CERTIFIED ISO 27034

APPLICATION SECURITY LEAD IMPLEMENTER

MASTERING THE IMPLEMENTATION OF APPLICATION SECURITY (AS) PROCESSES, ACTIVITIES & SECURITY TECHNIQUES ACROSS THE ORGANIZATION BASED ON THE INTERNATIONAL STANDARD ISO/IEC 27034 – APPLICATION SECURITY

SUMMARY

This five-day intensive course enables the participants to understand specific principles and concepts proposed by ISO/IEC 27034 for AS and understand how they can be implemented, step by step, to help organizations to develop, acquire, implement, use, and maintain trustworthy applications, according to their specific business context, at an acceptable cost. More specifically, the ISO/IEC 27034 framework proposes components and processes to provide verifiable evidences that an application have reached and maintained a targeted level of trust as specified by the organization. The responsibility of a Certified ISO/IEC 27034 Application Security Lead Implementer is to assist organizations to put in place required 27034 framework elements and guide the organization to integrate Application Security Controls (ASC) seamlessly throughout the life cycle of their applications. AS applies not only to the software of an application but also to its other components and contributing factors that impact its security, such as its technological context, its regulatory context, its business context, its specifications, the sensitivity of its data, and the processes and actors supporting its entire life cycle. This framework applies to all sizes and all types of organizations (e.g. not only to commercial enterprises, government agencies and non-profit organizations that are using applications, but also to large, medium and small vendors that develop software, application and business services) exposed to security risks on information associated with their applications.

DAY 1

Introduction: AS overview and concepts as proposed by ISO/IEC 27034

- Introduction to ISO/IEC 27034 AS and its global vision
- Fundamental principles in Information Security
- Overview, concepts, principles, definitions, scope, components, processes and actors involved in AS
- Embedded implicit concepts
- Presentation of the 27034 series:
  - ISO/IEC 27034-1: Overview & concepts
  - ISO/IEC 27034-2: AS in an organization
  - ISO/IEC 27034-3: AS in a project
  - ISO/IEC 27034-4: AS validation, verification and certification
  - ISO/IEC 27034-5: AS structures requirements
  - ISO/IEC 27034-5-1: XML Schemas
  - ISO/IEC 27034-6: Examples and cases study

DAY 2

Implementation of AS based on ISO/IEC 27034

- Security into application project
  - The Application Security Management Process
  - Provisioning and operating an application
  - Maintaining the Actual Level of Trust on the Targeted Level of Trust
  - Development of AS validation

DAY 3

Implementation of AS based on ISO/IEC 27034 (cont.)

- AS at the organization level
- Goals of AS for a organization
- The Organization Normative Framework (ONF)
- The ONF committee
- The ONF Management process
- Integration of ISO/IEC 27034 elements into the organization's existing processes
- Design, validation, implementation, verification, operation and evolution of ASCs
- The ASC libraries
- The AS Traceability matrix
- Drafting the certification process

Security guidance for specific organizations and applications

- Cases Study,
- 27034 implementation examples for small and large organizations
- How 27034 can help to resolve conflicting regulations requirements for an application
- Developing ASCs
- Acquiring ASCs

DAY 4

AS validation and certification

- The purpose of internal AS audit
- Minimize the cost of an audit
- Be sure you have all expected evidences ready
- Overview of the AS validation and certification process under 27034.
- How to help an organization to be certified
- How to help an application project to be certified

Protocols and ASC data structure based on ISO/IEC 27034

- An free formal languages for ASC communication
- ISO/27034 proposed XML schemas,
- Data structure, descriptions, graphical representation

ISO/IEC 27034 AS final review

DAY 5

Certification Exam

WHO SHOULD ATTEND?

