ISO/IEC 27005:2018 Certification Scheme

Approved By:	CEO
Effective date:	20130323

PECB

Table of Contents

1 Purpose and summary

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

- ISO/IEC 27005 Risk Manager
- ISO/IEC 27005 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 Risk Manager Certification

The "ISO/IEC 27005 Risk Manager" credential is a professional certification for individuals aiming to demonstrate the competence to maintain and manage the ongoing information security risk management process in accordance with ISO/IEC 27005:2018.

The most important skills required in the market are the ability to support an organization in implementing and managing a risk management framework as specified in PECB ISO/IEC 27005:2018 implementation of a risk management program, risk identification, risk analysis, risk evaluation, risk treatment, acceptance of risk, and management of residual risks, communicating, monitoring and reviewing risk.

Various professionals may apply for this certification:

- Information Security risk managers
- Information Security team members
- Individuals responsible for Information Security, compliance, and risk within an organization
- Individuals implementing ISO/IEC 27001, seeking to comply with ISO/IEC 27001 or involved in a risk management program
- IT consultants
- IT professionals
- Information Security officers
- Privacy officers

1.2 ISO/IEC 27005 Lead Risk Manager Certification

The "ISO/IEC 27005 Lead Risk Manager" credential is a professional certification for individuals aiming to demonstrate the competence to maintain and manage the ongoing information security risk management process in accordance with ISO/IEC 27005:2018.

The most important skills required in the market are the ability to support an organization in implementing and managing a risk management framework as specified in PECB ISO/IEC 27005:2018 implementation of a risk management program, risk identification, risk analysis, risk evaluation, risk treatment, acceptance of risk, and management of residual risks, communicating, monitoring and reviewing risk.

Various professionals may apply for this certification:

- Risk managers
- Auditors seeking to understand the implementation of the risk management program based on ISO/IEC 27005
- Persons responsible for information security or conformity within an organization
- Members of an information security team who need to ensure that information security risks are being effectively managed
- IT consultants, information security managers
- Staff implementing or seeking to comply with ISO/IEC 27001 or involved in the implementation of a risk management program
- Risk analysts

2 ISO/IEC 27005 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 27005 Risk Manager
- PECB Certified ISO/IEC 27005 Lead Risk Manager

They can download both their professional certificate and their certificate logo from their dashboard.

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 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 27005:2018 standard, the Deputy 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 information security risk management
2. Implementation of the information security risk management program
3. Information security risk management framework and process based on ISO/IEC 27005
4. Other information security risk assessment methods

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

Main objective: Ensure that the ISO/IEC 27005:2018 Risk Manager candidate understands, and is able to interpret and illustrate the main risk management guidelines and concepts related to a risk management framework based on ISO/IEC 27005:2018.

Competencies	Knowledge statements
1. Ability to understand and explain the operations of the ISO organization and the development of risk management standards. 2. Ability to explain and illustrate the main concepts in information security and information security risk management. 3. Ability to understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, likelihood, consequence and control. 4. Ability to distinguish the relationship between ISO/IEC 27005:2018, and other related standards and best practices.	1. Knowledge of ISO/IEC 27005:2018 and other standards related to risk management. 2. Knowledge of the main information security concepts and terminology as described in ISO/IEC 27000 and ISO/IEC 27005:2018. 3. Knowledge of the concept of risk and its application in information security. 4. Knowledge of the relationship between the concepts of asset, vulnerability, threat, likelihood, impact and control. 5. Knowledge of the ISO 31000 risk management principles and their application in organizations. 6. Knowledge of the relationship and differences between ISO/IEC 27005:2018, ISO/IEC 27001, ISO/IEC 27002 and ISO 31000.

Domain 2: Implementation of the information security risk management program

Main objective: Ensure that the ISO/IEC 27005:2018 Risk Manager candidate can implement an information security risk management program based on ISO/IEC 27005:2018

Competencies	Knowledge statements
1. Ability to understand, analyze needs and provide guidance in the context of the implementation and management of an information security risk management framework. 2. Ability to select a risk assessment approach for an organization. 3. Ability to define and write policies and procedures. 4. Ability to define the key responsibilities of the management and the principle stakeholders. 5. Ability to understand the objectives, values and strategies of the organization. 6. Ability to establish the external and internal context of the organization. 7. Ability to define the scope and boundaries related to the information security risk management process.	1. Knowledge of the roles and responsibilities of the key actors during the implementation and the operation of a risk management framework. 2. Knowledge of the main organizational structures applicable for an organization to manage its risk. 3. Knowledge of the best practices of the external and internal context of the organization. 4. Knowledge of the characteristics and the differences between the different documents related to policies and procedures. 5. Knowledge of defining the scope and boundaries of information security risk management. 6. Knowledge of techniques and best practices to draft policies, procedures and others types of documents.

