



PECB Certified ISO/IEC 27035 Lead Incident Manager

Master the Information Security Incident Management based on ISO/IEC 27035

Why should you attend?

ISO/IEC 27035 Lead Incident Manager training enables you to acquire the necessary expertise to support an organization in implementing an Information Security Incident Management plan based on ISO/IEC 27035. During this training course, you will gain a comprehensive knowledge of a process model for designing and developing an organizational incident management plan. The compatibility of this training course with ISO/IEC 27035 also supports the ISO/IEC 27001 by providing guidance for Information Security Incident Management.

After mastering all the necessary concepts of Information Security Incident Management, you can sit for the exam and apply for a "PECB Certified ISO/IEC 27035 Lead Incident Manager" credential. By holding a PECB Lead Incident Manager Certificate, you will be able to demonstrate that you have the practical knowledge and professional capabilities to support and lead a team in managing Information Security Incidents.



Who should attend?

- Information Security Incident managers
- IT Managers
- IT Auditors
- Managers seeking to establish an Incident Response Team (IRT)
- Managers seeking to learn more about operating effective IRTs
- Information Security risk managers
- IT system administration professionals
- IT network administration professionals
- Members of Incident Response Teams
- Individuals responsible for Information Security within an organization

Course agenda

Duration: 5 days

Day 1 | Introduction to Information Security Incident Management concepts as recommended by ISO/IEC 27035

- Course objectives and structure
- Standards and regulatory frameworks
- Information Security Incident Management
- ISO/IEC 27035 core processes
- Fundamental principles of Information Security
- Linkage to business continuity
- Legal and ethical issues

Day 2 | Designing and preparing an Information Security Incident Management plan

- Initiating an Information Security Incident Management Process
- Understanding the organization and clarifying the information security incident management objectives
- Plan and prepare
- Roles and functions
- Policies and procedures

Day 3 | Enacting the Incident Management process and handling Information Security incidents

- Communication planning
- First implementation steps
- Implementation of support items
- Detecting and reporting
- Assessment and decisions
- Responses
- Lessons learned
- Transition to operations

Day 4 | Monitoring and continual improvement of the Information Security Incident Management plan

- Further analysis
- Analysis of lessons learned
- Corrective actions
- Competence and evaluation of incident managers
- Closing the training

Day 5 | Certification Exam



Learning objectives

- Master the concepts, approaches, methods, tools and techniques that enable an effective Information Security Incident Management according to ISO/IEC 27035
- Acknowledge the correlation between ISO/IEC 27035 and other standards and regulatory frameworks
- Acquire the expertise to support an organization to effectively implement, manage and maintain an Information Security Incident Response plan
- Acquire the competence to effectively advise organizations on the best practices of Information Security Incident Management
- Understand the importance of establishing well-structured procedures and policies for Incident Management processes
- Develop the expertise to manage an effective Incident Response Team

Examination

Duration: 3 hours

The “PECB Certified ISO/IEC 27035 Lead Incident Manager” exam fully meets the requirements of the PECB Examination and Certification Programme (ECP). The exam covers the following competency domains:

- Domain 1** | Fundamental principles and concepts of Information Security Incident Management
- Domain 2** | Information Security Incident Management best practices based on ISO/IEC 27035
- Domain 3** | Designing and developing an Organizational Incident Management process based on ISO/IEC 27035
- Domain 4** | Preparing for Information Security incidents and implementing an Incident Management Plan
- Domain 5** | Enacting the Incident Management Process and handling Information Security Incidents
- Domain 6** | Performance measurement and monitoring
- Domain 7** | Improving the Incident Management processes and activities

For more information about exam details, please visit [Examination Rules and Policies](#).



Certification

After successfully completing the exam, you can apply for the credentials shown on the table below
 You will receive a certificate once you comply with all the requirements related to the selected credential

For more information about ISO/IEC 27035 certifications and the PECB certification process, please refer to the [Certification Rules and Policies](#).

Credential	Exam	Professional experience	ISIM experience	Other requirements
PECB Certified ISO/IEC 27035 Provisional Incident Manager	PECB Certified ISO/IEC 27035 Lead Incident Manager exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27035 Incident Manager	PECB Certified ISO/IEC 27035 Lead Incident Manager exam or equivalent	Two years: One year of work experience in Information Security Incident Management	ISIM activities: a total of 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 or equivalent	Five years: Two years of work experience in Information Security Incident Management	ISIM activities: a total of 300 hours	Signing the PECB Code of Ethics

General information

- Certification fees are included on the exam price
- Training material containing over 450 pages of information and practical examples will be distributed
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued
- In case of exam failure, you can retake the exam within 12 months for free