PECB CERTIFIED ISO/IEC 27035
LEAD INCIDENT MANAGER

MASTERING THE INCIDENT MANAGEMENT PROCESS BASED ON ISO/IEC 27035

SUMMARY

In this five-day intensive course participants develop the competence to master a model for implementing an incident management process throughout their organization using the ISO/IEC 27035 standard as a reference framework. Based on practical exercises, participants acquire the necessary knowledge and skills to manage information security incidents in time by being familiar with their life cycle. During this training, we will present the ISO/IEC 27035 information security incident management standard, a process model for designing and developing an organizational incident management process, and how companies may use the standard. This training is also fully compatible with ISO/IEC 27035 which supports ISO/IEC 27001 by providing guidance for incident management.

WHO SHOULD ATTEND?

- Incident managers
- Business Process Owners
- Information Security Risk Managers
- Regulatory Compliance Managers
- Members of Incident Response Team
- Persons responsible for information security or conformity within an organization

COURSE AGENDA

DURATION: 5 DAYS

DAY 1

Introduction, incident management framework according to ISO/IEC 27035

- Concepts and definitions related to information security and incident management
- Incident management standards, and best practices
- Choosing an incident management framework
- Understanding an organization and its context

DAY 2

Planning the implementation of an Organizational Incident Management Process based on ISO/IEC 27035

- Incident management strategy and project management
- Planning the implementation of an effective incident management process
- Preliminary analysis and selection of an approach and methodology
- Design and document an incident detection, reporting and management process
- Defining roles and responsibilities in the context of the implementation and management of an Incident Management Process

DAY 3

Implementing an Incident Management Process

- Define the document and record management processes
- Incident Management policies & procedures
- Implementation of security processes and controls related to incident management
- Change management process
- Incident analysis processes
- Effective communication and the communication strategies
- Establish the Information Security Incident Response Team

DAY 4

Monitoring, measuring and improving an Incident Management Process

- Monitoring and evaluating the effectiveness of incident management process in operations
- Development of metrics, performance indicators and dashboards
- Management reviews
- Implementation of a continual improvement program
- Develop and propos the best corrective and preventive action plans

DAY 5

Certification Exam

LEARNING OBJECTIVES

- To understand the concepts, approaches, methods, tools and techniques allowing an effective information security incident management according to ISO/IEC 27035
- To understand, interpret and provide guidance on how to implement and manage incident management processes based on best practices of ISO/IEC 27035 and other relevant standards
- To acquire the competence to implement, maintain and manage an ongoing information security incident management program according to ISO/IEC 27035
- To acquire the competence to effectively advise organizations on the best practices in information security management

EXAMINATION

The "PECB Certified ISO/IEC 27035 Lead Incident Manager" 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 Incident Management**

Main Objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can understand, interpret and illustrate the main Incident Management concepts related to published standards including ISO/IEC 27035

2 **Domain 2: Incident Management Best Practice based on ISO/IEC 27035**

Main Objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can understand, interpret and provide guidance on how to implement and manage Incident Management requirements based on best practices of ISO/IEC 27035 and other relevant standards

3 **Domain 3: Designing and Developing an Organisational Incident Management Process based on ISO/IEC 27035**

Main Objective:To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can plan the implementation of an effective Incident Management Process

4 **Domain 4: Preparing for Incident Management and Implementing an Incident Management Process**

Main Objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can implement the Incident Management process and associated security controls required for an effective Incident Management process

5 **Domain 5: Enacting the Incident Management Process and Handling Security Incidents**

Main Objective: To ensure that Certified ISO/IEC 27035 Lead Incident Manager candidate can lead the response to an Incident in an effective, legal and professional manner

6 **Domain 6: Performance Monitoring and Measuring**

Main Objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can evaluate, monitor and measure the performance of an Incident Management Process

7 **Domain 7: Improving the Incident Management Process**

Main Objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can provide guidance on the Continual improvement of an Incident Management Process

- The "PECB Certified ISO/IEC 27035 Lead Incident Manager" exam is available in different languages, such as English, French, Spanish and Portuguese
- Duration: 3 hours
- For more information about the exam, please visit: www.pecb.com

CERTIFICATION

- After successfully completing the "PECB Certified ISO/IEC 27035 Lead Incident Manager" exam, participants can apply for the credentials of PECB Certified ISO/IEC 27035 Provisional Incident Manager, PECB Certified ISO/IEC 27035 Incident Manager or PECB Certified ISO/IEC 27035 Lead Incident Manager, 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	Incident Management Experience	Other Requirements
PECB Certified ISO/IEC 27035 Provisional Incident Manager	PECB Certified ISO/IEC 27035 Lead Incident Manager Exam	None	None	Signing the PECB code of ethics
PECB Certified ISO/IEC 27035 Incident Manager	PECB Certified ISO/IEC 27035 Lead Incident Manager Exam	**Two years** One year of Incident Management related work experience	Incident Management activities totaling 200 hours	Signing the PECB code of ethics
PECB Certified ISO/IEC 27035 Lead Incident Manager	PECB Certified ISO/IEC 27035 Lead Incident Manager Exam	**Five years** Two year of Incident Management related work experience	Incident Management activities totaling 300 hours	Signing the PECB code of ethics

GENERAL INFORMATION

- Exam and certification fees are included in the training price
- A student manual containing over 450 pages of information and practical examples will be distributed to participants
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued to participants
- ISO 27035 standard provides guidance for incident management to which organizations cannot get certified against