



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

NIS2 & Cybersecurity Governance – Executive CISO Program

Course + certificate

2.450,00 €

VAT excluded

Course code

NIS2-CISO-EXEC

Minimum duration

360 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Executive NIS2 governance course for boards, CISOs, executives, risk managers and function owners, focusing on Italian Legislative Decree 138/2024, risk-management measures, incident reporting, supply chain, accountability and oversight.

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

Directive (EU) 2022/2555 (NIS2); Italian Legislative Decree 4 September 2024 No. 138; applicable ACN measures; ISO/IEC 27001:2022; ISO/IEC 27035-1/-2:2023; NIST CSF 2.0

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: 360 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 NIS2 scope, entities and governance

Minimum time: 45 min | Intermediate questions: 32

02 Management-body accountability and control model

Minimum time: 45 min | Intermediate questions: 32

03 Cybersecurity risk-management measures

Minimum time: 45 min | Intermediate questions: 32

04 Incident classification, notification and crisis governance

Minimum time: 45 min | Intermediate questions: 32

05 Supply chain, cloud and third parties

Minimum time: 45 min | Intermediate questions: 32

06 Vulnerability management and secure lifecycle

Minimum time: 45 min | Intermediate questions: 32

07 Business continuity, backup and cyber resilience

Minimum time: 45 min | Intermediate questions: 32

08 Audit readiness, evidence and compliance program

Minimum time: 45 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**NIS2 scope, entities and governance**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

Understand scope, sectors, essential/important entities and the relationship between EU law, Italian implementation and national competent-authority measures.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Build an applicability map covering legal entities, services, sectors, dependencies, registrations and compliance owners.

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: Build an applicability map covering legal entities, services, sectors, dependencies, registrations and compliance owners.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Applicability assessment, cyber governance chart, board resolutions, RACI, essential-service inventory and decision register.

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 operates across sectors and subsidiaries: determine which entities are in scope and how to govern shared responsibilities without confusing them. 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 entities/services classified with documented owner and rationale.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Scope based only on brand; responsibility delegated to IT alone; missing board-level decisions.

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 "NIS2 scope, entities and 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**Management-body accountability and control model**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

NIS2 governance requires effective top-management involvement, oversight of measures and sufficient knowledge to make risk-proportionate decisions.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define board reporting, escalation thresholds, delegations, executive training, budget, risk acceptance and oversight of corrective actions.

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 board reporting, escalation thresholds, delegations, executive training, budget, risk acceptance and oversight of corrective actions.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Board packs, minutes, training records, risk acceptance, budget approvals, cyber dashboards and action tracking.

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 board approves a generic annual report but receives no exposure indicators or incident trends: redesign reporting and decision rights. 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: Time between risk-threshold breach and decision by the authorized level.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Board informed only after incidents; technical reports not translated into business risk; delegation without oversight.

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 "Management-body accountability and control model".

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**Cybersecurity risk-management measures**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

Integrate policies, incident handling, continuity, supply-chain security, secure acquisition/development, vulnerability handling, effectiveness assessment, cyber hygiene, cryptography, access control and MFA according to risk.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Map obligations to concrete controls and link them to critical services, threat scenarios, owners, evidence and tests.

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: Map obligations to concrete controls and link them to critical services, threat scenarios, owners, evidence and tests.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Control matrix, risk register, policies, test results, vulnerability reports, backup/recovery tests, IAM evidence and supplier controls.

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 company has complete policies but no recovery tests and partial MFA on remote access: establish risk-based priorities. 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: Coverage of measures on critical services and share of controls effectiveness-tested in the last cycle.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Regulatory checklist not linked to risk; measures documented but unvalidated; exceptions without expiry.

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 "Cybersecurity risk-management

measures”.

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**Incident classification, notification and crisis governance**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

Distinguish event, incident, significant incident and crisis; govern triage, materiality, notification decisions, communications and evidence preservation.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Create a workflow with timestamps, owners, escalation, assessment, legal/privacy coordination and templates for required notification phases.

