Updated on 22/08/2025

Sign up

ISO/IEC 27035 Training - Information Security Incident Management - Foundation

ALL-IN-ONE: EXAM INCLUDED IN PRICE

2 days (14 hours)

Presentation

Our "ISO/IEC 27035 - Information Security Incident Management - Foundation" training course will enable you to understand the fundamentals of security incident management and acquire the practical skills needed to apply the standard in an organizational context. From the outset, you'll learn about the structure and objectives of the standard, and how it relates to other key standards (ISO/IEC 27001, 27002, 27005, RGPD, NIS2).

Using a process-centric approach, you will learn how to define roles and responsibilities, set up an appropriate escalation chain, effectively detect and analyze incidents, orchestrate response actions, and document feedback.

Throughout the course, progressive role-playing exercises will enable you to build step-by-step a comprehensive security incident management plan that can be directly transposed to your organization.

On completion of the course, you will be able to implement an information security incident management plan, in line with the latest version of ISO/IEC 27035, and be prepared for the Foundation certification exam.

Objectives

- Understand the fundamentals of information security incident management.
- Understand the relationship between ISO/IEC 27035 and other standards and regulatory frameworks.
- Understand the process-based approach to managing information security incidents.

Target audience

- Anyone interested in the process-based approach to managing information security incidents.

PREREQUISITES

- This ISO 27035 Foundation course has no specific prerequisites.

Program of our ISO/IEC 27035 certification course - Information Security Incident Management - Foundation

[Day 1 - Morning]

Introduction and understanding of ISO/IEC 27035

- Context and challenges of information security incident management
- Structure and objectives of ISO/IEC 27035
- The three parts: principles, processes and guidelines
- Terminology: events, incidents, vulnerabilities, weaknesses

[Day 1 - Afternoon]

Organization and roles in incident management

- Internal and external players (CISO, IT Department, CERT, CSIRT, service providers)
- Responsibilities, escalation processes and coordination
- Employee awareness and training
- Internal and external communication during an incident
- Practical workshop: Defining a suitable escalation chain for an SME.

Relationship with other standards and regulatory frameworks

- Articulation with ISO/IEC 27001 and ISO/IEC 27002
- Contribution of ISO/IEC 27005 (risk management) and ISO/IEC 22301 (business continuity)
- Integration with RGPD and NIS2 (notification obligations and legal responsibilities)
- Security governance and integration into an ISMS
- Practical workshop: Linking an incident management plan to RGPD and NIS2 requirements.

[Day 2 - Morning]

Incident life cycle according to ISO/IEC 27035

- Incident detection and recording
- Incident analysis and assessment
- Response, eradication and recovery
- Closure and capitalization (feedback, continuous improvement)
- Practical workshop: Incident simulation and action logging.

[Day 2 - Afternoon]

Implementation of an incident management process

- Development of policies and procedures
- Definition of indicators (KPI/KRI) and performance monitoring
- Integration with SOC, SIEM and ticketing tools
- Planning exercises and regular tests
- Practical workshop: Building a mini-incident management plan for a fictitious organization.

Exam preparation

- Summary of key concepts to be mastered for the exam
- Tips for approaching sample questions
- Review exercises and quizzes
- Progress plan for implementing ISO 27035 in your organization
- Practical workshop: Writing and correction of a mock exam.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.