Domain 3: Information security risk management framework and process based on ISO/IEC 27005:2018

Main objective: Ensure that the ISO/IEC 27005:2018 Risk Manager candidate can contribute in the development of an information security risk management framework, and is able to manage risks based on the risk management process, as recommended by ISO/IEC 27005:2018.

Competencies	Knowledge statements
1. Ability to choose a risk analysis methodology. 2. Ability to interpret and understand the results of a risk evaluation. 3. Ability to choose a risk treatment option for different risk scenarios. 4. Ability to prepare and implement the risk treatment plan. 5. Ability to ensure communication and consultation between the decision-makers, external and internal stakeholders. 6. Ability to monitor and review the risk management process and the implemented controls. 7. Ability to ensure continual improvement of the risk management program.	1. Knowledge of the qualitative and quantitative risk analysis methodologies. 2. Knowledge of planning risk assessment projects and activities by ensuring the participation and support of stakeholders throughout the risk assessment process. 3. Knowledge of estimating the risk level according to the evaluation criteria and the risk acceptance criteria. 4. Knowledge of the risk treatment options including risk modification, risk retention, risk avoidance and risk sharing. 5. Knowledge of monitoring and review of specific elements of risk factors and risk management. 6. Knowledge of setting continual improvement objectives.

Domain 4: Other information security risk assessment methods

Main objective: Ensure that the ISO/IEC 27005:2018 Risk Manager candidate can use other risk assessment methodologies such as OCTAVE, MEHARI, EBIOS and Harmonized Threat and Risk Assessment (TRA) Method

Competencies	Knowledge statements
1. Ability to understand the three OCTAVE versions: OCTAVE, OCTAVE-S, and OCTAVE-Allegro. 2. Ability to implement the results from OCTAVE-S process performed in three phases. 3. Ability to conduct a risk assessment using the OCTAVE Allegro process following its eight steps. 4. Ability to conduct a risk assessment using the MEHARI method and its four phases. 5. Ability to conduct a risk assessment using the EBIOS methodology and its five modules. 6. Ability to interpret the application of ISO/IEC 27005:2018 in EBIOS. 7. Ability to conduct a risk assessment using the Harmonized Threat and Risk Assessment (TRA) method and its five phases	1. Knowledge of the three phases of the OCTAVE method. 2. Knowledge of identifying infrastructure vulnerabilities and developing security strategy and plans as specified in the OCTAVE-S method. 3. Knowledge of the OCTAVE Allegro roadmap. 4. Knowledge of the four phases of the MEHARI approach. 5. Knowledge of the five modules of EBIOS risk assessment methodology. 6. Knowledge of the relationship between EBIOS & ISO/IEC 27005:2018. 7. Knowledge of the five phases of Harmonized Threat and Risk Assessment (TRA) methodology.

3.2 ISO/IEC 27005 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 27005:2018 standard, the Deputy 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:

- **Domain 1:** Fundamental principles and concepts of information security risk Management
- **Domain 2:** Implementation of the information security risk management program
- **Domain 3:** Information security risk assessment
- **Domain 4:** Information security risk treatment
- **Domain 5:** Information security risk communication, monitoring and improvement
- **Domain 6:** Information security risk assessment methodologies

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

Main objective: Ensure that the candidate can understand, and is able to interpret the main information security risk management guidelines and concepts related to the risk management framework based on ISO/IEC 27005:2018

Competencies	Knowledge statements
1. Ability to understand and explain the structure of ISO/IEC 27005:2018 and its framework 2. Ability to identify, analyze and evaluate the guidance of different information security risk management frameworks 3. Ability to explain and illustrate the main concepts in information security and information security risk management 4. Ability to distinguish the relationship between ISO/IEC 27005:2018, and other related standards 5. Ability to understand, interpret and illustrate the relationship between the concepts of asset, threat, likelihood, consequence and controls	1. Knowledge of basic concepts for the implementation of an information security risk management program 2. Knowledge of the main standards and frameworks of risk management 3. Knowledge of the main information security concepts and terminology as described in ISO/IEC 27000 & ISO/IEC 27005:2018 4. Knowledge of the concept of risk and its application in information security 5. Knowledge of the 11 principles of Risk Management as described in ISO 31000 6. Knowledge of the relationship between the concepts of asset, threat, likelihood, impact and controls 7. Knowledge of the relationship and differences between ISO/IEC 27005:2018, ISO/IEC 27001, ISO/IEC 27002 and ISO 31000

