Certified ISO/IEC 27035 Information Security Incident Management Training Course

25 – 29 October 2027
Kuala Lumpur

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Certified ISO/IEC 27035 Information Security Incident Management Training Course

Ref: 103600295_98809 **Date:** 25 – 29 October 2027 **Location:** Kuala Lumpur **Fees:** 6500 Euro

Course Overview

The ISO/IEC 27035 Information Security Incident Management Training and Certification Course equips participants with comprehensive knowledge and practical skills required to design, implement, and manage effective incident response processes aligned with ISO/IEC 27035. This ISO/IEC 27035 training course focuses on the lifecycle of incident management, from incident detection and reporting to containment, eradication, recovery, and lessons learned.

Participants will gain expertise in information security incident management training through hands-on exercises, case studies, and real-world scenarios. The course highlights the integration of ISO/IEC 27035 with ISO/IEC 27001 and ISO/IEC 27005, emphasizing risk management and compliance alignment. Through incident response training, participants will develop techniques to identify threats, assess incident impact, and activate incident response teams.

The ISO/IEC 27035 lead incident manager training also covers incident communication, reporting, and continual improvement, ensuring that participants can lead and enhance organizational incident response capabilities. Completing this ISO/IEC 27035 certification training prepares participants for the PECB ISO/IEC 27035 incident manager certification, boosting career opportunities for incident response professionals, risk managers, and IT security leaders.

Target Audience

- Information security incident managers
- IT and information security managers
- Incident response team IRT members
- Risk managers and compliance officers
- IT system and network administrators
- Internal auditors
- Consultants involved in information security incident management
- Professionals preparing for ISO/IEC 27035 lead incident manager certification

AGILE LEADERS
Training Center

Targeted Organizational Departments

- Information security and cybersecurity departments
- IT operations and network administration teams
- Incident response teams and security operations centers SOCs
- Risk management and compliance offices
- Internal audit and governance departments
- Business continuity and disaster recovery teams

Targeted Industries

- Banking and financial services
- Healthcare and pharmaceuticals
- Government and public sector
- Technology and telecommunications
- Manufacturing and supply chain sectors
- Critical infrastructure and utilities
- E-commerce and online services
- Consulting and professional services

Course Offerings

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

- Explain the ISO/IEC 27035 incident response life cycle
- Apply ISO/IEC 27035 implementation roadmap to build incident management processes
- Conduct information security threat identification training and incident risk analysis
- Design ISO/IEC 27035 incident detection and reporting procedures
- Implement incident containment and eradication training
- Apply information security incident investigation training techniques
- Manage post-incident reviews and lessons learned training
- Align ISO/IEC 27035 monitoring and continual improvement with ISO/IEC 27001 requirements
- Prepare for the PECB ISO/IEC 27035 certification exam preparation process

Training Methodology

This ISO/IEC 27035 training course uses a hands-on, interactive learning approach that combines expert instruction, practical case studies, group discussions, and scenario-based exercises. Participants work through the complete incident response process, from initial incident detection to recovery and follow-up, using the ISO/IEC 27035 incident response framework.

The course integrates interactive group work where participants develop incident management plans, define roles and responsibilities, and build communication strategies using information security incident communication training. Participants also conduct mock incident simulations, applying incident handling and response training to contain, eradicate, and recover from security incidents.

Throughout the training, participants review ISO/IEC 27035 monitoring and continual improvement strategies, incident post-mortem techniques, and audit preparation processes, ensuring alignment with ISO/IEC 27035 for ISO/IEC 27001 compliance and broader governance programs.

