CYBERSECURITY AUDIT e Fondamenti di Cybersicurezza

Corso di preparazione all'esame di certificazione Cybersecurity Audit di ISACA + casi pratici

Corso di certificazione CYBERSECURITY AUDIT accreditato da ISACA

CYBERSECURITY
AUDIT
An ISACA Certificate

24 ORE

Il corso Cybersecurity Audit, oltre a preparare alla certificazione Cybersecurity Audit di ISACA, fornisce: (1) agli IT Auditor una conoscenza a 360 gradi dei fattori chiave di Cybersecurity da contemplare in un Audit Plan, consentendo loro di comprendere come valutare e ridurre i rischi di Cybersecurity, come auditare i controlli di Cybersecurity e come interpretare le evidenze dell'area di Cybersecurity; (2) agli esperti di Cybersicurezza una chiara comprensione dei processi di Audit; (3) agli IT Risk Manager la capacità di approfondire la comprensione dei rischi Cyber e delle misure di controllo.

RISULTATI ATTESI:

Il corso prepara all'esame di certificazione Cybersecurity Audit di ISACA e rende i partecipanti in grado di:

- Comprendere i Cybersecurity Frameworks, tutti gli aspetti di cybersecurity governance, e identificare best practice adeguate, e i collegamenti agli obiettivi di controllo COBIT
- Presidiare il Sistema e gli strumenti di gestione Minacce e Vulnerabilità e Identificare i requisiti legali e di Cybersicurezza a supporto degli assessment di compliance
- Definire ed implementare processi di autorizzazione sicuri e Access Management a livello Enterprise
- Distinguere tra firewall e tecnologie di Network Security e identificare i controlli di Application Security
- Migliorare le procedure di Asset Configuration e di Change e Patch management
- Identificare i punti di debolezza nelle strategie e nei controlli per il Cloud
- Eseguire attività di Risk Assessment di Cybersecurity e di Terze parti

Chi frequenterà anche il modulo integrativo VA & PENTEST FUNDAMENTALS:

- Comprenderà come vengono svolti e che risultanze producono le attività di Vulnerability Assessment e di Penetration Testing.
- Imparerà a leggere i report di attività di VAPT.

Fino a 30 CPE validi per mantenimento delle certificazioni ISACA
Sconto 5% per inserimento codice
Sconto 10% aggiuntivo per almeno 3 iscritti della stessa azienda

INFO: corsi@aiea-formazione.it - Tel: 02.8716.9246

MODULO D'ISCRIZIONE AL CORSO CYBERSECURITY AUDIT e Fondamenti di Cybersicurezza

DATI FATTURAZIONE

Ragione Sociale - Cognome e nome	Partita iva/C.f.	Codice Destinatario/Pec
Via e Numero	CAP	Città e (PR)
E-mail Amministrazione	Telefono Azienda	Nr. Ordine d'acquisto/RdA

DATI PARTECIPANTI

Nome e Cognome	E-mail personale	Socio ISACA	Socio AIEA	ID ISACA

DATA E LOCATION: Verificare date e location sul sito www.aiea-formazione.it e specificare le proprie scelte di seguito

MODALITA' DI PAGAMENTO: Bonifico Bancario anticipato intestato a Profice

Coordinate Bancarie: IBAN:IT46 J030 3211 7020 1000 0806 292

Causale: Indicare cognome del partecipante e ragione sociale

PREZZO: Solo Cybersecurity Audit (24 ore)

- ☐ 1.350,00€ + IVA
- ☐ 1.300,00€ + IVA (Riservato Soci ISACA)
- ☐ 1.200,00€ + IVA (Riservato Soci AIEA/ISACA MI)

SECONDA OPZIONE PREZZO: Corso Completo CyberAudit + VA-PT (32 ore)

- ☐ 1.700,00€ + IVA
- ☐ 1.650,00€ + IVA (Riservato Soci ISACA)
- ☐ 1.550,00€ + IVA (Riservato Soci AIEA/ISACA MI)

AGEVOLAZIONI	☐ Sconto 5% per iscrizioni entro 30 giorni	☐ Sconto 10% aggiuntivo per almeno 3 iscritti
ACQUISTO VOUCHER ESAME	☐ 480,00€ + IVA	☐ 400,00€ + IVA (Riservato Soci AIEA/ISACA MI)
ACQUISTO MEMBERSHIP ISACA	☐ 250,00€ + IVA	

