PECB

BEYOND RECOGNITION

WHITEPAPER

ISO 27001

INFORMATION TECHNOLOGY – SECURITY TECHNIQUES
INFORMATION SECURITY – MANAGEMENT SYSTEMS - REQUIREMENTS

CONTENT

PRINCIPAL AUTHORS

Eric LACHAPELLE, PECB

Mustafe BISLIMI, PECB

INTRODUCTION

Many organizations take information security measures or controls to protect their information, information assets and business processes. However, without a formally specified information security management system (ISMS), these controls are inclined towards disorganization and disconnection, since they are mostly implemented as ad hoc temporary solutions to certain situations. The real challenge for small businesses and larger organizations is not to go beyond case by case solutions to information security vulnerabilities and incidents, but to engage in a holistic approach, which is where ISO/IEC 27001:20013 comes in.

Organizations of any size and type, regardless whether they are involved directly or indirectly in information technology, should engage in a preventive, protective, preparatory, and mitigation process. It is not sufficient to simply draft a response plan that anticipates and minimizes the consequences of information security incidents; thus, organizations need to take adaptive and proactive measures in order to reduce the probability of such an event.

Information security, as specified in ISO 27001, is critical in adding value to current quality systems in any organization, to identify and manage threats and vulnerabilities of prioritized information assets and to additionally increase trust by the incorporation of interested parties. It also allows independent audits or reviews to be conducted in relation to those processes.

ISO/IEC 27001:2013 is developed with the intent to help organizations improve their information security and minimize the risk of business disruptions. This standard crowns earlier partial attempts by other standards, which contributed to the Information Security Management, such as BSS 7799, COBIT, ITIL, PCIDSS, SOX, COSO, HIPAA, FISMA, and FIPS.

The Cost of Information Security Breaches

According to the '2014 Information Security Breaches Survey' in UK alone, the overall cost of security breaches for all types of organizations has increased from the past year (small organizations had an average cost of recovering from £ 35,000 to £ 65,000; whereas large organizations £ 850,000).

10% of organizations that suffered a breach in the last year were so badly damaged by the attack that they had to change the nature of their business.

.

AN OVERVIEW OF ISO 27001:2013

ISO 27001 specifies the requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a management system, as well as prepare, respond and deal with the consequences of information security incidents which are likely to happen.

ISO/IEC 27001:2013 is intended to bring information security under a formally specified management control. It has more than one hundred specific requirements.

The requirements set in ISO 27001 are generic, flexible and useful to all types of organizations. Thus, this ISO Standard, being a Management System, can be aligned with other Management Systems such as Quality Management, Business Continuity Management and other management systems due to their similar structure.

What is Information Security Management System?

An ISMS is part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

Key clauses of ISO 27001:2013

ISO 27001 is organized into the following main clauses:

Clause 4: Context of the organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement

Each of these key activities is listed and described below.

CLAUSE 4: CONTEXT OF THE ORGANIZATION

UNDERSTANDING THE ORGANIZATION AND ITS CONTEXT

External and internal issues shall be determined that are relevant to the organization's purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES

The organization shall determine interested parties that are relevant to the information security management system and the requirements of these interested parties relevant to information security.

DETERMINING THE SCOPE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

INFORMATION SECURITY MANAGEMENT SYSTEM

Based on the monitoring results, the organization needs to implement the identified improvements, communicate them to all the interested parties with sufficient details, and ensure that the improvements achieve their intended objectives.

To establish an ISMS the organization needs to define the ISMS which includes the following steps:

Important stages	Issues to consider when establishing an ISMS
Scope	Based on business characteristics, location, assets and technology, and justifications for any exclusion from scope
Risk assessment approach	1. Risk assessment methodology, and business information security, legal and regulatory requirements 2. Criteria for accepting risks, and acceptable risks levels
Risk identification	1. Asset identification and asset owner identification 2. Threats to those assets 3. Vulnerabilities 4. Impact of loss of confidentiality , integrity and availability
Risk analysis and evaluation	1. Business impacts assessment 2. Realistic likelihood assessment considering the threats and vulnerabilities 3. Risk level estimation 4. Risk acceptability or treatment, depending on the risk acceptance criteria
Risk treatment option	1. Application of appropriate controls 2. Objective risk acceptance in accordance with the organization's policies 3. Risk avoidance 4. Risk transfer to other parties (insures, suppliers)
Control objectives and controls for the treatment of risks	1. Selection and implementation of controls based on the requirements identified by the risk assessment and treatment process. 2. Selection of controls from Annex A of ISO 27001 when appropriate, to cover the risk assessment and treatment process. 3. Additional controls may be selected outside of Annex A

