Course technical sheet

Cyber Security Manager – Training Course

Fee
1.200,00 €
Final exam only

Course code	Test duration	Passing score	Issued
CSM_LA	60 min	70%	28/05/2026

Executive summary

The "Cyber Security Manager – Training Course" is designed to equip professionals with the skills needed to effectively manage cybersecurity within complex organizations. This program provides an in-depth understanding of key standards such as ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and the NIST Cybersecurity Framework. Participants will develop expertise in security governance, risk management, and the development and monitoring of security programs. The course also covers vendor management, KPIs/KRIs, and security architecture principles like Zero Trust and defence-in-depth. Practical scenarios from varied sectors including retail, public administration, logistics, and banking allow learners to apply methodologies for risk assessment and mitigation. Upon completion, participants will be prepared to make strategic decisions to strengthen organizational defenses, coordinate security teams, and engage effectively with stakeholders to ensure compliance and enhance organizational resilience.

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 (ISMS governance and controls) + ISO/IEC 27005 (risk management) + NIST Cybersecurity Framework (CSF) + security governance, program management, KPI/KRI and supplier management best practices

Learning Objectives

- Provide in-depth knowledge of IT security standards and frameworks
- Develop skills in security governance and risk management
- Apply best practices in security program and vendor management

Skills Acquired

- Understanding and implementation of ISO/IEC 27001, 27002, and 27005
- Use of the NIST Cybersecurity Framework
- Definition and monitoring of KPIs and KRIs
- Management of security operations and architecture (Zero Trust, defence-in-depth)

Target Audience

- IT and security professionals
- Managers interested in strategic cybersecurity management

Prerequisites

- Basic knowledge of IT and cybersecurity

Course Content

- Fundamentals of security standards and frameworks
- Governance and risk management
- Security architecture and operations
- Vendor management and compliance
- Case studies and practical scenarios

Teaching Methodology

- Theoretical lessons
- Real case analysis
- Quizzes and interactive discussions

Assessment

- Final test with 70% passing criteria

Duration

- 60 minutes

Certification

- Certificate of completion (certification fee applies)

Expected Outcomes

- Ability to manage and coordinate security programs
- Capability to support audits and improve organizational security posture