



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

Cloud Security Architecture Specialist – AWS · Azure · GCP

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

CLOUD-SEC-ARCH

Durata minima

480 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso specialistico per progettare, implementare e governare architetture cloud sicure in ambienti multi-cloud e ibridi, con forte attenzione a identità, rete, dati, logging, resilienza e shared responsibility.

La presente scheda tecnica estesa descrive il percorso così come pubblicato nella CIWZ Academy alla data di emissione. Riunisce finalità, riferimenti, architettura didattica, contenuti dei moduli, sistema delle verifiche, criteri di superamento e condizioni di attestazione. Il documento non sostituisce i testi ufficiali delle norme, delle leggi, delle linee guida o degli schemi richiamati.

2. Riferimenti normativi, regolamentari e tecnici

ISO/IEC 27017; ISO/IEC 27018; CSA CCM v4; NIST SP 800-207; CIS Benchmarks; AWS/Azure/GCP security best practices

I riferimenti sono utilizzati come quadro di studio e di valutazione nei limiti del contenuto pubblicato e delle fonti disponibili. Per l'applicazione professionale prevalgono sempre le versioni ufficiali e vigenti dei documenti richiamati.

3. Architettura didattica e sistema di verifica

- 8 moduli didattici strutturati
- tempo minimo tracciato: 480 min
- banca verifiche intermedie: 256 quesiti
- banca esame finale attiva: 240 quesiti
- esame finale: 30 quesiti selezionati dalla banca
- soglia di superamento: 75%
- Accesso al percorso attraverso il profilo Academy personale o tramite assegnazione aziendale.
- Studio sequenziale dei moduli, con registrazione server-side dell'avanzamento e del tempo minimo previsto.

- Verifiche intermedie associate ai moduli per controllare comprensione, capacità applicativa e qualità del ragionamento.
- Sblocco dell'esame finale solo dopo il completamento dei requisiti previsti dal percorso.
- Esame finale protetto, composto dalla piattaforma mediante selezione dalla banca attiva del corso.
- Registrazione dell'esito e, quando previsto, possibilità di richiedere l'attestato finale.

4. Informazioni tecniche ufficiali di catalogo

Scheda tecnica del corso

Percorso CIWZ Academy specialistico e operativo con contenuti originali, lezioni tracciate lato server, 8 moduli, verifiche intermedie randomizzate, assessment finale protetto e banca domande scenario-based. Benchmark medio di mercato indicativo: € 2.290 (range tipico € 1.490 – € 3.290). Accesso gratuito; eventuale costo solo per l'emissione del certificato dopo il superamento.

5. Programma analitico del percorso

Il programma seguente è ricavato dai moduli attivi pubblicati nella piattaforma. Per ciascun modulo sono indicati il tempo minimo e la consistenza della banca di verifica intermedia disponibile.

01 Modello di responsabilità condivisa e landing zone

Tempo minimo: 60 min | Quesiti intermedi: 32

02 Identity, accesso privilegiato e federation

Tempo minimo: 60 min | Quesiti intermedi: 32

03 Reti, segmentazione e accesso privato

Tempo minimo: 60 min | Quesiti intermedi: 32

04 Protezione dei dati, chiavi e segreti

Tempo minimo: 60 min | Quesiti intermedi: 32

05 Logging, detection e risposta nel cloud

Tempo minimo: 60 min | Quesiti intermedi: 32

06 Hardening workload, container e serverless

Tempo minimo: 60 min | Quesiti intermedi: 32

07 Resilienza, backup e disaster recovery

Tempo minimo: 60 min | Quesiti intermedi: 32

08 Governance economica, conformità e operations

Tempo minimo: 60 min | Quesiti intermedi: 32

6. Contenuti sviluppati modulo per modulo

Le pagine seguenti descrivono in modo analitico i contenuti effettivamente associati a ciascun modulo della piattaforma. La struttura è concepita per consentire a candidato, azienda, HR, Quality, HSE o CISO di comprendere con precisione cosa viene studiato e verificato.

MODULO 01**Modello di responsabilità condivisa e landing zone**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Comprendere come si distribuiscono responsabilità, controlli e rischi tra provider, tenant, platform team e workload owner in ambienti cloud enterprise.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire landing zone, account structure, guardrail, naming, tagging, policy baseline e segregation of duties.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Definire landing zone, account structure, guardrail, naming, tagging, policy baseline e segregation of duties.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Blueprint di landing zone, policy baseline, mappe account/subscription/project, matrici responsabilità.

