TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Insider Threat Analyst Support – Training Course

Price / certificate issuance
99,00 €
VAT excluded

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

1. Course identity, purpose and scope

The "Insider Threat Analyst Support – Training Course" is designed to offer specialized assistance to analysts handling internal threats within organizations. The course takes a focused approach covering identification, analysis, and management of insider threats across diverse operational contexts such as consulting firms, hospitals, SaaS companies, manufacturing groups, and retailers. Best practices are explored, including access controls, UEBA-based monitoring, auditing, and privileged account management, aligned with international standards like ISO/IEC 27001, ISO/IEC 27002, and NIST SP 800-53. The curriculum incorporates complex case studies to build capabilities in support of detection, investigation, offboarding, and privacy management phases, targeting professionals in IT security and compliance. Participants gain skills to apply objective evidence and proportionate measures to reduce internal risks, enhancing corporate security governance.

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 (access controls, logging, HR security) + UEBA and monitoring principles + NIST SP 800-53 (auditing and account management controls) + detection, investigations, privileged access management and privacy safeguards 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

Training Objectives

- Understand the support role for insider threat analysts
- Apply controls and best practices for identifying and managing internal threats
- Manage objective evidence in complex operational scenarios

Skills Acquired

- Knowledge of ISO/IEC 27001, 27002, and NIST SP 800-53 standards
- Ability to support investigations and UEBA monitoring
- Privileged account management and offboarding handling

Target Audience

- IT and security professionals
- Compliance officers
- Internal risk analysts

Prerequisites

- Basic cybersecurity knowledge
- Familiarity with access management and auditing

Program

- Introduction to insider threats and risk models
- Security standards and related regulations
- Monitoring and UEBA in real environments
- Investigation playbooks and operational support
- Privilege and offboarding management
- Privacy and compliance

Teaching Methodology

- Theoretical lessons
- Case studies and scenarios

- Situational assessment questions

Assessment Methods

- Multiple-choice test with 70% passing score

Duration

- 60 minutes

Certification

- Completion certificate upon positive outcome and possible fee

Expected Outcomes

- Ability to effectively support insider threat analysts
- Practical awareness of best practices and regulations
- Improved internal threat management

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: 99,00 € 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: INSIDER_THREAT_LA
- Document language: EN

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