



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Cyber Incident Response & Crisis Management – ISO/IEC 27035 / NIST SP 800-61r3

Course + certificate

780,00 €

VAT excluded

Course code

IR-27035-CYBER

Minimum duration

424 min

Final pass score

75%

Dossier issue

14/10/2026

1. Course identity, purpose and scope

Advanced pathway for CSIRT/SOC teams, CISOs, incident managers and executives covering preparation, detection, triage, containment, eradication, recovery, crisis communications and post-incident improvement.

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 27035-1:2023; ISO/IEC 27035-2:2023; ISO/IEC 27035-3:2020; ISO/IEC 27035-4:2024; NIST SP 800-61 Rev.3 (2025); NIST CSF 2.0; NIS2/Italian Legislative Decree 138/2024 where applicable

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 Incident response governance and preparation

Minimum time: 53 min | Intermediate questions: 32

02 Detection, logging and triage

Minimum time: 53 min | Intermediate questions: 32

03 Scoping, analysis and incident classification

Minimum time: 53 min | Intermediate questions: 32

04 Containment strategy and decisions under pressure

Minimum time: 53 min | Intermediate questions: 32

05 Eradication, recovery and validation

Minimum time: 53 min | Intermediate questions: 32

06 Forensic readiness and digital evidence during incidents

Minimum time: 53 min | Intermediate questions: 32

07 Communication, notification and crisis leadership

Minimum time: 53 min | Intermediate questions: 32

08 Post-incident review, lessons learned and resilience improvement

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**Incident response governance and preparation**

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

Executive briefing

Build policies, teams, roles, on-call coverage, escalation, decision authority, playbooks, asset context, contacts and dependencies before an incident occurs.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define CSIRT operating model, severity criteria, war room, legal/privacy liaison, executive escalation, evidence handling and vendor coordination.

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 CSIRT operating model, severity criteria, war room, legal/privacy liaison, executive escalation, evidence handling and vendor coordination.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: IR plan, call tree, RACI, playbooks, contact lists, tabletop results, tooling readiness and evidence procedures.

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 incident occurs overnight and no one knows who can authorize isolation of a critical system: fix governance 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: Average team activation time and share of playbooks tested in the latest cycle.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Untested plan; outdated contacts; implicit responsibilities; undefined containment authority.

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 response governance and preparation".

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**Detection, logging and triage**

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

Executive briefing

Turn alerts, logs, threat intelligence and reports into assessable events with context, priority and early evidence preservation.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define data sources, time synchronization, triage queues, enrichment, severity, false-positive handling and escalation criteria.

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 data sources, time synchronization, triage queues, enrichment, severity, false-positive handling and escalation criteria.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: SIEM/EDR evidence, alert history, timestamps, asset criticality, triage notes, source reliability and preserved artefacts.

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 EDR alert looks benign but coincides with privileged-account use and anomalous traffic: avoid premature closure based on one signal. 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, triage latency, false-positive rate and share of critical alerts with complete enrichment.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Alert fatigue; unsynchronized clocks; closure without notes; missing asset context and threat intelligence.

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 "Detection, logging and triage".

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**Scoping, analysis and incident classification**

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

Executive briefing

Determine what happened, when, which assets/accounts/data are involved, what access persists and which current/potential impact should drive decisions.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Build timelines, hypotheses, evidence matrices, blast radius, attacker objectives, confidence levels and classification rationale.

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 timelines, hypotheses, evidence matrices, blast radius, attacker objectives, confidence levels and classification rationale.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Timeline, IOCs, affected-asset list, identity evidence, network traces, hypothesis log, confidence and severity decisions.

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 single endpoint shows infostealer malware but credentials are reused in cloud systems: expand scope beyond the compromised host. 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 to establish blast radius with a stated confidence level.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Scoping limited to first asset; hypotheses confused with facts; severity based only on malware name.

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 "Scoping, analysis and incident classification".

