ISO/IEC 27001 Certification Scheme

PECB

Table of Contents

1 Purpose and summary

This document specifies the ISO/IEC 27001 certification schemes of PECB in compliance with the ISO/IEC 17024:2012 standard (Conformity assessment — General Requirements for bodies operating certification of persons).

The following ISO/IEC 27001 Certifications are covered:

- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27001 Lead Implementer
- ISO/IEC 27001 Master

The PECB Certification Schemes are reviewed and validated by the General Scheme Advisory Board, which acts as the governing board for certification.

1.1 ISO/IEC 27001 Lead Auditor Certification

The “ISO/IEC 27001 Lead Auditor” credential is a professional certification for individuals aiming to demonstrate the competence to audit an information security management system and lead an audit team.

ISO/IEC 27001:2022 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The most important skills required in the market are the ability to effectively plan and perform audits in conformance with the certification process of ISO/IEC 27001, master audit techniques, and manage (or be part of) ISMS audit teams and programs.

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

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

1.2 ISO/IEC 27001 Lead Implementer Certification

The “ISO/IEC 27001 Lead Implementer” credential is a professional certification for individuals aiming to demonstrate the competence to implement an ongoing information security management system and lead an implementation team.

ISO/IEC 27001:2022 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2022 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

The most important skills required in the market are the ability to effectively plan, implement, and manage the ISMS, assess and treat the information security risks, select and implement the information security controls, and manage (or be part of) ISMS implementation teams.

The ISO/IEC 27001 Lead Implementer certification is intended for:

- Managers or consultants involved in and/or concerned with the implementation of an information security management system in an organization
- Project managers, consultants, or expert advisers seeking to master the implementation of an information security management system; or individuals responsible to maintain conformity with the ISMS requirements within an organization
- Members of the ISMS team

1.3 ISO/IEC 27001 Master Certification

The ISO/IEC 27001 Master certification is a professional certification for professionals needing to implement an information security management system (ISMS), and to master the audit techniques and to manage (or be part of) audit teams and audit program.

The Master credential is the highest credential within the PECB Certification Structure.

The principal competencies and knowledge skills needed by the market are the ability to support an organization in implementing and managing an information security management system as specified in ISO/IEC 27001:2022 as well as to manage an audit program.

Various professionals may apply for this certification:

- Senior managers or senior consultants seeking to master the implementation of an information security management system (ISMS)
- Senior auditors wishing to master the information security management system (ISMS) audit process
- Senior experts in information security management

This certification is awarded to professionals who are BOTH certified ISO/IEC 27001 Lead Auditor and certified ISO/IEC 27001 Lead Implementer (or passed the respective exams) , as well as being able to demonstrate increased professional ISMS projects and audit experience.

2 ISO/IEC 27001 Certification marks

PECB has registered the following trademarks:

- PECB Certification Marks

Applicants who get certified by PECB are entitled to use the appropriate designation. PECB uses and authorizes as equivalent the following designations:

- PECB Certified ISO/IEC 27001 Lead Auditor
- PECB Certified ISO/IEC 27001 Lead Implementer
- PECB Certified ISO/IEC 27001 Master

They can download their certificate, as well as claim their digital badge from their dashboard. For more information about downloading the certificate and claiming the Digital Badge, click here.

3 Objectives, domains and skills related to the certification scheme

Based on the main required skills for each job category and survey results, the JTA panel proposed the following credentials and the competency domains (objectives, competencies and knowledge statements).

3.1 ISO/IEC 27001 Lead Auditor Certification

Based upon the previously described job/task analysis, ISO 19011:2018, and best practices (including, but not limited to, the International Personnel Certification Association (IPC), the American Society for Quality (ASQ), and the European Organization for Quality (EOQ) in the field, related with the ISO/IEC 27001:2022 standard, 7 different domains are defined. For each of these domains the competencies and skills are listed below, which form the basis for a candidate to show compliance to the objectives for that domain.

These domains are:

1 Fundamental principles and concepts of an information security management system (ISMS)
2 Information security management system (ISMS)
3 Fundamental audit concepts and principles
4 Preparing an ISO/IEC 27001 audit
5 Conducting an ISO/IEC 27001 audit
6 Closing an ISO/IEC 27001 audit
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 is able to explain and apply ISO/IEC 27001 principles and concepts.