REFERENTE ORGANIZZATIVO E AMMINISTRATIVO: Profice srl - P.iva 02487960201 - Codice Destinatario: M5UXCR1
Sede Legale: Via Fernelli, 28 - 46100 - Mantova (MN) - Tel: 02.8716.9246 - Fax: 02.8715.1741 - Email: direzione@profice.it
PARTNER DI AIEA (Associazione Italiana Information System Auditor) www.aiea-formazione.it - www.aiea.it

PRIVACY E DIRITTI DELL'INTERESSATO: I Suoi dati personali saranno trattati sia su supporto informatico che cartaceo e il loro conferimento è necessario per l'iscrizione al corso: la mancata fornitura dei dati non consentirà pertanto l'iscrizione. Accettando il presente regolamento, Lei autorizza il trattamento dei Suoi dati personali solo per fini organizzativi, contabili, e per aggiornarLa sulle nostre iniziative formative, nella piena tutela dei Suoi diritti e della Sua riservatezza e in conformità alle disposizioni di legge ai sensi del GDPR UE 679:2016 e del D.lgs. n. 101:18. Titolare del trattamento dei dati è Profice srls. In qualsiasi momento Lei potrà richiedere l'aggiornamento o la cancellazione dei Suoi dati personali scrivendo a direzione@profice.it.
RECESSO/DISDETTA : Il cliente, tramite fax o e-mail a corsi@aiea-formazione.it, potrà disdire dal contratto senza penali entro e non oltre il 15mo giorno precedente la data di inizio del corso: in questo caso Profice provvederà a rifondere l'intera quota versata. Oltre tale termine Profice potrà trattenere una penale di 50 Eu, o, qualora la richiesta di cancellazione pervenga negli ultimi 3 giorni dall'inizio corso, l'integrale quota di iscrizione.
ANNULLAMENTO DEL CORSO: Profice si riserva il diritto di annullare il corso per gravi impedimenti o per mancato raggiungimento del numero minimo di partecipanti, in qualsiasi momento, rifondendo quanto versato.
ASPETTI ORGANIZZATIVI: (1) L'iscrizione si intende perfezionata al momento del ricevimento, da parte della segreteria corsi, della presente scheda compilata in tutte le sue parti. Al raggiungimento del numero minimo di partecipanti verrà inviata una conferma d'iscrizione tramite fax o e-mail, al più tardi entro 10 giorni di calendario dalla data di inizio del corso. (2) Gli attestati verranno emessi in formato digitale successivamente alla partecipazione al corso ed a pagamento avvenuto.
PAGAMENTO: Il pagamento dovrà avvenire, a seguito della conferma inviata dalla segreteria corsi, a mezzo bonifico bancario (o Carta di Credito con 3% di sovrapprezzo)
FORMAZIONE FINANZIATA: è possibile avvalersi della Formazione Finanziata concordando con Profice gli adempimenti amministrativi prima del corso

Il Cliente previa lettura delle condizioni al presente contratto, in particolare delle clausole "aspetti organizzativi", "pagamento", "recesso/disdetta", "annullamento del corso",dichiara espressamente di approvarli specificatamente ai sensi e agli effetti di cui agli art. 1341 e 1342 cod. civ.