Scenario professionale

Un gruppo apre rapidamente nuove subscription senza baseline coerente: ridisegnare il modello di onboarding. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Copertura dei guardrail e tempo medio di conformazione dei nuovi ambienti.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Tenant creati in deroga, policy non enforce, ruoli privilegiati concessi per comodità.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Modello di responsabilità condivisa e landing zone".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 02**Identity, accesso privilegiato e federation**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Gestire identità cloud-native e federate, accessi amministrativi, ruoli temporanei e trust boundary tra directory, workload e pipeline.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare least privilege, MFA, access review, just-in-time, privileged session control e secret hygiene.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Applicare least privilege, MFA, access review, just-in-time, privileged session control e secret hygiene.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Evidence di role design, access review, privileged activity, secret rotation e break-glass governance.

Scenario professionale

Un amministratore usa credenziali permanenti in più cloud: progettare un modello più sicuro e tracciabile. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Copertura MFA privilegiata, età media dei secret, percentuale ruoli ad alto privilegio rivisti.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Ruoli eccessivi, account condivisi, federazione opaca, chiavi statiche dimenticate.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Identity, accesso privilegiato e federation".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 03**Reti, segmentazione e accesso privato**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Progettare topologie cloud sicure con segmentazione, private endpoints, egress control, DNS governance e connettività ibrida.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Separare management plane, data plane e user plane; definire pattern di accesso e ispezione coerenti.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Separare management plane, data plane e user plane; definire pattern di accesso e ispezione coerenti.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Diagrammi di rete, route table, firewall policy, flow logs, DNS zone design, peering/transit patterns.

Scenario professionale

Un workload critico è esposto su Internet per semplicità operativa: correggere l'architettura senza bloccare il servizio. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Numero di servizi pubblicamente esposti e copertura dei private endpoint.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Flat network, ingress non necessario, outbound non governato, DNS shadow IT.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Reti, segmentazione e accesso privato".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 04**Protezione dei dati, chiavi e segreti**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Applicare classificazione, cifratura, gestione chiavi, tokenizzazione e segregazione dei dati in storage, database, analytics e backup.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Stabilire uso corretto di KMS/HSM, BYOK/HYOK, rotation, envelope encryption e data residency.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Stabilire uso corretto di KMS/HSM, BYOK/HYOK, rotation, envelope encryption e data residency.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Key policy, encryption status, secret vault usage, backup evidence, DLP and retention settings.

Scenario professionale

Un team replica dati sensibili in una regione non prevista: gestire impatto, rimedio e prevenzione. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Copertura cifratura, rotazione chiavi, eccezioni di data residency, incidenti legati ai secret.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Chiavi senza owner, cifratura "enabled" ma non verificata, secret nei repository.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Protezione dei dati, chiavi e segreti".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 05**Logging, detection e risposta nel cloud**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Rendere osservabili control plane, identity events, workload, storage e rete per detection, audit e forensics nel cloud.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire use case, retention, normalizzazione e priorità di allarme legate al contesto business.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Definire use case, retention, normalizzazione e priorità di allarme legate al contesto business.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Log source inventory, SIEM mappings, alert tuning, trail integrity, incident playbook.

Scenario professionale

Mancano log su un account amministrativo ad alto rischio: costruire un piano di copertura e compensazione. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Copertura log per account critici, MTTR su eventi cloud, falsi positivi ad alta severità.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Logging attivato ma non centralizzato, retention insufficiente, detection non contestualizzate.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Logging, detection e risposta nel cloud".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 06**Hardening workload, container e serverless**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Difendere workload IaaS, PaaS, container e funzioni serverless con baseline, patching, posture management e runtime control.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Integrare CSPM, vulnerability management, image security, runtime protection e policy-as-code.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Integrare CSPM, vulnerability management, image security, runtime protection e policy-as-code.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Baseline di hardening, posture report, patch evidence, image scan, exception register.

