Today's employers are not just seeking information security professionals, but want proof that these professionals hold a predetermined set of knowledge and skills. Companies now place a high degree of importance on hiring, contracting with, and promoting certified security practitioners prepared to tackle today's and tomorrow's security challenges.

PECB certifications are not a license or simply a membership. They attest the candidates' knowledge and skills gained through our training courses and are issued to candidates that have the required experience and have passed the exam.

This document specifies the PECB ISO/IEC 27001 Lead Auditor certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact the PECB international office at certification@pecb.com.

PECB

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

All candidates are responsible for their own study and preparation for certification exams. Although candidates are not required to attend the training course to be eligible for taking the exam, attending it can significantly increase their chances of successfully passing the exam.

To schedule the exam, candidates have two options:

1. Contact one of our authorized partners. To find an authorized partner in your region, please go to Active Partners. The training course schedule is also available online and can be accessed on Training Events.
2. Take a PECB exam remotely through the PECB Exams application. To schedule a remote exam, please go to the following link: Exam Events.

To learn more about exams, competency domains, and knowledge statements, please refer to *Section III* of this document.

Rescheduling the exam

For any changes with regard to the exam date, time, location, or other details, please contact examination@pecb.com.

Application fees for examination and certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000[2]
- Manager Exam: $700
- Foundation Exam: $500
- Transition Exam: $500

The application fee for certification is $500.

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

[2] All prices listed in this document are in US dollars.

Competency domains

The objective of the "PECB Certified ISO/IEC 27001 Lead Auditor" exam is to ensure that the candidate has the necessary competence to: perform an information security management system (ISMS) audit in compliance with the ISO/IEC 27001 standard requirements; manage an audit team by applying widely recognized audit principles, procedures, and techniques; and, lastly, plan and carry out internal and external audits as per the guidelines of ISO 19011 and in compliance with the ISO/IEC 17021-1 certification processes.

The ISO/IEC 27001 Lead Auditor exam is intended for:

- Auditors seeking to perform and lead information security management system (ISMS) audits
- Managers or consultants seeking to master the information security management system audit process
- Individuals responsible to maintain conformity with the ISMS requirements in an organization
- Technical experts seeking to prepare for an information security management system audit
- Expert advisors in information security management

The content of the exam is divided as follows:

- **Domain 1:** Fundamental principles and concepts of an information security management system (ISMS)
- **Domain 2:** Information security management system (ISMS)
- **Domain 3:** Fundamental audit concepts and principles
- **Domain 4:** Preparing an ISO/IEC 27001 audit
- **Domain 5:** Conducting an ISO/IEC 27001 audit
- **Domain 6:** Closing an ISO/IEC 27001 audit
- **Domain 7:** Managing an ISO/IEC 27001 audit program

Domain 1: Fundamental principles and concepts of an information security management system (ISMS)

Main objective: Ensure that the candidate understands and is able to interpret ISO/IEC 27001 principles and concepts.

Competencies	Knowledge statements
1. Ability to understand and explain the main concepts of the information security management system	1. Knowledge of the information security laws, regulations, international and industry standards, contracts, market practices, internal policies, etc., an organization must comply with
2. Ability to understand and explain the organization's operations and the development of information security standards	2. Knowledge of the main standards related to information security
3. Ability to identify, analyze, and evaluate the information security compliance requirements for an organization	3. Knowledge the main concepts and terminology of ISO/IEC 27001
4. Ability to explain and illustrate the main concepts in information security and information security risk management	4. Knowledge of the concept of risk and its application in information security
5. Ability to distinguish and explain the difference between information asset, data and record	5. Knowledge of the relationship between information security aspects
6. Ability to understand, interpret, and illustrate the relationship between information security aspects such as controls, vulnerabilities, threats, risks, and assets	6. Knowledge of the difference and characteristics of security objectives and controls
7. Ability to identify and illustrate big data, artificial intelligence, machine learning, cloud computing, and outsourcing operations	7. Knowledge of the difference between preventive, detective, and corrective controls
	8. Knowledge of the main characteristics of big data, artificial intelligence, machine learning, cloud computing, and outsourcing operations

Domain 2 Information security management system (ISMS)

Main objective: Ensure that the candidate understands, is able to interpret, and identify the requirements for an information security management system based on ISO/IEC 27001.

