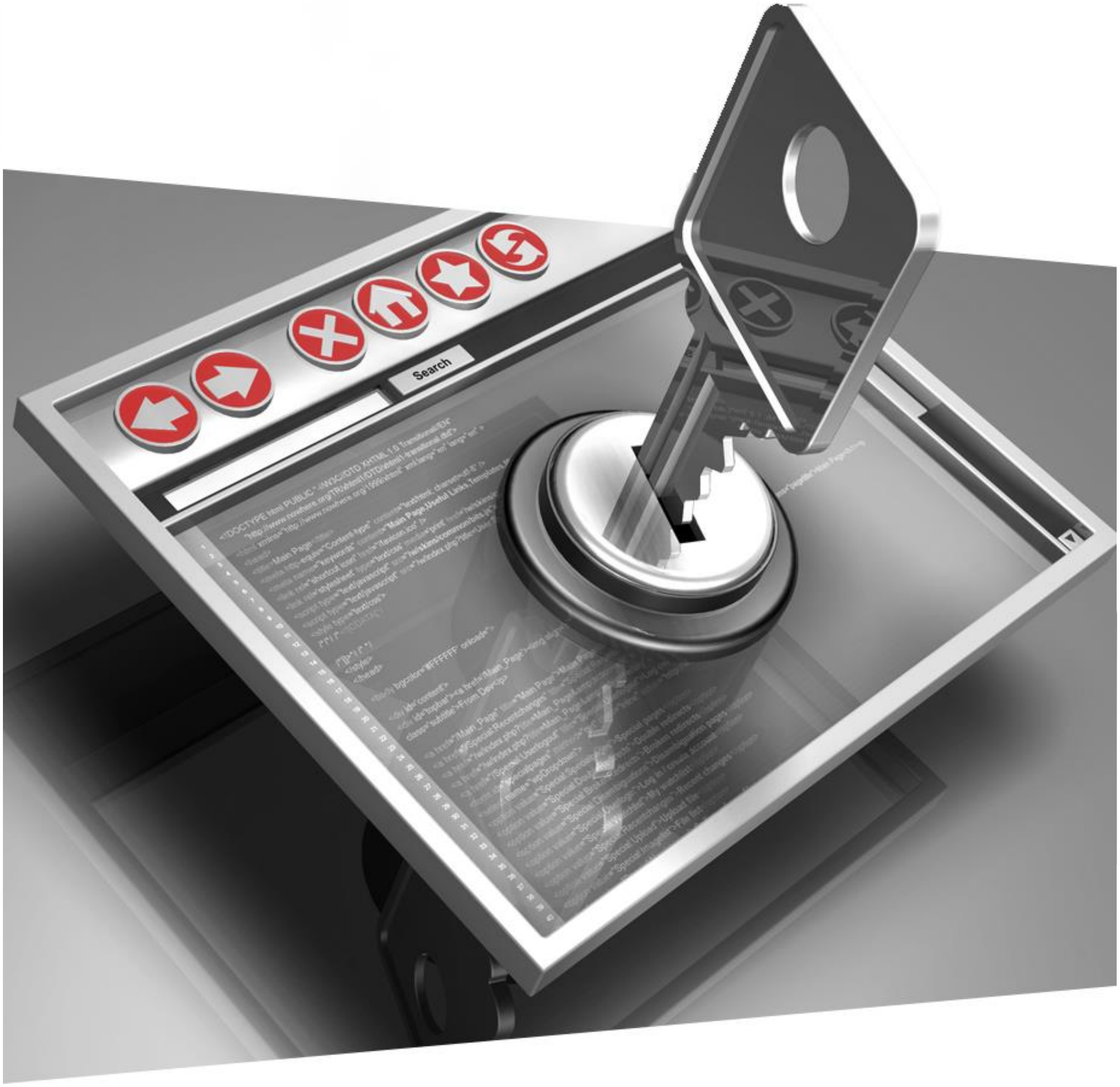
PECB

When Recognition Matters



EXAM PREPARATION GUIDE

PECB Certified ISO/IEC 27034 Lead Application Security Implementer

The objective of the “PECB Certified ISO/IEC 27034 Lead Application Security Implementer” examination is to ensure that the candidate has the knowledge and skills to support an organization in implementing and managing an Information Technology Application Security (AS) based on ISO/IEC 27034:2011.

