



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

Zero Trust, IAM & PAM Specialist

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

ZT-IAM-PAM

Durata minima

456 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso avanzato per progettare identità, accessi e privilegi secondo principi Zero Trust in organizzazioni enterprise ibride.

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

NIST SP 800-207; NIST SP 800-63; OAuth 2.0 / OpenID Connect / SAML / SCIM; FIDO2 and identity 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: 456 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: € 2.190 (range tipico € 1.490 – € 2.990). 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 Principi Zero Trust e architettura di identità

Tempo minimo: 57 min | Quesiti intermedi: 32

02 Identity lifecycle, joiner-mover-leaver e governance

Tempo minimo: 57 min | Quesiti intermedi: 32

03 Federation, SSO e standard di autenticazione

Tempo minimo: 57 min | Quesiti intermedi: 32

04 Authorization, ABAC/RBAC e policy engineering

Tempo minimo: 57 min | Quesiti intermedi: 32

05 PAM, JIT e session governance

Tempo minimo: 57 min | Quesiti intermedi: 32

06 Machine identity, secrets e workload trust

Tempo minimo: 57 min | Quesiti intermedi: 32

07 Access analytics, UEBA e risk-based access

Tempo minimo: 57 min | Quesiti intermedi: 32

08 Operating model, metriche e programma continuo

Tempo minimo: 57 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**Principi Zero Trust e architettura di identità**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Applicare il principio “never trust, always verify” a utenti, device, applicazioni e workload.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire policy decision point, signal sources, trust algorithm e enforcement point.

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 policy decision point, signal sources, trust algorithm e enforcement point.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Zero Trust architecture, identity map, policy model, trust signal inventory.

Scenario professionale

L'accesso dipende ancora dalla sola rete aziendale: ridisegnare l'architettura. 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: Percentuale accessi policy-based e copertura segnali di fiducia.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Zero Trust ridotto a slogan, identità scollegate, segnali non utilizzati.

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 “Principi Zero Trust e architettura di identità”.

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 lifecycle, joiner-mover-leaver e governance**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Mettere sotto controllo la creazione, modifica e revoca delle identità 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 authoritative source, provisioning, deprovisioning, role model e recertification.

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 authoritative source, provisioning, deprovisioning, role model e recertification.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Role catalog, lifecycle workflow, access review, orphan-account report.

Scenario professionale

Un dipendente cambia ruolo ma conserva vecchi privilegi: correggere il lifecycle. 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: Tempo di deprovisioning, account orfani, review completate.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Provisioning manuale, ruoli non governati, offboarding tardivo.

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 lifecycle, joiner-mover-leaver e governance".

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**Federation, SSO e standard di autenticazione**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Progettare un ecosistema coerente di federation, SSO e strong authentication.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare SAML, OIDC, OAuth, FIDO2, phishing-resistant MFA e conditional access.

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 SAML, OIDC, OAuth, FIDO2, phishing-resistant MFA e conditional access.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Federation inventory, app trust settings, MFA coverage, conditional-access policies.

Scenario professionale

Una app legacy non supporta controlli moderni: definire compensazioni realistiche. 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, app federate, exception on legacy auth.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: SSO senza review, auth legacy permanenti, MFA aggirabile.

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 "Federation, SSO e standard di autenticazione".

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**Authorization, ABAC/RBAC e policy engineering**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Disegnare politiche di accesso robuste e comprensibili per persone, API e workload.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Bilanciare RBAC, ABAC, SoD, policy granularity e maintainability.

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: Bilanciare RBAC, ABAC, SoD, policy granularity e maintainability.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Policy catalog, authorization model, SoD matrix, test evidence.

Scenario professionale

Un'applicazione assegna ruoli in modo incoerente tra reparti: normalizzare le policy. 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: Violazioni SoD, policy exception rate, role explosion index.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Ruoli proliferati, policy opache, autorizzazioni ereditate senza 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 "Authorization, ABAC/RBAC e policy engineering".

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**PAM, JIT e session governance**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Controllare accessi privilegiati, sessioni amministrative e break-glass in modo verificabile.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare vault, broker, approval workflow, JIT/JEA e session recording.

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 vault, broker, approval workflow, JIT/JEA e session recording.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Privileged vault report, session logs, approval evidence, emergency-access review.

Scenario professionale

Un team usa account admin generici per velocità: introdurre PAM senza bloccare il lavoro. 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: Privileged accounts vaulted, privileged session traceability, emergency-use frequency.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Account condivisi, password statiche, accessi elevati persistenti.

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 "PAM, JIT e session governance".

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**Machine identity, secrets e workload trust**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Estendere il governo dell'identità a workload, servizi, certificati e secret.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Gestire service principal, mTLS, certificate lifecycle, API credentials e rotation.

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: Gestire service principal, mTLS, certificate lifecycle, API credentials e rotation.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Secret inventory, certificate map, rotation evidence, service-identity policy.

Scenario professionale

Molte integrazioni dipendono da secret statici non inventariati: costruire un piano di rientro. 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: Secret rotation coverage, expiring certificates, machine identity ownership.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Macchine invisibili, certificati in scadenza, secret riutilizzati ovunque.

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 "Machine identity, secrets e workload trust".

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**Access analytics, UEBA e risk-based access**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Rendere l'accesso adattivo e contestuale usando segnali di comportamento e rischio.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Combinare device posture, geo, session risk, identity protection e anomaly detection.

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 device posture, geo, session risk, identity protection e anomaly detection.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Risk-policy tuning, anomaly review, session-risk logs, feedback loop.

Scenario professionale

Accessi leciti ma atipici generano dubbio operativo: progettare una risposta proporzionata. 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: Adaptive policies triggered, risky sign-in confirmed, false challenge rate.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Accesso adattivo troppo blando o troppo invasivo, segnali non calibrati.

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 "Access analytics, UEBA e risk-based access".

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**Operating model, metriche e programma continuo**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Strutturare IAM/PAM come programma enterprise e non solo come progetto tool-centric.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire roadmap, ownership, capability maturity, training e governance forum.

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 roadmap, ownership, capability maturity, training e governance forum.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Program roadmap, maturity score, governance minutes, executive dashboard.

Scenario professionale

L'azienda compra la suite IAM ma non cambia processi e ruoli: riportare il focus sul modello operativo. 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: Recertification coverage, privileged reduction, stale account trend, program maturity.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Tool first, process later; governance debole; successo misurato solo su deployment.

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 "Operating model, metriche e programma continuo".

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: ZT-IAM-PAM
- 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.