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: Create a workflow with timestamps, owners, escalation, assessment, legal/privacy coordination and templates for required notification phases.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Incident timeline, severity matrix, notification decision log, communications, evidence preservation, post-incident review.

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

An attack is quickly contained but affected an essential service: decide whether and how containment changes notification relevance. 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: Time from detection to classification and from classification to notification decision.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Notification decisions without timestamps; uncoordinated overlap with GDPR; incidents closed before lessons learned.

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 "Incident classification, notification and crisis 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 05**Supply chain, cloud and third parties**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

Assess dependencies on suppliers, MSPs, cloud, software, telecommunications and subcontractors as part of service risk, not merely procurement compliance.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define tiering, due diligence, minimum requirements, incident reporting, auditability, vulnerability disclosure, exit strategy and concentration risk.

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 tiering, due diligence, minimum requirements, incident reporting, auditability, vulnerability disclosure, exit strategy and concentration risk.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Supplier inventory, criticality tier, contract clauses, security assessments, SBOM where relevant, incident SLA, exit test.

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

Two critical suppliers depend on the same hyperscaler: assess concentration 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 tested exit strategy and verified contractual notification duty.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: External rating used as sole due diligence; no subcontractor visibility; automatic renewals without reassessment.

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 "Supply chain, cloud and third parties".

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**Vulnerability management and secure lifecycle**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

Govern asset inventory, vulnerability discovery, prioritization, patching, secure development/acquisition, change management and disclosure using real-exposure criteria.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define risk-based SLAs, exceptions, compensating controls, asset owners, remediation evidence, secure SDLC and software-dependency verification.

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 risk-based SLAs, exceptions, compensating controls, asset owners, remediation evidence, secure SDLC and software-dependency verification.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Asset inventory, scan results, threat/exploit evidence, patch tickets, exception approvals, secure code review, dependency inventories.

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 CVSS affects a non-exposed asset while a medium one is actively exploited on an internet-facing service: define priorities. 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: Remediation time by effective risk and share of critical assets with current ownership and scanning.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: CVSS-only prioritization; incomplete inventory; permanent exceptions; secure development not integrated into pipelines.

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 "Vulnerability management and secure

lifecycle”.

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**Business continuity, backup and cyber resilience**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

Link BIA, continuity, disaster recovery, backup, crisis management and ICT dependencies to service objectives and realistic cyber scenarios.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define RTO/RPO, recovery sequence, segregated/immutable copies, emergency access, tests, communications and manual fallbacks.

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 RTO/RPO, recovery sequence, segregated/immutable copies, emergency access, tests, communications and manual fallbacks.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: BIA, DR plan, restore tests, tabletop, immutable-backup evidence, dependency map, crisis contact lists.

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

Backups exist but use the same credentials as production: assess actual ransomware resilience. 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 services tested end-to-end against RTO/RPO and successful restores of representative samples.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Paper-only tests; unvalidated RTOs; always-mounted online backups; plans missing supplier dependencies.

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 "Business continuity, backup and cyber resilience".

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**Audit readiness, evidence and compliance program**

- Minimum required time: 45 min
- Available intermediate-check bank: 32 questions

Executive briefing

Build sustainable compliance based on evidence, ownership, deadlines and risk-based assurance rather than occasional document collection.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Create a control library, evidence calendar, testing plan, remediation governance and executive reporting integrated with ISMS and audit.

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: Create a control library, evidence calendar, testing plan, remediation governance and executive reporting integrated with ISMS and audit.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Control/evidence matrix, test scripts, issue register, remediation plan, board reporting and versioned evidence repository.

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

Weeks before an assessment the organization collects documents retroactively: transform the approach into continuous 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: Share of controls with evidence owner and current proof; average aging of high-risk findings.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Evidence assembled at year end; no owner; repeated findings; board reporting without trends and residual risk.

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 "Audit readiness, evidence and compliance program".

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: 2.450,00 € 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: NIS2-CISO-EXEC
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.