ISACA
Al servizio dei professionisti dell'IT Governance
Capitolo di Milano

InfoAIEA

n. 3 del 2006

n. 3 del 2006

Costantemente aggiornati

L'evoluzione continua e veloce del contesto tecnologico e delle conoscenze necessarie per gestirlo e controllarlo richiede un aggiornamento parimenti continuo dei professionisti che hanno responsabilità di IT Governance, Security, Assurance. Conclusione: dobbiamo studiare! Non basta essere d'accordo, occorre tempo e strumenti adeguati.

La comunità degli IS Auditor ci aiuta; non può studiare al nostro posto ma condivide con tutti le esperienze che presenta negli eventi associativi.

AIEA organizza nel corso dell'anno 16 sessioni di studio, gratuite per gli Associati, a: Milano, Roma, Torino, Vicenza; co-organizza una sessione anche a Lugano. Abbiamo così l'opportunità di conoscere le esperienze dei colleghi italiani, le opportunità presentate dai fornitori, i progetti di maggior successo, le specificità (mercato, normative, ...) nazionali.

ISACA offre agli Associati una modalità molto comoda e gratuita per le tematiche di fondo: i webinar. Dei seminari in inglese che frequenti dal tuo posto di lavoro e che vedono alternarsi professionisti di fama mondiale che approfondiscono i temi di attualità che ci servono per definire approcci consistenti per il nostro lavoro.

E' possibile, non solo per gli auditor, consultare sui siti AIEA ed ISACA le precedenti edizioni.

Pensi che queste opportunità di formazione gratuita e di alto livello professionale meritino la tua attenzione? Associati ad AIEA, aderirai automaticamente al Milan Charter di ISACA e potrai usufruire di queste opportunità. (O. N.)

In questo numero

L'Assemblea annuale è un momento associativo importante. Con l'aiuto della relazione tenuta dal Presidente ripercorriamo un anno intenso di attività e soddisfazioni. Abbiamo superato i 500 iscritti.

Con l'aiuto di alcuni associati, che hanno brillantemente superato l'esame CISA e CISM, cerchiamo di comunicarvi la validità di queste certificazioni. Pubblichiamo l'elenco dei promossi della sessione di giugno: complimenti a tutti.

Le associazioni professionali svolgono una importante funzione di promozione delle competenze specifiche. Vi proponiamo le interviste con alcune associazioni "gemellate" per coglierne le sinergie e lo spirito innovativo.

ISACA ha recentemente mappato COBIT sulle best practice in qualche modo collegate. Vi forniamo alcuni riferimenti. E infine un commento sul corso AIEA sull'ISO27001.

Share your knowledge. (O.N.)

Sommario:
numero 3/4 del 2006

Assemblea dei Soci Considerazioni del Presidente	2
Gli Esami CISA e CISM. Elenco dei promossi	6
Gli Esami CISA e CISM. Considerazioni e impressioni dei candidati	7
Recensione da BANCARIA	11
ISMS IUG Intervista al Presidente	12
COBIT e le altre best practice	14
Le domande frequenti su CISA e CISM	16
Commento al corso AIEA su ISO27001	22

Un sincero augurio per un sereno Natale e
un anno ricco di soddisfazioni personali e professionali.
Il Consiglio Direttivo AIEA.

Assemblea dei Soci
Considerazioni

Quest'anno il Consiglio Direttivo ha deciso di separare in due momenti l'Assemblea dei Soci e il Convegno annuale. Dall'anno 2001, infatti, l'Assemblea dei soci veniva tenuta in occasione del Convegno nazionale.

Tenendo conto delle osservazioni e dei suggerimenti da parte di molti soci, il CD ha ritenuto che, dopo una intensa giornata di lavori congressuali, non fosse opportuno sottoporre i soci ad un ulteriore impegno professionale rappresentato dall'ascolto, dalla discussione e dalle deliberazioni delle tematiche assembleari: resoconto di dettaglio delle attività associative, rendiconto annuale, proiezioni e quanto istituzionalmente previsto come informativa ai soci.

Il giorno 20 luglio u.s. si è quindi tenuta l'annuale Assemblea Soci.

I soci presenti in persona sono stati 55.

I soci che hanno inviato delega sono stati 143.

Nel corso dell'Assemblea, il Presidente Silvano Ongetta ha:

►►Comunicato i risultati della votazione per il rinnovo del Collegio dei Probiviri.

Sulla base delle schede pervenute allo studio dell'avv. Dall'Oglio, i risultati sono stati: Votanti **133**; voti nulli **7**.

Sono risultati eletti: F. Blanco (95 voti), A. Salvatici (108 voti); E. Schiocchet (88 voti).