Competencies	Knowledge statements
1. Ability to understand and explain the main concepts of the 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 usage of control attributes and 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) and ISO/IEC 27001 requirements

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

Competencies	Knowledge statements
1. Ability to understand the structure of the ISO/IEC 27001:2022 standard	1. Knowledge of the ISO/IEC 27001:2022 standard and its supporting standards
2. Ability to understand the components of an information security management system based on ISO/IEC 27001 and its principal processes	2. Knowledge of the concepts, principles and terminology related to management systems
3. Ability to understand, interpret, and analyze the requirements of ISO/IEC 27001	3. Knowledge of the principal characteristics of an integrated management system
4. Ability to understand, explain, and illustrate the main steps to establish, implement, operate, monitor, review, maintain, and improve an organization's ISMS	4. Knowledge of the ISO/IEC 27001 requirements presented in the clauses 4 to 10
5. Ability to establish the external and internal factors related to the ISMS and determine the interested parties and their needs	5. Knowledge of the 93 controls listed in ISO/IEC 27001 Annex A
6. Ability to determine the scope of the ISMS	6. Knowledge of the ISMS internal and external factors and interested parties
7. Ability to ensure management commitment, establish an information security policy, and assign the ISMS roles and responsibilities	7. Knowledge of the main steps to establish the ISMS scope and information security policy
8. Ability to plan changes and the actions to address risks	8. Knowledge of the top management's leadership and commitment and the organizational roles and responsibilities related to the ISMS
9. Ability to understand the risk assessment and risk treatment processes	9. Knowledge of 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
10. Ability to understand the selection of appropriate controls based upon Annex A of ISO/IEC 27001 and other sources	10. Knowledge of risk assessment and treatment approaches and methodologies
11. Ability to ensure that employees are aware and competent to perform their ISMS related tasks	11. Knowledge of the selection of Annex A controls and additional controls based on other sources and their inclusion in the Statement of Applicability
12. Ability to monitor and evaluate the performance of the ISMS and conduct internal audits and management reviews	12. Knowledge of the performance evaluation process including monitoring, measurement, analysis and evaluation, internal audit, and management review
13. Ability to ensure continual improvement and implement appropriate actions to treat nonconformities	13. Knowledge of the concept of continual improvement and its application to an ISMS

Domain 3: Fundamental audit concepts and principles

Main objective: Ensure that the candidate 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	1. Knowledge of the main audit concepts and terminology as described in ISO 19011
2. Ability to differentiate first, second, and third party audits	2. Knowledge of the differences between 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	3. Knowledge of the principles of auditing such as integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach
4. Ability to identify and judge ethical issues considering the obligations related to the audit client, auditee, law enforcement, and regulatory authorities	4. Knowledge of an auditor's professional responsibility and the PECB Code of Ethics
5. Ability to understand the actions that the auditor should take regarding the legal implications related to any irregularities committed by the auditee	5. Knowledge of evidence-based approach in an audit
6. Ability to explain, illustrate, and apply the audit evidence approach in the context of an ISMS audit	6. Knowledge of the different types of audit evidence such as physical, mathematical, confirmative, technical, analytical, documentary, and verbal
7. Ability to explain and compare evidence types and their characteristics	7. Knowledge of the laws and regulations applicable to the auditee and the country it operates in
8. Ability to determine and justify the type and amount of evidence required in an ISMS audit	8. Knowledge of the use of big data in audits
9. Ability to understand the impact of trends and technology in auditing	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 understand and illustrate the steps and activities to prepare an ISMS audit considering the specific context of the audit 2. Ability to determine and evaluate the level of materiality and apply the risk-based approach during the different stages of an ISMS audit 3. Ability to judge the appropriate level of reasonable assurance needed for an ISMS audit 4. Ability to understand and explain the roles and responsibilities of the audit team leader, audit team members, and technical experts 5. Ability to determine the audit feasibility 6. Ability to determine, evaluate, and confirm the audit objectives, the audit criteria, and the audit scope for an ISMS audit 7. 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	1. Knowledge of the audit plan preparation procedure 2. 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 3. Knowledge of the concept of materiality and its application to an audit 4. Knowledge of the concept of reasonable assurance and its application to an audit 5. Knowledge of the main responsibilities of the audit team leader, audit team members, and technical experts 6. Knowledge of the audit objectives, audit scope, and audit criteria 7. Knowledge of the difference between an ISMS scope and the audit scope 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 is able to 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 develop audit working papers and elaborate appropriate audit test plans 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 explain and apply the evidence evaluation process of drafting audit findings	10. Knowledge of the evidence analysis techniques of corroboration and evaluation
11. Ability to understand, explain, and illustrate the concept of the benefit of the doubt	11. Knowledge of the main concepts, principles, and evidence collection procedures used in an audit
12. Ability to report appropriate audit observations in accordance with audit rules and principles	12. Knowledge of the advantages and disadvantages of using audit checklists
13. Ability to conduct quality reviews to audit documentation	13. Knowledge of the main audit sampling methods and their characteristics
14. Ability to complete audit working documents	14. Knowledge of the audit plan preparation procedure
	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

Domain 6: Closing an ISO/IEC 27001 audit

Main objective: Ensure that the candidate is able to conclude an ISMS audit and conduct audit follow-up activities.

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

Domain 7: Managing an ISO/IEC 27001 audit program

Main objective: Ensure that the candidate is able to establish and manage an ISMS audit program.