The target population for this examination is:

- Project managers or consultants wanting to prepare and to support an organization in the implementation of an Application security
- Application security auditors who wish to fully understand the Application security implementation process
- Managers responsible for Application security or conformity
- Provisioning and operation teams of an Application security team
- Expert advisors in Application security System
- Technical experts wanting to prepare for an Application security function or for an project management function

The exam content covers the following domains:

- Domain 1: Fundamental concepts and principles in Application Security
- Domain 2: Application Security Control Best Practice based on ISO 27002
- Domain 3: Planning an AS based on ISO/IEC 27034
- Domain 4: Implementing an AS based on ISO/IEC 27034
- Domain 5: Performance evaluation, monitoring and measurement of an AS based on ISO/IEC 27034
- Domain 6: Continual improvement of an AS based on ISO/IEC 27034
- Domain 7: Preparation for an AS certification audit

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts in Application Security

Main objective: To ensure that the ISO/IEC 27034 Lead Application Security Implementer candidate can understand, interpret and illustrate the main Application Security concepts related to an Information technology Application security (AS)

Competencies	Knowledge statements
1. Understand and explain the operations of the ISO organization and the development of Application Security standards 2. Ability to identify, analyze and evaluate the Application Security compliance requirements for an organization 3. Ability to explain and illustrate the main concepts in Application Security and Application Security risk management	1. Knowledge of the management principles to Application Security 2. Knowledge of the main standards in Application Security 3. Knowledge of the application of the seven ISO management principles and their relationship to the Application Security. 4. Knowledge of the different sources of Application Security requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies 5. Knowledge of the main Application Security concepts and terminology as described in ISO/IEC 27034

Domain 2: Application Security Control Best Practice based on ISO/IEC 27034

Main objective: To ensure that the ISO/IEC 27034 Lead Application Security Implementer candidate can understand, interpret and provide guidance on how to implement and manage Application Security controls best practices based on ISO/IEC 27034

Competencies	Knowledge statements
1. Understand and explain the components of an Application security based on ISO/IEC 27034 and its principal processes 2. Ability to interpret and analyze ISO/IEC 27034 concepts and core subjects 3. Understand, explain and illustrate the main steps to establish, implement, operate, monitor, review, maintain and improve an organization's AS	1. Knowledge of the concepts, principles and terminology related to Application security 2. Knowledge of the principal characteristics 3. Knowledge of the main advantages of following guidance on application security 4. Knowledge of the ISO/IEC 27034 concepts 5. Knowledge of the main steps to establish the AS and security policies, security objectives, processes and procedures relevant to managing risk and improving Application Security to deliver results in accordance with an organization’s overall policies and objectives (Awareness level) 6. Knowledge of AS overview and core subjects

Domain 3: Planning an AS based on ISO/IEC 27034

Main objective: To ensure that the ISO/IEC 27034 Lead Application Security Implementer candidate can plan the implementation of an AS in accordance with ISO/IEC 27034 guidelines

Competencies	Knowledge statements
1. Ability to manage an AS implementation project following project management best practices 2. Ability to gather, analyze and interpret the necessary information to plan the AS implementation 3. Ability to observe, analyze and interpret the external and internal environment of an organization 4. Ability to perform a gap analysis and clarify the Application Security objectives of an organization 5. Ability to state and justify an AS scope adapted to the security objectives of a specific organization 6. Ability to select and justify the selected approach and methodology adapted to the needs of the organization	1. Knowledge of the main project management concepts, terminology, process and best practices 2. Knowledge of the principal approaches and methodology frameworks to implement an AS 3. Knowledge of the main concepts and terminology related to organizations 4. Knowledge of an organization's external and internal environment 5. Knowledge of the main interested parties related to an organization and their characteristics 6. Knowledge of techniques to gather information on an organization 7. Knowledge of the characteristics of an AS scope in terms of organizational, technological and physical boundaries