►►Presentato un estratto della relazione inviata a tutti i soci in data 18/7/2006.

In particolare, sono state elencate le attività svolte nel periodo tra l'Assemblea del maggio 2005 e quella del 2006 e le attività pianificate nei mesi a venire.

Il Segretario E. Toffanin ha illustrato il Rendiconto al 31.12.2005, che è stato approvato all'unanimità.

A chi non l'avesse ancora fatto, ricordiamo di leggere con attenzione la relazione che è stata inviata a tutti i soci e che è stata riassunta in Assemblea da S. Ongetta.

Ringraziamo nuovamente i soci che si sono candidati per il collegio dei Probiviri ed agli eletti Blanco, Salvatici e Schiocchet auguriamo "Buon lavoro".

(Continua a pagina 3)

Assemblea dei Soci - Considerazioni

(Continua da pagina 2)

Di seguito riportiamo alcuni spunti importanti ripresi dalla relazione del Presidente Silvano Ongetta.

Primo concetto: la professione di IS Auditor si è evoluta e il cambiamento continua. Così come COBIT è passato da strumento a supporto dei controlli, a modello a supporto dell'IT Governance, allo stesso modo, l'Auditor si propone sempre più spesso anche come esperto in Assurance, Security e nella stessa IT Governance. Ciò in un contesto mutevole non solo dal punto di vista tecnologico ma anche sotto i profili normativi (v. per. Es SOX)

Secondo concetto: COBIT appare strumento adeguato per gli obiettivi che ISACA si è prefissa. Il modello viene adottato in modo crescente, anche in Italia. Evidentemente ciò è risultato anche di un'attività divulgativa svolta dai nostri Soci.

Terzo concetto: AIEA è in crescita in termini numerici assoluti ed i Soci hanno superato il numero di 500. Ciò può comportare una riclassificazione del capitolo da parte di ISACA in "Very Large Charter". Anche il numero di Soci certificati CISA o CISM è in crescita e la percentuale di questi supera il 40% del totale.

La gestione di AIEA richiede pertanto crescente impegno nell'individuazione delle strategie e degli obiettivi, al fine di costituire per i Soci un riferimento affidabile e autorevole e servizi apprezzati.

In sintesi, le strategie (e le azioni) per il 2006 / 2007 sono:

1. Soddisfare le aspettative professionali degli associati.

   Migliorato e aumentato lo scambio di esperienze e di occasioni per fornire informazione e comunicazione.

   Messo in atto i presupposti per attivazione l'area riservata sul sito.

2. Soddisfare le aspettative "personali" degli associati.

   Attivato progetto relativo al censimento delle competenze per facilitare il coinvolgimento dei soci come relatori in Sessioni di Studio e Seminari

(Continua a pagina 4)

L'assemblea dei Soci - Considerazioni

(Continua da pagina 3)

in cui AIEA è chiamata a partecipare.

Studio di fattibilità del benchmark della professione in Italia.

3. Diffondere la conoscenza dell'Associazione a livello nazionale ed elevarne la leadership

   Attivato contatti con aziende e università

   Promosso il processo di sensibilizzazione dei livelli organizzativi aziendali sulla necessità di rinforzare i criteri di controllo e l'affidabilità dell'organizzazione dell'IT e della sicurezza dei sistemi

   Promosso l'approfondimento delle tematiche di controllo dei processi IT e dello sviluppo di metodologie / tecniche / modelli (COBIT)

   Divulgato la valenza delle certificazioni CISA e CISM

   Promosso azioni per rendere sempre più conosciuta la nostra Associazione e la nostra mission

4. Incrementare ulteriormente il numero degli associati

   Definito l'obiettivo di diventare un Very Large Chapter

   Ricercata una maggiore fidelizzazione dei soci attuali costruendo una rete di relazioni personali per facilitare il rapporto con gli attori geograficamente lontani

   Abbiamo cercato di riavvicinare, ove possibile, i vecchi soci per individuare le cause del mancato rinnovo.

5. Creare una rete di proficui collegamenti con altre associazioni professionalmente vicine

   Consolidato il rapporto con CLUSIT e attivato rapporti con altre associazioni

Alle strategie indicate hanno fatto riscontro attività continue focalizzate su:

a. L'associazione (attività amministrative e gestionali)
b. Le certificazioni (assistenza ai candidati, formazione, traduzioni, ecc.)
c. COBIT 4.0 (Traduzione in italiano, formazione specifica)
d. Gruppi di Ricerca (ISMS, Penetration Test, Outsourcing, Marketing, I-TIL—COBIT)
e. Sessioni di Studio

(Continua a pagina 5)

L'assemblea dei Soci — Considerazioni

(Continua da pagina 4)

f. Relazioni con ISACA (Supporto alle strategie di ISACA)
g. Relazioni con altre Associazioni, presenza ad eventi di interesse comune, presenza a comitati scientifici, gestione degli Sponsor, ecc.

