Course technical sheet

Incident Response Support – Training Course

Fee
99,00 €
Final exam only

Course code	Test duration	Passing score	Issued
IR_SUPPORT_LA	45 min	70%	28/05/2026

Executive summary

The "Incident Response Support – Training Course" is designed to deliver practical and operational knowledge for supporting cybersecurity incident management. In just 45 minutes, participants will learn how to effectively assist in key phases such as triage, escalation, evidence collection and preservation, and post-incident review. The course references international standards including ISO/IEC 27001, ISO/IEC 27035, and globally recognized best practices like the NIST SP 800-61 guidelines. The acquired skills enable support teams to operate efficiently in complex scenarios, including environments with mobile devices, IoT, OT/ICS systems, e-commerce, and critical infrastructures. This course is suited for IT technicians, SOC operators, and support personnel seeking a solid operational framework to contribute effectively to incident response, with a practical and immediately applicable approach.

Certification process

- Registration or login to the Academy platform.
- Completion of the final course examination only. Any training or preparation may be completed externally or through other channels.
- The test questions refer to the objectives, skills and topics described in this technical sheet.
- Assessment of the result, possible validation and certificate issuance according to the rules applicable to the course.

Important note

On Academy, candidates take only the final course examination. Any training or preparation activity may be delivered externally or through other channels. The test questions refer to the topics described in this technical sheet and in the course syllabus summary.

Syllabus summary

ISO/IEC 27001 and ISO/IEC 27002 (incident management) + ISO/IEC 27035 (Information security incident management) + NIST SP 800-61 (Computer Security Incident Handling Guide) + triage, escalation, evidence handling and post-incident review best practices

Learning Objectives

- Provide operational skills for supporting cybersecurity incident response
- Apply standards and best practices in incident management
- Enhance capabilities in triage, escalation, evidence collection, and post-incident review

Certification Bodies Management systems
IFZA Business Park - Building A2 - Nadd Hessa - Dubai Silicon Oasis
United Arab Emirates
Phone: +971 502475030
Email: info@certificatoiwz.org
VAT/Tax ID: 104216397000003

Skills Acquired

- Familiarity with key standards ISO/IEC 27001, 27002, 27035
- Ability to assist in evidence handling and chain of custody
- Skills in supporting containment, remediation, and communication operations

Target Audience

- IT technicians
- SOC operators
- Incident Response support staff
- Cybersecurity support personnel

Prerequisites

- Basic knowledge of cybersecurity and IT infrastructures

Course Content

- Incident management fundamentals
- Response lifecycle phases: triage, escalation, evidence collection
- Operational support tools and methods
- Post-incident review and reporting

Teaching Methodology

- Lectures with practical examples
- Case study analysis and sample questions

Assessment Method

- Final test with 70% pass threshold

Duration

- 45 minutes

Certification

- Certificate of attendance (with €99.00 fee)

Expected Outcomes

- Ability to effectively support Incident Response teams
- Improved operational incident management capabilities