



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

ISO/IEC 27001:2022 – Cybersecurity & ISMS Lead Manager

Course + certificate

1.250,00 €

VAT excluded

Course code

CYBER-27001-EXEC

Minimum duration

424 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Executive and operational pathway for CISOs, ICT leaders, risk managers, auditors and executives who must govern, implement and measure an ISMS according to ISO/IEC 27001:2022 and ISO/IEC 27002:2022 controls.

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 27001:2022 + Amd 1:2024; ISO/IEC 27002:2022; ISO/IEC 27000:2026; ISO 31000:2018; ISO 19011 current

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

- 8 structured learning modules
- minimum tracked time: 424 min
- intermediate-check bank: 256 questions
- active final-exam bank: 240 questions
- final exam: 30 questions selected from the bank
- passing threshold: 75%
- Access to the pathway through the personal Academy profile or a corporate assignment.
- Sequential study of the modules, with server-side recording of progress and required minimum time.

- Intermediate checks linked to modules to verify understanding, application capability and quality of reasoning.
- Final exam unlock only after the pathway requirements have been completed.
- Protected final exam assembled by the platform through selection from the active course question bank.
- Recording of the result and, where applicable, the option to request the final certificate.

4. Official catalogue technical information

Course technical sheet

CIWZ Academy executive/professional pathway with original content, server-tracked learning, 8 modules, randomized intermediate checks, Secure Proctor in assessments and a scenario-based final question bank. Free access; any fee applies only to certificate issuance after passing.

5. Detailed course syllabus

The following syllabus is derived from the active modules published on the platform. Each module shows its minimum study time and the size of its available intermediate-check bank.

01 Context, scope and ISMS governance

Minimum time: 53 min | Intermediate questions: 32

02 Risk assessment, risk treatment and Statement of Applicability

Minimum time: 53 min | Intermediate questions: 32

03 Leadership, competence and security culture

Minimum time: 53 min | Intermediate questions: 32

04 Organizational, people, physical and technological controls

Minimum time: 53 min | Intermediate questions: 32

05 Supplier, cloud and supply-chain security

Minimum time: 53 min | Intermediate questions: 32

06 Monitoring, detection and incident management

Minimum time: 53 min | Intermediate questions: 32

07 Performance, audit and management review

Minimum time: 53 min | Intermediate questions: 32

08 Improvement, resilience and maturity roadmap

Minimum time: 53 min | Intermediate questions: 32

6. Developed module-by-module contents

The following pages analytically describe the content actually associated with each platform module. The structure is designed so that learners, companies, HR, Quality, HSE or CISO functions can understand precisely what is studied and assessed.

MODULE 01**Context, scope and ISMS governance**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Define boundaries, dependencies, interested parties, contractual and regulatory requirements, critical assets and organizational interfaces that determine the real ISMS scope.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Translate strategy and accountability into a governance model with owners, escalation, committees, decision criteria and linkage to enterprise risk management.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Translate strategy and accountability into a governance model with owners, escalation, committees, decision criteria and linkage to enterprise risk management.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Approved scope, process/asset map, requirements matrix, RACI, decision minutes, dependency register and justified exclusion criteria.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A group acquires a company with separate infrastructure: decide whether to extend scope immediately, define transition and compensating controls. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Percentage of critical assets/processes covered by scope and average time to close governance gaps.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Scope defined only for certification convenience; unclear ownership; third-party requirements not translated into operational criteria.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Context, scope and ISMS governance".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 02**Risk assessment, risk treatment and Statement of Applicability**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Build repeatable risk criteria, threat scenarios, impact and likelihood/exposure assessment, including supply-chain, cloud, identity and critical-dependency risks.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Link each treatment to a decision, owner, time frame, resources and controls; use Annex A as a completeness reference, not an automatic checklist.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Link each treatment to a decision, owner, time frame, resources and controls; use Annex A as a completeness reference, not an automatic checklist.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Risk register, criteria, treatment plan, residual-risk approvals, SoA, implementation evidence and periodic reviews.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A high ransomware risk is formally accepted without analysing immutable backups and recovery capability: assess whether the acceptance is sustainable and authorized. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Percentage of above-threshold risks with overdue treatment and share of SoA controls with recent effectiveness testing.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Scores without criteria; copied SoA; controls declared implemented without evidence; residual risk accepted at the wrong authority level.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Risk assessment, risk treatment and Statement of Applicability".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 03**Leadership, competence and security culture**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Integrate security into management decisions, budgeting, operational priorities and expected behaviour of staff, suppliers and leadership.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define role-based competence, risk-based awareness, simulations, accountability and escalation mechanisms that make security part of daily work.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Define role-based competence, risk-based awareness, simulations, accountability and escalation mechanisms that make security part of daily work.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Competence matrix, training plans, simulation results, budget decisions, targeted campaigns and exception management evidence.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A team completes annual training but continues to fail phishing simulations and secret handling: define role- and behaviour-based interventions. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Recurrence rate for high-risk behaviours and escalation time for staff-reported events.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: One-size-fits-all training; attendance-only KPIs; leadership bypassing controls under urgency; undocumented exceptions.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Leadership, competence and security culture".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 04**Organizational, people, physical and technological controls**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Interpret ISO/IEC 27002 controls according to risk: identity, access, logging, endpoints, cloud, secure development, cryptography, backups, physical security and suppliers.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Design preventive, detective and corrective controls with configuration, ownership, thresholds, monitoring and effectiveness testing proportionate to criticality.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Design preventive, detective and corrective controls with configuration, ownership, thresholds, monitoring and effectiveness testing proportionate to criticality.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Baselines, configurations, logs, tickets, EDR/SIEM reports, restore tests, access reviews, vulnerability evidence, contracts and supplier audits.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A shared privileged account is justified by operations: assess alternatives, traceability and compensating measures. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Privileged MFA coverage, critical-vulnerability remediation time, restore-test success and access-review completion rate.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Controls present but not monitored; unusable logs; backups never restored; privileged access without individual accountability.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Organizational, people, physical and