- Managers, such as information security managers, project managers, administrators, software development managers, application owners and line managers, who wish to:
  balance the cost of implementing and maintaining AS against the risks and value it represents for the organization;
  prepare and to support an organization in the implementation of an AS project
- Provisioning and operation teams such as architects, analysts, programmers, testers, system administrators, DBA, network administrators, and technical personnel, who wish to:
  minimize the impact of introducing ASC into organizations' existing processes, such as design, development, test, deployment, operation, archival and destruction
  understand which controls should be applied at each stage of an application's life cycle and witch one should be implemented inside the application itself
- Acquirers and Suppliers who wish to: prepare/comply to requests for proposals that include requirements for ASC and Level of Trust
- Auditors who wish to: fully understand the AS processes involves in the ISO/IEC 27034

LEARNING OBJECTIVES

- To understand the implementation of AS in accordance with ISO/IEC 27034
- To gain a comprehensive understanding of the concepts, approaches, standards, methods and techniques required for the effective management of AS
- To understand the relationship between the components of an AS including risk management, controls and compliance with the requirements of different stakeholders of the organization
- To acquire necessary expertise to support an organization in implementing, managing and maintaining an AS as specified in ISO/IEC 27034
- To acquire necessary expertise to manage a team implementing ISO/IEC 27034
- To develop knowledge and skills required to advise organizations on best practices in the management of AS
- To improve the capacity for analysis and decision making in the context of AS

EXAMINATION

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

1 **Domain 1: Fundamental concepts and principles in application security**

Main Objective: To ensure that the ISO/IEC 27034 AS Lead Implementer candidate can understand, interpret and illustrate key AS concepts related to the implementation of AS in an organization and the implementation of AS in an application project under ISO/IEC 27034, including the AS scope, how AS is align with 27001, its pros and its limitations

2 **Domain 2: Applications security control (ASC) and others best practice in AS**

Main Objective: To ensure that the ISO/IEC 27034 AS Lead Implementer candidate can understand, interpret and provide guidance on how to implement and manage ASC best practices to support or support other standards and best practices such as ISO/IEC 27002, ISO/IEC 15288, Common Criteria, CMMI, PMI, ITIL, COBIT and OWASP.

3 **Domain 3: Preparation of an AS project based on ISO/IEC 27034**

Main Objective: To ensure that the ISO/IEC 27034 AS Lead Implementer candidate can plan and prepare appropriately the implementation of an AS organizational project or application project in the context of ISO 27034

4 **Domain 4: Implementing an AS project based on IOS/IEC 27034**

Main Objective: To ensure that the ISO/IEC 27034 AS Lead Implementer candidate can implement required processes and security controls in an AS organizational project or application project in the context of ISO 27034

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

Main Objective: To ensure that the ISO/IEC 27034 AS Lead Implementer candidate can monitor and evaluate the performance of an AS organizational project or application project in the context of the organization's AS needs under ISO/IEC 27034

6 **Domain 6: Continual improvement of an AS project based on ISO/IEC 27034**

Main Objective: To ensure that the ISO/IEC 27034 AS Lead Implementer candidate can provide guidance on the continuous improvement of an AS organizational project or application project in the context of ISO/IEC 27034

7 **Domain 7: Preparing an application project or an organization for an ISO/IEC 27034 certification audit**

Main Objective: To ensure that the ISO/IEC 27034 AS Lead Implementer candidate can prepare and assist an organization for a certification against the ISO/IEC 27034 standard. These certifications could be done at organizational level, or for specific applications.

- The "Certified ISO/IEC 27034 Lead Implementer" 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 Application Security Provisional Implementer, Certified ISO/IEC 27034 Application Security Implementer or Certified ISO/IEC 27034 Application Security Lead Implementer, depending on their level of experience
- A certificate will be issued to 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 Application Security Provisional Implementer	ISO/IEC 27034 Application Security Lead Implementer Exam	None	None	None	Signing the PECB code of ethics
ISO/IEC 27034 Application Security Implementer	ISO/IEC 27034 Application Security Lead Implementer Exam	Two years, including one year of Information Technology Security Techniques work experience	None	Project activities totaling 200 hours	Signing the PECB code of ethics
ISO/IEC 27034 Application Security Lead Implementer	ISO/IEC 27034 Application Security Lead Implementer Exam	Five years, including two years of Information Technology Security Techniques work experience	None	Project activities totaling 300 hours	Signing the PECB code of ethics

GENERAL INFORMATION

- Certification fees are included in the exam price
- Participant manual contains over 350 pages of information and practical examples
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued to participants
- In case of failure of the exam, participants are allowed to retake it for free under certain conditions
- Participants should have access to a legal copy of the International Standard ISO/IEC 27034 Information technology — Security techniques — Application security — Part 1: Overview and concepts, in class for consultation.