Competencies	Knowledge statements
1. Ability to conduct the activities following an initial audit, including audit follow-ups and surveillance activities	1. Knowledge of audit follow-ups, surveillance audits, and recertification audit requirements, steps, and activities
2. Ability to understand and explain the establishment of an audit program and the application of the PDCA cycle into an audit program	2. Knowledge of the conditions for the modification, extension, suspension, or withdrawal of an organization's certification
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	3. Knowledge of the application of the PDCA cycle in the management of an audit program
4. Ability to understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records	4. Knowledge of the requirements, guidelines, and best practices regarding audit resources, procedures, and policies
5. 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	5. Knowledge of the types of tools used by professional auditors
6. 6. Ability to understand and explain the way that the combined audits are handled in an audit program	6. Knowledge of the requirements, guidelines, and best practices regarding the management of audit records
7. Ability to understand the documented information management process	7. Knowledge of the application of the continual improvement concept to the management of an audit program
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	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. Ability to demonstrate the application of the personal attributes and behaviors associated with professional auditors	9. Knowledge of the management of combined audits
	10. Knowledge of the personal attributes and behaviors of a professional auditor

3.2 ISO/IEC 27001 Lead Implementer

Based upon the job/task analysis and related with the ISO/IEC 27001 standard and best practices in project management, 7 different domains are defined. For each of these domains the competencies and skills are listed that form the basis for a candidate to show compliance to the objectives for that domain.

These domains are:

1. Fundamental principles and concepts of an information security management system (ISMS)
2. Information security management system
3. Planning an ISMS implementation based on ISO/IEC 27001
4. Implementing the ISMS based on ISO/IEC 27001
5. Monitoring, and measurement of an ISMS based on ISO/IEC 27001
6. Continual improvement of the ISMS based on ISO/IEC 27001
7. Preparing for the ISMS certification audit

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

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

Competencies	Knowledge statements
1. Ability to understand and explain the main concepts of information security 2. Ability to explain the difference and relationship between information and asset 3. Ability to understand the difference between documents, specifications, and records 4. Ability to understand the relationship between the concepts of vulnerability, threat, risk, and their impact 5. Ability to understand the concepts of confidentiality, integrity, and availability of information 6. Ability to understand and interpret the classification of security controls and their objectives 7. Ability to understand the relationship between information security elements 8. Ability to explain the information security risk management process (assessment and treatment) – leads to 'knowledges 5 to 8)	1. Knowledge of the information security laws, regulations, international and industry standards, contracts, market practices, internal policies, best practices, etc., an organization must comply with 2. Knowledge of the main concepts and terminology of ISO/IEC 27001 3. Knowledge of information security risk and its importance in an ISMS 4. Knowledge of confidentiality, integrity, and availability of information 5. Knowledge of information security vulnerabilities, threats, and risks 6. Knowledge of the potential impacts that can affect confidentiality, integrity, or availability of information 7. Knowledge of the difference between security control types such as technical, legal, administrative, and managerial controls 8. Knowledge of the difference between security controls classified by their function such as preventive, corrective, and detective controls

Domain 2: Information security management system (ISMS) and ISO/IEC 27001 requirements

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

Competencies	Knowledge statements
1. Ability to select, design, and describe information security controls 2. Ability to define the organization's security architecture 3. Ability to identify and illustrate the activities involved in developing and deploying information systems 4. Ability to document the implementation of selected information security controls 5. Ability to understand, interpret, and analyze Annex A controls of ISO/IEC 27001 6. Ability to implement Annex A controls based on ISO/IEC 27001 and best practices	1. Knowledge of common security services such as access control services, boundary control services, integrity services, cryptographic services, and audit and monitoring services 2. Knowledge of the most common architecture frameworks 3. Knowledge of the 93 Annex A controls of ISO/IEC 27001 and their guidance specified in ISO/IEC 27002 4. Knowledge of the four groups of Annex A controls such as organizational controls, people controls, physical controls, technological controls 5. Knowledge of the selection and implementation of ISO/IEC 27001 Annex A controls 6. Knowledge of the documentation of the selected information security

Domain 3: Planning the ISMS implementation

Main objective: Ensure that the candidate is able to plan the implementation of the ISMS based on ISO/IEC 27001.