Domain 2: Implementation of the information security risk management program

Main objective: Ensure that the candidate can implement an information security risk management program based on ISO/IEC 27005:2018

Competencies	Knowledge statements
1. Ability to understand, analyze and provide guidance of the attribution of roles and responsibilities in the context of the implementation and management of an information security risk management framework	1. Knowledge of the roles and responsibilities of the key actors during the implementation of a risk management framework and its operation
2. Ability to implement the required processes of an information security risk management framework	2. Knowledge of the main organizational structures applicable for the management of the risk within an organization
3. Ability to define, write and establish risk management policies and procedures	3. Knowledge of the most frequently used practices during the establishment of external and internal context of the organization
4. Ability to understand several recognized risk assessment methodologies	4. Knowledge of techniques and best practices to write policies, procedures and others types of required documentation
5. Ability to identify, review and select a risk assessment approach appropriate for a specific organization	5. Knowledge of the objectives of a risk management program and risk assessment process
6. Ability to integrate the information security risk management framework into organizational processes by appointing key responsibilities of key players	6. Knowledge of key aspects of external and internal context
7. Ability to understand the objectives, values and strategies of the organization	7. Knowledge of different information security risk assessment approaches
8. Ability to identify the external and internal context of the organization	8. General knowledge of the main risk assessment methodologies, including EBIOS, MEHARI and OCTAVE
9. Ability to identify the basic criteria for the evaluation of information security risk	9. Knowledge of the process of information security risk management and its relation with the scope and boundaries
10. Ability to define the scope and boundaries related to the information security risk management process	10. Knowledge of typical stakeholders and their requirements
11. Ability to define and analyze the stakeholders of an organization	

Domain 3: Information security risk assessment

Main objective: Ensure that the candidate can perform a risk assessment according to the best practices and guidelines provided by ISO/IEC 27005:2018

Competencies

1. Ability to identify, recognize and record information security risks according to ISO/IEC 27005:2018
2. Ability to understand and interpret the identification of assets, threats, existing controls, vulnerabilities, and consequences
3. Ability to identify primary and supporting assets of an organization
4. Ability to identify the consequences in terms of confidentiality, integrity and availability of assets
5. Ability to generate, interpret and understand risk analysis reports
6. Ability to perform risk assessments in various settings and establishments
7. Ability to assess the likelihood and determine the level of risk for each identified incident scenario
8. Ability to choose a risk analysis methodology that suits the needs of the organization
9. Ability to calculate the level of risk in terms of the combination of consequences and their likelihood
10. Ability to conduct, interpret and understand a risk evaluation
11. Ability to set the evaluation criteria
12. Ability to plan activities for a risk assessment process and integrate risk assessment processes to information security risk management frameworks and an ISMS

Knowledge statements

1. Knowledge on planning risk assessment projects and activities by ensuring the participation and support of stakeholders throughout the risk assessment process.
2. Knowledge of information gathering techniques
3. Knowledge on identification of assets, risk sources, vulnerabilities, existing measures, impacts, incident likelihood and the relation between these concepts
4. Knowledge of the qualitative and quantitative risk analysis methodologies
5. General knowledge of ROSI quantitative method
6. Knowledge on likelihood assessment and risk level determination for different identified incident scenarios
7. Knowledge of risk level estimation according to the evaluation criteria and the risk acceptance criteria
8. Knowledge on the outcomes of risk analysis and risk prioritization
9. Knowledge of the guidelines and best practices of risk assessment integration based on ISO/IEC 27005:2018

Domain 4: Information security risk treatment

Main objective: Ensure that the candidate can apply and conduct a risk treatment process as part of an information security risk management framework based on ISO/IEC 27005:2018

Competencies	Knowledge statements
1. Ability to understand the risk treatment process based on ISO/IEC 27005:2018 2. Ability to understand and manage information security risk by identifying, analyzing, and evaluating whether the risk should be modified by risk treatment controls 3. Ability to select the appropriate controls to reduce, retain, avoid or share the risks 4. The ability to draft, propose and implement different risk treatment plans 5. Ability to evaluate the residual risk	1. General knowledge of the risk treatment process 2. Knowledge of the risk treatment options including risk modification, risk retention, risk avoidance and risk sharing 3. Knowledge of the best practices related with risk treatment options 4. Knowledge of residual risk evaluation based on the risk acceptance criteria 5. Knowledge of documenting the chosen treatment options by a risk treatment plan 6. General knowledge of information needed to compose a risk treatment plan

