TECHNICAL LEARNING AND ASSESSMENT DOSSIER

CISO (Chief Information Security Officer) – Training Course

Price / certificate issuance
On request
VAT excluded

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

1. Course identity, purpose and scope

The CISO (Chief Information Security Officer) training course aims to equip professionals with the skills to manage and oversee information security within organizations, focusing on international best practices such as ISO/IEC 27001, ISO/IEC 27002, and the NIST Cybersecurity Framework. Through a blend of theory and practical case studies, participants will deepen their ability to assess and mitigate risks, manage security incidents, and ensure protection of IT and OT/ICS infrastructures. The curriculum addresses asset management, access controls, network and application security, and incident response with a focus on specific environments including hospitals, SaaS companies, manufacturing groups, and public administrations. Graduates will gain a comprehensive understanding of corporate security and the tools to develop strategic security plans that support business objectives and regulatory compliance.

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 + ISO/IEC 27005 (risk management) + NIST Cybersecurity Framework (CSF) and information security governance 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

- Train professionals to lead organizational information security
- Deepen understanding of standards and frameworks such as ISO/IEC 27001, 27002, 27005 and NIST CSF
- Develop practical skills in risk management, OT/ICS security, network, application security and incident response

Skills Acquired

- Cybersecurity risk assessment and mitigation
- Security management in IT and OT/ICS environments
- Implementation of physical and logical security controls
- Coordination of security incident response

Target Audience

- IT professionals and security managers
- Compliance officers and auditors
- Security consultants and analysts

Prerequisites

- Basic knowledge of IT and networking
- Familiarity with cybersecurity concepts

Syllabus

- ISO/IEC 27001, 27002 and ISO/IEC 27005 standards
- NIST Cybersecurity Framework
- Asset management and information classification
- Security governance and change management
- Incident response and threat intelligence
- Operational controls for network, applications, IAM
- Case studies on hospitals, SaaS, manufacturing, and public authorities

Teaching Method

- Theoretical lectures

- Analysis of real cases
- High difficulty scenario questions

Evaluation Method

- Multiple-choice test on practical scenarios
- Passing score set at 70%

Duration

- 60 minutes

Certification

- Attendance certificate issued upon passing the test with a fee

Expected Outcomes

- Ability to develop and manage effective security strategies
- Increased awareness of technological risks
- Operational skills to improve security governance

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: CISO_LA
- Document language: EN

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