Competencies	Knowledge statements
1. Ability to collect, analyze, and interpret the information required to plan an ISMS implementation	1. Knowledge of the main project management concepts, terminology, process and best practices
2. Ability to understand and set information security and ISMS objectives	2. Knowledge of the principal approaches and methodology frameworks to implement an ISMS
3. Ability to identify and interpret ISMS risks and their impacts	3. Knowledge of typical information security and ISMS objectives and how to achieve specific results
4. Ability to analyze and consider the internal and external context of an organization	4. Knowledge of what typically constitutes an organization's internal and external context
5. Ability to identify the resources required for the ISMS implementation	5. Knowledge of the approaches used to understand the context of an organization
6. Ability to manage, estimate, and monitor the required resources for the ISMS implementation	6. Knowledge of the techniques used to gather information on an organization and to perform a gap analysis of a management system
7. Ability to identify the roles and responsibilities of key interested parties during and after the implementation and operation of an ISMS	7. Knowledge of an ISMS project plan and an ISMS project team
8. Ability to draft, file, and review an ISMS project plan	8. Knowledge of the resources required for an ISMS implementation
9. Ability to perform a gap analysis and clarify the information security management objectives	9. Knowledge of the main organizational structures applicable for an organization to manage an ISMS
10. Ability to define and justify an ISMS scope adapted to the organization's specific information security objectives	10. Knowledge of the characteristics of an ISMS scope in terms of organizational, technological, and physical boundaries
11. Ability to develop and establish an ISMS policy	11. Knowledge of the best practices and techniques used to draft and establish information security policies and procedures
12. Ability to perform the steps of the risk assessment process such as risk identification, risk analysis, and risk evaluation	12. Knowledge of the different approaches and methodologies used to perform the risk assessment process
13. Ability to perform risk treatment, risk communication and consultation, recording and reporting, and monitoring and review	13. Knowledge of the selection and implementation of risk treatment options
14. Ability to understand and draft the Statement of Applicability document	14. Knowledge of the characteristics of the Statement of Applicability document

Domain 4: Implementing an ISMS based on ISO/IEC 27001

Main objective: Ensure that the candidate is able to implement the processes of an ISMS required for an ISO/IEC 27001 certification.

Competencies	Knowledge statements
1. Ability to manage capacity building processes for the successful implementation of an ISMS	1. Knowledge of the best practices on documented information life cycle management
2. Ability to define the documentation and record management processes needed to support the implementation and operations of an ISMS and create documents that are understandable and available to all stakeholders	2. Knowledge of the characteristics and the differences between the different documented information related to an ISMS policy, procedure, guideline, standard, baseline, worksheet, etc.
3. Ability to develop a documented information management process to properly manage the document lifecycle	3. Knowledge of the documents that ensure compliance with ISO/IEC 27001 requirements
4. Ability to identify the documented information required to demonstrate conformity of the ISMS to the ISO/IEC 27001 requirements	4. Knowledge of the three V's of big data: volume, variety, and velocity
5. Ability to define, design and implement processes necessary for the operation of an ISMS and properly document them	5. Knowledge of weak and strong artificial intelligence, machine learning
6. Ability to understand, manage, and evaluate organizational knowledge	6. Knowledge of cloud computing services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS)
7. Ability to understand today's world trends and technologies such as big data, artificial intelligence, machine learning, cloud computing, and outsourced operations	7. Knowledge of the impact of new technologies in information security
8. Ability to define and implement appropriate information security training and awareness programs, and communication plans	8. Knowledge of the characteristics and the best practices of implementing information security training and awareness programs and communication plans
9. Ability to establish an ISMS communication plan to assist in the understanding of an organization's information security issues, policies, performance, and providing inputs or suggestions for improving the performance of the ISMS	9. Knowledge of the communication objectives, activities, and interested parties to enhance their support and confidence
10. Ability to establish an incident management policy and incident response team	10. Knowledge of the incident management process based on information security best practices
11. Ability to understand the difference between business continuity and disaster recovery	11. Knowledge of business continuity and disaster recovery
12. Ability to define and implement an incident management process based on information security best practices	

Domain 5: Monitoring, measurement, analysis, and evaluation of an ISMS

Main objective: Ensure that the candidate is able to evaluate, monitor, and measure the performance of an ISMS.

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of an ISMS 2. Ability to verify to what extent the identified ISMS objectives have been met 3. Ability to define and implement an ISMS internal audit program 4. Ability to perform regular and methodical reviews to ensure the suitability, adequacy, effectiveness, and efficiency of an ISMS based on the policies and objectives of the organization 5. Ability to define and perform a management review process	1. Knowledge of the best practices and techniques used to monitor and evaluate the effectiveness of an ISMS 2. Knowledge of the concepts related to measurement and evaluation 3. Knowledge of the main concepts and components related to the implementation and operation of an ISMS internal audit program 4. Knowledge of the difference between a major and a minor nonconformity 5. Knowledge of the guidelines and best practices to draft a nonconformity report 6. Knowledge of the best practices used to perform management reviews

Domain 6: Continual improvement of an ISMS

Main objective: Ensure that the candidate is able to provide guidance on the continual improvement of an ISMS.

Competencies	Knowledge statements
1. Ability to track and take action on nonconformities	1. Knowledge of the main processes, tools, and techniques used to identify the root causes of nonconformities
2. Ability to identify and analyze the root causes of nonconformities, and propose action plans to treat them	2. Knowledge of the treatment of nonconformities process
3. Ability to counsel an organization on how to continually improve the effectiveness and efficiency of an ISMS	3. Knowledge of the main processes, tools, and techniques used to develop corrective action plans
4. Ability to implement continual improvement processes in an organization	4. Knowledge of the main concepts related to continual improvement
5. Ability to determine the appropriate tools to support the continual improvement processes of an organization	5. Knowledge of the processes related to the continual monitoring of change factors
	6. Knowledge of the maintenance and improvement of an ISMS

Domain 7: Preparing for an ISMS certification audit

Main objective: Ensure that the candidate is able to prepare an organization for the certification against ISO/IEC 27001.