Domain 5: Information security risk communication, monitoring and improvement

Main objective: Ensure that the candidate can apply processes for information security risk communication, consultation, monitoring and review based on ISO/IEC 27005:2018

Competencies	Knowledge statements
1. Ability to comprehend and evaluate requirements of information security risk communication objectives 2. Ability to understand the importance of a good communication 3. The ability to establish an efficient internal communication within the organization 4. Ability to establish an efficient communication with the external stakeholders 5. Ability to ensure communication and consultation between the decision-makers and external & internal stakeholders 6. Ability to establish a risk communication plan 7. Ability to record the information security risk management decisions and activities 8. Ability to monitor and review the risk management process, risks and controls 9. Ability to ensure continual improvement of the risk management program	1. General knowledge of the information security communication process 2. Knowledge of the principles of an efficient communication strategy 3. Knowledge of establishing internal communication within the organization 4. Knowledge of establishing external communication with stakeholders 5. Knowledge of communication activities 6. Knowledge of monitoring and review of specific elements of risk factors 7. Knowledge of monitoring and review of risk management 8. Knowledge of setting continual improvement objectives 9. Knowledge of ensuring risk management recording

Domain 6: Information security risk assessment methodologies

Main objective: Ensure that the candidate can use other risk assessment methodologies such as OCTAVE, MEHARI, EBIOS and Harmonized Threat and Risk Assessment (TRA) Method

Competencies	Knowledge statements
1. Ability to understand the three OCTAVE versions: the original OCTAVE, OCTAVE-S, and OCTAVE-Allegro 2. Ability to implement the results from OCTAVE-S process performed in three phases 3. Ability to conduct a risk assessment using the OCTAVE Allegro process following its eight steps 4. Ability to understand the relationship between OCTAVE Allegro & ISO/IEC 27005 5. Ability to conduct a risk assessment using the MEHARI method and its four phases 6. Ability to conduct a risk assessment using the EBIOS methodology and its five modules 7. Ability to interpret the application of ISO/IEC 27005:2018 in EBIOS 8. Ability to conduct a risk assessment using the Harmonized Threat and Risk Assessment (TRA) method and its five phases	1. General knowledge of the three phases of the original OCTAVE method 2. Knowledge of building asset based threat profiles, identifying infrastructure vulnerabilities, and developing security strategy and plans as specified in the OCTAVE-S method 3. Knowledge of the OCTAVE-Allegro roadmap 4. Knowledge of the similarities and differences between OCTAVE Allegro & ISO/IEC 27005:2018 5. Knowledge of the four phases of the MEHARI approach 6. Knowledge of the five modules of EBIOS risk assessment methodology 7. Knowledge of the relationship between EBIOS & ISO/IEC 27005:2018 8. Knowledge of the five phases of Harmonized Threat and Risk Assessment (TRA) methodology

4 ISO/IEC 27005:2018 Examination Development

The job analysis results were utilized to delineate the test specifications for the ISO/IEC 27005 credentials. By using the data collected through this survey process, PECB ensured that the certification examinations reflected the current practice of the field.

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 27005 Risk Manager 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 27005 Risk Manager Certification

Education: At least secondary education
The candidate needs to have completed a minimum of secondary education.

Exam: PECB Certified ISO/IEC 27005:2018 Risk Manager Exam
Candidates must pass a comprehensive examination consisting of development questions exam covering 4 domains.

Professional experience
The minimum professional experience required is:

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

Risk Management: 200 Hours
Other requirements: Signing the PECB Code of Ethics

Credential	Exam	Professional experience	Risk Management experience	Other requirements
PECB Certified ISO/IEC 27005 Risk Manager	PECB Certified ISO/IEC 27005:2018 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

5.1.3 ISO/IEC 27005 Lead Risk Manager Certification

Education: At least secondary education
The candidate needs to have completed a minimum of secondary education.

Exam: PECB Certified ISO/IEC 27005:2018 Lead Risk Manager Exam
Candidates must pass a comprehensive examination consisting of development questions exam covering 6 domains.

Professional experience
The minimum professional experience required is:

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

Risk Management: 300 Hours
Other requirements: Signing the PECB Code of Ethics

Credential	Exam	Professional experience	Risk Management experience	Other requirements
PECB Certified ISO/IEC 27005 Lead Risk Manager	PECB Certified ISO/IEC 27005:2018 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

5.2 Examination methods

Passing the Exam:

PECB will organize two exams for the grade defined previously:

1. The ISO/IEC 27005:2018 Risk Manager Exam
2. The ISO/IEC 27005:2018 Lead Risk Manager Exam

The ISO/IEC 27005:2018 Risk Manager Exam is a 2h exam. The exam questions are relevant and sufficient and cover all domains defined for the "ISO/IEC 27005 Risk Manager" Certification. The exam questions are development questions.

