ISO 27035 Lead Incident Manager

⚢ **Online instructor-led**
Self-study
Modality

✗A **English**
Spanish
Language

🕐 **5 days**
Duration

Master the implementation and management of information security incident processes with the ISO/IEC 27035 Lead Incident Manager course. In just 5 days, you'll acquire the skills to detect, assess, respond to, and report security incidents — helping organisations reduce risks and safeguard critical information assets.

Aligned with ISO/IEC 27001, ISO/IEC 27005, and other related standards, this course provides practical tools for designing and managing effective incident response plans and teams. After passing the exam, you'll be eligible for the PECB Certified ISO/IEC 27035 Lead Incident Manager credential — proof of your ability to lead incident management operations strategically and efficiently.

Learning 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 organisation's needs

⊘ Conduct risk assessments to identify potential threats and vulnerabilities within an organization

⊘ Apply best practices from international standards to improve the efficiency and effectiveness of incident response efforts

⊘ Conduct post-incident analysis and identify lessons learned

Who Should Attend?

🔍 Managers or consultants seeking to expand their knowledge of information security incident management

⊛ Professionals aiming to establish and manage effective Incident Response Teams (IRTs)

☑ IT professionals and security risk managers improving incident handling capabilities

📖 Members of incident response teams

🗒 Incident response coordinators or roles with responsibilities in incident handling and response

What's Included?

📱 450+ pages of course content, exercises, case studies, and quizzes

🗎 Certification and exam fees included

☺ Course completion attestation, granting 31 CPD credits.

Course Agenda

Day 1 | Introduction to Information Security Incident Management and ISO/IEC 27035

- Training course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts of incident management

- Information security incident management
- Context establishment
- Policies and procedures

Day 2 Designing and preparing an Information Security Incident Management plan

- Risk management
- Incident management plan
- Incident management team
- Internal and external relationships
- Technical and other support
- Information security incident awareness and training

Day 3 Detecting and reporting information security incidents

- Testing
- Monitor systems and networks
- Detect and alert
- Information collection for incidents
- Report information security events
- Information security event assessment

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

- Resolve information security incidents
- Containment, eradication, and recovery
- Lessons learned
- Monitoring, measurement, analysis, and evaluation
- Continual improvement
- Closing of the training course

Day 5 Certification Exam.

Certification & Exam

🎓 Certification Prerequisites

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

	ISO/IEC 27035 Provisional Incident Manager	ISO/IEC 27035 Incident Manager	ISO/IEC 27035 Lead Incident Manager	ISO/IEC 27035 Senior Lead Incident Manager	Other requirements
General Work Experience	None	2 Years	5 Years	10 years	
Information security incident management experience	None	1 year	2 Years	7 years	Signing the PECB Code of Ethics
Incident management project experience	None	200 hours	300 hours	1000 hours	

📄 **Exam:** 3 hours, taken on Day 5

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 for Information Security incidents and implementing an Incident Management Plan.

Domain 5 | Implementing incident management processes and managing information security incidents.

Domain 6 | Improving the incident management processes and activities

✓ **Retake:** Free retake within 12 months if needed

📄 **Maintenance Fee:** First year included; fees applies from second year. Pay $120/year or save 10% by paying three years upfront.

🔗 For additional information, please contact us at hello@ttgi.tech **04**