When Recognition Matters

# EXAM PREPARATION GUIDE

## PECB Certified ISO/IEC 27034 Lead Auditor

The objective of the “PECB Certified ISO/IEC 27034 Lead Auditor” examination is to ensure that the candidate has the knowledge and skills to plan and perform an Application Security (AS) audit compliant with the ISO/IEC 27034:2011 standard, master audit principles and techniques, and manage (or be part of) audit teams and audit programs.

The target population for this examination is:

- Auditors wanting to perform and lead an Application security
- Project managers or consultants wanting to master the Application security and audit process
- Persons responsible for the Application security or conformity in an organization
- Members of an Application security team
- Expert advisors in Application security
- Technical experts wanting to prepare for an Application security audit function

The exam content covers the following domains:

- Domain 1: Fundamental principles and concepts in Application Security
- Domain 2: Information Technology Application Security (AS)
- Domain 3: Fundamental Audit Concepts and Principles
- Domain 4: Preparation of an ISO/IEC 27034 audit
- Domain 5: Conduct of an ISO/IEC 27034 audit
- Domain 6: Conclusion and follow-up of an ISO/IEC 27034 audit
- Domain 7: Management of an ISO/IEC 27034 audit program

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 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<br>2. Ability to identify, analyze and evaluate the Application Security compliance requirements for an organization<br>3. Ability to explain and illustrate the main concepts in Application Security and Application Security risk management<br>4. Ability to understand relationship between different standards | 1. Knowledge of the management principles to Application Security<br>2. Knowledge of the main standards in Application Security<br>3. Knowledge of the different sources of Application Security requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies<br>4. Knowledge of the main Application Security concepts and terminology as described in ISO/IEC 27034 |

## Domain 2: Information technology Application security (AS)

**Main objective:** To ensure that the ISO/IEC 27034 Lead Auditor candidate can understand, interpret and illustrate the main concepts and components of an Information technology Application security 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<br>2. Ability to interpret and analyze ISO/IEC 27034 concepts and core subjects<br>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 management systems<br>2. Knowledge of the principal characteristics<br>3. Knowledge of the main advantages of following guidance on application security<br>4. Knowledge of the ISO/IEC 27034 concepts<br>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)<br>6. Knowledge of AS overview and core subjects |

## Domain 3: Fundamental Audit Concepts and Principles

**Main objective:** To ensure that the ISO/IEC 27034 Lead Auditor candidate can understand, interpret and apply the main concepts and principles related to an AS audit in the context of ISO/IEC 27034

| Competencies | Knowledge statements |
|---|---|
| 1. Understand, explain and illustrate the application of the audit principles in the context of an ISO/IEC 27034 audit<br>2. Ability to identify and judge situations that would discredit the professionalism of the auditor and the PECB code of ethics<br>3. Ability to identify and evaluate ethical problems taking into account the obligations related to sponsors, auditee and law enforcement or regulatory authorities<br>4. Ability to explain, illustrate and apply the audit evidence approach in the context of an ISO/IEC 27034 audit<br>5. Ability to explain and compare the types and characteristics of evidence<br>6. Ability to determine and justify what type of evidence and how much evidence will be required in the context of a specific AS audit mission<br>7. Ability to determine and evaluate the level of materiality and apply the risk based approach during the different phases of an ISO/IEC 27034 audit<br>8. Ability to judge the appropriate level of reasonable assurance needed for a specific ISO/IEC 27034 audit mission | 1. Knowledge of the main audit concepts and terminology<br>2. Knowledge of the differences between first party, second party and third party audit and relationship to ISO/IEC 27034<br>3. Knowledge of the following audit principles: integrity, fair presentation, due professional care, professional judgment, professional skepticism, confidentiality and independence<br>4. Knowledge of professional responsibility of an auditor and the PECB code of ethics<br>5. Knowledge of evidence based approach in an audit<br>6. Knowledge of the different types of evidences: physical, mathematical, confirmative, technical, analytical, documentary and verbal<br>7. Knowledge of quality of audit evidences (competent, appropriate, reliable and sufficient) and the factors that will influence them.<br>8. Knowledge of the risk based approach in an audit and the different types of risk related to audit activities<br>9. Knowledge of the concept of materiality and its application in an audit<br>10. Knowledge of the concept of reasonable assurance and its applicable in an audit |