In sintesi si può concludere che AIEA è una associazione vitale e rappresenta per i Soci un'opportunità. Nel rimarcare come la quota associativa sia invariata dal 1998, si registra che AIEA dispone oggi di mezzi economici adeguati per fronteggiare con fiducia i prossimi esercizi.

Trattasi del frutto di una gestione che ha coniugato prudenza e accuratezza in un quadro di assoluta trasparenza.

Disponibile la versione italiana di COBIT 4.0

Il Gruppo di Ricerca COBIT 4.0 ha concluso la prima parte del lavoro ed ha rilasciato la versione 0.1 della traduzione di COBIT 4.0 pubblicata da ISACA. Entro alcuni mesi uscirà una nuova versione aggiornata; nel frattempo vi invitiamo a segnalare correzioni o miglioramenti. Gli associati che desiderano avere una copia del pdf (3 mega) sono pregati di richiederla alla segreteria (aiea@aiea.it).

AIEA ringrazia tutte le aziende di appartenenza dei componenti il Gruppo di Ricerca per la disponibilità e per il valore del contributo apportato dai rispettivi rappresentanti. A questi ultimi un particolare ringraziamento per l'impegno, la professionalità dimostrate e per aver contribuito al successo dell'iniziativa.

Coordinamento. Orillo Narduzzo, CISA, CISM (Banca Popolare di Vicenza)

Gruppo di Ricerca.

Stefano Arduini, CISA (Cedacri); Alfonso Elefante (Ernst & Young); Paola Galasso, CISA (Deloitte ERS); Alfredo Gallistru, CISA, CISM, CIA (PriceWaterhouseCoopers), Bruno Ghisu, CISA (Banco di Sardegna); Luigi Giambarini, CISA (BPU Banca); Francesco Marchiori, CISA (Banca Lombarda e Piemontese); Andrea Martini, CISA (Fed. BCC Piemonte V.Aosta Liguria); Andrea Pederiva, CISA (Banca Antonveneta); Mauro Porcelli, CISA (PriceWaterhouseCoopers); Giulio Spreafico, CISA, CISM (Spreafico); Andrea Trapè, CISA, CIA (RAS); Silvia Valenti, CISA (RAS).

Comitato di Qualità

Orillo Narduzzo, CISA, CISM (Banca Popolare di Vicenza); Silvano Ongetta, CISA, CISM (Presidente AIEA); Andrea Pagliari, CISA (SDA BOCCONI); Alberto Piamonte (WiseMap - Gruppo ADFOR); Marco Salvato, CISM (KPMG).

L'esame 2006 CISA e CISM
Elenco dei promossi

Di seguito i nominativi dei Soci che hanno superato l'esame CISA o CISM presso la Sede di Milano nella sessione di Giugno. Congratulazioni a tutti.

E a chi non ce l'ha fatta, un incoraggiamento per non demordere e riprovare, dopo aver valutato ed eliminato i propri punti di debolezza.

Daniela Cecagallina	CISA	Alberto Giovanni Medaglia	CISA
Anna Maria Fantappie	CISA	Marzio Scalise	CISA
Guido Leone	CISA	Sergio Napolitano	CISA
Massimiliano Nulli O Rinalducci	CISA	Paolo Garofalo	CISA
Marco Misitano, CISM, CISSP, CCSP	CISA	Stefano Gnocchi	CISA
Stefano Aiello	CISA	Carlo Patetta Rotta, CFE	CISA
Paolo Calise	CISA	Davide Lizzio, Auditor	CISA
Andrea Pagliari	CISA	Andrea Massei	CISA
Marco De Ritis	CISA	Andrea Enrico Lai	CISA
Paolo Lovisone, BS7799	CISA	Marika Lilla	CISA
Roberto Taiariol	CISA	Andrea Camillo Mariotti, CISA	CISM
Campri Giorgio	CISA	Fabio Brambani, CISA	CISM
Simone Pastori	CISA	Rosella Favino, CISSP	CISM
Francesca Pizzinga	CISA	Grazia Fanfoni, Sr., CISA	CISM
Francesca Gatti	CISA	Andrea Conrad	CISM

La richiesta della Certificazione (Application for Certification)

L'esame CISA / CISM è uno dei passi verso la certificazione!

La Certificazione è rilasciata da ISACA a fronte di diversi requisiti che il candidato attesta di avere e formalizza nella richiesta della certificazione, la APPLICATION FOR CERTIFICATION.

