+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 22/08/2025

Sign up

ISO/IEC 27035 Manager Certification Training

ALL-IN-ONE : EXAM INCLUDED

5 days (35 hours)

Presentation

Our "ISO/IEC 27035 - Information Security Incident Management Incident Manager" training course gives you the skills you need to build and manage a comprehensive security incident management system. Based on the ISO/IEC 27035 standard, it will enable you to master the key principles, techniques and methodologies of the incident lifecycle, from preparation and detection to feedback and continuous improvement. You'll learn how to define an incident policy, structure and lead a high-performance CSIRT, and conduct post-mortem analyses to sustainably strengthen your organization's resilience.

The course will highlight the close relationship between ISO/IEC 27035 and other standards and regulatory frameworks such as ISO/IEC 27001, 27002, 27005, 22301, the RGPD and the NIS2 directive. This integrated approach will enable you to understand how to fit incident management into an overall ISMS, while ensuring compliance with legal and sectoral requirements.

Particular emphasis will be placed on the organizational and managerial dimensions: managing and steering an incident response team, allocating roles and responsibilities, coordinating with the SOC, IT and business departments, and communicating in crisis situations. Through hands-on workshops and realistic scenarios, you will develop the skills needed to effectively organize the response to critical incidents and monitor operational performance using relevant indicators.

At the end of this course, you will be able to implement an incident management process that complies with international standards, is crisis-proof, continuously improves and can be successfully audited. You'll be ready to help your organization implement and manage an information security incident management plan in line with ISO/IEC 27035.

Like all our training courses, this one is based on the latest version of the standard.

is based on practical exercises, case studies and simulations, to guarantee a concrete and immediately operational increase in skills. It also includes full preparation for the certification exam, with a review of key points, a mock exam and corrections, to consolidate what you've learned and maximize your chances of success.

Objectives

- Understand the principles, techniques and methodology of information security incident management.
- Understand the relationship between ISO/IEC 27035 and other standards and regulatory frameworks
- Manage an appropriate team for incident follow-up and management
- Implement and manage an incident management process
- Analyze incidents and improve processes

Target audience

- Security managers / CISOs / Cybersecurity consultants or auditors
- ISS or crisis management project managers
- Anyone involved in IT security incident management

Prerequisites

- Good knowledge of incident management processes, information security principles and the ISO/IEC 27000 family of standards.

Program of our ISO/IEC 27035 Information Security Incident Management Incident - Manager training course

[Day 1 - Morning]

Incident management fundamentals

- Why is every incident a learning opportunity?
- Definition: incident vs. event, alert, vulnerability
- Objectives and challenges of ISO/IEC 27035 incident management
- Scope covered by the standard
- Roles, players and associated governance
- Business impacts and cyber risks

[Day 1 - Afternoon]

Architecture and understanding of ISO/IEC 27035

- Overview of the 3 parts: 27035-1, -2, -3
- Incident lifecycle logic
- Preparation vs. operations vs. feedback
- Positioning within an overall ISMS
- Practical workshop: Mapping the stages of an incident management cycle.

Initial diagnosis & maturity audit

- Why measure the maturity of your current system?
- ISO/IEC 27035 self-assessment grid
- Gap analysis: organization, procedures, tools
- Preparing an upgrade plan

[Day 2 - Morning]

Relationship with other standards and regulatory frameworks

- Articulation with ISO/IEC 27001, 27002, 27005 and 22301
- RGPD and NIS2 alignment: notification obligations, responsibilities
- Sector-specific requirements (healthcare, finance, OSE/SE)
- Complementary standards (NIST, ENISA/ANSSI)
- Practical workshop: Linking an incident plan to RGPD/NIS2 requirements.

[Day 2 - Afternoon]

Drawing up an incident management policy

- Structure and content of an ISO/IEC 27035 policy
- Links with global security policies and RGPD compliance
- Validation, communication and updating processes
- Governance and management sponsorship

Operational organization and key players

- Composition of an internal CSIRT: roles and responsibilities
- Complementarity with SOC, IT, business and compliance departments
- Key skills and human resources required
- RACI model and inter-departmental coordination
- Practical workshop: Defining the operational structure of a CSIRT.

[Day 3 - Morning]

Incident response team management

- Leadership and management of a CSIRT team
- Managing stress, workload and priorities during a crisis
- Internal/external managerial communication
- Skills development and conflict management

[Day 3 - Afternoon]

Triage, classification and prioritization of incidents

- Steps in qualifying an event as an incident
- Criticality levels (impact, likelihood, urgency)
- Incident categories: malware, compromise, data leakage, etc.
- Incident log: structure and key elements
- Introduction to the MITRE ATT&CK framework for classifying and analyzing operating modes
- Using Threat Intelligence Feeds to enhance incident qualification and tracking
- Practical workshop: Simulating multi-source triage.

Response: containment, eradication, recovery

- Containment techniques according to incident type
- Eradication: eliminating the cause, neutralizing the vector
- Restoration: backups, revalidation, failover
- Continuous documentation and the role of CSIRT
- Practical workshop: Putting together a complete response plan.

[Day 4 - Morning]

Crisis communication and external coordination

- Internal and external communication plan
- Interface with management, legal and compliance departments
- Notification obligations (CNIL, customers, authorities...)
- Collaboration with CERT/ANSSI and partners
- Practical workshop: Drawing up a crisis communication plan.

[Day 4 - Afternoon]

Resumption of activity and return to normal

- Post-restoration checks: integrity, availability
- Authorization to return to production
- Update of safety controls
- Short-term post-incident follow-up

- Documentation of incident closure

Feedback and capitalization

- Post-mortem analysis methodology
- Full incident report and causal analysis
- Corrective action plans and follow-up
- Capitalization and continuous improvement
- Practical workshop: Producing an incident report + improvement plan.

[Day 5 - Morning]

Control, supervision and maintenance in operational condition

- Choosing KPI/KRI (MTTD, MTTR, detection rate, etc.)
- ERP management dashboards and periodic reviews
- Rely on supervision tools (Grafana, Kibana, etc.)
- Overview of modern solutions: SIEM, SOAR, XDR, Threat Intelligence, AI/ML applied to event detection and correlation
- Simulation exercises, regular testing, ongoing training
- Update of detection/treatment scenarios

[Day 5 - Afternoon] Auditability

and compliance

- ISO/IEC 27001 & 27035 evidence requirements
- Incident log and traceability of responses
- RGPD/NIS2 alignment and sector-specific requirements
- Preparing for an audit (internal, external)
- Documentation expected during an ISO audit

Exam preparation

- Summary of key program points
- Methodological advice (format, questions, pitfalls)
- Sample tests and guided corrections
- Post-certification orientation
- Practical workshop: Mock exam and correction.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer 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 which enables 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% hands-on, 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 is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.