Scenario professionale

Una function serverless accede a dati sensibili con permessi eccessivi: ridurre il blast radius. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Copertura scan, eccezioni aperte, non conformità critiche, tempo di remediazione.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Golden image obsolete, patching reattivo, image drift, policy non automatizzate.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Hardening workload, container e serverless".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 07**Resilienza, backup e disaster recovery**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Pianificare disponibilità, backup, restore e DR multi-account/multi-region coerenti con RTO/RPO e dipendenze applicative.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Tradurre impatti di business in architetture resilienti e in prove periodiche di ripristino.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Tradurre impatti di business in architetture resilienti e in prove periodiche di ripristino.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Runbook DR, report di restore, dependency map, RTO/RPO evidence, chaos/game day notes.

Scenario professionale

Un backup esiste ma non consente restore applicativo completo: ridefinire il programma di resilienza. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Esiti test restore, servizi con DR provato, scostamento da RTO/RPO target.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Backup senza test, DR solo documentato, dipendenze esterne non considerate.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Resilienza, backup e disaster recovery".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 08**Governance economica, conformità e operations**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Combinare sicurezza, conformità, operations e cost control per mantenere sostenibile il modello cloud nel tempo.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare dashboard, owner, risk acceptance, exception workflow e periodic review.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Usare dashboard, owner, risk acceptance, exception workflow e periodic review.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: KPI cloud security, cost anomalies, compliance score, exception register, operating review.

Scenario professionale

La riduzione dei costi porta alla disattivazione di controlli critici: decidere un compromesso accettabile. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Trend posture/costi, eccezioni oltre scadenza, risorse orfane, owner coverage.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Costi governati separatamente dal rischio, risorse senza owner, eccezioni perpetue.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Governance economica, conformità e operations".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

7. Sistema di verifica, esame finale e criteri di superamento

- Le verifiche intermedie sono collegate ai singoli moduli e costituiscono un controllo progressivo dell'apprendimento prima dell'accesso alla prova finale.
- La prova finale è composta da 30 quesiti selezionati dalla banca attiva del corso. La piattaforma applica una logica anti-ripetizione per i nuovi tentativi quando la consistenza della banca lo consente.
- Consistenza della banca finale rilevata al momento della generazione: 240 quesiti attivi.
- Soglia di superamento pubblicata per il corso: 75%.
- Le domande sono finalizzate a verificare non soltanto il richiamo mnemonico, ma anche interpretazione, applicazione, selezione delle evidenze, valutazione di scenari e qualità della decisione, in funzione della materia trattata.

8. Tracciamento, continuità didattica e integrità della sessione

- Lo stato del percorso, i moduli completati e il tempo registrato sono gestiti lato server quando il corso utilizza la modalità formativa Academy.
- La piattaforma consente la ripresa del percorso dal punto registrato e conserva gli esiti delle verifiche previste.
- Le sessioni di verifica possono essere soggette ai controlli di integrità e proctoring attivati dalla piattaforma e descritti nelle regole di utilizzo applicabili.
- Gli eventi tecnici e di integrità sono elementi di supporto alla valutazione e non sostituiscono il giudizio professionale quando è prevista una revisione umana.

9. Attestazione, utilizzo e limiti del documento

L'attestato CIWZ, quando previsto dal percorso e richiesto dopo il superamento, documenta il risultato ottenuto nel percorso o nella prova CIWZ indicata. Non sostituisce automaticamente certificazioni di persona, iscrizioni ad albi, abilitazioni professionali, qualifiche legali o credenziali rilasciate da organismi o soggetti terzi quando tali requisiti sono previsti dallo schema applicabile.

10. Condizioni economiche e fiscali

- Corso + attestato: Su richiesta IVA/VAT esclusa.
- La UAE VAT viene applicata ai clienti UAE secondo i dati di fatturazione e la normativa fiscale applicabile.
- Eventuali condizioni commerciali specifiche, convenzioni o ordini aziendali prevalgono sul prezzo pubblico solo se formalmente accettati da Certificato IWZ FZCO.

11. Controllo documentale della scheda

- Documento generato automaticamente dalla CIWZ Academy sulla base dei dati del corso pubblicati al momento della richiesta.
- Codice corso: CLOUD-SEC-ARCH
- Lingua documento: IT
- Data di generazione: 13/10/2026
- Per l'applicazione normativa e professionale fanno fede le fonti ufficiali vigenti e le eventuali procedure/schema applicabili.