Considerando la severità dei requisiti per il rilascio della certificazione, ISACA concede 5 anni per l'invio dell'Application: trascorso il periodo il risultato dell'esame è annullato.

ISACA segnala che non tutti i promossi agli esami inviano l'Application: a livello globale si tratta di **centinaia** di casi nel periodo 2001—2005.

Si rammenta che non è possibile fregiarsi del marchio CISA o CISM senza l'invio da parte di ISACA del certificato.

Dopo la chiusura di una sessione di esami ISACA riceve una grande quantità di "Applications for Certification" e l'esame di ciascuna comporta una certa lentezza del processo. Possono quindi trascorrere settimane prima che il candidato ottenga la sua risposta.

Ulteriori dettagli sono disponibili ai seguenti indirizzi: *www.isaca.org/cisaapp o www.isaca.org/cismapp*.

L'esame CISA e CISM: la parola ai protagonisti

Fabio Brambani

L'esigenza di completare la mia formazione professionale con l'esame CISM è da ricollegare alla nuova funzione di IT Security Compliance Officer che a partire da metà 2004 ricopro presso la Banca del Gottardo di Lugano, dopo una lunga esperienza nel campo dell'IT Auditing. Esercitando questa nuova attività mi sono confrontato con aspetti di Information Security Management per i quali avvertivo l'esigenza di approfondire le mie conoscenze. Da qui la spinta decisiva che mi ha portato verso il corso e l'esame CISM.

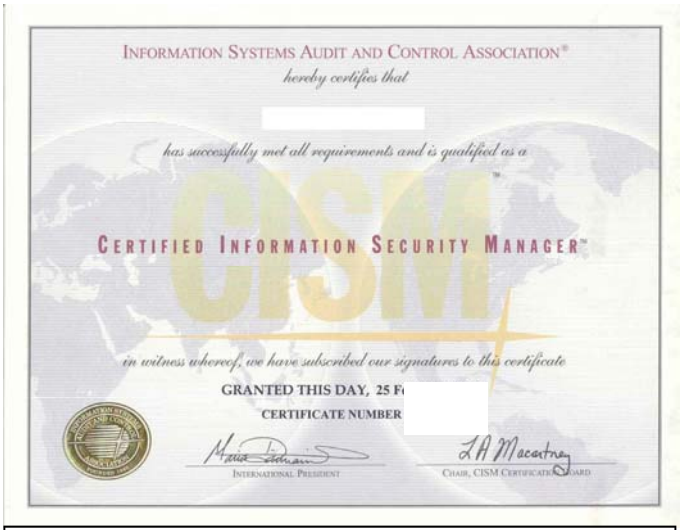
Forte dell'esperienza acquisita tre anni prima con l'esame CISA, ho affrontato la preparazione all'esame con un certo metodo, cercando innanzitutto di ottenere una buona visione complessiva delle tematiche in oggetto e cogliendone quindi gli aspetti essenziali. Da questo punto di vista il corso di preparazione tenuto da Luigi Vedani ha risposto pienamente alle mie aspettative. Le numerose discussioni durante le lezioni ed il contributo dato da tutti i partecipanti al corso, hanno dato la giusta "profondità" agli argomenti trattati.

In seguito ho completato la preparazione all'esame con i classici metodi ormai consolidati: ripasso del manuale, riordino degli appunti, test con domande campione, simulazioni d'esame...insomma, un impegno costante, qualche week-end sacrificato allo studio, una settimana di "vacanza" prima dell'esame, per completare al meglio la preparazione e tutto il tempo per maledire il giorno in cui rinunciai alla "grandfathering application" ritenendo che per un neo-CISA era troppo presto richiedere una nuova qualifica...

Il 10 giugno 2006, fatidico giorno dell'esame, mi sembra di tornare indietro nel tempo. A parte il clima (allora faceva un caldo terribile...) tutto sembra ricordarmi l'esame CISA del 2003: stesso luogo, stessa aula... scaramanticamente mi sono precipitato sullo stesso banco! Dopo 4 ore d'esame (sono come sempre tra gli ultimi a riconsegnare il materiale) ritrovo all'uscita i miei compagni di corso: anche qui provo sensazioni già vissute, sguardi poco convinti... esame difficile, domande tutte nuove, mah... le sensazioni post-esame tendono sempre al negativo, soprattutto se confrontate con quelle altrui. Cerco comunque di tranquillizzare me e gli altri: sono le medesime sensazioni di tre anni prima, e sapendo come andò a finire allora... e poi, in fondo, l'importante è essere consapevoli di aver dato il meglio di sé stessi.