Data	Firma e Timbro

INVIARE MODULO a corsi@aiea-formazione.it o via FAX: 02.8715.1741

CORSO:	**CYBERSECURITY AUDIT e Fondamenti di Cybersicurezza** **Corso di preparazione all'esame di certificazione Cybersecurity Audit di ISACA + casi pratici**
DESCRIZIONE:	Con il continuo incremento delle minacce di Cybersecurity, includere gli ambiti di dettaglio di Cybersecurity nei piani di audit di ogni organizzazione sta diventando un fattore sempre più critico. Questo richiede agli Auditor di saper auditare adeguatamente i processi e le policies di cybersecurity e di presidiare gli strumenti per assicurare che le proprie organizzazioni implementino gli appropriati controlli Il programma del corso copre le 4 aree chiave di Cybersecurity Audit: (1) cybersecurity and audit's role, (2) cybersecurity governance, (3) cybersecurity operations, (4) cybersecurity technology topics. Inoltre fornisce un approfondimento su come collegare gli obiettivi di controllo COBIT alle misure di sicurezza definite secondo il NIST Cybersecurity Framework. Il corso è anche abbinabile al MODULO INTEGRATIVO di 8 ore VA & PENTEST FUNDAMENTALS, al fine di conseguire maggiori competenze nella valutazione e interpretazione delle attività di VA e PT In particolare il percorso complessivo fornisce: - agli IT AUDITOR una conoscenza a 360 gradi dei fattori chiave di Cybersecurity da contemplare in un Audit Plan, consentendo loro di comprendere come valutare e ridurre i rischi di Cybersecurity, come auditare i controlli di Cybersecurity e come interpretare le evidenze dell'area di Cybersecurity; - agli ESPERTI DI CYBERSICUREZZA una chiara comprensione dei processi di Audit; - agli IT RISK MANAGER la capacità di approfondire la comprensione dei rischi Cyber e delle misure di controllo.
RISULTATI ATTESI:	Il corso prepara all'esame di certificazione Cybersecurity Audit di ISACA e rende i partecipanti in grado di: - Comprendere i Cybersecurity Frameworks, tutti gli aspetti di cybersecurity governance, e identificare best practice adeguate, e i collegamenti agli obiettivi di controllo COBIT - Presidiare il Sistema e gli strumenti di gestione Minacce e Vulnerabilità e Identificare i requisiti legali e di Cybersicurezza a supporto degli assessment di compliance - Definire ed implementare processi di autorizzazione sicuri e Access Management a livello Enterprise - Distinguere tra firewall e tecnologie di Network Security e identificare i controlli di Application Security - Migliorare le procedure di Asset Configuration e di Change e Patch management - Identificare i punti di debolezza nelle strategie e nei controlli per il Cloud - Eseguire attività di Risk Assessment di Cybersecurity e di Terze parti Chi frequenterà anche il modulo integrativo VA & PENTEST FUNDAMENTALS: - Comprenderà come vengono svolti e che risultanze producono le attività di Vulnerability Assessment e di Penetration Testing. - Imparerà a leggere i report di attività di VAPT.
DURATA:	24 ORE
DESTINATARI:	IT Auditors, Security Professionals, CISO, Audit/Assurance professionals, IT Risk professionals, IT Risk Managers. Il corso si rivolge inoltre a Manager, Professionisti ed Avvocati che intendano acquisire le competenze di base necessarie per comprendere scenari di rischio, vulnerabilità e minacce di Cybersecurity, inquadrate nell'ambito del Cybersecurity Framework del NIST, riconosciuto internazionalmente come schema di riferimento di Cyber-Sicurezza.
PRE-REQUISITI:	Per la partecipazione al corso si suggerisce una conoscenza base dei fondamenti di Sicurezza Informatica. Qualora si sia completamente a digiuno di tali conoscenze sono disponibili, su richiesta, sessioni integrative in elearning da completare prima della partecipazione al corso
CONTENUTI:	GIORNI 1 e 2: FONDAMENTI DI CYBERSECURITY e PREPARAZIONE ALLA CERTIFICAZIONE CYBERSECURITY AUDIT 1) Cybersecurity vs Audit's Role: Digital Asset Protection; Lines of Defense; Role of Audit; Audit Objectives; Audit Scope 2) Cybersecurity Governance: Security Organization Goals and Objectives; Cybersecurity Risk Assessment; Service Providers; Performance Measurement 3) Cybersecurity Operations – Cyberattacks: Threat Assessment; Cybersecurity Measures; Vulnerability Management; Penetration Testing; Red Team/Blue Team/Purple Team Exercises

4) Cybersecurity Operations - Identity and Access Management:
Enterprise Identity and Access Management; Identity Management; Federated Identity Management; Key Objectives of Identity Management; Provisioning and Deprovisioning; Authorization; Privileged User Management and Controls; Third-party Access; Authentication Protocols; Configuration Management; Asset Management; Change Management; Patch Management; Network Security; Security Architecture; Security Perimeter; Network Perimeter; Interdependencies; Network Architecture; Remote Access; System Hardening

5) Cybersecurity Operations - Security Measures:
Incident Management; Digital Forensics; Client Endpoint Protection; Security within SDLC; Data Backup and Recovery

