ISO/IEC 27005:2022 Certification Scheme

PECB

Table of Contents

1 Purpose and summary

This document specifies the ISO/IEC 27005:2022 certification scheme 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 27005:2022 certifications are covered:

- ISO/IEC 27005:2022 Risk Manager
- ISO/IEC 27005:2022 Senior Risk Manager
- ISO/IEC 27005:2022 Lead Risk Manager
- ISO/IEC 27005:2022 Senior Lead Risk Manager

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 27005:2022 Risk Manager Certification

The “ISO/IEC 27005:2022 Risk Manager” credential is a professional certification for information security professionals that aim to demonstrate their competence to effectively manage information security risks. An internationally recognized certification adds great value to your career and will help you reach your professional objectives.

The ISO/IEC 27005:2022 Risk Manager certification is intended for:

- Managers or consultants involved in or responsible for information security in an organization
- Individuals responsible for managing information security risks
- Members of information security teams, IT professionals, and privacy officers
- Individuals responsible for maintaining conformity with the information security requirements of ISO/IEC 27001 in an organization
- Project managers, consultants, or expert advisers seeking to master the management of information security risks

1.2 ISO/IEC 27005:2022 Lead Risk Manager Certification

The “ISO/IEC 27005:2022 Lead Risk Manager” credential is a professional certification for individuals aiming to demonstrate the competence to effectively manage information security risks. An internationally recognized certification adds great value to your career and will help you reach your professional objectives.

The ISO/IEC 27005:2022 Lead Risk Manager certification is intended for:

- Managers or consultants involved in or responsible for information security in an organization
- Individuals responsible for managing information security risks, such as ISMS professionals and risk owners
- Members of information security teams, IT professionals, and privacy officers
- Individuals responsible for maintaining conformity with the information security requirements of ISO/IEC 27001 in an organization
- Project managers, consultants, or expert advisers seeking to master the management of information security risks

2 ISO/IEC 27005:2022 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:

- Certified ISO/IEC 27005:2022 Risk Manager
- Certified ISO/IEC 27005:2022 Senior Risk Manager
- Certified ISO/IEC 27005:2022 Lead Risk Manager
- Certified ISO/IEC 27005:2022 Senior Lead Risk Manager

They can download both their certificate and their certificate logo, as well as claim their digital badge from their dashboard. For more information about downloading the certificate, click here, and for more information about 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 27005:2022 Risk Manager 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 27005:2022 standard, the CEO with the panel of experts, defined 4 different domains. For each of these domains the competencies and skills are listed below, which form the basis for a candidate to show compliancy to the objectives for that domain.

These domains are:

1. Fundamental principles and concepts of an information security risk management
2. Implementation of an information security risk management program
3. Information security risk management framework and processes based on ISO/IEC 27005
4. Other information security risk assessment methods

Domain 1: Fundamental principles and concepts of an information security risk management

Main objective: Ensure that the candidate understands and is able to interpret the main principles and concepts of information security risk management.

Competencies	Knowledge statements
1. Ability to understand and explain the structure of ISO/IEC 27005	1. Knowledge of the main concepts and terminology of ISO/IEC 27005
2. Ability to understand the relation between ISO/IEC 27005 and other risk management frameworks	2. Knowledge of the main standards of the ISO/IEC 27000 family
3. Ability to describe the purpose of risk management and advantages of ISO/IEC 27005	3. Knowledge of international and industry standards and frameworks for information security and risk management
4. Ability to understand and explain the concept of information security	4. Knowledge of information security risks, as defined by ISO/IEC 27005
5. Ability to understand the principles of information security: confidentiality, integrity, and availability	5. Knowledge of the definition of vulnerability
6. Ability to understand and interpret the definition of risk	6. Knowledge of the differences between the concepts of risks and opportunities
7. Ability to understand the main concepts and principles of risk management	7. Knowledge of the definition of threat
8. Ability to understand information security vulnerabilities and threats	8. Knowledge of confidentiality, integrity, and availability of information
9. Ability to explain the concepts of event, opportunity, consequence, and likelihood	9. Knowledge of the type and function of security controls
10. Ability to understand the classification of security controls by type and function	10. Knowledge of risk management principles
11. Ability to understand the role of the risk owner	11. Knowledge of the roles and responsibilities of the risk owner
	12. Knowledge of risk management advantages

Domain 2: Implementation of an information security risk management program

Main objective: Ensure that the candidate understands and is able to initiate the implementation of a risk management program based on ISO/IEC 27005.

