

CA-IS - Cybersecurity Audit di ISACA

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. 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 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.

Programma

1.Cybersecurity vs Audit's Role:

1. Digital Asset Protection
2. Lines of Defense
3. Role of Audit
4. Audit Objectives
5. Audit Scope

2.Cybersecurity Governance:

6. Security Organization Goals and Objectives
7. Cybersecurity Risk Assessment
8. Service Providers
9. Performance Measurement

3.Cybersecurity Operations – Cyberattacks:

10. Threat Assessment
11. Cybersecurity Measures
12. Vulnerability Management
13. Penetration Testing
14. Red Team/Blue Team/Purple Team Exercises

4. Cybersecurity Operations – Identity and Access Management:

15. Enterprise Identity and Access Management
16. Identity Management
17. Federated Identity Management
18. Key Objectives of Identity Management
19. Provisioning and Deprovisioning
20. Authorization
21. Privileged User Management and Controls
22. Third-party Access
23. Authentication Protocols
24. Configuration Management
25. Asset Management
26. Change Management
27. Patch Management
28. Network Security
29. Security Architecture

30. Security Perimeter
31. Network Perimeter
32. Interdependencies
33. Network Architecture
34. Remote Access
35. System Hardening

5.Cybersecurity Operations – Security Measures:

36. Incident Management
37. Digital Forensics
38. Client Endpoint Protection
39. Security within SDLC
40. Data Backup and Recovery

6.Cybersecurity Operations – Compliance and Cryptography:

41. Security Compliance
42. Cryptography

7.Security Technologies:

43. Firewall and Network Security technologies
44. Security Incident & Event Management (SIEM)
45. Wireless Technology
46. Cloud Computing
47. Mobile Security
48. Internet of Things (IoT)

8.Correlazioni con COBIT

49. Gli obiettivi di controllo COBIT per l'Audit della Cybersecurity secondo il NIST Cybersecurity Framework
50. 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