Competencies	Knowledge statements
1. Ability to understand the ISO/IEC 27001 requirements and the structure of the standard 2. Ability to understand the components of an information security management system based on ISO/IEC 27001 and its principal processes 3. Ability to understand, interpret, and analyze the requirements of ISO/IEC 27001 4. Ability to understand whether the organization has satisfied the needs of the interested parties 5. Ability to understand, explain, and illustrate the main steps to establish, implement, operate, monitor, review, maintain, and improve an organization's ISMS 6. Ability to understand the risk assessment approach and methodology 7. Ability to understand the selection of appropriate controls based upon Annex A of ISO/IEC 27001	1. Knowledge of the supporting standards of ISO/IEC 27001 2. Knowledge of the concepts, principles and terminology related to management systems 3. Knowledge of the principal characteristics of an integrated management system 4. Knowledge of the ISO/IEC 27001 requirements presented in the clauses 4 to 10 5. Knowledge of the main steps to establish the ISMS and security policies, security objectives, processes and procedures relevant to managing risks, and improving information security to deliver results in accordance with an organization's overall policies and objectives 6. Knowledge of risk assessment approach and methodology 7. Knowledge of the concept of continual improvement and its application to an ISMS 8. Knowledge of security objectives and controls 9. Knowledge of the Statement of Applicability document

Domain 3: Fundamental audit concepts and principles

Main objective: Ensure that the candidate understands, is able to interpret, and apply the main concepts and principles related to an ISMS audit.

Competencies	Knowledge statements
1. Ability to understand, explain, and illustrate the application of the audit principles in an ISMS audit 2. Ability to differentiate first, second, and third party audits 3. Ability to identify and judge situations that would discredit the professionalism of the auditor and violate the PECB Code of Ethics 4. Ability to identify and judge ethical issues considering the obligations related to the audit client, auditee, law enforcement, and regulatory authorities 5. Ability to understand the legal implications related to any irregularities committed by the auditee 6. Ability to understand the impact of trends and technology in auditing 7. Ability to explain, illustrate, and apply the audit evidence approach in the context of an ISMS audit 8. Ability to explain and compare evidence types and their characteristics 9. Ability to determine and justify the type and amount of evidence required in an ISMS audit	1. Knowledge of the main audit concepts and principles as described in ISO 19011 2. Knowledge of the differences between first, second, and third party audits 3. Knowledge of the principles of auditing: integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach 4. Knowledge of an auditor's professional responsibility and the PECB Code of Ethics 5. Knowledge of evidence based approach in an audit 6. Knowledge of the different types of audit evidence: physical, mathematical, confirmative, technical, analytical, documentary, and verbal 7. Knowledge of the laws and regulations applicable to the auditee and the country it operates in, etc. 8. Knowledge of the use of big data in audits 9. Knowledge of the auditing of outsourced operations

Domain 4: Preparing an ISO/IEC 27001 audit

Main objective: Ensure that the candidate is able to prepare an information security management system audit.

Competencies	Knowledge statements
1. Ability to determine and evaluate the level of materiality and apply the risk-based approach during the different stages of an ISMS audit	1. 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
2. Ability to judge the appropriate level of reasonable assurance needed for an ISMS audit	2. Knowledge of the concept of materiality and its application to an audit
3. Ability to understand and illustrate the steps and activities to prepare an ISMS audit considering the specific context of the audit	3. Knowledge of the concept of reasonable assurance and its application to an audit
4. Ability to understand and explain the roles and responsibilities of the audit team leader, audit team members, and technical experts	4. Knowledge of the main responsibilities of the audit team leader and audit team members
5. Ability to determine and evaluate the level of materiality during the different stages of an ISMS audit	5. Knowledge of the roles and responsibilities of technical experts
6. Ability to determine the audit feasibility	6. Knowledge of the audit objectives, audit scope, and audit criteria
7. Ability to determine, evaluate, and confirm the audit objectives, the audit criteria, and the audit scope for an ISMS audit	7. Knowledge of the difference between an ISMS scope and the audit scope
8. 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 auditee	8. Knowledge of the factors to take into account during the audit feasibility
	9. Knowledge of the cultural aspects to consider in an audit
	10. Knowledge of the characteristics of terms of the audit engagement and the best practices to establish the initial contact with an auditee

Domain 5: Conducting an ISO/IEC 27001 audit

Main objective: Ensure that the candidate can efficiently conduct an ISMS audit.