CLAUSE 5: LEADERSHIP

LEADERSHIP AND COMMITMENT: Top management shall demonstrate leadership and commitment with respect to the information security management system by:

- Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
- Ensuring the integration of the information security management system requirements into the organization's processes;
- Ensuring that the resources needed for the information security management system are available;
- Communicating the importance of effective information security management and of conforming to the information security management system requirements;
- Ensuring that the information security management system achieves its intended outcome(s);
- Directing and supporting persons to contribute to the effectiveness of the information security management systems;
- Promoting continual improvement; and
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

POLICY: Top management shall establish an information security policy that:

- Is appropriate to the purpose of the organization;
- Includes information security objectives or provides the framework for setting information security objectives;
- Includes a commitment to satisfy applicable requirements related to information security; and
- Includes a commitment to continual improvement of the information security management system.

The information security policy shall:

- Be available as documented information.
- Be communicated within the organization; and
- Be available to interested parties, as appropriate.

ORGANIZATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES:
Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:
- Ensuring that the information security management system conforms to the requirements of this International Standard; and
- Reporting on the performance of the information security management system to top management.

CLAUSE 6: PLANNING

When planning for the information security management system, the organization shall consider the issues and the requirements referred in the standard and determine the risks and opportunities that need to be addressed to:
- Ensure the information security management system can achieve its intended outcome(s);
- Prevent, or reduce, undesired effects; and
- Achieve continual improvement.

The organization shall plan:
- Actions to address these risks and opportunities; and
- How to:
    - Integrate and implement the actions into its information security management system processes;
    - Evaluate the effectiveness of these actions.

CLAUSE 7: SUPPORT

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system, such as:

- Competence,
- Awareness,
- Communication, and
- Documented information.

CLAUSE 8: OPERATION

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in the standard. The organization shall perform information security risk assessments at planned intervals, and shall also implement the information security risk treatment plan.

CLAUSE 9: PERFORMANCE EVALUATION

The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organization's own requirements and to the International Standard requirements.

CLAUSE 10: IMPROVEMENT

Improvement of ISMS consists of corrective actions. They should fulfill the requirements as listed in the table below:

Corrective action Requirements
Identifying
Determing the causes of nonconformities
Evaluating the need for actions to ensure that the nonconformities are not repeated
Determining and implementing the corrective action needed
Recording results of the action taken
Reviewing of the corrective action taken

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

LINK BETWEEN ISO 27001 AND OTHER INFORMATION SECURITY STANDARDS AND GUIDELINES

The following standards that relate to information security are:

- OECD Principles (2002)
- PCI-DSS - Payment Card Industry Data Security Standard (2004)
- Basel II (2004)
- COBIT – Control Objectives for Business and related Technology (1994+)
- ITIL – Information Technology Infrastructure Library (1980+)

LINK WITH ISO 22301 – BUSINESS CONTINUITY

The ISO 27001 International Standard is useful as part of the certification process against ISO 22301 (Business Continuity). The ISO 27001 objectives in clause A.14 (Business Continuity Management) can be used to comply with ISO 22301.

- To implement and execute a risk assessment, an organization could refer to ISO/IEC 27005:2011, or in a broader context to ISO 31000:2009 – Risk management – Principles and guidelines.
- To execute the assessment itself, an organization could refer to ISO 31010:2009 – Risk management – Risk assessment techniques.