Competencies	Knowledge statements
1. Ability to understand the integration of the PDCA cycle into the information security risk management program	1. Knowledge of the risk management process
2. Ability to understand and explain the main steps needed for establishing and implementing an information security risk management program	2. Knowledge of how the top management can demonstrate leadership and commitment regarding risk management
3. Ability to identify the roles and responsibilities of key stakeholders during and after the implementation and operation of an information security risk management program	3. Knowledge of the roles and responsibilities of a risk manager regarding the risk management program
4. Ability to understand the concept of risk assessment	4. Knowledge of the roles and responsibilities of key stakeholders in the implementation of a risk management program
5. Ability to understand the importance of a risk management policy	5. Knowledge of what typically constitutes an organization's internal and external context
6. Ability to identify the resources required for the implementation of a risk management program	6. Knowledge of the importance of understanding key processes and activities of an organization in risk management
7. Ability to analyze and understand the internal and external context of an organization	7. Knowledge of risk assessment objectives and how to achieve specific results
8. Ability to understand key processes and activities of an organization	8. Knowledge of how risk acceptance criteria and information security risk assessment criteria are established
9. Ability to understand and set objectives for the risk management program	9. Knowledge of information security risk management cycles
10. Ability to establish and maintain information security risk criteria, including risk acceptance criteria and criteria for performing information security risk assessments	10. Knowledge of the applicability of quantitative and qualitative analysis in determining risk acceptance criteria
11. Ability to define and justify the information security risk management process scope and adapt it to organization's objectives	11. Knowledge of the resources required for information security risk management
12. Ability to define an appropriate information security risk management method	12. Knowledge of the information security risk management scope and boundaries
	13. Knowledge of the approaches and methodologies used for information security risk assessment
	14. Knowledge of the main steps for planning risk assessment activities

Domain 3: Information security risk management framework and processes based on ISO/IEC 27005

Main objective: Ensure that the candidate is able to identify, analyze, evaluate, treat, communicate, record, and continually monitor information security risks based on ISO/IEC 27005.

Competencies	Knowledge statements
1. Ability to understand the processes of information security risk identification, analysis, and evaluation	1. Knowledge of information security risk assessment processes, including risk identification, analysis, and evaluation
2. Ability to determine the risk identification approach and understand and interpret information gathering techniques	2. Knowledge of the approaches to perform information security risk identification
3. Ability to identify assets, threats, existing controls, vulnerabilities, potential consequences and risk owners	3. Knowledge of information gathering techniques
4. Ability to understand and interpret risk analysis methodologies	4. Knowledge of the definition of an asset and the identification of primary and supporting assets
5. Ability to understand and perform assessment of consequences	5. Knowledge of the identification and classification of vulnerabilities, threats, and existing controls
6. Ability to determine the levels of risk based on the risk evaluation criteria	6. Knowledge of the identification of potential consequences that may affect availability, confidentiality, integrity
7. Ability to understand risk prioritization	7. Knowledge of risk analysis techniques
8. Ability to understand the risk treatment process and risk treatment options based on ISO/IEC 27005	8. Knowledge of how consequences and likelihood should be assessed and how the level of risk should be determined
9. Ability to select appropriate controls to reduce, retain, avoid, or share the risks	9. Knowledge of the evaluation of the levels of risk based on risk evaluation criteria
10. Ability to understand and explain information security risk acceptance criteria	10. Knowledge of risk prioritization
11. Ability to understand the management of residual risk	11. Knowledge of the risk treatment process and options including risk modification, risk retention, risk avoidance, and risk sharing
12. Ability to comprehend and interpret the concept of risk communication and consultation	12. Knowledge of the formulation and approval of a risk treatment plan
13. Ability to understand and interpret principles of effective communication	13. Knowledge of how residual risks are evaluated and accepted
14. Ability to understand and establish internal and external communication	14. Knowledge of the information security risk communication process
15. Ability to understand communication objectives and activities	15. Knowledge of the principles of an efficient communication strategy
16. Ability to understand communication approaches and tools	16. Knowledge of how internal and external communication should be established
17. Ability to document the information security risk management processes	17. Knowledge of communication approaches and tools
18. Ability to record and report the risk assessment and risk treatment results	18. Knowledge of documented information and the importance of recording risks
	19. Knowledge of the documentation of risk management results

19. Ability to monitor and review the effectiveness of an information security risk management program 20. Ability to understand the concept of continual improvement and its advantages regarding risk management 21. Ability to advise an organization on how to continually improve the effectiveness and efficiency of an information security risk management program	20. Knowledge of the main concepts related to continual improvement 21. Knowledge of the processes that need to be monitored and reviewed continually

Domain 4: Other information security risk assessment methods

Main objective: Ensure that the candidate can utilize risk assessment methodologies and frameworks, such as OCTAVE, MEHARI, EBIOS, NIST, Harmonized TRA, and CRAMM.