Tutto il resto è storia recente: arrivano i risultati, oltre le mie aspettative, la grande soddisfazione di veder ripagati gli sforzi fatti, i complimenti dei colleghi, dei superiori... Soprattutto la soddisfazione di essersi nuovamente messi alla prova in un ambito nel quale l'impegno deve essere sempre mantenuto costante.

Finalmente CISM: una qualifica che contribuisce a dare più autorevolezza al mio lavoro e quindi anche


INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION®
hereby certifies that
has successfully met all requirements and is qualified as a
CERTIFIED INFORMATION SECURITY MANAGER™
CISM
in witness whereof, we have subscribed our signatures to this certificate
GRANTED THIS DAY, 25 F
CERTIFICATE NUMBER

Un certificato CISM

(Continua a pagina 8)

L'esame CISA e CISM: la parola ai protagonisti

(Continua da pagina 7)

maggiore visibilità e peso alle tematiche di IT Security all'interno della mia azienda. CISM significa però anche il costante impegno per mantenere aggiornate le proprie competenze e per fornire una prestazione professionale qualitativamente elevata.

Da parte mia posso senz'altro consigliare questo percorso formativo, che al di là dell'indubbia utilità pratica, mi ha permesso di conoscere nuove persone con cui ho condiviso momenti molto belli e formativi.

= = = = =

Daniela Cecagallina

La mia avventura per l'esame CISA è iniziata più o meno in dicembre 2005, quando è stato il momento di predisporre il piano personale di formazione. L'anno scorso mi ero orientata sul CISM (…superato!) dato che, per caratteristiche e contenuti, era più vicino al mio lavoro (consulente di sicurezza) ed alle mie competenze. Il CISM è tuttavia un esame "giovane" e nel nostro Paese è ancora noto solo entro ristretti confini (in effetti meriterebbe più pubblicità). Il CISA invece, esistendo da più anni, ha il vantaggio di essere maggiormente conosciuto.

Dato che anche questo "titolo" era sicuramente molto utile al mio lavoro (e quindi anche all'azienda), ho richiesto di partecipare ai corsi di preparazione e di sostenere l'esame.

Il periodo che ha preceduto l'esame è stato abbastanza fitto di impegni lavorativi e non, ma credo che sia così per tutti o quasi. La mole del manuale è rilevante, e per questo anche la pianificazione del tempo per poterselo leggere tutto almeno una volta è il primo elemento da tenere in considerazione. Fondamentalmente nella preparazione ho fatto riferimento al testo di esame ed alle raccolte di test che lo accompagnano, cercando di suddividere al meglio la massa degli argomenti sul tempo a disposizione. Ho scelto di rivedere più volte o di dedicare più tempo possibile agli argomenti con cui avevo meno a che fare nella pratica quotidiana.

Purtroppo gli impegni di lavoro mi hanno impedito di prendere parte a molte delle lezioni del corso. Ho comunque cercato di fare tesoro soprattutto delle esperienze portate dai docenti, perché credo che i casi concreti siano un'ottima base di conoscenza (peraltro anche nell'esame ci sono domande relative a "casi pratici").

Gli esercizi (test) allegati al manuale sono molto utili per fissare i concetti e rispecchiano in modo abbastanza fedele la maggior parte delle domande che vengono poste (alcune volte però è stato notato, anche durante il corso, che le risposte date come esatte sono opinabili…nessuno è perfetto… quindi attenzione); tuttavia credo che sia meglio cominciare a fare i test avendo dato almeno una lettura ai relativi capitoli del manuale. Peraltro segnalo a tutti che nella edizione di quest'anno, alcune domande riguardano argomenti affrontati in altri capitoli del libro, per cui attenzione anche a questo aspetto.

Ciascuno, a seconda delle proprie esperienze, troverà alcuni argomenti trattati in modo non del tutto soddisfacente. Personalmente ho sopperito con altre fonti di informazione. Anche se il tempo non basta mai, uno dei valori aggiunti della preparazione, per la mia esperienza, è stato costituito proprio negli approfondimenti che mi sono trovata a dover fare per poter meglio comprendere quanto brevemente illustrato nel testo.

Il mio suggerimento, visto anche il tipo di esame, è proprio quello di non considerare esclusiva-

(Continua a pagina 9)

L'esame CISA e CISM: la parola ai protagonisti

(Continua da pagina 8)

mente il manuale, poiché spesso l'esame pone quesiti che richiedono di attingere alle proprie conoscenze ed esperienze.

Nei due giorni pre-esame, come ultimo test ho fatto una simulazione con domande volutamente mai affrontate (almeno 200) e tenendo conto del tempo. Rispetto al CISM, il fatto di avere le domande in italiano mi ha consentito in effetti di risparmiare un po' di tempo, ma questo vale solo in media perché, a volte, il modo con cui è posta la domanda o la risposta "tradotta" non facilitano.