Domain 4: Implementing an AS based on ISO/IEC 27034

Main objective: To ensure that the ISO/IEC 27034 Lead Application Security Implementer candidate can implement the processes and security controls of an AS as per ISO/IEC 27034

Competencies	Knowledge statements
1. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of an AS 2. Ability to define the document and record management processes needed to support the implementation and the operations of an AS 3. Ability to define and design processes and document them 4. Ability to define and write an AS policy and Application Security policies & procedures 5. Ability to implement the required processes and security controls of an AS 6. Ability to define and implement appropriate Application Security training, awareness and communication plans 7. Ability to transfer an AS project to operations and manage the change management process	1. Knowledge of the roles and responsibilities of the key actors during the implementation of an AS and in its operation after the end of the implementation project 2. Knowledge of the main organizational structures applicable for an organization to manage Application Security 3. Knowledge of the best practices on document and record management processes and the document management life cycle 4. Knowledge of the characteristics and the differences between the different documents related to AS: policy, procedure, guideline, standard, baseline, worksheet, etc. 5. Knowledge of model-building controls and processes techniques and best practices 6. Knowledge of techniques and best practices to write Application Security policies, procedures and others types of documents include in an AS 7. Knowledge of the characteristics and the best practices to implement Application Security training, awareness and communication plans 8. Knowledge of change management techniques best practices

Domain 5: Performance evaluation, monitoring and measurement of an AS based on ISO/IEC 27034

Main objective: To ensure that the ISO/IEC 27034 Lead Application Security Implementer candidate can evaluate, monitor and measure the performance of an AS as required by the ISO/IEC 27034 guidelines

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of an AS 2. Ability to verify the extent to which identified security requirements have been met 3. Ability to define and implemented an internal audit program for ISO/IEC 27034 4. Ability to perform regular and methodical reviews regarding the suitability, adequacy, effectiveness and efficiency of an AS with policies and security objectives of an organization 5. Ability to define and implement a management review process and counsel management on it	1. Knowledge of the techniques and best practices to monitor the effectiveness of an AS 2. Knowledge of the main concepts and components related to an Application Security Measurement Programme: measures, attributes, indicators, dashboard, etc. 3. Knowledge of the characteristics and the differences between an operational, tactical and strategic Application Security indicators and dashboard 4. Knowledge of the techniques and methods to define and document an adequate and reliable indicators 5. Knowledge of the main concepts and components related to the implementation and operation of an AS internal audit program 6. Knowledge of the best practices on how to perform management reviews

Domain 6: Continuous improvement of an AS based on ISO/IEC 27034

Main objective: To ensure that the ISO/IEC 27034 Lead Application Security Implementer candidate can provide guidance on the continuous improvement of an AS in the context of ISO/IEC 27034

Competencies	Knowledge statements
1. Ability to understand the principle and concepts related to continual improvement 2. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of an AS 3. Ability to implement AS continual improvement processes in an organization 4. Ability to determine the appropriate business improvement tools to support continual improvement processes of a specific organization 5. Ability to identify, analyze the root-causes of nonconformities and proposed action plans to treat them 6. Ability to identify, analyze the root-cause of potential nonconformities and proposed action plans to treat them	1. Knowledge of the main concepts related to continual improvement 2. Knowledge of the characteristics and the difference between the concept of effectiveness and the efficiency 3. Knowledge of the concept and techniques to perform a benchmarking 4. Knowledge of the main processes, tools and techniques used by professionals 5. Knowledge of the characteristics and the difference between corrective actions and preventive actions 6. Knowledge of the main processes, tools and techniques used by professionals to develop and propose the best corrective and preventive action plans

Domain 7: Preparation for an audit

Main objective: To ensure that the ISO/IEC 27034 Lead Application Security Implementer candidate can prepare and assist an organization for the audit of an AS against the ISO/IEC 27034 standard