Competencies	Knowledge statements
1. Ability to understand and interpret OCTAVE methodologies: OCTAVE method, OCTAVE-S, OCTAVE-Allegro, and OCTAVE FORTE	1. Knowledge of the three phases of the OCTAVE method
2. Ability to conduct information security risk assessment based on the OCTAVE Allegro methodology	2. Knowledge of the OCTAVE-S phases for conducting risk assessment
3. Ability to analyze and manage risks based on the MEHARI method	3. Knowledge of how OCTAVE-Allegro phases can be utilized to conduct an information security risk assessment
4. Ability to understand and utilize EBIOS method for conducting risk assessments	4. Knowledge of the steps of the OCTAVE FORTE for risk management
5. Ability to identify NIST publications for risk management	5. Knowledge of MEHARI three main phases for risk management
6. Ability to understand and interpret the NIST risk management framework and utilize it in managing information security risks	6. Knowledge of how information security risks can be identified, estimated, evaluated, and treated using MEHARI
7. Ability to understand and interpret CRAMM methodology for risk management	7. Knowledge of EBIOS risk assessment methodology and its five workshops and modules
8. Ability to understand and explain how Harmonized Threat and Risk Assessment (TRA) method can be utilized for conducting risk assessment	8. Knowledge of the NIST publications for risk management
	9. Knowledge of the seven steps of the NIST risk management framework
	10. Knowledge of CRAMM risk analysis and management methodology and tool
	11. Knowledge of the five phases of Harmonized Threat and Risk Assessment (TRA) methodology

3.2 ISO/IEC 27005:2022 Lead Risk Manager 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 27005:2022 standard, the CEO with the panel of experts, defined 6 different domains. For each of these domains the competencies and skills are listed below, which form the basis for a candidate to show compliancy to the objectives for that domain.

These domains are:

1. Fundamental principles and concepts of information security risk management
2. Implementation of an information security risk management program
3. Information security risk assessment
4. Information security risk treatment
5. Information security risk communication, monitoring, and improvement
6. Information security risk assessment methodologies

Domain 1: Fundamental principles and concepts of information security risk management

Main objective: Ensure that the candidate understands and is able to interpret the main principles and concepts of information security risk management.

Competencies	Knowledge statements
1. Ability to understand and explain the structure of ISO/IEC 27005	1. Knowledge of the main concepts and terminology of ISO/IEC 27005
2. Ability to understand the relation between ISO/IEC 27005 and other risk management frameworks	2. Knowledge of the main standards of the ISO/IEC 27000 family
3. Ability to describe the purpose of risk management and advantages of ISO/IEC 27005	3. Knowledge of international and industry standards and frameworks for information security and risk management
4. Ability to understand and explain the concept of information security	4. Knowledge of information security risks, as defined by ISO/IEC 27005
5. Ability to understand the principles of information security: confidentiality, integrity, and availability	5. Knowledge of the definition of vulnerability
6. Ability to understand and interpret the definition of risk	6. Knowledge of the differences between the concepts of risks and opportunities
7. Ability to understand the main concepts and principles of risk management	7. Knowledge of the definition of threat
8. Ability to understand information security vulnerabilities and threats	8. Knowledge of confidentiality, integrity, and availability of information
9. Ability to explain the concepts of event, opportunity, consequence, and likelihood	9. Knowledge of the type and function of security controls
10. Ability to understand the classification of security controls by type and function	10. Knowledge of risk management principles
11. Ability to understand the role of the risk owner	11. Knowledge of the roles and responsibilities of the risk owner
	12. Knowledge of risk management advantages

Domain 2: Implementation of an information security risk management program

Main objective: Ensure that the candidate understands and is able to initiate the implementation of a risk management program based on ISO/IEC 27005.

