



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Zero Trust, IAM & PAM Specialist

Course + certificate

On request

VAT excluded

Course code

ZT-IAM-PAM

Minimum duration

456 min

Final pass score

75%

Dossier issue

14/10/2026

1. Course identity, purpose and scope

Advanced pathway to design identity, access and privilege according to Zero Trust principles in hybrid enterprise organizations.

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

NIST SP 800-207; NIST SP 800-63; OAuth 2.0 / OpenID Connect / SAML / SCIM; FIDO2 and identity security 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

- 8 structured learning modules
- minimum tracked time: 456 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

Specialist CIWZ Academy pathway with original content, server-tracked lessons, 8 modules, randomized intermediate checks, protected final assessment and a scenario-based question bank. Indicative average market benchmark: EUR 2,190 (typical range EUR 1,490 – EUR 2,990). 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 Zero Trust principles and identity architecture

Minimum time: 57 min | Intermediate questions: 32

02 Identity lifecycle, joiner-mover-leaver and governance

Minimum time: 57 min | Intermediate questions: 32

03 Federation, SSO and authentication standards

Minimum time: 57 min | Intermediate questions: 32

04 Authorization, ABAC/RBAC and policy engineering

Minimum time: 57 min | Intermediate questions: 32

05 PAM, JIT and session governance

Minimum time: 57 min | Intermediate questions: 32

06 Machine identity, secrets and workload trust

Minimum time: 57 min | Intermediate questions: 32

07 Access analytics, UEBA and risk-based access

Minimum time: 57 min | Intermediate questions: 32

08 Operating model, metrics and continuous program

Minimum time: 57 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**Zero Trust principles and identity architecture**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Apply the “never trust, always verify” principle to users, devices, applications and workloads.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define policy-decision points, signal sources, trust algorithms and enforcement points.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Define policy-decision points, signal sources, trust algorithms and enforcement points.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Zero Trust architectures, identity maps, policy models and trust-signal inventories.

Professional scenario

Access still depends solely on the corporate network: redesign the architecture. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Percentage of policy-based accesses and trust-signal coverage.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Zero Trust reduced to a slogan, disconnected identities, unused signals.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme “Zero Trust principles and identity architecture”.

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 02**Identity lifecycle, joiner-mover-leaver and governance**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Bring identity creation, modification and revocation under control over time.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use authoritative sources, provisioning, deprovisioning, role models and recertification.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Use authoritative sources, provisioning, deprovisioning, role models and recertification.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Role catalogs, lifecycle workflows, access reviews and orphan-account reports.

Professional scenario

An employee changes role but retains old privileges: correct the lifecycle. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Deprovisioning time, orphan accounts, completed reviews.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Manual provisioning, unmanaged roles, delayed offboarding.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Identity lifecycle, joiner-mover-leaver and governance".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 03**Federation, SSO and authentication standards**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Design a coherent ecosystem of federation, SSO and strong authentication.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply SAML, OIDC, OAuth, FIDO2, phishing-resistant MFA and conditional access.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Apply SAML, OIDC, OAuth, FIDO2, phishing-resistant MFA and conditional access.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Federation inventories, application trust settings, MFA coverage and conditional-access policies.

Professional scenario

A legacy application does not support modern controls: define realistic compensating measures. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: MFA coverage, federated apps, exceptions on legacy auth.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: SSO without review, permanent legacy auth, bypassable MFA.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Federation, SSO and authentication standards".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 04**Authorization, ABAC/RBAC and policy engineering**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Design robust, understandable access policies for people, APIs and workloads.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Balance RBAC, ABAC, SoD, policy granularity and maintainability.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Balance RBAC, ABAC, SoD, policy granularity and maintainability.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Policy catalogs, authorization models, SoD matrices and test evidence.

Professional scenario

An application assigns roles inconsistently across departments: normalize policies. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: SoD violations, policy-exception rate, role-explosion index.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Role proliferation, opaque policies, inherited authorizations without control.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Authorization, ABAC/RBAC and policy engineering".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 05**PAM, JIT and session governance**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Control privileged access, administrative sessions and break-glass scenarios in a verifiable way.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use vaults, brokers, approval workflows, JIT/JEA and session recording.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Use vaults, brokers, approval workflows, JIT/JEA and session recording.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Privileged-vault reports, session logs, approval evidence and emergency-access reviews.

Professional scenario

A team uses generic admin accounts for speed: introduce PAM without blocking work. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Privileged accounts vaulted, privileged-session traceability, emergency-use frequency.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Shared accounts, static passwords, persistent elevated access.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "PAM, JIT and session governance".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 06**Machine identity, secrets and workload trust**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Extend identity governance to workloads, services, certificates and secrets.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Manage service principals, mTLS, certificate lifecycle, API credentials and rotation.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Manage service principals, mTLS, certificate lifecycle, API credentials and rotation.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Secret inventories, certificate maps, rotation evidence and service-identity policies.

Professional scenario

Many integrations rely on uninventoried static secrets: build a remediation plan. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Secret-rotation coverage, expiring certificates, machine-identity ownership.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Invisible machines, expiring certificates, secrets reused everywhere.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Machine identity, secrets and workload trust".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 07**Access analytics, UEBA and risk-based access**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Make access adaptive and contextual using behavioural and risk signals.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Combine device posture, geo, session risk, identity protection and anomaly detection.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Combine device posture, geo, session risk, identity protection and anomaly detection.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Risk-policy tuning, anomaly reviews, session-risk logs and feedback loops.

Professional scenario

Legitimate but atypical accesses create operational doubt: design a proportionate response. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Adaptive policies triggered, confirmed risky sign-ins, false challenge rate.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Adaptive access too weak or too intrusive, uncalibrated signals.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Access analytics, UEBA and risk-based access".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 08**Operating model, metrics and continuous program**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Structure IAM/PAM as an enterprise program rather than a tool-centric project.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define roadmaps, ownership, capability maturity, training and governance forums.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Define roadmaps, ownership, capability maturity, training and governance forums.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Program roadmaps, maturity scores, governance minutes and executive dashboards.

Professional scenario

The organization buys an IAM suite but does not change processes or roles: bring focus back to the operating model. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Recertification coverage, privileged reduction, stale-account trend and program maturity.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Tool first, process later; weak governance; success measured only on deployment.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Operating model, metrics and continuous program".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

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: 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: ZT-IAM-PAM
- Document language: EN
- Generation date: 14/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.