Course Toolbox

- ISO/IEC 27035 training manual
- Incident management policy and procedure templates
- Incident communication and escalation templates
- Incident detection and reporting checklists
- Incident management roles and responsibilities matrix
- Sample incident risk assessment templates
- Incident post-mortem and lessons learned documentation templates
- ISO/IEC 27035 certification exam preparation guide
- Case studies illustrating ISO/IEC 27035 incident management best practices
- Incident tracking and monitoring tools examples

Course Agenda

Day 1: Introduction and Core Principles of Incident Management

- Topic 1: Overview of ISO/IEC 27035 training course and certification process
- Topic 2: Understanding information security incident management training fundamentals
- Topic 3: ISO/IEC 27035 incident response life cycle and integration with ISO/IEC 27001
- Topic 4: Defining incident management roles and responsibilities training
- Topic 5: Incident management policies and procedures development
- Topic 6: Information security threat identification training and initial risk assessment
- Reflection & Review: Review of ISO/IEC 27035 incident manager certification requirements and key takeaways

Day 2: Incident Detection, Reporting, and Assessment

- Topic 1: ISO/IEC 27035 incident detection techniques and monitoring best practices
- Topic 2: Incident reporting and tracking software guidance
- Topic 3: Incident communication and escalation procedures training
- Topic 4: Incident assessment and decision-making training
- Topic 5: Conducting information security event assessment training
- Topic 6: Preparing incident management documentation training and reporting templates
- Reflection & Review: Review of incident detection and reporting processes

AGILE LEADERS
Training Center

Day 3: Incident Response and Eradication

- Topic 1: Incident response team IRT training and activation processes
- Topic 2: Incident handling and response training using ISO/IEC 27035
- Topic 3: Incident containment and eradication training best practices
- Topic 4: Information security incident investigation training methods
- Topic 5: Legal and regulatory considerations in incident response
- Topic 6: Integrating incident response with ISO/IEC 27035 risk management integration
- Reflection & Review: Review of incident response strategies and techniques

Day 4: Post-Incident Review and Continuous Improvement

- Topic 1: Conducting incident post-mortem and lessons learned training
- Topic 2: Applying ISO/IEC 27035 continual improvement framework to incident management
- Topic 3: ISO/IEC 27035 internal audit and review training for incident programs
- Topic 4: Monitoring and continual improvement techniques for incident processes
- Topic 5: ISO/IEC 27035 incident management case studies and real-world examples
- Topic 6: Aligning ISO/IEC 27035 with ISO/IEC 27001 and other governance frameworks
- Reflection & Review: Review of continuous improvement and audit strategies

Day 5: Certification Preparation and Final Review

- Topic 1: Reviewing key concepts for PECB ISO/IEC 27035 certification exam preparation
- Topic 2: ISO/IEC 27035 incident management best practices and case study review
- Topic 3: Reviewing ISO/IEC 27035 incident manager career development opportunities
- Topic 4: Final review of ISO/IEC 27035 implementation roadmap and audit preparation
- Topic 5: Final certification exam
- Reflection & Review: Final peer feedback and participant action plans

FAQ

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

There are no formal prerequisites for this ISO/IEC 27035 training course. However, basic knowledge of information security, risk management, or incident response processes will be beneficial. This course is ideal for those seeking ISO/IEC 27035 incident manager certification.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session lasts approximately 4-5 hours, including presentations, interactive exercises, and group discussions. The total duration of the ISO/IEC 27035 certification training spans approximately 20-25 hours across one week.

How does ISO/IEC 27035 integrate with ISO/IEC 27001 and ISO/IEC 27005?

ISO/IEC 27035 complements ISO/IEC 27001 by enhancing incident response capabilities within the broader information security management system. It also supports ISO/IEC 27005 by addressing incident-related risks and aligning incident management processes with enterprise risk management frameworks.

How This Course is Different from Other ISO/IEC 27035 Information Security Incident Management Training and Certification Courses

This iso/iec 27035 training course stands out by offering a practical, hands-on approach to managing the full incident response life cycle, from detection to lessons learned. Unlike other courses, it integrates iso/iec 27035 certification training with real-world case studies, helping participants apply threat identification, risk assessment, and incident containment techniques in realistic scenarios.

The course also focuses heavily on incident communication, incident reporting, and compliance alignment with iso/iec 27001 and iso/iec 27005. Participants not only learn how to develop incident response plans, but also how to manage incident response teams and ensure continual improvement using the iso/iec 27035 continual improvement framework. Combined with comprehensive pecb iso/iec 27035 certification exam preparation, this training ensures participants are both technically prepared and professionally certified, making it ideal for incident managers, risk officers, and security leaders.