Competencies	Knowledge statements
1. Ability to conduct the stage 1 audit, taking into account the documented information evaluation criteria	1. Knowledge of the objectives and the content of the opening meeting in an audit
2. Ability to organize and conduct an opening meeting	2. Knowledge of the difference between stage 1 audit and stage 2 audit
3. Ability to conduct the stage 2 audit by appropriately following the procedures that this stage entails	3. Knowledge of stage 1 audit requirements, steps, and activities
4. Ability to apply the best practices of communication to collect the appropriate audit evidence	4. Knowledge of the documented information evaluation criteria and ISO/IEC 27001 requirements
5. Ability to consider the roles and responsibilities of all the interested parties involved	5. Knowledge of stage 2 audit requirements, steps, and activities
6. Ability to explain, illustrate, and apply evidence collection procedures and tools	6. Knowledge of the best communication practices during an audit
7. Ability to explain, illustrate, and apply the main audit sampling methods	7. Knowledge of the roles and responsibilities of guides and observers during an audit
8. Ability to gather appropriate evidence from the available information during an audit and evaluate it objectively	8. Knowledge of the different conflict resolution techniques
9. Ability to explain, illustrate, and apply the audit evidence approach in an ISMS audit	9. Knowledge of the evidence collection procedures and tools such as interview, documented information review, observation, analysis, sampling and technical verification
10. Ability to develop audit working papers and elaborate appropriate audit test plans in an ISMS audit	10. Knowledge of the evidence analysis techniques: corroboration and evaluation
11. Ability to explain and apply the evidence evaluation process: drafting audit findings	11. Knowledge of the main concepts, principles, and evidence collection procedures used in an audit
12. Ability to understand, explain, and illustrate the concept of the benefit of the doubt	12. Knowledge of the advantages and disadvantages of using audit checklists
13. Ability to report appropriate audit observations in accordance with audit rules and principles	13. Knowledge of the main audit sampling methods and their characteristics
14. Ability to conduct quality reviews to audit documentation	14. Knowledge of the audit plan preparation procedure
15. Ability to complete audit working documents	15. Knowledge of the preparation and development of audit working papers
	16. Knowledge of the best practices for the creation of audit test plans
	17. Knowledge of the evidence evaluation process: to draft audit findings

	18. Knowledge of the characteristics and differences between the concepts of conformity, minor nonconformity, major nonconformity, anomaly, and observation 19. Knowledge of the guidelines and best practices to draft nonconformity reports 20. Knowledge of the guidelines and best practices to draft and report audit observations 21. Knowledge of the benefit of the doubt principle and its application in the management system audits 22. Knowledge of the guidelines and best practices to complete audit working documents and perform a quality review

Domain 6: Closing an ISO/IEC 27001 audit

Main objective: Ensure that the candidate is able to conclude an ISMS audit.

Competencies	Knowledge statements
1. Ability to explain and apply the evidence evaluation process: preparing audit conclusions	1. Knowledge of the evidence evaluation process: to prepare audit conclusions
2. Ability to justify the recommendation for certification	2. Knowledge of the guidelines and best practices to present audit conclusions to the management of an audited organization
3. Ability to draft and present audit conclusions	3. Knowledge of the possible recommendations that an auditor can issue during the certification audit
4. Ability to organize and conduct a closing meeting	4. Knowledge of the closing meeting agenda
5. Ability to write and distribute an ISO/IEC 27001 audit report	5. Knowledge of the guidelines and best practices to evaluate action plans
6. Ability to evaluate action plans	

Domain 7: Managing an ISO/IEC 27001 audit program

Main objective: Ensure that the candidate understands how to establish and manage an ISMS audit program and conduct audit follow-up activities.

Competencies	Knowledge statements
1. Ability to conduct the activities following an initial audit, including audit follow-ups and surveillance activities 2. Ability to understand and explain the establishment of an audit program and the application of the PDCA cycle into an audit program 3. Ability to understand and explain the importance of protecting the integrity, availability, and confidentiality of audit records and the auditors' responsibilities in this regard 4. Ability to understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records 5. Ability to understand the requirements related to the components of the management system of an audit program as quality management, record management, complaint management 6. Ability to understand and explain the way that the combined audits are handled in an audit program 7. Ability to understand the documented information management process 8. Ability to understand the process of evaluating the efficiency of the audit program by monitoring the performance of each auditor and audit team member 9. Ability to demonstrate the application of the personal attributes and behaviors associated with professional auditors	1. Knowledge of audit follow-ups, surveillance audits, and recertification audit requirements, steps, and activities 2. Knowledge of the conditions for the modification, extension, suspension, or withdrawal of an organization's certification 3. Knowledge of the application of the PDCA cycle in the management of an audit program 4. Knowledge of the requirements, guidelines, and best practices regarding audit resources, procedures, and policies 5. Knowledge of the types of tools used by professional auditors 6. Knowledge of the requirements, guidelines, and best practices regarding the management of audit records 7. Knowledge of the application of the continual improvement concept to the management of an audit program 8. Knowledge of the particularities to implement and manage a first, second or third party audit program Knowledge of the competency concept and its application to auditors 9. Knowledge of the management of combined audits 10. Knowledge of the personal attributes and behaviors of a professional auditor

