



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Cloud Security Architecture Specialist – AWS · Azure · GCP

Course + certificate

On request

VAT excluded

Course code

CLOUD-SEC-ARCH

Minimum duration

480 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Specialist pathway to design, implement and govern secure cloud architectures in multi-cloud and hybrid environments, with strong focus on identity, networking, data, logging, resilience and shared responsibility.

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 27017; ISO/IEC 27018; CSA CCM v4; NIST SP 800-207; CIS Benchmarks; AWS/Azure/GCP 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: 480 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 2,290 (typical range EUR 1,490 – EUR 3,290). 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 Shared responsibility model and landing zone

Minimum time: 60 min | Intermediate questions: 32

02 Identity, privileged access and federation

Minimum time: 60 min | Intermediate questions: 32

03 Networks, segmentation and private access

Minimum time: 60 min | Intermediate questions: 32

04 Data protection, keys and secrets

Minimum time: 60 min | Intermediate questions: 32

05 Logging, detection and response in the cloud

Minimum time: 60 min | Intermediate questions: 32

06 Hardening workloads, containers and serverless

Minimum time: 60 min | Intermediate questions: 32

07 Resilience, backup and disaster recovery

Minimum time: 60 min | Intermediate questions: 32

08 Cost governance, compliance and operations

Minimum time: 60 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**Shared responsibility model and landing zone**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Understand how accountability, controls and risk are distributed across provider, tenant, platform team and workload owner in enterprise cloud environments.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define landing zone, account structure, guardrails, naming, tagging, policy baseline and segregation of duties.

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 landing zone, account structure, guardrails, naming, tagging, policy baseline and segregation of duties.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Landing-zone blueprint, policy baseline, account/subscription/project maps, accountability matrices.

Professional scenario

A group rapidly opens new subscriptions without a coherent baseline: redesign the onboarding 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: Guardrail coverage and average time to bring new environments into compliance.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Tenants created by exception, unenforced policies, privileged roles granted for convenience.

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 "Shared responsibility model and landing zone".

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, privileged access and federation**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Manage cloud-native and federated identity, administrative access, temporary roles and trust boundaries among directories, workloads and pipelines.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply least privilege, MFA, access review, just-in-time access, privileged-session control and secret hygiene.

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 least privilege, MFA, access review, just-in-time access, privileged-session control and secret hygiene.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Evidence of role design, access review, privileged activity, secret rotation and break-glass governance.

Professional scenario

An administrator uses permanent credentials across multiple clouds: design a safer and more traceable 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: Privileged MFA coverage, average secret age, percentage of high-privilege roles reviewed.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Excessive roles, shared accounts, opaque federation, forgotten static keys.

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, privileged access and federation".

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**Networks, segmentation and private access**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Design secure cloud topologies with segmentation, private endpoints, egress control, DNS governance and hybrid connectivity.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Separate management plane, data plane and user plane; define coherent access and inspection patterns.

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: Separate management plane, data plane and user plane; define coherent access and inspection patterns.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Network diagrams, route tables, firewall policy, flow logs, DNS zone design, peering/transit patterns.

Professional scenario

A critical workload is exposed to the Internet for operational convenience: correct the architecture without disrupting 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: Number of publicly exposed services and private-endpoint coverage.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Flat network, unnecessary ingress, unmanaged outbound traffic, DNS shadow IT.

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 “Networks, segmentation and private 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 04**Data protection, keys and secrets**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Apply classification, encryption, key management, tokenization and data segregation across storage, databases, analytics and backups.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Set proper use of KMS/HSM, BYOK/HYOK, rotation, envelope encryption and data residency.

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: Set proper use of KMS/HSM, BYOK/HYOK, rotation, envelope encryption and data residency.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Key policy, encryption status, secret-vault usage, backup evidence, DLP and retention settings.

Professional scenario

A team replicates sensitive data to an unintended region: manage impact, remediation and prevention. 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: Encryption coverage, key rotation, data-residency exceptions, incidents involving secrets.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Keys without owners, encryption “enabled” but not verified, secrets in repositories.

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 “Data protection, keys and secrets”.

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**Logging, detection and response in the cloud**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Make control plane, identity events, workloads, storage and network observable for detection, audit and cloud forensics.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define use cases, retention, normalization and alert priorities linked to business context.

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 use cases, retention, normalization and alert priorities linked to business context.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Log-source inventory, SIEM mappings, alert tuning, trail integrity and incident playbooks.

Professional scenario

Logs are missing on a high-risk administrative account: build a coverage and compensating-control 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: Log coverage for critical accounts, MTTR on cloud events, high-severity false positives.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Logging enabled but not centralized, insufficient retention, detections lacking context.

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 "Logging, detection and response in the cloud".

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**Hardening workloads, containers and serverless**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Defend IaaS, PaaS, container and serverless workloads through baselines, patching, posture management and runtime control.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Integrate CSPM, vulnerability management, image security, runtime protection and policy-as-code.

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: Integrate CSPM, vulnerability management, image security, runtime protection and policy-as-code.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Hardening baselines, posture reports, patch evidence, image scans and exception register.

Professional scenario

A serverless function accesses sensitive data with excessive permissions: reduce the blast radius. 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: Scan coverage, open exceptions, critical misconfigurations, remediation time.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Obsolete golden images, reactive patching, image drift, non-automated 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 “Hardening workloads, containers and serverless”.

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**Resilience, backup and disaster recovery**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Plan availability, backup, restore and multi-account/multi-region DR aligned with RTO/RPO and application dependencies.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Translate business impact into resilient architectures and periodic recovery testing.

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: Translate business impact into resilient architectures and periodic recovery testing.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: DR runbooks, restore reports, dependency maps, RTO/RPO evidence, chaos/game-day notes.

Professional scenario

A backup exists but does not enable full application recovery: redefine the resilience program. 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: Restore-test outcomes, services with proven DR, variance from target RTO/RPO.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Backups without testing, DR only documented, external dependencies ignored.

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 “Resilience, backup and disaster recovery”.

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**Cost governance, compliance and operations**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Combine security, compliance, operations and cost control to keep the cloud model sustainable 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 dashboards, ownership, risk acceptance, exception workflows and periodic review.

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 dashboards, ownership, risk acceptance, exception workflows and periodic review.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Cloud-security KPIs, cost anomalies, compliance score, exception register and operating review.

Professional scenario

Cost reduction drives the disabling of critical controls: decide an acceptable compromise. 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: Posture/cost trend, overdue exceptions, orphaned resources, owner coverage.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Costs managed separately from risk, ownerless resources, perpetual 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 "Cost governance, compliance and 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.

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