ISO/IEC 27035 Information Security Incident Management Lead Incident Manager (PECB Certified) - Including Exam

Duration: 4 Days **Course Code: ISO27035LI** **Delivery Method: Company Event**

Overview:

The ISO/IEC 27035 Lead Incident Manager training course equips participants with the knowledge and skills necessary to support organizations in establishing and implementing a process for managing information security incidents. This training course is based on the ISO/IEC 27035 series and other good practices of incident management and covers the entire incident lifecycle, from incident planning to post-incident activities. In addition, participants will also learn about the role of key stakeholders and the importance of working with other organizations to handle information security incidents.
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.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

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

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

Prerequisites:

- The main requirement for participating in this training course is having a general knowledge of incident management processes, information security principles, and the ISO/IEC 27000 family of standards.

Testing and Certification

The “PECB Certified ISO/IEC 27035 Lead Incident Manager” exam meets the PECB Examination and Certification Program (ECP) requirements. It 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 and executing the incident response plan for information security incidents

- **Domain 5:** Implementing incident management processes and managing information security incidents
- **Domain 6:** Improving the incident management processes and activities

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

PECB Certified ISO/IEC 27035 Provisional Incident Manager

- Exam: PECB Certified ISO/IEC 27035 Lead Incident Manager exam or equivalent
- Professional experience: None
- ISIMMS project experience: None
- Other requirements: Signing the PECB Code of Ethics

PECB Certified ISO/IEC 27035 Incident Manager

- Exam: PECB Certified ISO/IEC 27035 Lead Incident Manager exam or equivalent
- Professional experience: Two years, including one year of work experience in Information Security Incident Management
- ISIMMS project experience: ISIM activities totaling 200 hours
- Other requirements: Signing the PECB Code of Ethics

PECB Certified ISO/IEC 27035 Lead Incident Manager

- Exam: PECB Certified ISO/IEC 27035 Lead Incident Manager exam or equivalent
- Professional experience: Five years, including two years of work experience in Information Security Incident Management
- ISIMMS project experience: ISIM activities totaling 300 hours
- Other requirements: Signing the PECB Code of Ethics

PECB Certified ISO/IEC 27035 Senior Lead Incident Manager

- Exam: PECB Certified ISO/IEC 27035 Lead Incident Manager exam or equivalent
- Professional experience: Ten years, including seven years of work experience in Information Security Incident Management
- ISIMMS project experience: ISIM activities totaling 1,000 hours
- Other requirements: Signing the PECB Code of Ethics

The incident management project experience should follow best implementation practices and include the following:

- Defining an incident management approach
- Determining the incident management objectives and scope
- Performing risk assessment
- Developing an incident management program
- Defining risk evaluation and risk acceptance criteria
- Evaluating risk treatment options
- Monitoring and reviewing the incident management program

Content:

Day 1: Introduction to information security incident management concepts and ISO/IEC 27035

Day 2: Designing and preparing an information security incident management plan

Day 3: Detecting and reporting information security incidents

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

Additional Information:

Educational Approach
- This training course combines theoretical concepts with best practices for implementing an information security incident management process.
- The training course contains essay-type exercises and multiple-choice quizzes, some of which are scenario-based.
- The participants are encouraged to collaborate and engage in meaningful discussions with fellow learners while tackling quizzes and exercises.
- The quiz format closely mirrors that of the certification exam, ensuring participants are well-prepared for their exam.

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.

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/