Based on the abovementioned domains and their relevance, 12 questions are included in the exam, as summarized in the table below:

			Level of understanding (Cognitive/Taxonomy) required					
		Points per question	Questions that measure comprehension, application, and analysis	Questions that measure 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 an information security management system (ISMS)	5	X		2	16.67	15	20
		10	X					
	Information security management system (ISMS)	5	X		2	16.67	10	13.33
		5	X					
	Fundamental audit concepts and principles	5	X		1	8.33	5	6.67
	Preparing an ISO/IEC 27001 audit	5	X		1	8.33	5	6.67
	Conducting an ISO/IEC 27001 audit	5	X		1	8.33	5	6.67
	Closing an ISO/IEC 27001 audit	10		X	3	25	25	33.33
		5		X				
		10		X				
	Managing an ISO/IEC 27001 audit program	5		X	2	16.67	10	13.34
		5		X				
	Total points	75						
	Number of questions per level of understanding		7	5				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		58.33	41.67				

The passing score of the exam is **70%**.

After successfully passing the exam, candidates will be able to apply for obtaining the "PECB Certified ISO/IEC 27001 Lead Auditor" credential.

Taking the exam

General information about the exam
Candidates are required to arrive/be present at least 30 minutes before the exam starts.

Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (a national ID card, driver's license, or passport) and show it to the invigilator.

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:
- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB exam format and type
1. **Paper-based:** Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course.
2. **Online:** Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more information about online exams, go to the PECB Online Exam Guide.

PECB exams are available in two types:
1. Essay-type question exam
2. Multiple-choice question exam

This exam comprises essay-type questions. Essay-type questions are used to determine and evaluate whether a candidate can clearly answer questions related to the defined competency domains. Additionally, problem-solving techniques and arguments that are supported with reasoning and evidence will also be evaluated. The exam aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates are required to provide logical and convincing answers and explanations in order to demonstrate that they have understood the content and the main concepts of the competency domains.

This is an open-book exam. The candidate is allowed to use the following reference materials:
- A hard copy of the ISO/IEC 27001 standard
- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate).

For specific information about exam types, languages available, and other details, please contact examination@pecb.com or go to the List of PECB Exams.

Sample exam questions

Question 1:
Determine how you would verify each of the following control measures. You must provide examples of evidence you would look for to have a reasonable guarantee that the control measure has been effectively implemented. State at least two elements of proof for each.

- Policies for information security (A.5.1.1):

Possible answer:

- *Documentation review of the information security policy to validate the content*
- *Interview with the person in charge of information security to validate the approval and distribution process of the policy*
- *Verification of the policy distribution media (Website, hard copy version, information in the employee manual, etc.)*

Question 2:
You have received a plan for corrective actions. Evaluate the adequacy of the proposed corrective actions. If you agree with the corrective actions, explain why. If you disagree, explain why and propose what you think would be adequate corrective actions.

- A non-conformity was observed because the Human Resources team was not aware of the procedure that requires them to validate all future employee references before hiring them
- Corrective action: Inform (Timeframe: immediately) and train (Timeframe: within 6 months) the Human Resources team with this procedure and require that each member of the team follow it

Possible answer:
I agree. This solves the problem that was ignorance of the procedure. As auditor, a sampling will be performed during the surveillance audit to find out if the procedure is followed.

Question 3:
Determine threats and vulnerabilities associated to the following situations and indicate the possible impacts. Also indicate if the risks would affect confidentiality, data integrity and/or availability.
For each risk identified, provide the appropriate controls (by providing the clause number of the control) which allows to reduce, transfer or avoid risks.