Il giorno dell'esame … c'erano molti candidati, i vari capannelli fuori dai cancelli alla mattina presto mi ricordavano la maturità … o anche i più temuti esami all'università ;-), anche perché la sede dell'esame a Milano è una vera scuola...


INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION®
hereby certifies that
has successfully met all requirements and is qualified as a
CISA
Certified Information Systems Auditor
in witness whereof, we have subscribed our signatures to this certificate
GRANTED THIS DAY, 15
CERTIFICATE NUMBER
MARIOS DAMIANIDES
INTERNATIONAL PRESIDENT
RIA LUCAS
CHAIR, CERTIFICATION BOARD

Un certificato CISA

E come per tutti gli esami, la domanda comune era "ma chi ce lo ha fatto fare…?"

Poi la tensione si scioglie (o aumenta…?) appena si cominciano a leggere le domande… le quattro ore di esame sono passate in fretta, alla fine rimanevano una decina di minuti per fugare i dubbi sulle domande più ostiche (o affidarsi alla sorte…!!).

La difficoltà maggiore in effetti credo sia quella di mantenere la concentrazione per tutto quel tempo, che è invece essenziale.

Il fatto di poter diventare CISA nel mio lavoro sicuramente aumenta la "qualificazione professionale" ed apre qualche porta in più verso nuove aree di business o comunque verso altri interlocutori. Personalmente sono molto contenta del risultato e delle prospettive. Credo anche di aver affrontato l'esame "al momento giusto", dopo aver maturato una "massa critica" di esperienza che l'esame mi ha comunque aiutato a "sistematizzare" e anche ad approfondire, almeno per alcuni argomenti. Ritengo che il CISA possa essere sfruttato al meglio proprio se pensato in quest'ottica, come del resto anche il CISM.

In bocca al lupo a tutti!

= = = = =

Andrea Conrad

Tra le motivazioni che mi hanno spinto a sostenere l'esame CISM vi sono sicuramente delle necessità di aggiornamento. Non sono però stato confrontato con una richiesta pressante da parte dell'azienda,. Si è trattato piuttosto di una decisione presa in autonomia, motivata soprattutto dal desiderio di poter sostenere con maggiore autorevolezza i miei punti di vista in ambito professionale.

Naturalmente era anche mio desiderio verificare se avevo ancora la motivazione sufficiente per sostenere con successo una prova che, tutto sommato, richiede un impegno ragguardevole, considerando anche il fatto, non trascurabile, che l'esame è esclusivamente in lingua inglese.

(Continua a pagina 10)

L'esame CISA e CISM: la parola ai protagonisti

(Continua da pagina 9)

La mia preparazione si è basata principalmente sullo studio del manuale CISM e sui questionari con le domande di simulazione d'esame, che ho ripetuto parecchie volte. Tutto sommato credo che questo approccio sia stato davvero utile, anche se poi le domande "vere" erano praticamente tutte diverse!

Per quanto riguarda il corso di preparazione, è mia opinione che dia delle indicazioni estremamente importanti su come affrontare l'esame. Ricordo alcune domande emerse durante le esercitazioni la cui risposta "ufficiale" lasciava dubbiosi tutti. La discussione che ne seguiva permetteva, in genere, di chiarire la problematica.

Il nostro istruttore, ci ha anche esortato a studiare assieme e a discutere sui punti controversi. La cosa non è stata purtroppo possibile. Credo che nessuno di noi avesse il tempo sufficiente per prepararsi prima degli incontri. Sarà forse ovvio, ma vorrei anche sottolineare che le ricerche su Internet sono state una preziosa fonte di informazione supplementare.

L'esame si è svolto in un ambiente composto da candidati CISM e CISA. Tra questi ultimi, alcuni affrontavano l'esame in italiano, altri in inglese. A parte una certa confusione iniziale, dovuta proprio a questo fatto, l'esame si è poi svolto senza particolari inconvenienti.

All'uscita vi è stato il tipico scambio di opinioni tra i partecipanti. Era convinzione quasi generale, da me condivisa, che l'esame non fosse dei più facili. Sarà forse stato per scaramanzia, ma il pessimismo era comunque il sentimento prevalente.

Concludo dicendo che, a mio modo di vedere, chi lavora nell'ambito della sicurezza informatica dovrebbe considerare seriamente l'opportunità di affrontare l'esame CISM, anche se non gli viene richiesto o imposto dall'azienda.