6) Cybersecurity Operations - Compliance and Cryptography:
Security Compliance; Cryptography

7) Security Technologies:
Firewall and Network Security technologies; Security Incident & Event Management (SIEM); Wireless Technology; Cloud Computing; Mobile Security; Internet of Things (IoT)

8) Correlazioni con COBIT
Gli obiettivi di controllo COBIT per l'Audit della Cybersecurity secondo il NIST Cybersecurity Framework
Esercizi di gruppo ed esempi pratici

GIORNO 3: APPROFONDIMENTI PRATICI A SUPPORTO DELL'IT AUDIT e CONCETTI CHIAVE DI VA-PT

1) Concetti base di Vulnerability Management
Principali vulnerabilità, come e quando effettuare un assessment e con quali strumenti, remediation plan, prioritizzazione criticità, reporting e classificazione.

2) Concetti base di Penetration Test e linee guida
A cosa serve, chi lo fa, quando va fatto, Definizione dell'ambito, raccomandazioni sull'uso degli strumenti, Non Disclosure Agreement, etc…

3) Cenni ai principali framework utilizzabili (PCI, OSSTMM, etc.)

4) Fasi del PT con focus sulla fase di attacco

5) Definizione, ruoli e competenze di Blue/Red/Purple Team

6) Presentazione e lettura ragionata di un report reale di Vulnerability Assessment e di PenTest

GIORNO 4: MODULO INTEGRATIVO VA-PT (EXTRA)

1) Fondamenti di Vulnerability Assessment per le reti LAN
- Principali tipologie di vulnerabilità di host ed applicazioni
- L'attività di Vulnerability Assessment (Le fasi, gli standard, i soggetti coinvolti, il report finale)
- Ricerca di vulnerabilità (Ricerca "Manuale'; Vulnerability scanner general purpose (Nessus e OpenVas); Vulnerability scanner per applicazioni web)

2) Fondamenti di Penetration Testing di reti LAN
- Le attività di Penetration Testing
- Differenze rispetto al VA
- Tipologie di PenTest
- Criticità nello svolgimento di un PenTest
- Il report finale
- Framework utilizzabili per il Penetration Test di reti LAN

3) Esercizi di gruppo ed esempi pratici

CERTIFICAZIONE:

CYBERSECURITY AUDIT riconosciuto da ISACA

MATERIALE DI STUDIO:

Il corso include le slide presentate nel corso delle lezioni.
Per chi intende sostenere l'esame, acquistando il voucher d`esame viene anche fornita la Guida Ufficiale ISACA «Cybersecurity Audit Certificate Study Guide» in formato elettronico.
La guida approfondisce i seguenti temi: Cybersecurity and Audit's role, Cybersecurity Governance, Cybersecurity Operations, Case studies, esempi ed approfondimenti su ambiti mirati delle tecnologie di Cybersecurity.

DATE E LOCATION:	Verificare Date e Location sul sito www.aiea-formazione.it prima di iscriversi
CREDITI FORMATIVI:	Fino a 30 CPE validi ai fini del mantenimento delle certificazioni ISACA
NOTE:	Per chi desidera sostenere l'esame, insieme all'acquisto del voucher sarà fornita la guida ufficiale ISACA «Cybersecurity Audit Certificate Study Guide» in formato elettronico. La guida approfondisce i seguenti temi: Cybersecurity and Audit's role, Cybersecurity Governance, Cybersecurity Operations, Case studies, esempi ed approfondimenti su ambiti mirati delle tecnologie di Cybersecurity. Se di interesse oltre le 3 giornate del corso di Cybersecurity Audit è possibile anche acquistare la giornata aggiuntiva con il modulo integrativo VA e PENTEST FUNDAMENTALS
ESAME:	L'esame Cybersecurity Audit può essere schedulato entro 12 mesi dal corso, in una data a discrezione di ciascun partecipante e si svolge accedendo alla piattaforma online d'esame di ISACA, sotto il monitoraggio di un supervisore (proctor) online ISACA. L'esame è in lingua inglese, dura 120 minuti e richiede che il candidato risolva 75 domande a risposta multipla.
DOCENTE:	Docenti accreditati Cybersecurity Audit, Cobit2019 Foundation Cobit5 Foundation. Esperto senior in ambito IT Audit, IT Governance e Cybersecurity, certificato CISA, CISM, ISO27001 A/LA, ISO22301 A/LA, Privacy Officer -TUV, Cobit5 e Cobit 2019 Foundation, Cybersecurity Audit. Per il modulo VA-PT Fundamentals, interverranno docenti certificati CEH e CHFI, ed esperti senior sui temi di VA e PenTest.
FORMAZIONE FINANZIATA:	PROFICE è certificata EN ISO 9001:2015 per il sistema di gestione per la Qualita, settori IAF/EA 35 e 37 - Certificato No. IT18-27105A del 9 Ottobre 2018 (Progettazione ed erogazione corsi di formazione professionale; Consulenza direzionale, organizzativa e di Compliance)
FORMAZIONE PER P.A.:	Profice è iscritta al MEPA per le attività di formazione e servizi specialistici. Questo corso è registrato con codice MEPA: profice_68