## Domain 4: Preparation of an ISO/IEC 27034 audit

**Main objective:** To ensure that the ISO/IEC 27034 Lead Auditor candidate can prepare appropriately an AS audit in the context of ISO/IEC 27034

| Competencies | Knowledge statements |
|---|---|
| 1. Understand and explain the steps and activities to do to prepare an AS audit taking in consideration the specific context and conditions of the mission<br>2. Understand and explain the roles and responsibilities of the audit team leader, audit team members and technical experts<br>3. Ability to determine, evaluate and confirm the audit objectives, the audit criteria and the audit scope for a specific ISO/IEC 27034 audit mission<br>4. Ability to do a feasibility study of an audit in the context of a specific ISO/IEC 27034 audit mission<br>5. Ability to explain, illustrate and define the characteristics of the audit terms of engagement and apply the best practices to establish a first contact with an auditee in the context of a specific ISO/IEC 27034 audit mission<br>6. Ability to develop audit working papers and to elaborate appropriate audit test plans in the context of a specific ISO/IEC 27034 audit mission | 1. Knowledge of the main responsibilities of the audit team leader and audit team members<br>2. Knowledge of the roles and responsibilities of technical experts used for an audit<br>3. Knowledge of the definition of audit objectives, audit scope and audit criteria<br>4. Knowledge of the difference between the AS scope and the audit scope<br>5. Knowledge of the elements to review during the feasibility study of an audit<br>6. Knowledge of the cultural aspects to consider in an audit<br>7. Knowledge of the characteristics of audit terms of engagement and the best practices to establish a first contact with an auditee<br>8. Knowledge of the preparation of an audit plan<br>9. Knowledge of the preparation and development of audit working paper<br>10. Knowledge of advantages and disadvantages of using audit checklists<br>11. Knowledge of the best practices to creation audit test plans |

## Domain 5: Conduct of an ISO/IEC 27034 audit

**Main objective:** To ensure that the ISO/IEC 27034 Lead Auditor candidate can conduct efficiently an AS audit in the context of ISO/IEC 27034

| Competencies | Knowledge statements |
|---|---|
| 1. Ability to organize and conduct the opening meeting in the context of a specific ISO/IEC 27034 audit mission<br>2. Ability to conduct audit in the context of a specific ISO/IEC 27034 audit mission and taking into account the documentation review conditions and criteria by applying the best practices of communication to collect the appropriate evidence and taking into account the roles and responsibilities of all people involved<br>3. Ability to explain, illustrate and apply statistical techniques and main audit sampling methods<br>4. Ability to gather appropriate evidences objectively from the available information in an audit and to evaluate them objectively | 1. Knowledge of the objectives and the content of the opening meeting of an audit<br>2. Knowledge of the difference of the different audit stages<br>3. Knowledge of the documentation review criteria<br>4. Knowledge of best practices of communication during an audit<br>5. Knowledge of the roles and responsibilities of guides and observers during an audit<br>6. Knowledge of the conflict resolution techniques<br>7. Knowledge of evidence collection procedures: observation, documentation review, interviews, analysis and technical verification<br>8. Knowledge of evidence analysis procedures: corroboration and evaluation<br>9. Knowledge of main concepts, principles and statistical techniques used in an audit<br>10. Knowledge of the main audit sampling methods and their characteristics |

## Domain 6: Conclusion and follow-up of an ISO/IEC 27034 audit

**Main objective:** To ensure that the ISO/IEC 27034 Lead Auditor candidate can conclude an AS audit and conduct follow-up activities in the context of ISO/IEC 27034

| Competencies | Knowledge statements |
|---|---|
| 1. Ability to explain and apply the evaluation process of evidences to draft audit findings and prepare audit conclusions<br>2. Understand, explain and illustrate the different levels of conformity and the concept of benefits of doubt<br>3. Ability to report appropriate audit observations in order to help an organization to improve an AS in respect of audit rules and principles<br>4. Ability to complete audit working documents and do a quality review of an ISO/IEC 27034 audit<br>5. Ability to draft audit conclusions and present these to the management of the audited organization<br>6. Ability to organize and conduct an audit closing meeting<br>7. Ability to conduct the activities following an initial audit including the evaluation of action plans, follow up audits, surveillance audits | 1. Knowledge of the evaluation process of evidences to draft audit findings and prepare audit conclusions<br>2. Knowledge of the guidelines and best practices to write nonconformity report<br>3. Knowledge of the guidelines and best practices to draft and report audit observation<br>4. Knowledge of the principle of benefits of doubt and his application in the context of an audit<br>5. Knowledge of the guidelines and best practices to complete audit working documents and do a quality review of an audit<br>6. Knowledge of the guidelines and best practices to present audit findings and conclusions to management of an audited organization<br>7. Knowledge of the guidelines and best practices to evaluate action plans |

## Domain 7: Management of an ISO/IEC 27034 audit program

**Main objective:** To ensure that the ISO/IEC 27034 Lead Auditor understands how to establish and manage an AS audit program

| Competencies | Knowledge statements |
|---|---|
| 1. Understand and explain the establishment of an audit<br>2. Understand and explain the responsibilities to protect the integrity, availability and confidentiality of audit records<br>3. Understand the requirements related to the components of the application security of an audit program, record management, complaint management<br>4. Understand the evaluation of the efficiency of the audit program by monitoring the performance of each auditor, each team and the entire certification body<br>5. Understand and explain the way combined audits are handled in an audit program<br>6. Ability to demonstrate the application of the personal attributes and behaviors associated to professional auditors | 1. Knowledge of requirements, guidelines and best practices regarding audit resources, procedures and policies<br>2. Knowledge of the types of tools used by professional auditors<br>3. Knowledge of requirements, guidelines and best practices regarding the management of audit records<br>4. Knowledge of the application of the concept of continual improvement to the management of an audit program<br>5. Knowledge of the management of combined audit activities<br>6. Knowledge of the concept of competency and its application to auditors<br><br>Knowledge of the personal attributes and behavior of a professional auditor |