Possible answer:

Statements	Vulnerabilities	Threats	C	I	A	Potential Impacts	Controls
The webmaster who designed the corporate Website takes care of the updates and the uploading of the site	*Absence of segregation of duties.* *Only one person is available for this function*	*Treatment errors* *Malicious act* *Webmaster leaves the company or becomes sick*		*X*	*X*	*Website containing erroneous information: loss of credibility* *Unavailable website: loss in revenues*	*A.12.1.1* *A.6.1.2* *A.9.2.3* *A.14.1.2* *A.12.4.3* *A.14.2.2*

Question 4:
For each of the following 5 controls, indicate if it used as a preventive, corrective, and/or detective control; and indicate, if the control is an administrative, technical, managerial or legal measure. Explain your answer.

- Encryption of electronic communications

Possible answer:
Preventive control: prevents unauthorized people reading messages
Technical (could be legal) measure: encryption is a technical solution to ensure information confidentiality (could be a law requirement)

Question 5:
Write a test plan to validate the following control identifying the different applicable audit procedures (observation, documentation review, interview, technical verification and analysis):

- Protection of journalized information (A.12.4.2). Logging facilities and log information shall be protected against tampering and unauthorized access

Possible answer:

Protection of logged information (A.12.4.2): Logging facilities and log information shall be protected against tampering and unauthorized access.	
Observation	*Observation of protection measures implemented against sabotage and unauthorized accesses*
Document	*Documentation of controls in place to protect information logged against sabotage and unauthorized accesses, information logging policy and related procedures, intrusion test reports*
Interview	*Interview with the information security manager and validate the logging policy objectives, interview with the network administrator to validate the operation of the controls in place to protect the logged information against sabotage and unauthorized accesses*
Technical verification	*Observation of logging equipment configurations to verify their compliance to the organization's policies and procedures*
Analysis	*Analysis of a sample of logged information*

Exam Security Policy

PECB is committed to protect the integrity of its exams and the overall examination process, and relies upon the ethical behavior of applicants, potential applicants, candidates and partners to maintain the confidentiality of PECB exams. This Policy aims to address unacceptable behavior and ensure fair treatment of all candidates.

Any disclosure of information about the content of PECB exams is a direct violation of this Policy and PECB's Code of Ethics. Consequently, candidates taking a PECB exam are required to sign an Exam Confidentiality and Non-Disclosure Agreement and must comply with the following:

1. The questions and answers of the exam materials are the exclusive and confidential property of PECB. Once candidates complete the submission of the exam to PECB, they will no longer have any access to the original exam or a copy of it.
2. Candidates are prohibited from revealing any information regarding the questions and answers of the exam or discuss such details with any other candidate or person.
3. Candidates are not allowed to take with themselves any materials related to the exam, out of the exam room.
4. Candidates are not allowed to copy or attempt to make copies (whether written, photocopied, or otherwise) of any exam materials, including, without limitation, any questions, answers, or screen images.
5. Candidates must not participate nor promote fraudulent exam-taking activities, such as:
    - Looking at another candidate's exam material or answer sheet
    - Giving or receiving any assistance from the invigilator, candidate, or anyone else
    - Using unauthorized reference guides, manuals, tools, etc., including using "brain dump" sites as they are not authorized by PECB

Once a candidate becomes aware or is already aware of the irregularities or violations of the points mentioned above, they are responsible for complying with those, otherwise if such irregularities were to happen, candidates will be reported directly to PECB or if they see such irregularities, they should immediately report to PECB.

Candidates are solely responsible for understanding and complying with PECB Exam Rules and Policies, Confidentiality and Non-Disclosure Agreement and Code of Ethics. Therefore, should a breach of one or more rules be identified, candidates will not receive any refunds. In addition, PECB has the right to deny the right to enter a PECB exam or to invite candidates for an exam retake if irregularities are identified during and after the grading process, depending on the severity of the case.

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction. PECB will take action against individuals that violate the rules and policies, including permanently banning them from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam results

Exam results will be communicated via email.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request a re-evaluation by writing to results@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Any complaint received after 30 days will not be processed.

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

If a candidate does not pass the exam on the 1st attempt, they must wait 15 days after the initial date of the exam for the next attempt (1st retake).

Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received (the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

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

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. Online Exam: when scheduling the exam retake, use initial coupon code to waive the fee
2. Paper-Based Exam: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this Policy. The process to schedule the exam retake is the same as for the initial exam.