ISO 22301 Requirements	***A.14.1 Information security aspects of business continuity management*** *Objective:* To counteract interruptions to business activities, protect critical business processes from the effects of major failures of information systems, or disasters, and ensure their timely resumption.		
4.4 Business continuity management system	A.14.1.1	Including information security in the business continuity management process	*Control* A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
8.2 BIA and Risk assessment	A.14.1.2	Business continuity and risk assessment	*Control* Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security
8.4 Business continuity procedures	A.14.1.3	Developing and implementing continuity plans including information security	*Control* Plans shall be developed and implemented to maintain or restore operations, and ensure the availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
6 Planning the BCMS	A.14.1.4	Business continuity planning framework	***Control*** The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
8.5 Exercising and testing	A.14.1.5	Testing, maintaining and reassessing Business continuity plans	***Control*** Business continuity plans shall be tested and updated regularly to ensure that they are effective and up to date. .

INTEGRATION WITH OTHER MANAGEMENT SYSTEMS

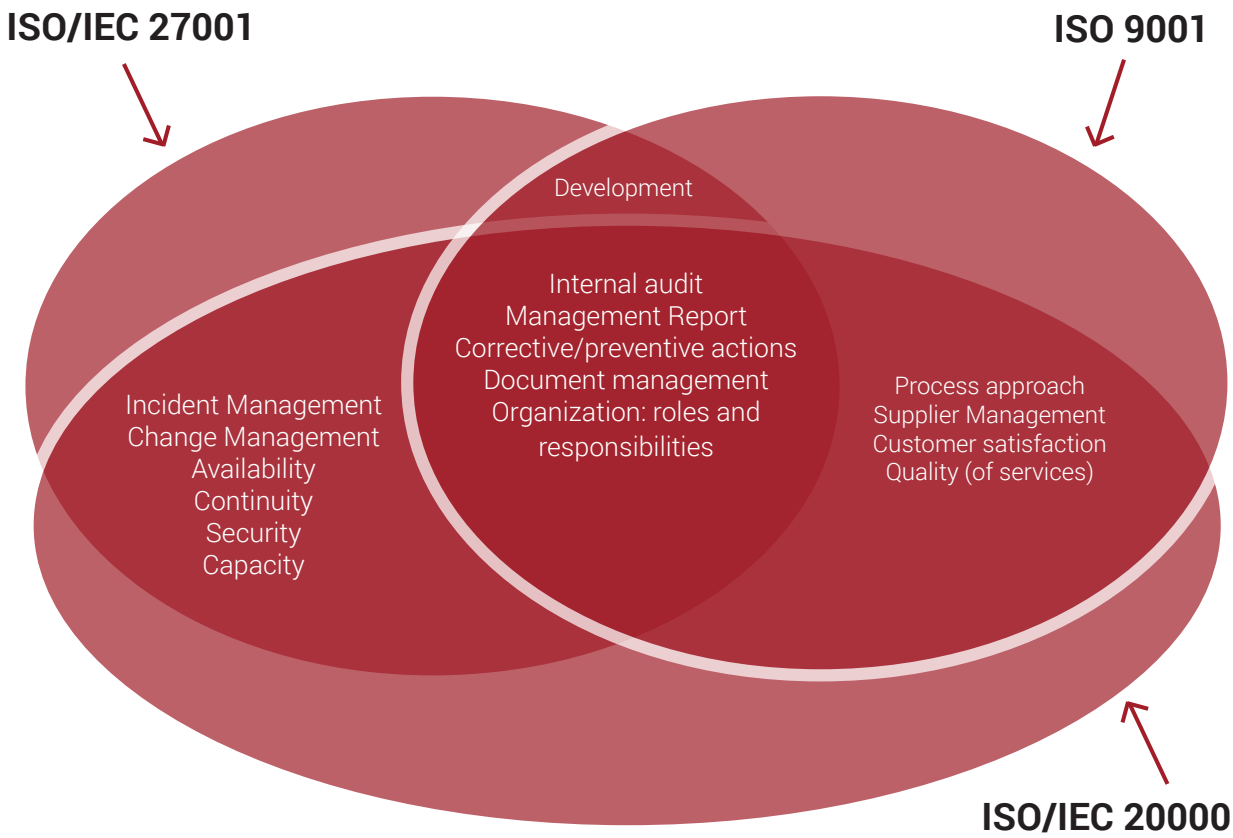
The general requirements are ordinarily identified in every management system. These requirements assist in:

- determining and applying objectives according to the organization's habits and needs;
- upholding the objectives based on strong management commitment by monitoring and reviewing;
- documenting pertinent management system processes;
- regular 'health-checks' via internal or external audits;
- and gaining benefits through continual improvement as achieved by a regular management review.