Chi è AIEA (ISACA Milan Chapter)

L'Associazione Italiana Information Systems Auditors - AIEA -, costituita in Milano nel 1979, riunisce coloro che in Italia svolgono professionalmente attività di Auditing e Controllo di sistemi ICT promuovendo la conoscenza e ampliando l'esperienza dei suoi aderenti nel campo dell'Information Systems Audit , Assurance, Governance e Security. L'Associazione,Capitolo di Milano di ISACA, favorisce lo scambio di metodologie, promuove un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo sia di affidabilità dell'organizzazione che di sicurezza dei sistemi. Promuove inoltre ricerche quale quella sulla Governance IT commissionata a SDA Bocconi, organizza un Convegno annuale, cura la traduzione in italiano di Val IT, COBIT®, e da oltre 15 anni del Manuale CISA e delle correlata documentazione, sostiene la diffusione delle certificazioni professionali CISA (Certified Information Systems Auditor), CISM(Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in Risk and Information Systems).

Chi è ISACA

Con oltre 100.000 associati in 180 Paesi, ISACA® (www.isaca.org) è leader mondiale nel fornire competenze, certificazioni, community, patrocinio e formazione nei settori dell'assurance e sicurezza, del governo dell'impresa,della gestione dell'IT e dei rischi e della compliance correlati all'IT. Fondata nel 1969, ISACA, associazione indipendente senza fini di lucro, organizza conferenze internazionali, pubblica l'ISACA Control Journal®, e sviluppa standard internazionali relativi all'audit e al controllo dei sistemi IT, che contribuiscono a garantire i propri componenti sull'affidabilità e a trarre valore dai sistemi informativi. ISACA favorisce inoltre l'acquisizione delle competenze e delle conoscenze IT e le attesta mediante le certificazioni riconosciute a livello internazionale quali: CISA® (Certified Information Systems Auditor™),CISM® (Certified Information Security Manager®), CGEIT™ (Certified in the Governance of Enterprise ITTM) e CRISC™ (Certified in Risk and Information Systems Control™). ISACA aggiorna continuamente COBIT® che assiste i professionisti dell'IT e i manager delle imprese ad adempiere le proprie responsabilità relativamente all'IT governance e alla gestione manageriale, in particolare nell'ambito dell'assurance, sicurezza, rischio e controllo e a fornire valore al business.

Quali vantaggi per i soci AIEA

E' possibile iscriversi ad AIEA tramite ISACA, selezionando il Milan chapter (http://www.isaca.org/Membership/Join-ISACA).

I soci possono accedere a:

1) accesso gratuito
- a più di 20 Sessioni di Studio annuali, con crediti CPE utili al mantenimento delle certificazioni;
- all'ISACA eLibrary (raccolta di quasi tutte le pubblicazioni ISACA/ITGI);
- alle versioni elettroniche dei framework ISACA;
- ai webcasts e agli e-Simposi organizzati da ISACA;

2) sconti
- sulle pubblicazioni nel Bookstore ISACA;
- sulle quote d'iscrizione e sulle pubblicazioni di preparazione agli esami CISA, CISM, CGEIT e CRISC;
- su corsi ed eventi organizzati da AIEA Formazone o da altri Enti ed Associazioni in partnership o patrocinati;
- invio gratuito del magazine bimestrale ISACA Journal e delle newsletter AIEA.

Partner dei corsi AIEA Formazione

Profice
AIEA Training Partner