Competencies	Knowledge statements
1. Ability to understand the main steps, processes, and activities related to the ISO/IEC 27001 certification audit 2. Ability to understand, explain, and illustrate the audit evidence approach in an of an ISMS audit 3. Ability to counsel an organization to identify and select a certification body that meets their expectations 4. Ability to determine whether an organization is ready and prepared for the ISO/IEC 27001 certification audit 5. Ability to train and prepare an organization's personnel for an ISO/IEC 27001 certification audit 6. Ability to argue and challenge the audit findings and conclusions with external auditors	1. Knowledge of the evidence-based approach to an audit 2. Knowledge of the types of audit and their differences 3. Knowledge of the differences between Stage 1 and Stage 2 audits 4. Knowledge of the Stage 1 audit requirements, steps, and activities 5. Knowledge of the documented information review criteria 6. Knowledge of the Stage 2 audit requirements, steps, and activities 7. Knowledge of the audit follow-up requirements, steps, and activities 8. Knowledge of the surveillance audits and recertification audit requirements, steps, and activities 9. Knowledge of the requirements, guidelines, and best practices for developing action plans following an ISO/IEC 27001 certification audit

4 ISO/IEC 27001 Examination Development

The test specifications are presented in the table below.

4.1 ISO/IEC 27001 Lead Auditor

Based on the abovementioned domains and their relevance, 80 questions are included in the exam, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Fundamental principles and concepts of an information security management system (ISMS)	13	16.25	X	
	Information security management system (ISMS)	8	10	X	
	Fundamental audit concepts and principles	14	17.5		X
	Preparing an ISO/IEC 27001 audit	12	15	X	
	Conducting an ISO/IEC 27001 audit	18	22.5		X
	Closing an ISO/IEC 27001 audit	7	8.75	X	
	Managing an ISO/IEC 27001 audit program	8	10		X
	Total	**80**	**100%**		
	Number of questions per level of understanding			**40**	**40**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**50%**	**50%**

4.2 ISO/IEC 27001 Lead Implementer

Based on the abovementioned domains and their relevance, 80 questions are included in the exam, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Fundamental principles and concepts of an information security management system (ISMS)	15	18.75	X	
	Information security management system (ISMS)	12	15	X	
	Planning an ISMS implementation based on ISO/IEC 27001	18	22.5		X
	Implementing an ISMS based on ISO/IEC 27001	14	17.5		X
	Monitoring and measurement of an ISMS based on ISO/IEC 27001	10	12.5	X	
	Continual improvement of an ISMS based on ISO/IEC 27001	6	7.5	X	
	Preparing for an ISMS certification audit	5	6.25		X
	Total	**80**	**100%**		
	Number of questions per level of understanding			**43**	**37**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**53.75%**	**46.25%**

5 Certification schemes requirements

With the input gathered in the previous chapters, the different PECB Certification Schemes are defined in the following sections.

5.1 Requirements for certification

5.1.1 General requirements

In general, the requirements for any ISO/IEC 27001 certification are:

- Having successfully passed the appropriate PECB certification examination
- Having demonstrated sufficient and relevant professional experience
- Having indicated at least two referrals in their application form
- Having fulfilled all other requirements
- Having paid all certification application fees

The detailed requirements for each of the different grades are listed below.

5.1.2 ISO/IEC 27001 Lead Auditor Certification

Exam: PECB Certified ISO/IEC 27001 Lead Auditor Exam or equivalent
Candidates must pass a comprehensive examination consisting of development questions exam covering 7 domains of the audit of an Information Security Management System.

Professional experience:
The minimum professional experience required for Lead Auditor is:

- Five years of professional experience in total of which
- Two years of work experience in Information Security Management

MS audit/assessment experience: Audit activities: 300 hours
Other requirements: Signing the PECB Code of Ethics

Credential	Exam	Professional experience	MS audit/ assessment experience	Other requirements
PECB Certified ISO/IEC 27001 Lead Auditor	PECB Certified ISO/IEC 27001 Lead Auditor exam or equivalent	**Five years:** Two years of work experience in Information Security Management	Audit activities: a total of 300 hours	Signing the PECB Code of Ethics

5.1.3 ISO/IEC 27001 Lead Implementer Certification

Exam: PECB Certified ISO/IEC 27001 Lead Implementer Exam or equivalent
Candidates must pass a comprehensive examination consisting of development questions exam covering 7 domains of the implementation of an Information Security Management System.