In addition, the table below presents the general requirements of several standards, which also serves as a comparing tool between ISMS and other management systems. This will authorize the organization to envision "combined audits" in order to achieve their compliance goals with adequate effort and budget.

Requirements	ISO 9001:2008	ISO 14001:2004	ISO 20000:2011	ISO 22301:2012	ISO 27001:2013
Objectives of the management system	5.4.1	4.3.3	4.5.2	6.2	4.2.1
Management commitment	5.1	4.4.1	4.1	5.2	5
Documentation requirements	4.2	4.4	4.3	7.5	4.3
Internal audit	8.2.2	4.5.5	4.5.4.2	9.2	6
Continual improvement	8.5.1	4.5.3	4.5.5	10	8
Management review	5.6	4.6	4.5.4.3	9.3	7

The diagram below shows how the contents of a few important standards are related:



INFORMATION SECURITY MANAGEMENT – THE BUSINESS BENEFITS

As with all the major undertakings within an organization, it is essential to gain the backing and sponsorship of the executive management. By far, the best way to achieve this is to illustrate the positive gains of having an effective information security management process in place, rather than highlight the negative aspects of the contrary.

Today an effective information security management is not about being forced into taking action to address external pressures, but its importance relies on recognizing the positive value of information security when good practice is embedded throughout your organization.

PREDICTABLE AND EFFECTIVE RESPONSE TO INFORMATION SECURITY INCIDENTS	PROTECTION OF PEOPLE	MAINTENANCE OF VITAL ACTIVITIES OF THE ORGANIZATION	BETTER UNDERSTANDING OF THE ORGANIZATION
COST REDUCTION	RESPECT OF THE INTERESTED PARTIES	PROTECTION OF THE REPUTATION AND BRAND	CONFIDENCE OF CLIENTS
COMPETITIVE ADVANTAGE	LEGAL COMPLIANCE	REGULATORY COMPLIANCE	CONTRACT COMPLIANCE

The adoption of an effective information security management process within an organization will have benefits in a number of areas, examples of which include:

1.Protection of shareholder value;
2.Increase confidence in the organization from interested parties;
3.Good governance;
4.Conformity;
5.The implications for information security legislation and duties of care can be correctly considered;
6.Avoidance of liability actions;
7.Cost reduction;
8.Improved overall security; and
9.Marketing;

IMPLEMENTATION OF A SCSMS WITH IMS2 METHODOLOGY

Considering the well documented benefits of implementing an Information Security Management System based on ISO 27001, makes the proposal easier to decide on.

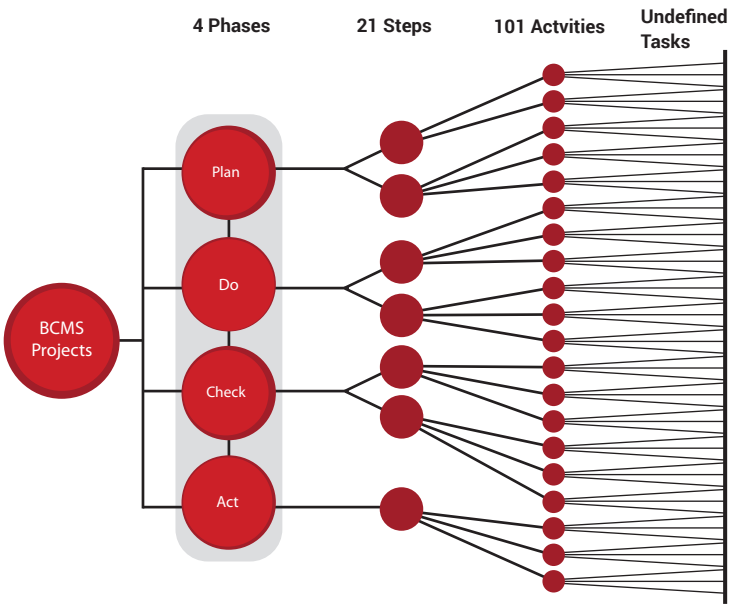
Most companies now realize that it is not sufficient to implement a generic, “one size fits all” security plan. For an effective response, with respect to maintaining the information security system, such a plan must be customized to fit to a company. A more difficult task is the compilation of an implementation plan that balances the requirements of the standard, the business needs and the certification deadline.

