

PECB Certified ISO/IEC 27035
Lead Incident Manager

Master the implementation and management of information security incident management processes based on ISO/IEC 27035

Why should you attend?

Whether deliberate or accidental, information security incidents are almost inevitable in the digital age, impacting organizations of all sizes and sectors. Learning to navigate the complexities of information security incident detection, assessment, response, and reporting allows participants to assist organizations in ensuring the safety of their information and reducing negative business consequences.

This training course aligns with ISO/IEC 27001, ISO/IEC 27005, and other standards in the ISO/IEC 27000 series and provides practical guidance on information security.

Upon completing the course and its exam, participants can apply for the "PECB Certified ISO/IEC 27035 Lead Incident Manager" credential, showcasing their proficiency in strategically and effectively managing and mitigating information security incidents.



Who should attend?

This training course is intended for:

- Managers or consultants seeking to expand their knowledge of information security incident management
- Professionals seeking to establish and manage effective incident response teams (IRTs)
- IT professionals and information security risk managers seeking to enhance their knowledge in information security incident management
- Members of incident response teams
- Incident response coordinators or other roles with responsibilities for incident handling and response

Course agenda

Duration: 5 days

Day 1 | Introduction to Information Security Incident Management and ISO/IEC 27035

- Training course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts of incident management
- Information security incident management
- Context establishment
- Policies and procedures

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

- Risk management
- Incident management plan
- Incident management team
- Internal and external relationships
- Technical and other support
- Information security incident awareness and training

Day 3 | Detecting and reporting information security incidents

- Testing
- Monitor systems and networks
- Detect and alert
- Information collection for incidents
- Report information security events
- Information security event assessment

Day 4 | Monitoring and continual improvement of the information security incident management process

- Resolve information security incidents
- Containment, eradication, and recovery
- Lessons learned
- Monitoring, measurement, analysis, and evaluation
- Continual improvement
- Closing of the training course

Day 5 | Certification Exam



Learning objectives

By the end of this training course, you will be able to:

- Explain the fundamental principles of incident management
- Develop and implement effective incident response plans tailored to the organization's needs and select an incident response team
- Conduct thorough risk assessments to identify potential threats and vulnerabilities within an organization
- Apply good practices from various international standards to enhance the efficiency and effectiveness of incident response efforts
- Conduct post-incident analysis and identify lessons learned

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 process 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 | Implementing incident management processes and managing information security incidents

Domain 6 | Improving the incident management processes and activities

For specific information about the exam type, languages available, and other details, please visit the List of PECB Exams and Exam Rules and Policies



Certification

After passing the exam, you can apply for one of the credentials listed in the table below. You will receive a certification once you fulfill all the requirements of the selected credential.

Professional credential	Education	Exam	Professional experience	Incident management project experience	Other requirements
PECB Certified ISO/IEC 27035 Provisional Incident Manager	At least secondary education	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			2 years (1 in information security incident management)	200 hours	
PECB Certified ISO/IEC 27035 Lead Incident Manager			5 years (2 in information security incident management)	300 hours	
PECB Certified ISO/IEC 27035 Senior Lead Incident Manager			10 years (7 in information security incident management)	1,000 hours	

General information

- Certification and examination fees are included in the price of the training course.
- Participants receive training course materials containing over 450 pages of information, practical examples, exercises, and quizzes.
- An attestation of course completion worth 31 CPD (Continuing Professional Development) credits will be issued to the participants who have attended the training course.
- Candidates who have completed the training course but failed the exam are eligible to retake the exam once for free within 12 months from the initial date of the exam.