Professional experience:
The minimum professional experience required for Lead Implementer is:

- Five years of professional experience in total of which
- Two years of work experience in Information Security Management

ISMS project experience: Project activities: 300 hours
Other requirements: Signing the PECB Code of Ethics

Credential	Exam	Professional experience	ISMS project experience	Other requirements
PECB Certified ISO/IEC 27001 Lead Implementer	PECB Certified ISO/IEC 27001 Lead Implementer exam or equivalent	**Five years:** Two years of work experience in Information Security Management	Project activities: a total of 300 hours	Signing the PECB Code of Ethics

5.1.4 ISO/IEC 27001 Master Certification

Exam: Having successfully passed **both** PECB Certified ISO/IEC 27001 Lead Auditor Exam and PECB Certified ISO/IEC 27001 Lead Implementer Exam.
Professional experience: 20 years of experience, 10 years in the respective field
Activities experience: 5000 hours combination of auditing and project activities
Other requirements: Signing the PECB Code of Ethics

Credential	Exam	Professional experience	Activities Experience	Other requirements
PECB Certified ISO/IEC 27001 Master	PECB ISO/IEC 27001 Lead Implementer + PECB ISO/IEC 27001 Lead Auditor	20 years of experience, 10 years in a leadership role in the respective field	5000 hours combination of auditing and project activities	Signing the PECB Code of Ethics

5.2 Examination methods and evaluation process

Passing the Exam:

PECB will organize two different exams for the grades defined previously. These are:

1. The PECB Certified ISO/IEC 27001 Lead Auditor Exam
2. The PECB Certified ISO/IEC 27001 Lead Implementer Exam

The PECB Certified ISO/IEC 27001 Lead Auditor Exam is a 3h exam. The exam questions are relevant and sufficient and cover all domains defined for the “ISO/IEC 27001 Lead Auditor” and ‘’ISO/IEC 27001 Senior Lead Auditor’’ Certification. The exam format is multiple-choice exam.

The PECB Certified ISO/IEC 27001 Lead Implementer Exam is a 3h exam. The exam questions are relevant and sufficient and cover all domains defined for the “ISO/IEC 27001 Lead Implementer” and ‘’ISO/IEC 27001 Senior Lead Implementer’’ Certification. The exam format is multiple-choice exam.

A minimum score of 70% is required to pass the PECB Certified ISO/IEC 27001 Lead Auditor Exam
A minimum score of 70% is required to pass the PECB Certified ISO/IEC 27001 Lead Implementer Exam

5.3 Certification evaluation process

Examination: Candidate needs to pass the respective exam

Professional experience: Candidates are required to add information about work experience by attaching a CV, and adding two references.

Professional experience is validated by requiring the applicant to indicate in the application form the following information for each employer:

1. Date started
2. End date (if applicable)
3. Business name
4. Business address
5. Project name
6. Reference position
7. Reference name
8. Reference email
9. Reference phone number
10. Reference job title
11. Reference hours
12. Experience details

MS audit/assessment experience: The applicant’s application and resume will be checked to ensure that the applicant has the minimal required number of audit hours.

These audits should follow best audit practices and include the following activities:

1. Planning an audit
2. Managing an audit program

3. Drafting audit reports
4. Drafting nonconformity reports
5. Drafting audit working documents
6. Documented information review
7. On-site audit
8. Following up on nonconformities
9. Leading an audit team

ISMS project experience: The applicant's application and resume will be checked to ensure that the applicant has the minimal required number of implementation hours.

These implementation activities should follow best implementation practices and include the following activities:

1. Drafting the ISMS plan
2. Initiating the ISMS implementation
3. Implementing the ISMS
4. Managing, monitoring, and maintaining the ISMS
5. Identifying and acting upon continual improvement opportunities

Other requirements: The documents provided by the candidate will be checked. Candidates will need to read and agree with the Certification Rules and Polices, Certification Maintenance Policy, and PECB Code of Ethics.

5.4 Equivalencies clause requirements

PECB does accept certifications and exams provided from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalency process to decide whether the respective certification(s) and/or exam(s) can be accepted as equivalent to the respective PECB Certificate (ex. ISO/IEC 27001 Lead Auditor Certificate).

The Certification Department verifies the provided information for certificates, as to whether an individual holds a current valid certification from an accredited and recognized body.

5.5 Requirements for recertification

5.5.1 Validity period of PECB certifications

PECB certifications are valid for three years. In order to maintain a certificate, PECB Certified Professionals are encouraged to demonstrate that they are performing certification related activities on an annual basis, by submitting Continuing Professional Development (CPD) credits. In addition, PECB Professionals are required to pay a maintenance fee, which PECB encourages to pay on an annual basis (Annual Maintenance Fee).

PECB Certified Professional will need to provide PECB with the required hours of auditing and/or implementing related tasks they have performed, including the contact details of the individuals who can validate these tasks.

The annual reporting begins with the initial certificate date; however, the maintenance fee for the first year is included in the certification application payment.

