CERTIFIED ISO/IEC 27034
APPLICATION SECURITY LEAD AUDITOR

MASTERING THE AUDIT OF IT – SECURITY TECHNIQUES – APPLICATION SECURITY BASED ON ISO/IEC 27034, IN COMPLIANCE WITH THE REQUIREMENTS OF ISO 19011 AND ISO 17021

SUMMARY

This five-day intensive course enables the participants develop the necessary expertise to audit an Information Technology – Security Techniques – Application Security as specified in ISO/IEC 27034, and manage a team of auditors by applying widely recognized audit principles, procedures and techniques. During this training, the participant will acquire the necessary knowledge and skills to proficiently plan and perform internal and external audits in compliance with ISO 19011 and ISO 17021. Based on practical exercises, the participant will develop the skills (mastering audit techniques) and competencies (managing audit teams and audit program, communicating with customers, conflict resolution, etc.) necessary for efficient conduct of an audit.

WHO SHOULD ATTEND?

- Internal auditors
- Auditors wanting to perform and lead IT – Security techniques – Application Security audit
- Project managers or consultants who want to master the IT – Security Techniques – Application Security audit process
- CxO and senior managers responsible for the IT governance of an enterprise and the management of its risks
- Members of an information security team
- Expert advisors in Information Technology
- Technical experts wanting to prepare for Application Security audit function

COURSE AGENDA

DURATION: 5 DAYS

DAY 1

Introduction to IT – Security techniques – Application Security overview and concepts as required by ISO/IEC 27034

- Normative, regulatory and legal framework related to application security
- Fundamental principles of Application Security
- ISO/IEC 27034 certification process
- IT – Security Techniques – Application Security
- Detailed presentation of the clauses of ISO/IEC 27034

DAY 2

Planning and initiating an ISO/IEC 27034 audit

- Fundamental audit concepts and principles
- Audit the approach based on evidence and risk
- Preparation of an ISO/IEC 27034 audit
- Application Security documentation audit
- Conducting an opening meeting

DAY 3

Conducting an ISO/IEC 27034 audit

- Communication during the audit
- Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation
- Audit test plans
- Formulation of the audit findings
- Documenting nonconformities

DAY 4

Concluding and ensuring the follow–up of an ISO/IEC 27034 audit

- Audit documentation
- Quality review
- Conducting a closing meeting and conclusion of an ISO/IEC 27034 audit
- Evaluation of corrective action plans
- ISO/IEC 27034 surveillance audit
- ISO/IEC 27034 internal audit management program

DAY 5

Certification Exam

LEARNING OBJECTIVES

- To acquire the expertise needed to perform an ISO/IEC 27034 internal audit following the ISO 19011 guidelines
- To acquire the expertise needed to perform an ISO/IEC 27034 audit following the ISO 19011 guidelines and the specifications of ISO 17021 and ISO 27006
- To acquire the necessary expertise to manage an IT – Application Security audit team
- To understand the operation of an ISO/IEC 27034 conformant Application Security management system
- To understand the relationship between an IT – Security techniques – Application Security, including risk management, controls and compliance with the requirements of different stakeholders of the organization
- To improve the ability to analyze the internal and external environment of an organization, its risk assessment and audit decision–making

EXAMINATION

The "Certified ISO/IEC 27034 Lead Auditor" exam fully meets the requirements of the PECB Examination and Certification Program (ECP). The exam covers the following competence domains:

1 **Domain 1: Fundamental principles and concepts in Application Security**

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

2 **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

3 **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

4 **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

5 **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

6 **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

7 **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

- The "Certified ISO/IEC 27034 Lead Auditor" exam is available in different languages, including English, French, Spanish and Portuguese
- Duration: 3 hours
- For more information about the exam, please visit: www.pecb.com

CERTIFICATION

- After successfully completing the exam, participants can apply for the credentials of Certified ISO/IEC 27034 Provisional Auditor, Certified ISO/IEC 27034 Auditor or Certified ISO/IEC 27034 Lead Auditor depending on their level of experience. Those credentials are available for internal and external auditors
- A certificate will be issued to those participants who successfully pass the exam and comply with all the other requirements related to the selected credential:

Credential	Exam	Professional Experience	ITST Audit Experience	ITST Project Experience	Other Requirements
ISO/IEC 27034 Provisional Auditor	ISO/IEC 27034 Lead Auditor Exam	None	None	None	Signing the PECB code of ethics
ISO/IEC 27034 Auditor	ISO/IEC 27034 Lead Auditor Exam	**Two years** One year of Information Technology Security Techniques work experience	Audit activities totaling 200 hours	None	Signing the PECB code of ethics
ISO/IEC 27034 Lead Auditor	ISO/IEC 27034 Lead Auditor Exam	**Five years** Two years of Information Technology Security Techniques work experience	Audit activities totaling 300 hours	None	Signing the PECB code of ethics

GENERAL INFORMATION

- Certification fees are included in the exam price
- Participant manual contains over 450 pages of information and practical examples
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued to the participants
- In case of failure of the exam, participants are allowed to retake it for free under certain conditions