



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

SASE / SSE & Secure Access Architecture Specialist

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

SASE-SSE-ARCH

Durata minima

392 min

Soglia finale

75%

Edizione scheda

14/10/2026

1. Identità, finalità e perimetro del percorso

Percorso specialistico per progettare architetture di accesso sicuro moderne con ZTNA, SWG, CASB, DLP, RBI e integrazione con rete enterprise e cloud.

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

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

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: 392 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: € 1.690 (range tipico € 1.090 – € 2.390). 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 Perché SASE/SSE e cosa cambia

Tempo minimo: 49 min | Quesiti intermedi: 32

02 ZTNA e accesso alle applicazioni private

Tempo minimo: 49 min | Quesiti intermedi: 32

03 SWG, DNS security e protezione web

Tempo minimo: 49 min | Quesiti intermedi: 32

04 CASB, SaaS governance e shadow IT

Tempo minimo: 49 min | Quesiti intermedi: 32

05 DLP, classificazione e controllo dei dati

Tempo minimo: 49 min | Quesiti intermedi: 32

06 Integrazione con rete, SD-WAN e ambienti ibridi

Tempo minimo: 49 min | Quesiti intermedi: 32

07 Telemetria, incidenti e operations del servizio

Tempo minimo: 49 min | Quesiti intermedi: 32

08 Governance, cost model e roadmap di adozione

Tempo minimo: 49 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**Perché SASE/SSE e cosa cambia**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Capire i driver di business e sicurezza che spostano il perimetro verso servizi di accesso distribuiti.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Mappare use case utente, filiale, remoto, cloud e applicazioni private/SaaS.

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: Mappare use case utente, filiale, remoto, cloud e applicazioni private/SaaS.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Use-case map, current-state architecture, gap assessment.

Scenario professionale

L'accesso remoto si basa ancora su VPN all-or-nothing: definire l'evoluzione. 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: Applicazioni migrate a modello zero trust e utenti coperti dal nuovo accesso.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: SASE inteso solo come nuovo vendor, nessun ridisegno del servizio.

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 "Perché SASE/SSE e cosa cambia".

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**ZTNA e accesso alle applicazioni private**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Progettare accesso applicativo least privilege senza esposizione di rete inutile.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire broker, posture check, policy, publishing e segmentation.

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 broker, posture check, policy, publishing e segmentation.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Application inventory, ZTNA policy, connector design, access logs.

Scenario professionale

Un'applicazione critica non è ancora pronta per ZTNA: introdurre un percorso graduale. 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: App dietro ZTNA, accessi con posture check, eccezioni alla VPN.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Rete ancora il vero perimetro, publish diretto, policy troppo larghe.

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 "ZTNA e accesso alle applicazioni private".

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**SWG, DNS security e protezione web**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Governare navigazione web, ispezione, malware delivery e policy Internet.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare categorization, TLS inspection proporzionata, DNS policy e browser isolation dove serve.

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 categorization, TLS inspection proporzionata, DNS policy e browser isolation dove serve.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Web-policy set, exception register, DNS policy evidence, RBI use cases.

Scenario professionale

La navigazione business richiede siti dinamici rischiosi: costruire policy bilanciate. 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: Coverage web policy, DNS blocked events, RBI adoption for high risk.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Policy troppo permissive o troppo bloccanti, eccezioni fuori controllo.

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 "SWG, DNS security e protezione web".

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**CASB, SaaS governance e shadow IT**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Ottenere visibilità e controllo su applicazioni SaaS, condivisione dati e rischio shadow IT.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Mappare sanctioned/unsanctioned app, posture SaaS, OAuth app e tenant risk.

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: Mappare sanctioned/unsanctioned app, posture SaaS, OAuth app e tenant risk.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: CASB reports, sanctioned app list, sharing policy, OAuth governance.

Scenario professionale

Il business adotta nuovi SaaS senza security review: introdurre governance efficace. 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: App shadow IT, file condivisi esternamente, posture SaaS remediation.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: CASB solo informativo, app non classificate, OAuth consents ignorati.

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 "CASB, SaaS governance e shadow IT".

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**DLP, classificazione e controllo dei dati**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Proteggere i dati in movimento verso web, email, SaaS e applicazioni cloud.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Combinare classificazione, fingerprint, context rule e workflow di eccezione.

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: Combinare classificazione, fingerprint, context rule e workflow di eccezione.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: DLP rule set, classification labels, incident handling, exception approvals.

Scenario professionale

I team condividono file sensibili con partner esterni: stabilire regole e deroga. 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: DLP incidents confermati, falsi positivi, eccezioni scadute.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: DLP rumorosa, classificazione assente, eccezioni eterne.

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 "DLP, classificazione e controllo dei dati".

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**Integrazione con rete, SD-WAN e ambienti ibridi**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Integrare SASE/SSE con WAN, branch, data center e cloud in modo coerente.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire traffic steering, PoP selection, HA, split tunnel e coexistence strategy.

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 traffic steering, PoP selection, HA, split tunnel e coexistence strategy.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Traffic architecture, branch rollout plan, resilience model, migration runbook.

Scenario professionale

Una filiale ha connettività instabile e applicazioni miste: progettare 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: Branch migrate, user experience, failover tested, cloud path coverage.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Routing caotico, split tunnel casuale, alta dipendenza dal vendor senza fallback.

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 "Integrazione con rete, SD-WAN e ambienti ibridi".

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**Telemetria, incidenti e operations del servizio**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Gestire osservabilità, troubleshooting e incident response in un access fabric distribuito.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare log utente/app/policy, service health, incident runbook e support model.

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 log utente/app/policy, service health, incident runbook e support model.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Operations dashboard, incident playbook, provider SLA, troubleshooting tree.

Scenario professionale

Un blocco policy genera impatto business diffuso: rispondere in modo ordinato. 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: Mean time to restore, policy rollback, incident trend.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Service operations non definite, dipendenza totale dal vendor support.

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 "Telemetria, incidenti e operations del servizio".

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, cost model e roadmap di adozione**

- Tempo minimo previsto: 49 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Rendere sostenibile l'adozione di SASE/SSE con governance, costi e risultati misurabili.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Pianificare roadmap, owner, KPI, risk acceptance e change communication.

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: Pianificare roadmap, owner, KPI, risk acceptance e change communication.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Program roadmap, cost model, adoption dashboard, governance decisions.

Scenario professionale

Il progetto nasce IT-driven ma senza sponsorship business: consolidare il caso d'uso enterprise. 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: Adoption rate, policy coverage, branch migration status, cost per protected user.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Roadmap vaga, costi non letti, successo misurato solo su attivazione tecnica.

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, cost model e roadmap di adozione".

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: SASE-SSE-ARCH
- Lingua documento: IT
- Data di generazione: 14/10/2026
- Per l'applicazione normativa e professionale fanno fede le fonti ufficiali vigenti e le eventuali procedure/schema applicabili.