PECB continuously notifies each PECB Professional to maintain their certificate(s). The notifications are sent several times throughout the certification cycle. Disregarding if CPDs and maintenance fees are reported/paid

annually or not, all required CPDs/AMFs must be submitted/paid in full, before the end of the three-year certification cycle for the certification to be eligible for renewal.

5.5.2 Certification renewal process

To be able to renew a certificate, PECB Professionals will need to demonstrate that they have fulfilled the certification maintenance requirements within the three-year certification cycle. Certified Professionals are encouraged to complete CPD activities each year; however, the total required CPD hours must be achieved within the three-year certification cycle (see Appendix 1).

For example, a PECB Professional that holds a Lead Certificate has performed 20 hours of certification-related activities in year 1; 10 hours in year 2 and 60 hours in year 3. Although during the first and second year he/she did not perform sufficient certification-related activities, his/her tri-annual total is equal to the minimal tri-annual requirements. In this case, he/she fulfills the requirements to get recertified.

After three years of successful maintenance of a PECB Certificate, you can apply for a renewal of your certificate.

PECB certificate(s) can be renewed online through the PECB Member Dashboard by reporting CPDs and paying the AMF. PECB professionals can submit CPDs and AMF by clicking the respective icons under the CPD and AMF tabs in their MyPECB account at mypecb.com.

Note: Reduction of certification scope is not applicable. When the recertification requirements are not met, the certification will result in a 12-month suspension period, during which the candidate can address any outstanding AMFs and CPDs. If the candidate fails to fulfill these requirements within the suspension period, PECB may revoke (withdraw) the certification.

5.5.3 Reporting CPD and Paying AMF

Reporting of CPDs

PECB Certified Professionals will need to provide PECB with the required hours of auditing and/or implementation related tasks they have performed, including the contact details of the individuals who can validate these tasks.

Certified professionals can update their CPD credits at anytime by logging in to mypecb.com.

Note: On their MyPECB account, PECB professionals will see their certificates. To submit CPDs, they should click on the **CPD** icon next to the corresponding certificate and complete the submission process.

Payment of AMF

To submit the AMF, PECB professionals can log in to their dashboard at mypecb.com. They will see their certificates on the dashboard menu. Click on the **money** icon next to the relevant certificate to complete the AMF payment.

PECB continuously notifies each PECB Professional to maintain their certificate(s). The notifications are sent several times throughout the certification cycle. The first one is sent three months before your annual certificate issuance date, which based on the example above would be 2024-10-15. In this case, the payment of AMF would be due by 2025-04-15 (three months after the annual certificate issuance date).

For more information, go to the Certification Maintenance page on the PECB website.

5.5.4 Upgrade

PECB Professionals can apply for a higher credential once they provide evidence that proves that they fulfill the requirements of the higher credential.

PECB certifications can be upgraded online through the dashboard. PECB professionals can log in to their PECB account, open “View Certificate” for the certification they want to upgrade, and click the “Upgrade” button. For more information about the upgrade fee, go to the Certification Maintenance page on the PECB website.

Note: *An evaluation will be done to determine if an exam is required prior to obtain an upgraded certification.*

5.5.5 Suspension

Failure to submit the CPD and AMF payment during the certification cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs.

Additional reasons for suspension can be if:

- 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/certificate program.

Individuals whose certification has been suspended, are not authorized to further promote their certification while it is suspended.

A suspended certification can either be:

- Reinstated – if reasons for suspension are corrected within the given time frame by PECB
- Revoked – if reasons for suspension are not corrected within the given time frame by PECB

Suspended members must remediate their suspension within a maximum period of 12 months.

5.5.6 Revocation

PECB can revoke (that is, to withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Additional reasons can be if candidates:

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

Individuals whose certification has been revoked, are not authorized to use any references to a certified status.

Individuals whose certification has been revoked may file an appeal by following the complaint and appeal process (Complaint and Appeal Policy - PECB).

PECB

Appendix 1 - Certification Maintenance Requirements

Certification	Activities	3-Year/Total CPD hours
Foundation, Provisional, and Transition	**None**	**None**
Implementer	Hours of project experience, implementation or consulting-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**60 hours**
Auditor, Assessor	Hours of audit or assessment-related experience, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**60 hours**
Manager	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**60 hours**
EBIOS, MEHARI	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**60 hours**
Six Sigma Green Belt	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**60 hours**
Lead Implementer	Hours of project experience, implementation, or consulting-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**
Senior Lead Implementer	Hours of project experience, implementation, or consulting-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**180 hours**
Lead Auditor, Lead Assessor	Hours of auditing or assessment-related experience, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**
Senior Lead Auditor	Hours of auditing or assessment-related experience, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**180 hours**
Lead Manager	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**