Competencies	Knowledge statements
1. Ability to understand the integration of the PDCA cycle into the information security risk management program	1. Knowledge of the risk management process
2. Ability to understand and explain the main steps needed for establishing and implementing an information security risk management program	2. Knowledge of how the top management can demonstrate leadership and commitment regarding risk management
3. Ability to identify the roles and responsibilities of key stakeholders during and after the implementation and operation of an information security risk management program	3. Knowledge of the roles and responsibilities of a risk manager regarding the risk management program
4. Ability to understand the concept of risk assessment	4. Knowledge of the roles and responsibilities of key stakeholders in the implementation of a risk management program
5. Ability to differentiate between strategic cycle and operational cycle of risk assessment	5. Knowledge of what typically constitutes an organization's internal and external context
6. Ability to understand the importance of a risk management policy	6. Knowledge of the importance of understanding key processes and activities of an organization in risk management
7. Ability to identify the resources required for the implementation of a risk management program	7. Knowledge of risk assessment objectives and how to achieve specific results
8. Ability to analyze and understand the internal and external context of an organization	8. Knowledge of how risk acceptance criteria and information security risk assessment criteria are established
9. Ability to understand key processes and activities of an organization	9. Knowledge of information security risk management cycles
10. Ability to understand and set objectives for the risk management program	10. Knowledge of the applicability of quantitative and qualitative analysis in determining risk acceptance criteria
11. Ability to establish and maintain information security risk criteria, including risk acceptance criteria and criteria for performing information security risk assessments	11. Knowledge of the resources required for information security risk management
12. Ability to define and justify the information security risk management process scope and adapt it to organization's objectives	12. Knowledge of the information security risk management scope and boundaries
13. Ability to define an appropriate information security risk management method	13. Knowledge of the approaches and methodologies used for information security risk assessment
	14. Knowledge of the main steps for planning risk assessment activities

Domain 3: Information security risk assessment

Main objective: Ensure that the candidate is able to identify, analyze, and evaluate risks based on ISO/IEC 27005.

Competencies	Knowledge statements
1. Ability to understand the processes of information security risk identification, analysis, and evaluation	1. Knowledge of information security risk assessment processes, including risk identification, analysis, and evaluation
2. Ability to determine the risk identification approach and understand and interpret information gathering techniques	2. Knowledge of the approaches to perform information security risk identification
3. Ability to identify assets, threats, existing controls, vulnerabilities, and consequences	3. Knowledge of information gathering techniques
4. Ability to understand the types of assets, as defined in ISO/IEC 27005	4. Knowledge of the definition of an asset and the identification of primary and supporting assets
5. Ability to understand the process of asset valuation	5. Knowledge of the relationship of primary and supporting assets
6. Ability to understand how risk owners are identified and their responsibilities	6. Knowledge of the process of asset valuation and inventory of assets
7. Ability to identify the types of threats and vulnerabilities, as defined in ISO/IEC 27005	7. Knowledge of the identification and classification of threats
8. Ability to understand various methods for identifying existing controls	8. Knowledge of the identification of existing controls
9. Ability to understand and explain the methods for vulnerability assessment	9. Knowledge of how vulnerabilities should be identified using vulnerability assessment techniques
10. Ability to interpret and determine risk analysis techniques	10. Knowledge of the relationship between assets, vulnerabilities, and threats
11. Ability to understand how consequences can be defined based on nonnumerical categories, numerical rating scales, and practical values	11. Knowledge of the identification of consequences that may affect availability, confidentiality, integrity
12. Ability to understand and perform assessment of consequences and likelihood and determine the level of risk	12. Knowledge of risk analysis techniques
13. Ability to understand the types of risk ratings: inherent, residual, and target risk	13. Knowledge of how consequences and likelihood should be assessed and how the level of risk should be determined
14. Ability to evaluate the levels of risk based on the risk evaluation criteria	14. Knowledge of the evaluation of the levels of risk based on risk evaluation criteria
15. Ability to compare the results of the risk analysis with the established risk criteria to determine if an additional action is required	15. Knowledge of inherent, residual, and target risks, and their relationship
16. Ability to understand risk prioritization	16. Knowledge of risk prioritization
	17. Knowledge of the main concepts that are relevant to quantitative risk assessment

Domain 4: Information security risk treatment

Main objective: Ensure that the candidate is able to treat the identified risks as part of the information security risk management process.