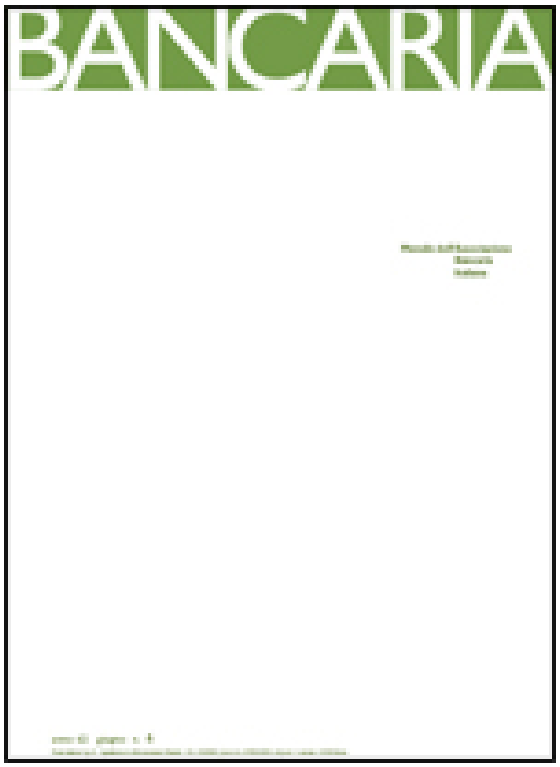
Sono convinto che si tratti di un ambito estremamente interessante e, se c'è la passione, ripagherà in ogni caso ampiamente delle risorse investite nella preparazione.

Continua nel prossimo numero di InfoAIEA: altri Associati presenteranno la loro esperienza e il loro punto di vista sugli esami di certificazione.

Nel prossimo numero continueranno le interviste ai Presidenti delle Associazioni con le quali collaboriamo.

Rubrica. Le Buone Letture.

Articoli, libri, ... dei nostri associati



Da *Bancaria n. 7-8/2006*

Information system audit, outsourcing It e compliance: le particolarità nelle banche medio-piccole

Paolo Pogliaghi, Stefano Niccolini

In questi ultimi decenni l'Information Technology sta divenendo fattore critico di successo per molte organizzazioni, nonché parte integrante del business e suo principale supporto e sostegno per lo sviluppo. Molte aziende e tra di esse banche di successo, oltre a riconoscere i potenziali benefici dell'IT, iniziano a comprendere l'importanza della gestione dei rischi inerenti all'implementazione di queste nuove tecnologie.

Di qui nasce la necessità di avere un'efficiente funzione di IT Audit che si muova secondo metodologie e schemi condivisi. In più, nella realtà delle banche di medio-piccola dimensione, non debbono essere trascurati aspetti quali l'esternalizzazione del sistema informativo in uso ma anche della stessa attività di Audit.

Più in dettaglio l'articolo prende in considerazione come attraverso l'utilizzo del modello COBIT 4.0 sia possibile ottenere indicazioni su diversi aspetti inerenti l'utilizzo delle funzioni informatiche e sulla Sicurezza realizzata all'interno della Banca.

La pubblicazione di un proprio lavoro è una soddisfazione che è anche in relazione anche al numero di persone che leggono il frutto della nostra fatica. InfoAIEA può essere un veicolo per fare conoscere questi nostri sforzi. Si sollecitano quindi gli Associati che "scrivono" a inviare, possibilmente in formato elettronico, i pezzi che saranno quindi recensiti in questa rubrica.

ISMS IUG Italy

Iniziamo con questo numero la pubblicazione di alcune interviste effettuate ai Presidenti delle Associazioni con le quali intratteniamo rapporti di collaborazione e che chiamiamo “gemellate”.

La prima è ISMS IUG Italy ed il Presidente è il Dott. Fabrizio Cirilli che ringraziamo per la disponibilità. Seguirà nel prossimo numero l’intervista ad Erminio Severo Presidente di AUSED.

———————— – ————————

Breve descrizione dell’associazione: obiettivo / mission, anno di fondazione, eventi chiave che ne hanno scandito l’evoluzione, diffusione, altro…

Il capitolo italiano del Gruppo Utenti Internazionali (IUG) dei Sistemi di Gestione per la Sicurezza delle Informazioni (ISMS) promuove lo sviluppo e l’evoluzione dello standard ISO 27001 e delle norme ad esso collegate. Il capitolo italiano è parte di un network di altri capitoli che trova la propria origine a Londra nella figura di Ted Humphreys (autore della norma e riferimento del relativo Comitato ISO).

Il capitolo italiano è stato fondato ufficialmente nel settembre del 2005 sebbene abbia iniziato l’attività nel marzo dello stesso anno.