Senior Lead Manager	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**180 hours**
Risk Manager	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**60 hours**
Senior Risk Manager	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**180 hours**
Lead Risk Manager	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**
Senior Lead Risk Manager	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**180 hours**
CLFE	Hours of project experience related to certification field, assessment-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**
CLPI	Hours of project experience, implementation, or consulting-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**
CDPO	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**
CLSIP	Hours of project experience related to the certification field, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**
Master	Hours of implementation, management, or auditing-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**270 hours**

6 Revision History

Version	Change description	Date
1.0	Initial release	2010-01-28
1.1	• Added new logo and two tables: “Approving authority and date” and “Revision History”.	2011-04-04
2.0	• Added new updated statistical facts about the growth of ISO/IEC 27001 worldwide. • Revised certification maintenance requirements and change of scope policy. • 5.1 first paragraph changed	2011-08-01
2.1	• Expanded Job/task analysis with additional data from initial research	2011-09-26
2.2	• Included survey results and examination development part removed to prevent redundancy because it is already included in PECB-403 Examination Development.	2012-01-06
2.3	• Removed foundation, auditor, provisional auditor, provisional implementer and implementer.	2012-03-23
2.4	• Changed Domain 2 information to reflect ISO 27001 by removing 27002 and updating the number of clauses, security categories and controls.	2015-01-28
2.5	• Updated the RACI in the flowchart (page 8, 9, 10, 11). • Updated domains (page 34-48). • Updated the payment of PECB maintenance fee and reporting of CPD credits (page 62). • Update hours for the Lead Auditor and Lead Implementer (page 62).	2017-04-21
2.6	• Updated process flowchart • Updated colors related to the new brand	2017-05-24
3.0	• Updated the RACI • Updated Domains • Updated Certification Requirements • Updated Certification Renewal Process • Updated payment of AMF and submission of CPDs	2017-08-15
3.1	Reviewed by Certification Processing Manager. Changes applied: • New requirements for Master credential	2018-07-01
3.2	Updates done from Certification Manager: • Updated Purpose and Summary • Updated Certification Marks • Updated Objectives, domains and skills related to the certification scheme • Updated Certification schemes requirements Update from Certification Processing Manager on: 1.1 Examination methods and evaluation process	2018-08-30
3.3	Reviewed from Certification Manager:	2019-01-25

	• Added point 7.4.5 Suspension • Added point 7.4.6 Revocation • Updated point 7.4.7 Reporting CPDs and AMF	
3.4	Reviewed by Certification Manager: • Updated the document with the new brand logo • Minor changes throughout the document • Added the certification scheme committee members	2019-09-07
3.5	Reviewed by CAS: • Updated the tables as per new survey published by ISO • Updated the scheme committee members	2020-10-30
3.6	Reviewed by CS: • Minor updates through the document	2021-02-02
3.7	Reviewed by CS: • Added reference validation, surveillance methods • Updated scheme committee members	2021-07-17
3.8	Added: Updated ISO Survey 2020 data	2021-10-10
3.9	Reviewed by CD: • Updated the ISO Survey 2021 data • Updated Process Flowchart table • Updated owner and approver • Changed « General Scheme Committee » for « General Scheme Advisory Board» and « Technical Scheme Committee » for « Technical Scheme Advisory Board » • Added latest review of the General Scheme Advisory Board members and interested parties/fields represented by the General Scheme Advisory Board members.	2022-11-29
3.10	Reviewed by CD-CD and CCO: • Updates done based on ISO/IEC 27001:2022 standard • Integrated comments from the General Scheme Advisory Board review	2022-12-21
4.0	Reviewed by CD-CD: • Added information about digital badges • Updated competency domains • Updated the criteria for revocation • Updated policy code from 08200 to 05071 • Updated technical parts in the document	2023-07-11
4.1	Reviewed by CD-CD: • Updated AMF price from $100 to $120 • Removed RACI table	2023-10-02
4.2	Reviewed by TL-CD • Updated the term PECB Surveillance Method/Surveillance Audit to CPD Verification	2023-11-14
4.3	Reviewed by CD-CD: • Updated General Scheme Advisory Board members • Updated ISO Survey data	2024-01-10
4.4	Reviewed by TL-CD • Updated the header • Removed footnote regarding the transition period for multiple-choice and essay-type exams	2024-10-17

4.5	Reviewed by AL, CD-CD: • Removed the Education Requirements • Updated the number of sections in chapter 2 • Removed the reference validation • Updated the Appendix 1 - Certification Maintenance Requirements • Removed Appendix 2 • Removed a member of the General Scheme Advisory Board • Reworded and updated sections 7.5.5, 7.5.6, and 7.5.8 • Updated the 'Related Documents' section in the table.	2025-07-01
4.6	Reviewed by CCO, CD-CD: • Updated the links in Chapter 3 • Updated the wording in section 7.5.2, 7.5.3, 7.5.5, 7.5.6, 7.5.7	2025-09-03
4.7	Reviewed by TL-CD • Updated tables based on the ISO 2024 survey	2025-12-17