



PECB Certified ISO/IEC 27035 Incident Manager Training Module

Trainer

Michael
Redmond
PhD



Sept 25-29, 2023

Dear Colleagues,

In today's world, effectively handling cyber-attacks requires being well-prepared and possessing the necessary skills and expertise. The initial moments after discovering an incident are crucial for efficient management and mitigating potential risks to the company. Failure to plan for such incidents will result in delayed response times and uncontrolled risks, which are unacceptable. It is imperative to take action and ensure that proper protocols are in place to risk managing cyber incidents.

The **ISO/IEC 27035 Lead Incident Manager** instructor-led online virtual-training course on **September 25-29, 2023**, will enable 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.

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

Course Agenda

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

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

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

General Information

- Certification and examination fees are included in the price of the training course
- 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

An organisations that have an Information Security Incident Management framework in place will be capable of managing the incidents efficiently and effectively; from the beginning to the end of the Incident Lifecycle. Likewise, an ISO/IEC 27035 framework implementation is an important matured security step in the security operations of an organisation, providing it an effective and efficient process in incident management, while at the same time, providing business (cyber) resilience.

We look forward to your participation as you aim to gain the necessary expertise and competencies to guide your organization towards attaining maximum Cyber Resilience in a proficient and streamlined manner.

Best Regards,

Team CSG

[Register \(USD\)](#)

[Register \(BBD\)](#)



Copyright (C) 2023 CariSec Global Inc.. All rights reserved.