CA-IS - Cybersecurity Audit e fondamenti di Cybersecurity

ISACA - ISACA - Cyber Security

Durata:	Lingue:	Certificazione:
3 Giorni	**Italiano**	**Cybersecurity Audit**

Descrizione del corso

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

Programma

GIORNO 1-2

Modulo 1: Cybersecurity vs Audit’s Role:

- Digital Asset Protection; Lines of Defense; Role of Audit; Audit Objectives; Audit Scope

Modulo 2: Cybersecurity Governance:

- Security Organization Goals and Objectives; Cybersecurity Risk Assessment; Service Providers; Performance Measurement

Modulo 3: Cybersecurity Operations – Cyberattacks:

- Threat Assessment; Cybersecurity Measures; Vulnerability Management; Penetration Testing; Red Team/Blue Team/Purple Team Exercises

Modulo 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

Modulo 5: Cybersecurity Operations – Security Measures:

- Incident Management; Digital Forensics; Client Endpoint Protection; Security within SDLC; Data Backup and Recovery

Modulo 6: Cybersecurity Operations – Compliance and Cryptography:

- Security Compliance; Cryptography

Modulo 7: Security Technologies:

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

Modulo 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

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.

Modulo 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...

Modulo 3: Cenni ai principali framework utilizzabili (PCI, OSSTMM, etc.)
Modulo 4: Fasi del PT con focus sulla fase di attacco
Modulo 5: Definizione, ruoli e competenze di Blue/Red/Purple Team
Modulo 6: Presentazione e lettura ragionata di un report reale di Vulnerability Assessment e di PenTest