There is no single blueprint for implementing ISO 27001 that will work for every company, but there are some common steps that will allow you to balance the frequent conflicting requirements and prepare you for a successful certification audit.

PECB has developed a methodology (please see example below) for implementing a management system; the “Integrated Implementation Methodology for Management Systems and Standards (IMS2)”, and it is based on applicable best practices. This methodology is based on the guidelines of ISO standards and also meets the requirements of ISO 27001.

1. Plan	2. Do	3. Check	4. Act
1.1 Initiating the SMS	2.1 Organizational strategy	3.1 Monitoring, Measurement, Analysis and Evaluation	4.1 Treatment of Non-conformities
1.2 Understanding the organization	2.2 Document Management	3.2 Internal Audit	4.2 Continuous Improvement
1.3 Analyze the existing System	2.3 Design of Controls and Procedures	3.3 Management Review	
1.4 Leadership and Project Approval	2.4 Communication		
1.5 Scope	2.5 Awareness and Training		
1.6 Security Policy	2.6 Implementation of Controls		
1.7 Risk Assessment	2.7 Incident Management Review		
1.8 Statement of Applicability	2.8 Operations Management		

IMS2 is based on the PDCA cycle which is divided into four phases: Plan, Do, Check and Act. Each phase has between 2 and 8 steps for a total of 21 steps. In turn, these steps are divided into 101 activities and tasks. This 'Practical Guide' considers the key phases of the implementation project from the starting point to the finishing point and suggests the appropriate 'best practice' for each one, while directing you to further helpful resources as you embark on your ISO 27001 journey.



The sequence of steps can be changed (inversion, merge). For example, the implementation of the management procedure for documented information can be completed before the understanding of the organization. Many processes are iterative because of the need for progressive development throughout the implementation project; for example, communication and training.

By following a structured and effective methodology, an organization can be sure it covers all minimum requirements for the implementation of a management system. Whatever methodology used, the organization must adapt it to its particular context (requirements, size of the organization, scope, objectives, etc...) and not apply it like a cookbook.

CERTIFICATION OF ORGANIZATIONS

The following common processes for an organization that wishes to be certified against ISO 28000 are:

1. Implementation of the management system: Before being audited, a management system must be in operation for some time. Usually, the minimum time required by the certification bodies is 3 months.

2. Internal audit and review by top management: Before a management system can be certified, it must have had at least one internal audit report and one management review.

3. Selection of the certification body (registrar): Each organization can select the certification body (registrar) of its choice.

4. Pre-assessment audit (optional): An organization can choose to perform a pre-audit to identify any possible gap between its current management system and the requirements of the standard.

5. Stage 1 audit: A conformity review of the design of the management system. The main objective is to verify that the management system is designed to meet the requirements of the standard(s) and the objectives of the organization. It is recommended that at least some portion of the Stage 1 audit should be performed on-site at the organization's premises.

6. Stage 2 audit (On-site visit): The Stage 2 audit objective is to evaluate whether the declared management system conforms to all requirements of the standard is actually being implemented in the organization and can support the organization in achieving its objectives. Stage 2 takes place at the site(s) of the organization's sites(s) where the management system is implemented.

7. Follow-up audit (optional): If the auditee has non-conformities that require additional audit before being certified, the auditor will perform a follow-up visit to validate only the action plans linked to the non-conformities (usually one day).

8. Confirmation of registration: If the organization is compliant with the conditions of the standard, the Registrar confirms the registration and publishes the certificate.