A minimum score of 70% is required to pass the PECB Certified ISO/IEC 27005:2018 Risk Manager Exam.

The ISO/IEC 27005:2018 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 Lead Risk Manager" Certification. The exam questions are development questions.

A minimum score of 70% is required to pass the PECB Certified ISO/IEC 27005:2018 Lead Risk Manager Exam.

The evaluation grading will be according to the *Control of examination grading process* described in the **"PECB-400 Examination Process".**

5.3 Certification evaluation process

Education: All PECB certifications require the applicant to minimally hold a high school/secondary education diploma.

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 following information for each employer:

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.

5.4 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 Risk Manager 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 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. 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.

5.5.2 Certification renewal process

To be able to renew a certificate, PECB Professionals will need to demonstrate that they have maintained their certificate(s) on a yearly basis. However, they are not required to fulfill the requirements every year, but they need to have performed the required amount of CPD hours within three years certification cycle.

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 '**Renewal'** button.

5.5.3 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 'My 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

A PECB Certificate requires the payment of the maintenance fee. The annual reporting begins with the initial certification date; however, the maintenance fee for the first year is included in the certification application payment.

The annual maintenance fee can be paid online through your PECB Member Dashboard, by logging into your member dashboard (www.pecb.com/login), clicking 'My Certifications' and then the 'Submit AMF' button.

5.5.4 Upgrade of credentials

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.

5.5.5 Downgrade of credential

A PECB Certificate can be downgraded to a lower credential because of the following reasons:

- AMF has not been paid;
- CPD hours have not been submitted;
- Insufficient CPD hours have been submitted;
- Inability to provide evidences of CPD hours upon request;

5.5.6 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.

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

5.5.7 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:

- Violation of the PECB's Code of Ethics;
- Misrepresentation of the certificate of scope;
- Any other major breach of PECB requirements and 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	Annual CPD hours	3-Year/Total CPD hours
Foundation, Provisional, and Transition	**None**	**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	**20 hours**	**60 hours**
Auditor, Assessor	Hours of audit or assessment-related experience, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**20 hours**	**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	**20 hours**	**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	**20 hours**	**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	**20 hours**	**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	**30 hours**	**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	**60 hours**	**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	**30 hours**	**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	**60 hours**	**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	**30 hours**	**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	**60 hours**	**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	**30 hours**	**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	**30 hours**	**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	**30 hours**	**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	**30 hours**	**90 hours**
Master	Hours of implementation, management, or auditing-related tasks, training, private study, coaching, attendance of seminars and conferences, or other relevant activities	**90 hours**	**270 hours**

PECB

AMF Requirements

Certification	AMF (rate per year)
Foundation, Provisional and Transition	**None**
All other certifications	**$120**

6 Revision History

Version	Change description	Date
1.0	Initial release	20120323
1.1	Updated the RACI in the flowchart (page 7-9). Updated domains (page 25-27). Updated the payment of PECB maintenance fee and reporting of CPD credits (page 35).	20170421
2.0	Updated the RACI Updated Domains Updated Certification Requirements Updated Certification Renewal Process Updated payment of AMF and submission of CPDs Other cosmetic changes	20170921
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 Updated 7.1, 7.1.1, 7.1.2, Updated 7.2, 7.3, 7.4 Updated 7.4.1, 7.4.2, 7.4.3, 7.4.4, 7.4.5	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 Other updated throughout the document	2019-09-10
2.4	Reviewed by CAS: Updated the process flowchart Updated the scheme committee members	2020-10-30
2.5	Reviewed by CS: Added reference validation, and surveillance methods Updated scheme committee members Registered the document as policy	2021-08-18
2.6	Reviewed by CS: Added the ISO/IEC 27005 Lead Risk Manager	2021-11-24
2.7	Reviewed by AL and CD-CD based on the updated version of the standard Integrated comments from the General Scheme Advisory Board review	2023-02-06
2.8	Reviewed by CD-CD: • 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 CD-CD: • Updated the AMF price from $100 to $120	2023-10-02

	Removed RACI table	
3.0	Reviewed by TL-CD • Updated the term PECB Surveillance Method/Surveillance Audit to CPD Verification • Updated General Scheme Advisory Board members	2023-11-14