PECB

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB ISO/IEC 27001 credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB ISO/IEC 27001 scheme have the following requirements:

Credential	Education	Exam	Professional experience	MS audit/assessment experience	Other requirements
PECB Certified ISO/IEC 27001 Provisional Auditor	At least secondary education	PECB Certified ISO/IEC 27001 Lead Auditor exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Auditor			Two years: One year of work experience in information security management	Audit activities: a total of 200 hours	
PECB Certified ISO/IEC 27001 Lead Auditor			Five years: Two years of work experience in information security management	Audit activities: a total of 300 hours	
PECB Certified ISO/IEC 27001 Senior Lead Auditor			Ten years: Seven years of work experience in information security management	Audit activities: a total of 1,000 hours	

To be considered valid, the audit activities should follow best audit practices and include the following:

1. Planning an audit
2. Managing an audit program
3. Drafting audit reports
4. Drafting nonconformity reports
5. Drafting audit working documents
6. Reviewing and managing documented information related to the audit
7. Conducting on-site audits
8. Following up on nonconformities
9. Leading an audit team

Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB account), including contact details of individuals who will be contacted to validate the candidates' professional experience. Candidates can submit their application in English, French, German, Spanish or Korean languages. They can choose to either pay online or be billed. For additional information, please contact certification@pecb.com.

The online certification application process is very simple and takes only a few minutes:

- Register your account
- Check your email for the confirmation link
- Log in to apply for certification

For more information on how to apply for certification, click here.

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge. For more information about downloading the certificate, click here, and for more information about claiming the Digital Badge, click here.

PECB provides support both in English and French.

Professional experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the résumé.

Professional references

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their information security management experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

ISMS audit experience

The candidate's audit log will be checked to ensure that they have completed the required number of audit hours. The following audit types constitute valid audit experience: pre-audit, internal audits, second party audits, or third party audits.

Evaluation of certification applications

The Certification Department will evaluate each application to validate the candidates' eligibility for certification or certificate program. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates' credential downgrade.

PECB

SECTION IV: CERTIFICATION POLICIES

Denial of certification

PECB can deny certification/certificate program if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics

Candidates whose certification/certificate program has been denied can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

The application payment for the certification/certificate program is nonrefundable.

Certification status options

Active

Means that your certification is in good standing and valid, and it is being maintained by fulfilling the PECB requirements regarding the CPD and AMF.

Suspended

PECB can temporarily suspend candidates' certification if they fail to meet the requirements. Other reasons for suspending certification include:

- PECB receives excessive or serious complaints by interested parties (suspension will be applied until the investigation has been completed.)
- The logos of PECB or accreditation bodies are willfully misused.
- The candidate fails to correct the misuse of a certification mark within the determined time by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revoked

PECB can revoke (that is, to withdraw) the certification if the candidate fails to satisfy its requirements. In such cases, candidates are no longer allowed to represent themselves as PECB Certified Professionals. Additional reasons for revoking certification can be if the candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of certification
- Break any other PECB rules
- Any other reasons that PECB deems appropriate

Candidates whose certification has been revoked can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

Other statuses
Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. To learn more about these statuses and the permanent cessation status, go to Certification Status Options.

Upgrade and downgrade of credentials

Upgrade of credentials
Professionals can upgrade their credentials as soon as they can demonstrate that they fulfill the requirements.

To apply for an upgrade, candidates need to log into their PECB account, visit the "My Certifications" tab, and click on "Upgrade." The upgrade application fee is $100.

Downgrade of credentials
A PECB Certification can be downgraded to a lower credential due to the following reasons:

- The AMF has not been paid.
- The CPD hours have not been submitted.
- Insufficient CPD hours have been submitted.
- Evidence on CPD hours has not been submitted upon request.

Note: *PECB certified professionals who hold Lead certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. The holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

Renewing the certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual professional development (CPD) hours. In addition, they need to pay the annual maintenance fee ($100). For more information, go to the Certification Maintenance page on the PECB website.

Closing a case

If candidates do not apply for certification within one year, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing to certification@pecb.com and pay the required fee.

Complaint and Appeal Policy

Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If candidates do not find the response satisfactory, they have the right to file an appeal.

For more information about the Complaint and Appeal Policy, click here.

PECB

SECTION V: GENERAL POLICIES

Exams and certifications from other accredited certification bodies

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27001 Lead Auditor certification).

Non-discrimination and special accommodations

All candidate applications will be evaluated objectively, regardless of the candidates' age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations[3] for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the partner/distributor in order for them to make proper arrangements[4]. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click here.

Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click here.

Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click here.

[3] According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

[4] ADA Amendments Act of 2008 (P.L. 110–325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.

Address:

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

Tel./Fax:

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

Emails:

Examination:
examination@pecb.com

Certification:
certification@pecb.com

Customer Service:
customer@pecb.com

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.

www.pecb.com