9. Continual improvement and surveillance audits: Once an organization is registered, surveillance activities are conducted by the Certification Body to ensure that the management system still complies with the standard. The surveillance activities must include on-site visits (at least 1/year) that allow verifying the conformity of the certified client's management system and can also include: investigations following a complaint, review of a website, a written request for follow-up, etc.

TRAINING AND CERTIFICATIONS OF PROFESSIONALS

PECB has created a training roadmap and personnel certification schemes which is strongly recommended for implementers and auditors of an organization that wish to get certified against ISO 27001. Whereas certification of organizations is a vital component of the information security field as it provides evidence that organizations have developed standardized processes based on best practices. Certifications of individuals serve as documented evidence of professional competencies and experience for/of those individuals that have attended one of the related courses and exams.

It serves to demonstrate that a certified professional holds defined competencies based on best practices. It also allows organizations to make intelligent choices of employee selection or services based on the competencies that are represented by the certification designation. Finally, it provides incentives to the professional to constantly improve his/her skills and knowledge and serves as a tool for employers to ensure that training and awareness have been effective.

PECB training courses are offered globally through a network of authorized training providers. They are available in several languages and include introduction, foundation, implementer and auditor courses.
The table below gives a short description relating PECB's official training courses for information security management system based on ISO 27001..

Training title	Short description	Who should attend?
ISO 27001 Introduction	• One day training • Introduction to concepts management and implementation of an ISMS • Do not lead to certification	• IT Professionals • Staff involved in the implementation of an ISMS • IT Expert advisors • Managers responsible for implementing an ISMS • Auditors
ISO 27001 Foundation	• A two day training • Become familiar with best practices for implementation and management of ISMS • One hour exam	• Members of an information security team • IT Professionals • Staff involved in ISMS • Technicians • Auditors
ISO 27001 Lead Implementer	• A five day training • Manage the implementation and a management of an ISMS • Three hours exam	• Project managers and/or consultants • Information security auditors • Members of an information security team • Technical experts
ISO 27001 Lead Auditor	• A five day training • Manage the audit of an ISMS • Three hours exam	• Internal auditors • Auditors • Project managers and/or consultants • Members of an information security team • Technical experts

Although a specified set of courses or curriculum of study is not required as part of the certification process, the completion of a recognized PECB course or program of study will significantly enhance your chance of passing a PECB certification examination. The list of approved organizations that offer PECB official training sessions is found on our website http://pecb.com/partnerEvent/event_schedule_list.

CHOOSING THE RIGHT CERTIFICATION

The ISO 27001 Foundation certification is a professional certification for professionals in need of gaining an overall understanding of the ISO 27001 standard and its requirements.

The ISO 27001 Lead Implementer certifications are professional certifications for professionals needing to implement ISMS and, in case of the ISO 27001 Lead Implementer Certification, manage an implementation project.

The ISO 27001 Auditor certifications are credentials for professionals needing to audit an ISMS and, in case of the "ISO 27001 Lead Auditor" Certification, needing to manage a team of auditors.

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

Based on your overall professional experience and acquired qualifications, you will be granted one or more of these certifications based on projects or audits activities you have performed in the past, or you are currently working on.

Certification	Exam	Professional experience	Audit experience	Project experience
Foundation	Foundation Exam	None	None	None
Provisional Implementer	Lead Implementer Exam	**Two years** One year of work experience in the field of certification	None	Project activities totaling 200 hours
Lead Implementer	Lead Implementer Exam	**Five years** Two years of work experience in the field of certification	None	Project activities totaling 300 hours
Provisional Auditor	Lead Auditor Exam	None	None	None
Auditor	Lead Auditor Exam	**Two years** One year of work experience in the field of certification	Audit activities totaling 200 hours	None
Lead Auditor	Lead Auditor Exam	**Five years** Two years of work experience in the field of certification	Audit activities totaling 300 hours	None
Master	Lead Auditor Exam Lead Implementer Exam	**Ten years** Two years of work experience in the field of certification	Audit activities totaling 500 hours	Project activities totaling 500 hours

PECB

+1-844-426-7322

customer@pecb.com

Customer Service