

Associazione Italiana Information Systems Auditors



Agenda

- AIEA - ruolo ed obiettivi
- ISACA - struttura e finalità
- La certificazione CISA
- La certificazione CISM

- Costituita a Milano nel 1979

- Finalità:

promuovere l'approfondimento dei problemi connessi al controllo dei processi di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie e tecniche uniformi per la loro soluzione

A I E A - Principali obiettivi

- Ampliare la conoscenza e l'esperienza dei suoi aderenti nel campo dell'Information Systems Auditing
- Facilitare i rapporti con analoghe associazioni estere
- Promuovere a livello nazionale la partecipazione degli IS Auditor alle certificazioni
 - C.I.S.A. (Certified Information Systems Auditor)
 - C.I.S.M. (Certified Information Security Manager)

- Riconosciuta come "Capitolo" della Information Systems Auditors and Control Association Inc. (ISACA)
- Primo Capitolo Europeo (1979) riconosciuto

- Adesione codice etico
- Possesso requisiti allineati al codice etico
- Iscrizione vincolata a esame Probiviri

Agenda

- AIEA - ruolo ed obiettivi
- ISACA - struttura e finalità
- La certificazione CISA
- La certificazione CISM

ISACA

- Costituita nel 1969 a Los Angeles
- Sviluppa, promuove e regola l'attività professionale degli auditor
- Rilascia l'abilitazione C.I.S.A. e C.I.S.M.

- Attualmente aderiscono circa
 - 28.000 auditor e consulenti (100+ Paesi)
 - 3.000 in Europa

Agenda

- AIEA - ruolo ed obiettivi
- ISACA - struttura e finalità
- La certificazione C.I.S.A.
- La certificazione CISM

C.I.S.A.

- Riconosciuta nel mondo come segno di distinzione professionale dal 1978
- Premia l'esperienza di audit, sicurezza, controllo IS
- Richiede un aggiornamento professionale continuo
- Più di 30000 C.I.S.A. nel mondo dal 1978

L'esame C.I.S.A.

- Una volta all'anno, contemporaneamente in tutto il mondo
- La procedura di certificazione è allineata ai criteri guida di riferimento delle normative europee
- La certificazione ha validità annuale - per essere mantenuta occorre completare un percorso formativo di 40 ore
- Esame sostenuto in 11 lingue, in più di 200 sedi

Agenda

- AIEA - ruolo ed obiettivi
- ISACA - struttura e finalità
- La certificazione C.I.S.A.
- La certificazione C.I.S.M.



- Focus sulla **GESTIONE** della Sicurezza Informatica

Requisiti

■ Esame Etica Formazione Esperienza

- Superare l'esame
- Aderire al codice di etica professionale
- Impegnarsi per l'aggiornamento professionale
- Evidenziare sufficienti qualifiche e titoli di esperienza

Requisiti di esperienza

- Minimo 5 anni esperienza operativa nel campo
- Minimo 3 anni di esperienza come gestore in ambito di almeno tre dei 5 domini di conoscenza
- Sostitutivi parziali (CISSP - CISA ..)

Domini

- Information Security Governance
- Risk Management
- Information Security Program Management
- Information Security Management
- Response Management

Information Security Governance

- Definire e mantenere uno schema per cui è possibile accertare che le strategie di sicurezza sono in linea con gli obiettivi aziendali, con le norme di legge e i regolamenti di categoria

Information Security Governance

- Sviluppare la strategia della sicurezza a supporto di quella aziendale
- Ottenere l'incarico dalla Direzione e il suo supporto
- Garantire la definizione dei ruoli e delle responsabilità
- Definire i canali di riporto e di comunicazione

Information Security Governance

- Identificare le problematiche di carattere legale pertinenti la sicurezza e gli accessi ai dati e il loro impatto sull'organizzazione
- Statuire e mantenere le policy che supportino gli obiettivi e il business aziendale
- Garantire lo sviluppo di procedure e linee guida per supportare le policy
- Supportare i programmi di investimento per la sicurezza mediante sviluppo di "business case"

Risk Management

- Identificare e gestire i rischi di sicurezza pregiudiziali agli obiettivi aziendali per consentire il loro raggiungimento

Risk Management

- Sviluppare un processo sistematico, analitico e continuo di risk management
- Assicurare che l'identificazione del rischio, l'analisi e le attività che lo riducono siano integrate nello stesso ciclo di vita del processo
- Applicare l'identificazione del rischio e i metodi di analisi

Risk Management

- Definire le strategie e le opzioni prioritarie per portare il rischio a livelli accettabili
- Relazionare il management sulle modifiche significative del livello di rischio

Information Security Program Management

- Progettare, realizzare e gestire un programma di sicurezza per la messa in atto dello schema di Governance della sicurezza

Information Security Program Management

- Creare e mantenere piani per implementare lo schema di governo della sicurezza
- Sviluppare le linee di base, le procedure, le linee guida per garantire che i processi aziendali tengano conto dei rischi della sicurezza
- Sviluppare procedure e linee guida per le attività relative all'infrastruttura per assicurare la loro coerenza con le policy

Information Security Program Management

- Integrare i requisiti dei programmi di sicurezza nel ciclo di vita delle attività aziendali
- Sviluppare metodi per soddisfare i requisiti delle policy che tengano conto dell'impatto sugli utenti finali

Information Security Program Management

- Promuovere l'accountability da parte dei proprietari dei processi e altre parti coinvolte nella gestione dei rischi
- Stabilire delle metriche per gestire lo schema del governo della sicurezza
- Garantire che le risorse interne ed esterne siano identificate, appropriate e gestite

Information Security Management

- Supervisionare e dirigere le attività pertinenti alla sicurezza in modo da attuare il programma

Information Security Management

- Garantire che i ruoli, le procedure amministrative di sistemi, i servizi forniti da altre entità tra cui gli outsourcer, siano in linea con le policy aziendali
- Utilizzare metriche per misurare, monitorare e "riportare" l'efficienza ed efficacia dei controlli e il loro allineamento con le policy
- Garantire che la sicurezza non sia compromessa durante il processo di cambiamento

Information Security Management

- Garantire che la valutazione della vulnerabilità sia effettuata per valutare efficientemente l'esistenza dei controlli
- Garantire che quanto non in linea e ogni scostamento siano risolti in tempi brevi
- Garantire lo sviluppo delle attività che possono influenzare la cultura e il comportamento del personale - comprese momenti formativi e di sensibilizzazione

Response Management

- Sviluppare e gestire una capacità di rispondere/reagire ed essere in grado di ripristinare a fronte di turbative e di eventi distruttivi

Response Management

- Sviluppare dei processi in grado di rilevare, identificare e analizzare gli eventi relativi alla sicurezza
- Sviluppare risposte e piani di ripristino organizzando, addestrando il personale coinvolto
- Garantire verifiche periodiche dei piani quando approntati

Response Management

- Garantire procedure per la documentazione degli eventi come base, se necessario, per successive indagini
- Gestire la revisione del dopo evento per identificare le cause e le azioni correttive

- www.aiea.it
- aiea@aiea.it