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**Containment strategy and decisions under pressure**

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

Executive briefing

Balance damage reduction, business continuity, evidence preservation and the ability to observe the attacker without increasing risk.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Choose immediate or staged containment, segmentation, credential reset, isolation, blocks and compensating measures with a decision log.

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: Choose immediate or staged containment, segmentation, credential reset, isolation, blocks and compensating measures with a decision log.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Containment plan, approvals, actions, timestamps, impact assessment, evidence snapshots and communication records.

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

Immediately isolating a server may stop production and lose useful volatile evidence: decide based on risk, criticality and alternatives. 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 to effective containment and number of urgent actions executed without required authorization.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Reflexive containment without impact analysis; uncoordinated password resets; undocumented 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 "Containment strategy and decisions under

pressure”.

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**Eradication, recovery and validation**

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

Executive briefing

Remove persistence/technical root cause, restore services from trusted sources and validate the environment before declaring normalization.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define clean-build criteria, patching, credential rotation, restore, heightened monitoring, staged return and business validation.

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 clean-build criteria, patching, credential rotation, restore, heightened monitoring, staged return and business validation.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Rebuild records, patch evidence, credential resets, restore tests, validation checklist, monitoring results and service acceptance.

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

Restoring an earlier backup without removing stolen credentials may recreate compromise: coordinate recovery and eradication. 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: Validated recovery time and share of restored systems with completed control validation.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Recovery treated as “system online”; no validation; all services restored simultaneously; monitoring reduced too early.

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 “Eradication, recovery and validation”.

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**Forensic readiness and digital evidence during incidents**

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

Executive briefing

Integrate evidence collection and preservation into incident response without unnecessarily delaying containment, maintaining traceability and integrity.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define volatility priorities, imaging/log export, hashing, chain of custody, time sources, evidence repositories and access control.

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 volatility priorities, imaging/log export, hashing, chain of custody, time sources, evidence repositories and access control.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Acquisition notes, hashes, chain of custody, tool/version records, time sources, evidence storage and analyst notes.

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 administrator runs troubleshooting commands before acquisition: document changes and assess reliability of remaining evidence. 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 major incidents with complete evidence packs and gap-free chain of custody.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Screenshots instead of acquisitions; missing hashes; tool version unrecorded; evidence stored on writable shared folders.

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 "Forensic readiness and digital evidence during incidents".

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**Communication, notification and crisis leadership**

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

Executive briefing

Coordinate management, legal, privacy, customers, authorities, insurers, suppliers and external communications with consistent messages and traceable decisions.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define audiences, owners, approvals, facts/unknowns, cadence, notification triggers, spokespersons and secure channels.

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 audiences, owners, approvals, facts/unknowns, cadence, notification triggers, spokespersons and secure channels.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Situation reports, decision logs, notification records, stakeholder matrices, approved statements and communication timelines.

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

Management wants to state “no exfiltration” before analysis is complete: communicate uncertainty without false reassurance. 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 to first reliable situation report and number of messages corrected/withdrawn for errors.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Absolute statements with incomplete data; insecure channels; notifications managed without coordination with the technical timeline.

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 “Communication, notification and crisis leadership”.

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**Post-incident review, lessons learned and resilience improvement**

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

Executive briefing

Turn incidents into measurable improvement, distinguishing technical, organizational and governance root causes and verifying that actions reduce risk.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Conduct blameless PIRs, build causal chains, prioritize actions, update risk registers/playbooks/detections and test 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: Conduct blameless PIRs, build causal chains, prioritize actions, update risk registers/playbooks/detections and test effectiveness.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: PIR reports, root-cause analysis, action registers, risk updates, control changes, new detection rules and effectiveness tests.

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

After ransomware, a new tool is purchased but identity governance and backup design remain unchanged: assess whether the cause was addressed. 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 by cause and share of PIR actions closed with effectiveness verification.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Descriptive PIR; individual blame; actions without owners; lessons learned not integrated into risk, training and testing.

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 "Post-incident review, lessons learned and resilience improvement".

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: 780,00 € 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: IR-27035-CYBER
- Document language: EN
- Generation date: 14/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.