Competencies	Knowledge statements
1. Ability to understand the risk treatment process based on ISO/IEC 27005	1. Knowledge of the risk treatment process
2. Ability to understand and interpret risk treatment options	2. Knowledge of the risk treatment options, including risk modification, risk retention, risk avoidance, and risk sharing
3. Ability to select appropriate information security risk treatment options	3. Knowledge of controls that are necessary to implement the information security risk treatment options
4. Ability to select appropriate controls to modify, retain, avoid, or share the risks	4. Knowledge of how the risk level can be reduced through the selection of adequate security controls
5. Ability to understand how the risk level can be reduced through the selection of security controls	5. Knowledge of the best practices related to risk treatment options
6. Ability to draft and implement risk treatment plans	6. Knowledge of the formulation of a risk treatment plan
7. Ability to understand steps needed to define risk ownership	7. Knowledge of the implementation of risk treatment plans
8. Ability to evaluate the residual risk	8. Knowledge of how residual risks are evaluated
9. Ability to understand the processes of risk treatment plan acceptance and residual risk acceptance	9. Knowledge of the acceptance of residual risk

Domain 5: Information security risk communication, monitoring, and improvement

Main objective: Ensure that the candidate understands and is able to apply processes for information security risk management communication, consultation, monitoring, review, and recording based on ISO/IEC 27005.

Competencies	Knowledge statements
1. Ability to comprehend and interpret the concept of risk communication and consultation	1. Knowledge of the information security risk communication process
2. Ability to understand and interpret principles of effective communication	2. Knowledge of the principles of an efficient communication strategy
3. Ability to understand the objectives of a risk communication	3. Knowledge of how the risk communication plan should be established
4. Ability to establish a risk communication plan to assist in the understanding of an organization's information security issues, policies, and performance	4. Knowledge of the risk communication objectives and activities
5. Ability to understand and establish internal and external communication	5. Knowledge of how internal and external communication should be established
6. Ability to ensure communication and consultation between decision-makers and external and internal stakeholders	6. Knowledge of communication approaches and tools
7. Ability to understand communication methods and tools	7. Knowledge of documented information and the importance of recording risks
8. Ability to document the information security risk management processes	8. Knowledge of the documentation of risk management results
9. Ability to record and report the risk assessment and risk treatment results	9. Knowledge of how risk management records should be maintained
10. Ability to maintain the risk management records	10. Knowledge of the best practices and techniques used to monitor and review the effectiveness of an information security risk management program
11. Ability to monitor and review the effectiveness of an information security risk management program	11. Knowledge of management review of the information security risk management process
12. Ability to understand the concept of continual improvement and its advantages regarding risk management	12. Knowledge of the implementation of corrective actions regarding the risk treatment plan
13. Ability to advise an organization on how to continually improve the effectiveness and efficiency of an information security risk management program	13. Knowledge of the main concepts related to continual improvement
14. Ability to determine the appropriate tools to support the continual improvement of an organization	14. Knowledge of the maintenance and improvement of an information security risk management program

Domain 6: Information security risk assessment methodologies

Main objective: Ensure that the candidate can utilize risk assessment methodologies and frameworks, such as OCTAVE, MEHARI, EBIOS, NIST, Harmonized TRA, and CRAMM.

Competencies	Knowledge statements
1. Ability to understand and interpret OCTAVE methodologies: OCTAVE method, OCTAVE-S, OCTAVE-Allegro, and OCTAVE FORTE 2. Ability to conduct information security risk assessment based on the OCTAVE Allegro methodology 3. Ability to analyze and manage risks based on the MEHARI method 4. Ability to understand and utilize EBIOS method for conducting risk assessments 5. Ability to identify NIST publications for risk management 6. Ability to understand and interpret the NIST risk management framework and utilize it in managing information security risks 7. Ability to understand and interpret CRAMM methodology for risk management 8. Ability to understand and explain how Harmonized Threat and Risk Assessment (TRA) method can be utilized for conducting risk assessment	1. Knowledge of the three phases of the OCTAVE method 2. Knowledge of the OCTAVE-S phases for conducting risk assessment 3. Knowledge of how OCTAVE-Allegro phases can be utilized to conduct an information security risk assessment 4. Knowledge of the steps of the OCTAVE FORTE for risk management 5. Knowledge of MEHARI three main phases for risk management 6. Knowledge of how information security risks can be identified, estimated, evaluated, and treated using MEHARI 7. Knowledge of EBIOS risk assessment methodology and its five workshops and modules 8. Knowledge of the NIST publications for risk management 9. Knowledge of the seven steps of the NIST risk management framework 10. Knowledge of CRAMM risk analysis and management methodology and tool 11. Knowledge of the five phases of Harmonized Threat and Risk Assessment (TRA) methodology

4 ISO/IEC 27005 Examination Development

The test specifications are presented in the table below.

