



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

NIS2 & Cybersecurity Governance – Executive CISO Program

Corso + attestato

2.450,00 €

IVA/VAT esclusa

Codice corso

NIS2-CISO-EXEC

Durata minima

360 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Corso executive sulla governance NIS2 per organi amministrativi, CISO, dirigenti, risk manager e responsabili di funzione, con focus su D.Lgs. 138/2024, misure di gestione del rischio, incident reporting, supply chain, accountability e supervisione.

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

Direttiva (UE) 2022/2555 (NIS2); D.Lgs. 4 settembre 2024 n. 138; atti ACN applicabili; ISO/IEC 27001:2022; ISO/IEC 27035-1/-2:2023; NIST CSF 2.0

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: 360 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 Perimetro NIS2, soggetti e governance

Tempo minimo: 45 min | Quesiti intermedi: 32

02 Responsabilità degli organi di amministrazione e modello di controllo

Tempo minimo: 45 min | Quesiti intermedi: 32

03 Misure di gestione del rischio cyber

Tempo minimo: 45 min | Quesiti intermedi: 32

04 Incident classification, notification e crisis governance

Tempo minimo: 45 min | Quesiti intermedi: 32

05 Supply chain, cloud e terze parti

Tempo minimo: 45 min | Quesiti intermedi: 32

06 Vulnerability management e secure lifecycle

Tempo minimo: 45 min | Quesiti intermedi: 32

07 Business continuity, backup e cyber resilience

Tempo minimo: 45 min | Quesiti intermedi: 32

08 Audit readiness, evidenze e programma di conformità

Tempo minimo: 45 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**Perimetro NIS2, soggetti e governance**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Comprendere logica, ambito, settori, soggetti essenziali/importanti e relazione tra normativa UE, recepimento italiano e atti dell'Autorità nazionale competente.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Costruire una mappa di applicabilità con entità giuridiche, servizi, settori, dipendenze, registrazioni e owner della conformità.

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: Costruire una mappa di applicabilità con entità giuridiche, servizi, settori, dipendenze, registrazioni e owner della conformità.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Assessment di applicabilità, organigramma cyber, delibere, RACI, inventario servizi essenziali e registro delle decisioni.

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 opera in più settori e società controllate: stabilire quali entità rientrano e come governare responsabilità comuni senza confonderle. 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 entità/servizi classificati con owner e motivazione documentata.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Perimetro basato solo sul brand; responsabilità delegate al solo IT; assenza di decisioni dell'organo amministrativo.

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 «Perimetro NIS2, soggetti e governance».

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**Responsabilità degli organi di amministrazione e modello di controllo**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

La governance NIS2 richiede coinvolgimento effettivo del vertice, supervisione delle misure e conoscenza sufficiente per assumere decisioni proporzionate al rischio.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire reporting al board, soglie di escalation, deleghe, formazione executive, budget, risk acceptance e controllo delle azioni correttive.

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 reporting al board, soglie di escalation, deleghe, formazione executive, budget, risk acceptance e controllo delle azioni correttive.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Board pack, verbali, training records, risk acceptance, budget approvals, cyber dashboard and action tracking.

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

Il board approva annualmente un report generico ma non riceve indicatori di esposizione né incident trend: ridisegnare reporting e decision rights. 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: Tempo tra superamento soglia di rischio e decisione del livello autorizzato.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Board informato solo dopo incidenti; report tecnici non traducibili in rischio business; deleghe senza supervisione.

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 «Responsabilità degli organi di amministrazione e modello di controllo».

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**Misure di gestione del rischio cyber**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Integrare policy, incident handling, business continuity, supply-chain security, secure acquisition/development, vulnerability handling, effectiveness assessment, cyber hygiene, crittografia, access control e MFA secondo rischio.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Mappare obblighi in controlli concreti e collegarli a servizi critici, threat scenarios, owner, evidenze e test.

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: Mappare obblighi in controlli concreti e collegarli a servizi critici, threat scenarios, owner, evidenze e test.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Control matrix, risk register, policies, test results, vulnerability reports, backup/recovery tests, IAM evidence and supplier controls.

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

L'azienda ha policy complete ma nessun test di recovery e MFA parziale sugli accessi remoti: stabilire priorità basata sul rischio. 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 delle misure sui servizi critici e quota di controlli con test di efficacia nell'ultimo ciclo.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Checklist normativa non collegata ai rischi; misure "documentate" ma non validate; eccezioni senza 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 «Misure di gestione del rischio cyber».

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**Incident classification, notification e crisis governance**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Distinguere evento, incidente, incidente significativo e crisi; governare triage, materialità, decisione di notifica, comunicazioni e preservazione delle evidenze.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Creare un workflow con orari, owner, escalation, assessment, legal/privacy coordination e template per le diverse fasi di notifica previste.

