TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Cyber Security Manager – Training Course

Price / certificate issuance
On request
VAT excluded

Course code	Minimum duration	Final pass score	Dossier issue
CSM_LA	60 min	70%	28/11/2026

1. Course identity, purpose and scope

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.

This extended technical dossier describes the pathway as published in CIWZ Academy on the issue date. It consolidates purpose, references, learning architecture, module contents, assessment system, passing criteria and certificate conditions. It does not replace the official texts of the standards, laws, guidelines or schemes referenced.

2. Normative, regulatory and technical references

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

References are used as the learning and assessment framework within the limits of published content and available sources. For professional application, the official and current versions of the referenced documents always prevail.

3. Learning architecture and assessment system

- minimum tracked time: 60 min

- active final-exam bank: 200 questions
- final exam: 30 questions selected from the bank
- passing threshold: 70%

- Direct access to the final assessment under the published rules for the exam-only pathway.
- Exam assembly from the active course bank and scoring against the published pass threshold.
- Recording of the result and, where applicable, request for the final certificate.

4. Official catalogue technical information

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

7. Assessment system, final exam and passing criteria

- The final assessment consists of 30 questions selected from the active course bank. The platform applies an anti-repetition logic for new attempts when the bank size allows it.
- Final question-bank size detected at generation time: 200 active questions.
- Published passing threshold for the course: 70%.
- Questions are intended to assess not only recall but also interpretation, application, evidence selection, scenario assessment and quality of decision-making, depending on the subject matter.

8. Tracking, learning continuity and session integrity

- Path status, completed modules and recorded time are managed server-side when the course uses the Academy learning mode.
- The platform allows the pathway to resume from the recorded point and retains the results of required checks.
- Assessment sessions may be subject to the integrity and proctoring controls enabled by the platform and described in the applicable usage rules.
- Technical and integrity events support assessment and do not replace professional judgement where human review is required.

9. Certificate, use and limitations

The CIWZ certificate, where provided by the pathway and requested after passing, records the result achieved in the stated CIWZ pathway or assessment. It does not automatically replace personnel certification, professional registration, statutory licence, legal qualification or credentials issued by third-party bodies where such requirements are imposed by the applicable scheme.

10. Commercial and tax conditions

- Price / certificate issuance: On request VAT excluded.
- UAE VAT is applied to UAE customers according to billing data and the applicable tax rules.
- Any specific commercial terms, agreements or corporate orders override the public price only when formally accepted by Certificato IWZ FZCO.

11. Dossier document control

- Document automatically generated by CIWZ Academy from the course data published at the time of the request.
- Course code: CSM_LA
- Document language: EN

- Generation date: 28/11/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.