Based on these 7 domains and their relevance, 12 questions are included in the exam, as summarized in the following table:

| | | | | Level of Understanding (Cognitive/Taxonomy) Required | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Question Number | Points per Question | Questions that measure Comprehension, Application and Analysis | Question 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 | 3 | 5 | x | | 1 | 8.33 | 5 | 6.67 |
| | Information Technology Application Security (AS) | 1 | 5 | x | | 1 | 8.33 | 5 | 6.67 |
| | Fundamental Audit Concepts and Principles | 4 | 10 | x | | 2 | 16.67 | 15 | 20.00 |
| | | 5 | 5 | x | | | | | |
| | Preparation of an ISO 27034 audit | 2 | 5 | x | | 3 | 25.00 | 15 | 20.00 |
| | | 6 | 5 | x | | | | | |
| | | 7 | 5 | x | | | | | |
| | Conduct of an ISO 27034 audit | 8 | 10 | | x | 2 | 16.67 | 15 | 20.00 |
| | | 9 | 5 | | x | | | | |
| | Conclusion and follow-up of an ISO 27034 audit | 11 | 5 | | x | 2 | 16.67 | 15 | 20.00 |
| | | 12 | 10 | | x | | | | |
| | Management of an ISO 27034 audit program | 10 | 5 | | x | 1 | 8.33 | 5 | 6.67 |
| Total Points | | | 75 | | | | | | |
| Number of Questions per level of understanding | | | | 7 | 5 | | | | |
| % of Test Devoted to each level of understanding | | | | 58.33 | 41.67 | | | | |

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 Auditor, 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 proctor and the exam confirmation letter.

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. Evidence in an audit

Determine how you would verify each of the following control measures. You must provide examples of evidence you would look for to have a reasonable guarantee that the control measure has been effectively implemented. State at least two elements of proof for each.

- **8.1.2.6.5.2 ASC Identification:**

**Possible answers:**

- A report that contains information of the organization data, ASC names regulatory and technological contexts.
- An employee's job description that describes the responsibility of updating the list of applicable legislation.

## 2. Evaluation of corrective actions

You have received a plan for corrective actions. Evaluate the adequacy of the proposed corrective actions. If you agree with the corrective actions, explain why. If you disagree, explain why and propose what you think would be some adequate corrective actions.

**Non-conformity 1: The auditor has indicated a nonconformity because the applications were not protected against unauthorized modifications.**

**Corrective action plan 1: Perform a manual adjustment about the importance of the**

**Applications and who is authorized for using them.**

**Possible answers:**

I agree. This step is important as it should be defined who is authorized to improve or modify the documents. Each person in the organization should have the list of the responsibilities and what is authorized to do.

## 3. Risk evaluation and selection of controls

Determine threats and vulnerabilities associated to the following situations and indicate the possible impacts. Also indicate if the risks would affect confidentiality, data integrity and/or availability.

For each risk identified, provide the appropriate controls (by providing the clause number of the control) which allows to reduce, transfer or avoid risks.

**Possible answers:**

| Statements | Vulnerabilities | Threats | C | I | A | Potential Impacts | Controls |
|---|---|---|---|---|---|---|---|
| **Example:**<br><br>*Many employees of the organization work remotely from their home.* | *Transfer of data via an external network.* | *Service Failure*<br><br>*Non-authorized access* | X | X | X | *Loss of productivity*<br><br>*Deterioration of the network*<br><br>*Disclosure of confidential information*<br><br>*Data loss* | AC-17 (1) (2) (3)<br><br>(4) |

## 4. Classification of controls

For each of the following 5 controls, indicate if it is 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.

### *6.3.9 Organization and user data*

**Possible answers:**

*A report that includes the implementation of all applicable legislations, and all data are protected.*

*Ensure that employees are informed for their duties and responsibilities.*

## 5. Writing of a test plan

Write a test plan to validate the following control identifying the different applicable audit procedures (observation, documentation review, interview, technical verification and analysis):

- **Clause 7.3 Application Security Management Process**

**Possible answers:**

| **Clause 7.3 Application Security Management Process** | |
|---|---|
| **Observation** | Observation of protection measures implemented Application Security and management process. |
| **Document** | Documentation of controls in place to protect information security. |
| **Interview** | Interview with the application security manager and validate the application policy objectives, interview with the network administrator to validate the operation of the controls in place to protect the application security processes. |
| **Technical verification** | Observation of the process of applications security. Verifying the implementation and documents updates. |
| **Analysis** | Analysis of a sample of application security, management process. |