4.1 ISO/IEC 27005:2022 Risk Manager

Based on the abovementioned domains and their relevance, 60 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 risk management	13	21.67	X	
	Implementation of an information security risk management program	7	11.67	X	
	Information security risk management framework and processes based on ISO/IEC 27005	31	51.67		X
	Other information security risk assessment methods	9	15	X	
	Total	**60**	**100%**		
	Number of questions per level of understanding			**29**	**31**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**48.3%**	**51.7%**

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

After successfully passing the exam, candidates will be able to apply for the "Certified ISO/IEC 27005:2022 Risk Manager" credential or for the ''Certified ISO/IEC 27005:2022 Senior Risk Manager'', depending on their level of experience.

4.2 ISO/IEC 27005:2022 Lead Risk Manager

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 information security risk management	13	16.25	X	
	Implementation of an information security risk management program	7	8.75	X	
	Information security risk assessment	20	25	X	
	Information security risk treatment	15	18.75		X
	Information security risk communication, monitoring, and improvement	10	12.5		X
	Information security risk assessment methodologies	15	18.75		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%**

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

After successfully passing the exam, candidates will be able to apply for the "Certified ISO/IEC 27005:2022 Lead Risk Manager" credential or for the ''Certified ISO/IEC 27005:2022 Senior Lead Risk Manager'' credential, depending on their level of experience.

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 ISO/IEC 27005:2022 Risk Manager Certification

5.1.1 Prerequisites for ISO/IEC 27005:2022 Risk Manager Certification

Professional experience:
The minimum professional experience required is:

- Two years of professional experience in total
- One year of work experience in Risk Management

- **Risk Management:** 200 Hours

This information is submitted by candidates in the eligibility application.

5.1.2 Evaluation of the eligibility applications

The Certification Department will evaluate each application to validate the candidates' eligibility for certification. 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 or does not meet the prerequisites, the Certification Department will reject the application.

If the candidate meets the prerequisites, the eligibility application is approved and the candidate can continue with the exam preparation.

5.1.3 General requirements

In general, the requirements for any ISO/IEC 27005:2022 Risk Manager Certification are:

- Having successfully passed the appropriate certification examination
- Having indicated at least two referrals in their application form and having obtained the validation of the professional experience
- Having fulfilled all other requirements
- Having paid all certification application fees

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

Exam: PECB Certified ISO/IEC 27005:2022 Risk Manager Exam or equivalent
Candidates must pass a comprehensive examination consisting of development questions exam covering 4 domains.

Other requirements: Signing the PECB Code of Ethics

Prerequisites				
Credential	**Exam**	**Professional experience**	**Risk Management experience**	**Other requirements**
Certified ISO/IEC 27005:2022 Risk Manager	PECB Certified ISO/IEC 27005:2022 Risk Manager exam or equivalent	**Two years:** One year of work experience in ISRM	Information Security Risk Management activities: a total of 200 hours	Signing the PECB Code of Ethics
Certified ISO/IEC 27005:2022 Senior Risk Manager	PECB Certified ISO/IEC 27005:2022 Risk Manager exam or equivalent	**Ten years:** Seven years of work experience in Information Security Management	Information Security Risk Management activities: 1000 hours	Signing the PECB Code of Ethics

5.2 ISO/IEC 27005:2022 Lead Risk Manager Certification

5.2.1 Prerequisites for ISO/IEC 27005:2022 Lead Risk Manager Certification

Professional experience

The minimum professional experience required is:

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

- **Risk Management:** 300 Hours

This information is submitted by candidates in the eligibility application.

5.2.2 Evaluation of the eligibility applications

The Certification Department will evaluate each application to validate the candidates' eligibility for certification. 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 or does not meet the prerequisites, the Certification Department will reject the application.

If the candidate meets the prerequisites, the eligibility application is approved and the candidate can continue with the exam preparation.

5.2.3 General requirements

In general, the requirements for any ISO/IEC 27005:2022 Lead Risk Manager certification are:

- Having successfully passed the appropriate certification examination
- Having indicated at least two referrals in their application form and having obtained the validation of the professional experience
- Having fulfilled all other requirements
- Having paid all certification application fees

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

Exam: PECB Certified ISO/IEC 27005:2022 Lead Risk Manager Exam or equivalent. Candidates must pass a comprehensive examination consisting of development questions exam covering 6 domains.

Candidates must pass a comprehensive examination consisting of development questions exam covering 6 domains.