Competencies	Knowledge statements
1. Ability to understand the main steps, processes and activities related to ISO/IEC 27034 2. Ability to understand, explain and illustrate the audit evidence approach in the context of an ISO/IEC 27034 3. Ability to review the readiness of an organization for the ISO/IEC 27034 assessment 4. Ability to coach and prepare the personnel of an organization for the ISO/IEC 27034 assessment 5. Ability to argue and challenge the audit findings and conclusions with auditors	1. Knowledge of the evidence based approach in an audit 2. Knowledge of the different types of evidences in the context of ISO/IEC 27034 3. Knowledge of follow-up audit requirements, steps and activities 4. Knowledge of preparing the personnel for the ISO/IEC 27034 assessment 5. Knowledge of the readiness of an organization for an ISO/IEC 27034 audit 6. Knowledge of the concepts and core subjects and best practice to develop action plans following the ISO/IEC 27034 review

Based on these 7 domains and their relevance, 21 questions are included in the exam, as summarized in the following table:

			Level of Understanding (Cognitive/Taxonomy) Required					
		Points per Question	Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points per competency domain
Competency/Domains	Fundamental principles and concepts in Application Security	15	X		3	14.29	35	17.94
		18	X					
		2	X					
	Application Security Control Best Practice based on ISO 27034	5	X		3	14.29	20	10.28
		10		X				
		5	X					
	Planning an AS based on ISO 27034	20		X	3	14.29	35	17.94
		5	X					
		10		X				
	Implementing an AS based on ISO 27034	15		X	3	14.29	35	17.94
		10		X				
		10	X					
	Performance evaluation, monitoring and measurement of an AS based on ISO 27034	5		X	3	14.28	15	7.69
		5	X					
		5		X				
	Continual improvement of an AS based on ISO 27034	15		X	3	14.28	30	15.39
		10	X					
		5	X					
	Preparing for an AS audit	5		X	3	14.28	25	12.82
		5	X					
		15		X				
Total points		195						
Number of Questions per level of understanding			11	10				
% of Test Devoted to each level of understanding (cognitive/taxonomy)								

The passing score is established at **70%.**

After successfully passing the exam, candidates will be able to apply for the credentials of PECB Certified ISO/IEC 27034 Lead Application Security Implementer, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is three (3) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be "open book" and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are "open book"; candidates are authorized to use the following reference materials:

- A copy of the ISO/IEC 27034:2011 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limitation on how many times a candidate can retake the same exam. However, there are some limitations in terms of allowed time-frame in between exams.

When candidates fail the examination, they are only allowed to retake the examination once within 12 months after the first attempt. If second examination is unsuccessful, candidates will be allowed to retake the exam only after 1 year (12 months). Retake fee applies.

Only candidates, who have completed a full PECB training but fail the written exam, are eligible to retake the exam for free, under one condition:

"A candidate can only retake the exam once and this retake must occur within 12 months from the initial exam's date."

When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of

PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. Security controls

For each of the following clauses of the ISO/IEC 27034 standard, please provide an action plan with at least two concrete actions that would be acceptable to ensure conformity to the clause and satisfy the control objectives.

- Clause 6.5.3 Threats to applications

Possible answers:

- *Process of evidence collection for the applications*
- *Use of anti-virus application to prevent threat for applications.*

2. Development of information security indicators

For each of the following clauses of the ISO/IEC 27034 standard, please provide two examples of metrics that would be acceptable to measure the conformity to the clause.

- ***8.1. Organization Normative Framework***

Possible answers:

- *ONF meetings completed to date*
- *Average participation rates in ONF meetings to date*

3. Classification of controls

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

- Clause 8.1.2.7.2 “Application provisioning management”

Possible answers:

- *Preventive control: it will prevent unauthorized access to offices*
- *Managerial measure: managing the process of applications*

4. Recommendations

The management of the organization would like to receive recommendations from you to improve the processes in place to comply with the requirements of ISO/IEC 27034 on change management.

Possible answers:

1. Document and implement formal change control procedures (documentation, specification, testing, quality control and implementation).
2. This process should provide a risk assessment, impact analysis of the change and a specification of required security controls.
3. Maintain a change log with records of the approvals.
4. Communicating the new process and organize training session.