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: Creare un workflow con orari, owner, escalation, assessment, legal/privacy coordination e template per le diverse fasi di notifica previste.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Incident timeline, severity matrix, notification decision log, communications, evidence preservation, post-incident review.

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 attacco viene contenuto rapidamente ma ha coinvolto un servizio essenziale: decidere se e quando il contenimento modifica la rilevanza notificativa. 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: Tempo da detection a classificazione e da classificazione a decisione di notifica.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Decisioni di notifica senza timestamp; sovrapposizione con GDPR non coordinata; incidenti chiusi prima di valutare lezioni apprese.

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 «Incident

classification, notification e crisis governance”.

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**Supply chain, cloud e terze parti**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Valutare dipendenze da fornitori, MSP, cloud, software, telecomunicazioni e subfornitori come parte del rischio del servizio, non come mera procurement compliance.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire tiering, due diligence, requisiti minimi, reporting incidenti, auditability, vulnerability disclosure, exit strategy e concentrazione.

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 tiering, due diligence, requisiti minimi, reporting incidenti, auditability, vulnerability disclosure, exit strategy e concentrazione.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Supplier inventory, criticality tier, contract clauses, security assessments, SBOM where relevant, incident SLA, exit test.

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

Due fornitori critici dipendono dallo stesso hyperscaler: valutare concentrazione e impatto su 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 di fornitori critici con exit strategy testata e obbligo di notifica contrattuale verificato.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Rating esterno usato come unica due diligence; nessuna visibilità sui subfornitori; rinnovi automatici senza reassessment.

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 «Supply chain, cloud e terze parti».

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**Vulnerability management e secure lifecycle**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Governare asset inventory, vulnerability discovery, prioritizzazione, patching, secure development/acquisition, change management e disclosure con criteri legati all'esposizione reale.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire SLA per rischio, eccezioni, compensazioni, asset owner, remediation evidence, secure SDLC e verifica delle dipendenze software.

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 SLA per rischio, eccezioni, compensazioni, asset owner, remediation evidence, secure SDLC e verifica delle dipendenze software.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Asset inventory, scan results, threat/exploit evidence, patch tickets, exception approvals, secure code review, dependency inventories.

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 CVSS alta riguarda un asset non esposto, mentre una media è sfruttata attivamente su servizio internet-facing: definire priorità. 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: Tempo remediation per rischio effettivo e percentuale asset critici con ownership e scanning aggiornati.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Priorità solo CVSS; inventario incompleto; eccezioni permanenti; sviluppo sicuro non integrato nelle pipeline.

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 «Vulnerability

management e secure lifecycle”.

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**Business continuity, backup e cyber resilience**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Collegare BIA, continuità, disaster recovery, backup, crisis management e dipendenze ICT agli obiettivi di servizio e agli scenari cyber realistici.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire RTO/RPO, recovery sequence, copie segregate/immutabili, accessi di emergenza, test, communication plan e fallback manuali.

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 RTO/RPO, recovery sequence, copie segregate/immutabili, accessi di emergenza, test, communication plan e fallback manuali.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: BIA, DR plan, restore tests, tabletop, evidence of immutable backup, dependency map, crisis contact lists.

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

Il backup esiste ma con stesse credenziali dell'ambiente produzione: valutare reale resilienza a ransomware. 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 servizi critici testati end-to-end rispetto a RTO/RPO e successo restore di campioni rappresentativi.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Test solo documentali; RTO non validati; backup online sempre montati; piani senza dipendenze di fornitori.

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 «Business

continuity, backup e cyber resilience”.

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**Audit readiness, evidenze e programma di conformità**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Costruire una compliance sostenibile basata su evidenze, ownership, scadenze e risk-based assurance anziché su raccolte documentali occasionali.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Creare control library, evidence calendar, testing plan, remediation governance e reporting executive integrati con ISMS e audit.

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: Creare control library, evidence calendar, testing plan, remediation governance e reporting executive integrati con ISMS e audit.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Control/evidence matrix, test scripts, issue register, remediation plan, board reporting and evidence repository with versioning.

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

A poche settimane da un controllo l'organizzazione raccoglie documenti retroattivamente: trasformare il lavoro in continuous compliance. 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 controlli con evidence owner e prova aggiornata; aging medio delle finding ad alto rischio.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Evidence “costruita” a fine anno; nessun owner; finding ripetute; reporting al board senza trend e rischio residuo.

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 «Audit readiness».

evidenze e programma di conformità”.

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: 2.450,00 € 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: NIS2-CISO-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.