Other requirements: Signing the PECB Code of Ethics

Prerequisites				
Credential	**Exam**	**Professional experience**	**Risk Management experience**	**Other requirements**
Certified ISO/IEC 27005:2022 Lead Risk Manager	PECB Certified ISO/IEC 27005:2022 Lead Risk Manager exam or equivalent	**Five years:** two year of work experience in ISRM	Information Security Risk Management activities: a total of 300 hours	Signing the PECB Code of Ethics
Certified ISO/IEC 27005:2022 Senior Lead Risk Manager	PECB Certified ISO/IEC 27005:2022 Lead Risk Manager or equivalent	**Ten years:** Seven years of work experience in Information Security Management	Information Security Risk Management activities: 1000 hours	Signing the PECB Code of Ethics

5.3 Examination methods and evaluation process

Passing the Exam:

PECB will organize two exams for the grade defined previously:

1. The ISO/IEC 27005:2022 Risk Manager Exam
2. The ISO/IEC 27005:2022 Lead Risk Manager Exam

The PECB Certified ISO/IEC 27005:2022 Risk Manager Exam is a 2h exam. The exam questions are relevant and sufficient and cover all domains defined for the “ISO/IEC 27005:2022 Risk Manager” Certification.

The PECB Certified ISO/IEC 27005:2022 Lead Risk Manager Exam is a 3h exam. The exam questions are relevant and sufficient and cover all domains defined for the “ISO/IEC 27005:2022 Lead Risk Manager” Certification.

A minimum score of 70% is required to pass the PECB Certified ISO/IEC 27005:2022 Risk Manager Exam
A minimum score of 70% is required to pass the PECB Certified ISO/IEC 27005:2022 Lead Risk Manager Exam

5.4 Certification evaluation process

Examination: Candidate needs to pass the respective exam

Professional experience

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

All references will then be sent an email containing the information the applicant entered related to the position held at their organization.

To be considered valid, the information security activities should follow best implementation and management practices and include the following:

- Defining a risk management approach
- Designing and implementing an overall risk management process for an organization
- Defining risk evaluation criteria
- Performing risk assessment
- Identifying assets, threats, existing controls, vulnerabilities and consequences (impacts)
- Assessing consequences and incident likelihood
- Evaluating risk treatment options
- Selecting and implementing Information Security controls
- Performing risk management reviews

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.

5.5 Equivalencies clause requirements

PECB does accept certifications and exams provided from other recognized and 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 (e.g. ISO/IEC 27005:2022 Risk Manager Certificate)

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

5.6 Rejection of the certification application

PECB may refuse an application for certification if a candidate:

- Falsifies the eligibility application or certification application
- Violates examination procedures
- Violates the PECB Code of Ethics
- Fails the examination
- Does not obtain validation of professional experience through referrals

For more detailed information, please refer to Section Complaints and Appeals.

Payment for certification is non-refundable.

5.7 Requirements for recertification

5.7.1 Validity period of PECB certifications

PECB certifications are valid for three years. In order to maintain a certificate, PECB Certified Professionals are required to demonstrate that they are performing certification related activities. In addition to this, PECB Professionals are required to pay an Annual Maintenance Fee (AMF) and submit the Continuing Professional Development (CPDs).

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.

A PECB Certificate requires the payment of the maintenance fee.

PECB continuously notifies each PECB Professional to maintain their certificate(s). The notifications are sent several times throughout the certification cycle.

If the candidate has taken an earlier version of the exam (not 2022) they are required to retake an examination at the end of the certificate of conformity's validity (3 years).

When scheduling the new exam, they will be required to fill out an eligibility form to confirm that they meet the requirements for the certification they wish to obtain.

5.7.2 Certification renewal process

To be able to renew a certificate, PECB Professionals will need to demonstrate that they have maintained their certificate(s) by submitting CPDs and AMFs. They need to have performed the required amount of CPD hours within three years certification cycle see appendix 1).

After three years of successful maintenance of a PECB Certificate, the PECB Professionals can apply for a renewal of their certificate.

The PECB Certificate(s) can be renewed online through the PECB Member Dashboard, by logging into their member dashboard (www.pecb.com/login), clicking on '**My Certifications'** and then the '**Renew'** button.

Note:

- *PECB Certified Professionals who hold an ISO/IEC 27005:2022 Risk Manager/ Lead Risk Manager Certificates and fail evidence of certification maintenance requirements, will have their credentials revoked.*

5.7.3 Reporting CPD and 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 as they are earned through their PECB Member Dashboards, by logging into their member dashboard (www.pecb.com/login), clicking 'Certifications' and then the 'Submit CPD' button.

