



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

SASE / SSE & Secure Access Architecture Specialist

Course + certificate

On request

VAT excluded

Course code

SASE-SSE-ARCH

Minimum duration

392 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Specialist pathway to design modern secure-access architectures using ZTNA, SWG, CASB, DLP, RBI and integration with enterprise networks and cloud.

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

Zero Trust access principles; SWG/CASB/ZTNA design best practices; DLP and cloud-access governance guidance

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: 392 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 1,690 (typical range EUR 1,090 – EUR 2,390). 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 Why SASE/SSE and what changes

Minimum time: 49 min | Intermediate questions: 32

02 ZTNA and access to private applications

Minimum time: 49 min | Intermediate questions: 32

03 SWG, DNS security and web protection

Minimum time: 49 min | Intermediate questions: 32

04 CASB, SaaS governance and shadow IT

Minimum time: 49 min | Intermediate questions: 32

05 DLP, classification and data control

Minimum time: 49 min | Intermediate questions: 32

06 Integration with networks, SD-WAN and hybrid environments

Minimum time: 49 min | Intermediate questions: 32

07 Telemetry, incidents and service operations

Minimum time: 49 min | Intermediate questions: 32

08 Governance, cost model and adoption roadmap

Minimum time: 49 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**Why SASE/SSE and what changes**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Understand the business and security drivers that move the perimeter toward distributed access services.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Map user, branch, remote, cloud and private/SaaS application use cases.

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: Map user, branch, remote, cloud and private/SaaS application use cases.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Use-case maps, current-state architectures and gap assessments.

Professional scenario

Remote access still relies on all-or-nothing VPNs: define the evolution. 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: Applications migrated to zero-trust access and users covered by the new model.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: SASE understood only as a new vendor, no service redesign.

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 "Why SASE/SSE and what changes".

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**ZTNA and access to private applications**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Design least-privilege application access without unnecessary network exposure.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define brokers, posture checks, policies, publishing and segmentation.

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 brokers, posture checks, policies, publishing and segmentation.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Application inventories, ZTNA policies, connector designs and access logs.

Professional scenario

A critical application is not yet ready for ZTNA: introduce a gradual path. 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: Apps behind ZTNA, accesses with posture checks, VPN exceptions.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: The network remains the real perimeter, direct publishing, overly broad policies.

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 "ZTNA and access to private applications".

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**SWG, DNS security and web protection**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Govern web browsing, inspection, malware delivery and Internet policies.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply categorization, proportionate TLS inspection, DNS policies and browser isolation where needed.

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 categorization, proportionate TLS inspection, DNS policies and browser isolation where needed.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Web-policy sets, exception registers, DNS-policy evidence and RBI use cases.

Professional scenario

Business browsing requires risky dynamic sites: build balanced 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: Web-policy coverage, blocked DNS events, RBI adoption for high-risk use cases.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Policies too permissive or too restrictive, exceptions out of 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 "SWG, DNS security and web protection".

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**CASB, SaaS governance and shadow IT**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Gain visibility and control over SaaS applications, data sharing and shadow-IT risk.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Map sanctioned/unsanctioned apps, SaaS posture, OAuth apps and tenant risk.

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: Map sanctioned/unsanctioned apps, SaaS posture, OAuth apps and tenant risk.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: CASB reports, sanctioned-app lists, sharing policies and OAuth governance.

Professional scenario

The business adopts new SaaS without security review: introduce effective governance. 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: Shadow-IT apps, externally shared files, SaaS-posture remediation.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: CASB used only for information, unclassified apps, ignored OAuth consents.

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 "CASB, SaaS governance and shadow IT".

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**DLP, classification and data control**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Protect data in motion to web, email, SaaS and cloud applications.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Combine classification, fingerprints, contextual rules and exception workflows.

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 classification, fingerprints, contextual rules and exception workflows.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: DLP rule sets, classification labels, incident handling and exception approvals.

Professional scenario

Teams share sensitive files with external partners: establish rules and exceptions. 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: Confirmed DLP incidents, false positives, overdue exceptions.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Noisy DLP, missing classification, never-ending exceptions.

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 "DLP, classification and data control".

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**Integration with networks, SD-WAN and hybrid environments**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Integrate SASE/SSE with WAN, branches, data centres and cloud coherently.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define traffic steering, PoP selection, HA, split tunnelling and coexistence strategy.

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 traffic steering, PoP selection, HA, split tunnelling and coexistence strategy.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Traffic architectures, branch rollout plans, resilience models and migration runbooks.

Professional scenario

A branch has unstable connectivity and mixed applications: design the service. 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: Migrated branches, user experience, failover tested, cloud-path coverage.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Chaotic routing, arbitrary split tunnelling, high vendor dependency without fallback.

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 "Integration with networks, SD-WAN and hybrid environments".

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**Telemetry, incidents and service operations**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Manage observability, troubleshooting and incident response in a distributed access fabric.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use user/app/policy logs, service health, incident runbooks and support models.

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 user/app/policy logs, service health, incident runbooks and support models.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Operations dashboards, incident playbooks, provider SLAs and troubleshooting trees.

Professional scenario

A policy block creates widespread business impact: respond in an orderly way. 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: Mean time to restore, policy rollback, incident trends.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Undefined service operations, total dependency on vendor support.

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 "Telemetry, incidents and service operations".

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**Governance, cost model and adoption roadmap**

- Minimum required time: 49 min
- Available intermediate-check bank: 32 questions

Executive briefing

Make SASE/SSE adoption sustainable with governance, costs and measurable outcomes.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Plan roadmaps, ownership, KPIs, risk acceptance and change communication.

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: Plan roadmaps, ownership, KPIs, risk acceptance and change communication.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Program roadmaps, cost models, adoption dashboards and governance decisions.

Professional scenario

The project starts IT-driven but without business sponsorship: strengthen the enterprise use case. 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: Adoption rate, policy coverage, branch-migration status, cost per protected user.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Vague roadmaps, unread cost data, success measured only on technical activation.

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 "Governance, cost model and adoption roadmap".

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: SASE-SSE-ARCH
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.