technological controls”.

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 05**Supplier, cloud and supply-chain security**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Govern risk arising from cloud, MSPs, SaaS, software, subcontractors and concentrated dependencies, including shared responsibility and continuity.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Classify suppliers by criticality; define minimum requirements, due diligence, clauses, monitoring, incident notification, exit plans and continuity testing.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Classify suppliers by criticality; define minimum requirements, due diligence, clauses, monitoring, incident notification, exit plans and continuity testing.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Supplier register, risk tiering, security annexes, attestations, assessments, SLA, breach-notification clauses, exit plan and test results.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A critical SaaS uses undisclosed subprocessors and changes data region: assess security, privacy and continuity impact. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Share of critical suppliers with current assessment, incident-notification SLA and tested exit plan.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Initial-only due diligence; blind trust in certificates; no subcontractor inventory; inability to exit the service.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Supplier, cloud and supply-chain security".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 06**Monitoring, detection and incident management**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Connect logging, detection engineering, triage and incident response to risk assessment and ISO/IEC 27035 processes.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define use cases, log sources, retention, ownership, severity, playbooks, escalation, decision authority and lessons learned.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Define use cases, log sources, retention, ownership, severity, playbooks, escalation, decision authority and lessons learned.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Use-case catalogue, SIEM rules, alert history, incident records, timeline, communication log, post-incident review and corrective actions.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A high-severity alert is closed as false positive without preserving evidence: assess impact on investigation capability and compliance. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: MTTD, MTTR, tested-use-case coverage, false-positive rate and post-incident action closure.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Too many unprioritized alerts; unsynchronized logging; untested playbooks; lessons learned without owner or deadline.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Monitoring, detection and incident management".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 07**Performance, audit and management review**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Turn data, audits and management review into decisions on risk, resources and improvement, avoiding dashboards with little operational meaning.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define indicators with formula, source, frequency, threshold and expected decision; plan audits by risk and verify action effectiveness.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Define indicators with formula, source, frequency, threshold and expected decision; plan audits by risk and verify action effectiveness.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: KPIs/KRIs, trends, audit plan, reports, follow-up, management-review inputs/outputs, decisions and resource changes.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A dashboard shows all KPIs green but uses an incomplete dataset after migration: decide whether the information is still reliable. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Share of indicators with verified data quality, audit-finding closure rate and average time from review to funded decision.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: KPIs chosen because easy; calendar-based audits ignoring risk; descriptive management review; actions closed without effectiveness checks.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Performance, audit and management review".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 08**Improvement, resilience and maturity roadmap**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Use nonconformities, incidents, near misses, threat intelligence and business change to drive improvement, resilience and multi-year priorities.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Distinguish correction from corrective action, verify systemic causes, update risk/SoA and build a roadmap with dependencies, milestones and indicators.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Distinguish correction from corrective action, verify systemic causes, update risk/SoA and build a roadmap with dependencies, milestones and indicators.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Root-cause analysis, corrective-action records, updated risk assessment, revised SoA, maturity roadmap, investment case and effectiveness evidence.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

The same provisioning error recurs across different systems: decide whether to fix cases individually or redesign the cross-cutting process. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Recurrence rate, high-risk action backlog, maturity progress and reduction in residual exposure.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Local fixes without root cause; unfunded roadmap; self-referential maturity score; no link between incidents and risk assessment.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Improvement, resilience and maturity roadmap".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

7. Assessment system, final exam and passing criteria

- Intermediate checks are linked to individual modules and provide progressive learning control before access to the final assessment.
- 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: 240 active questions.
- Published passing threshold for the course: 75%.
- 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

- Course + certificate: 1.250,00 € 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: CYBER-27001-EXEC
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.