Note: CPDs need to be reported for each specific certificate located under your 'My Certifications' tab in your PECB Member Dashboard.

Payment of AMF
PECB Certified Professionals will need to pay the AMFs in order for their certificate to be renewed.

5.7.4 Upgrade

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

The PECB Certificates can be upgraded online through PECB Professionals Member Dashboard, by logging into their Member Dashboard (www.pecb.com/login), clicking '**My Certifications'** and then the '**Upgrade**'.

The application fee for an upgrade is $100.

5.7.5 Suspension

Suspending Certification means the state that the individual's certification is temporary suspended for not fulfilling the PECB requirements. Certification will be suspended for any of the following reasons:

- PECB receives excessive or serious complaints by interested parties and social conflicts, suspension will be applied until the investigation has been completed
- Any willful misuse of logo of PECB or Accreditation body(ies)
- Not correcting misuse of certification mark, within the determined time by PECB
- Any other condition deemed appropriate by PECB management
- The certified individual has voluntarily requested a suspension
- Failure to comply with the recertification requirements

Individuals whose certificate has been suspended, are refrained from further promotion of the certification while it is suspended.

5.7.6 Revocation

Revoking Certification means the state that the individual's certification is revoked (also referred as "withdrawn") for not fulfilling the PECB requirements, through which the individuals will have their PECB Certificates revoked and will no longer be allowed to present themselves as PECB Certified Professionals. Certification will be revoked for any of the following reasons:

- Failure to reinstate the suspended certification within the given timeframe
- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of certification
- Provide false information in the eligibility application and/or in the application for certification
- Break any other PECB rules

Individuals whose certificate has been revoked, are refrained to use of all references to a certified status.

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**

Appendix 2 - AMF Requirements

Certification	AMF (rate per 3-year)
Foundation, Provisional and Transition	**None**
All other certifications	**$360**

6 Revision History

Version	Change description	Date
1.0	Initial release	2012-03-23
1.1	Reviewed by Certification Manager: Updated competency domains and recertification requirements	2017-04-21
2.0	Reviewed by Certification Manager: Updated Competency Domains and Recertification Requirements	2017-09-21
2.1	Reviewed by Certification Processing Manager: Updated 1. Purpose and summary Updated 1.1 ISO/IEC 27005 Risk Manager Certification Updated 3. ISO/IEC 27005 Risk Manager Certification marks Updated 5. Objectives, domains and skills related to the certification scheme Updated 5.1 ISO/IEC 27005 Risk Manager Certifications Updated 7 Certification schemes requirements	2018-10-03
2.2	Reviewed from Certification Manager. Changes applied: • Added point 7.4.5 Suspension • Added point 7.4.6 Revocation • Updated point 7.4.7 Reporting CPDs and AMF	2019-01-25
2.3	Reviewed by Certification Manager: • Updated the document with the new design logo • Added the scheme committee members	2019-09-10
2.4	Reviewed by Compliance Associate Supervisor: • Updated the process flowchart • Updated the scheme committee members	2020-10-30
2.5	Reviewed by Compliance Supervisor: • Added reference validation, and surveillance methods • Updated scheme committee members • Registered the document as policy	2021-08-18
2.6	Reviewed by Compliance Supervisor: • Added the ISO/IEC 27005 Lead Risk Manager	2021-11-24
2.7	Reviewed by Accreditation Leader and Compliance Director-Certification Department based on the updated version of the standard Integrated comments from the General Scheme Advisory Board review	2023-02-06
2.8	Reviewed by Compliance Director-Certification Department • Added information about digital badges • Updated competency domains • Updated the criteria for revocation • Updated policy code from 08200 to 05071	2023-07-10
2.9	Reviewed by Compliance Director-Certification Department • Updated the AMF price from $100 to $120	2023-10-02
3.0	Reviewed by Team Leader – Certification Department: • Updated the term PECB Surveillance Method/Surveillance Audit to CPD Verification	2023-11-14

	• Updated General Scheme Advisory Board members	
4.0	Reviewed by Team Leader – Certification Department: • Updated the numbers of the sections • Removed the section ‘’Downgrade of credentials ‘’ • Updated section 8 ‘’Certification scheme requirements’’ • Updated the Annex A, by removing the Annual Maintenance	2024-02-14
5.0	Reviewed by Team Leader – Certification Department: • Added the senior levels for Risk Manager and Lead Risk Manager • Update the Appendix 1 - Certification Maintenance Requirements	2024-10-28