



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

ISO/IEC 27001:2022 – Cybersecurity & ISMS Lead Manager

Corso + attestato

1.250,00 €

IVA/VAT esclusa

Codice corso

CYBER-27001-EXEC

Durata minima

424 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso executive e operativo per CISO, responsabili ICT, risk manager, auditor e dirigenti che devono governare, implementare e misurare un ISMS secondo ISO/IEC 27001:2022 e i controlli ISO/IEC 27002:2022.

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 27001:2022 + Amd 1:2024; ISO/IEC 27002:2022; ISO/IEC 27000:2026; ISO 31000:2018; ISO 19011:2018/edizione vigente

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: 424 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 executive/professionale con contenuti originali, lezioni tracciate lato server, 8 moduli, verifiche intermedie randomizzate, Secure Proctor negli assessment e banca finale scenario-based. Accesso gratuito; eventuale costo solo per 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 Contesto, campo di applicazione e governance ISMS

Tempo minimo: 53 min | Quesiti intermedi: 32

02 Risk assessment, risk treatment e Statement of Applicability

Tempo minimo: 53 min | Quesiti intermedi: 32

03 Leadership, competenze e security culture

Tempo minimo: 53 min | Quesiti intermedi: 32

04 Controlli organizzativi, persone, fisici e tecnologici

Tempo minimo: 53 min | Quesiti intermedi: 32

05 Supplier, cloud e supply-chain security

Tempo minimo: 53 min | Quesiti intermedi: 32

06 Monitoring, detection e incident management

Tempo minimo: 53 min | Quesiti intermedi: 32

07 Performance, audit e management review

Tempo minimo: 53 min | Quesiti intermedi: 32

08 **Miglioramento, resilienza e roadmap di maturità**

Tempo minimo: 53 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**Contesto, campo di applicazione e governance ISMS**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Definire confini, dipendenze, parti interessate, requisiti contrattuali e regolatori, asset critici e interfacce organizzative che determinano il perimetro reale del sistema.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Tradurre strategia e responsabilità in un modello di governance con owner, escalation, comitati, criteri decisionali e raccordo con enterprise risk management.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Tradurre strategia e responsabilità in un modello di governance con owner, escalation, comitati, criteri decisionali e raccordo con enterprise risk management.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Campo di applicazione approvato, mappa processi/asset, matrice requisiti, RACI, verbali decisionali, registro dipendenze e criteri di esclusione motivati.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un gruppo acquisisce una società con infrastrutture separate: decidere se ampliare subito il perimetro, definire transizione e controlli compensativi. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Percentuale di asset e processi critici coperti dal perimetro e tempo medio di chiusura delle gap di governance.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Campo di applicazione definito solo per comodità certificativa; responsabilità non assegnate; requisiti di terze parti non tradotti in criteri operativi.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità).

Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Contesto, campo di applicazione e governance ISMS».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 02**Risk assessment, risk treatment e Statement of Applicability**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Costruire criteri di rischio ripetibili, scenari di minaccia, valutazione di impatto e probabilità/esposizione, inclusi rischi di supply chain, cloud, identità e dipendenze critiche.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Collegare ogni trattamento a una decisione, a un owner, a tempi, risorse e controlli; usare l'Annex A come riferimento di completezza, non come checklist automatica.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Collegare ogni trattamento a una decisione, a un owner, a tempi, risorse e controlli; usare l'Annex A come riferimento di completezza, non come checklist automatica.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Registro rischi, criteri, piano di trattamento, accettazioni del rischio residuo, SoA, evidenze di implementazione e riesami periodici.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un rischio ransomware elevato è formalmente accettato senza analisi di backup immutabili e capacità di recovery: valutare sostenibilità e autorità dell'accettazione. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Percentuale di rischi oltre soglia con trattamento scaduto e quota di controlli SoA con verifica di efficacia recente.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Punteggi senza criteri; SoA copiata; controlli dichiarati implementati senza evidenza; rischio residuo accettato dal livello organizzativo errato.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità).

Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Risk assessment, risk treatment e Statement of Applicability».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 03**Leadership, competenze e security culture**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Integrare sicurezza nelle decisioni manageriali, nel ciclo budget, nelle priorità operative e nei comportamenti attesi da personale, fornitori e management.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire competenze per ruolo, awareness basata sul rischio, simulazioni, responsabilità e meccanismi di escalation che rendano la sicurezza parte del lavoro quotidiano.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire competenze per ruolo, awareness basata sul rischio, simulazioni, responsabilità e meccanismi di escalation che rendano la sicurezza parte del lavoro quotidiano.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Matrice competenze, piani formativi, risultati di simulazioni, evidenze di decisioni budgetarie, campagne mirate e gestione delle eccezioni.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un team completa il training annuale ma continua a fallire phishing simulation e gestione segreti: definire interventi basati su comportamento e ruolo. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Tasso di recidiva per comportamento ad alto rischio e tempo di escalation degli eventi segnalati dal personale.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Formazione uguale per tutti; KPI solo di partecipazione; leadership che aggira i controlli in urgenza; eccezioni non registrate.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità).

Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Leadership, competenze e security culture».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 04**Controlli organizzativi, persone, fisici e tecnologici**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Interpretare i controlli ISO/IEC 27002 in funzione del rischio: identità, accessi, logging, endpoint, cloud, sviluppo sicuro, crittografia, backup, sicurezza fisica e fornitori.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Disegnare controlli preventivi, rilevativi e correttivi con configurazioni, ownership, soglie, monitoraggio e test di efficacia proporzionati alla criticità.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Disegnare controlli preventivi, rilevativi e correttivi con configurazioni, ownership, soglie, monitoraggio e test di efficacia proporzionati alla criticità.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Baseline, configurazioni, log, ticket, report EDR/SIEM, test restore, access review, vulnerability evidence, contratti e audit di fornitori.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un account privilegiato condiviso è giustificato da esigenze operative: valutare alternative, tracciabilità e compensazioni. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Copertura MFA privilegiata, remediation time vulnerabilità critiche, successo test restore e percentuale access review completate nei tempi.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Controlli presenti ma non monitorati; log non utilizzabili; backup mai ripristinati; accessi privilegiati senza accountability individuale.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità).

Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Controlli organizzativi, persone, fisici e tecnologici».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 05**Supplier, cloud e supply-chain security**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Governare rischio derivante da cloud, MSP, SaaS, software, subfornitori e dipendenze concentrate, considerando responsabilità condivise e continuità.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Classificare fornitori per criticità, definire requisiti minimi, due diligence, clausole, monitoraggio, incident notification, exit plan e prove di continuità.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Classificare fornitori per criticità, definire requisiti minimi, due diligence, clausole, monitoraggio, incident notification, exit plan e prove di continuità.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Supplier register, risk tiering, security annexes, attestazioni, assessment, SLA, breach notification clauses, exit plan and test results.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un SaaS critico usa subprocessor non dichiarati e cambia data region: valutare impatto su sicurezza, privacy e continuità. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Quota fornitori critici con assessment aggiornato, incident notification SLA e piano di uscita testato.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Due diligence solo iniziale; fiducia cieca nelle certificazioni; nessun inventario subfornitori; impossibilità di uscita dal servizio.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità).

Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Supplier, cloud e supply-chain security».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 06**Monitoring, detection e incident management**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Collegare logging, detection engineering, triage e incident response alla valutazione del rischio e ai processi ISO/IEC 27035.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire use case, sorgenti log, retention, ownership, severità, playbook, escalation, decision authority e lezioni apprese.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire use case, sorgenti log, retention, ownership, severità, playbook, escalation, decision authority e lezioni apprese.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Catalogo use case, SIEM rules, alert history, incident records, timeline, communication log, post-incident review and corrective actions.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un alert ad alta severità è chiuso come falso positivo senza preservare evidenze: valutare impatto su capacità investigativa e conformità. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: MTTD, MTTR, percentuale use case testati, tasso falsi positivi e chiusura delle azioni post-incident.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Troppi alert senza prioritizzazione; logging non sincronizzato; playbook non testati; lessons learned senza owner e scadenza.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Monitoring, detection e incident management».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 07**Performance, audit e management review**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Trasformare dati, audit e riesame in decisioni sul rischio, sulle risorse e sul miglioramento, evitando dashboard prive di significato operativo.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire indicatori con formula, fonte, frequenza, soglia e decisione attesa; pianificare audit per rischio e verificare l'efficacia delle azioni.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire indicatori con formula, fonte, frequenza, soglia e decisione attesa; pianificare audit per rischio e verificare l'efficacia delle azioni.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: KPI/KRI, trend, audit plan, report, follow-up, management review inputs/outputs, decisions and resource changes.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Una dashboard mostra tutti KPI verdi ma usa dataset incompleto dopo una migrazione: decidere se il dato è ancora affidabile. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Percentuale indicatori con data quality verificata, closure rate audit findings e tempo medio tra review e decisione finanziata.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: KPI scelti perché facili; audit calendar-based senza rischio; management review descrittivo; azioni chiuse senza effectiveness check.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Performance,

audit e management review”.

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 08**Miglioramento, resilienza e roadmap di maturità**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Usare non conformità, incidenti, near miss, threat intelligence e cambiamenti di business per guidare miglioramento, resilienza e priorità pluriennali.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Distinguere correzione da azione correttiva, verificare cause sistemiche, aggiornare rischio/SoA e costruire una roadmap con dipendenze, milestone e indicatori.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Distinguere correzione da azione correttiva, verificare cause sistemiche, aggiornare rischio/SoA e costruire una roadmap con dipendenze, milestone e indicatori.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Root-cause analysis, corrective-action records, updated risk assessment, revised SoA, maturity roadmap, investment case and effectiveness evidence.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Lo stesso errore di provisioning ricompare su sistemi diversi: decidere se trattare casi singoli o riprogettare il processo trasversale. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Recurrence rate, backlog di azioni ad alto rischio, maturity progress e riduzione dell'esposizione residua.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Correzioni locali senza root cause; roadmap non finanziata; maturity score autoreferenziale; nessun legame tra incidenti e risk assessment.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità).

Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Miglioramento, resilienza e roadmap di maturità».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

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: 1.250,00 € 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: CYBER-27001-EXEC
- 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.