Tra gli eventi chiave: la partecipazione al Global Security Forum del 2005, l’inserimento all’interno del Comitato ISO JTC1 SC27 WG1 e nella Task Force ISO/IAF nel 2006 che ne sanciscono il ruolo di riferimento per quanto concerne la ISO 27001 e norme collegate.

Ad oggi il capitolo italiano conta oltre 50 iscritti.

Che cosa accomuna i soci dell’Associazione, ovvero perché ci si associa (aspettative, esperienze, ramo di attività aziendale, altro)?

Ad oggi il capitolo italiano conta oltre 50 iscritti in maggioranza essi rappresentano organizzazioni pubbliche e private di rilievo nazionale. Per l’iscrizione al capitolo è richiesto l’invio di un CV che dimostri le competenze in materia di sicurezza delle informazioni affinché ciascun socio possa contribuire attivamente allo sviluppo dello standard e del capitolo stesso.

Fra gli iscritti: organismi di certificazione, aziende di consulenza, aziende del settore bancario e delle telecomunicazioni, università e centri di ricerca, regioni e comuni.

L’iscrizione al capitolo permette di ottenere copia degli standard ISO della famiglia 270-00 in via di definizione per poterne provare i contenuti e permetterne lo sviluppo. Inoltre gli associati partecipano alle sessioni di formazione ed alle riunioni plenarie partecipando attivamente alla vita associativa.

Quali sono i tratti peculiari dell’associazione, quelli che la caratterizzano in modo inequivocabile?

Elemento caratterizzante principale è il legame diretto con lo standard ISO 27001 e la partecipazione ai comitati ISO relativi.

Quali associazioni sono i parenti più prossimi ?

AIEA. AIPSI-ISSA, CLUSIT.

(Continua a pagina 13)

(Continua da pagina 12)

Quali sono i rischi di insufficiente definizione della mission ?

La dispersione delle energie e delle risorse risulta essere il maggior rischio in tal senso.

Quali iniziative dell'associazione rappresentano un particolare valore aggiunto per i soci?

Formazione tematica, forum internazionale, legami con altre associazioni.

Come si sta evolvendo la professionalità dei soci?

La spinta della ISO 27001 sta fornendo interessanti opportunità di lavoro per gli associati, le richieste per professionalità specifiche pervengono al capitolo che provvede a smistarle in modo da assicurare al richiedente la miglior soluzione tecnica e logistica.

Quali azioni avete intrapreso per supportare i soci in tale evoluzione?

Istituzione di un registro delle competenze degli associati che elenchi le eventuali certificazioni possedute ed i registri di riferimento.

Italian ISMS Chapter

Le Associazioni "gemellate".

ACFE Italy Charter

Associazione Italiana Certified Fraud Examiners

A.I.I.A.

Associazione Italiana Internal Auditors

AIPSI

Associazione Italiana Professionisti Sicurezza Informatica,
Capitolo Italiano di ISSA - The Information Systems Security Association, Inc.

ANSSAIF

Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria

ASIS Italy

capitolo italiano di American Society Industrial Security (ASIS International)

AUSED

Associazione tra Utenti di Sistemi e Tecnologie dell'Informazione

CLUSIT

Associazione Italiana per la Sicurezza Informatica

ISMS IUG Italy

International User Group dei sistemi di gestione della sicurezza delle informazioni

ITSMF Italy

Capitolo italiano di itSMF International

Rubrica. Le Buone Letture.

Novità ISACA/ITGI
COBIT e le altre best practice

ISACA ha promosso alcuni progetti per mappare COBIT su altre best practice correlate e di vasto utilizzo. Alcune pubblicazioni sono a disposizione degli Associati all'indirizzo *www.isaca.org/downloads*, altre lo saranno a breve.

COBIT Mapping: Mapping of SEI's CMM for Software With COBIT 4.0

Il Software Engineering Institute (SEI) Capability Maturity Model (CMM) è un insieme di descrizioni di "best practices" per lo sviluppo del software e può essere utilizzato per migliorare le prestazioni di una organizzazione IT. L'impatto di SEI CMM è ampiamente influenzato dai domini COBIT.

Quasi tutte le aree chiave di SEI (key practice areas - KPA) sono coerenti con i processi di COBIT. Il documento di mappatura pone in relazione le attività chiave CMM e le origini comuni nella metodologia di misura con ogni obiettivo di controllo di COBIT di dettaglio. La struttura segue i domini, i processi e gli obiettivi di controllo di COBIT e la mappatura mostra la copertura dei SEI CMM KPA all'interno di ogni livello di maturità SEI.

Il documento è disponibile da Agosto 2006 per il download per gli Associati ISACA.

COBIT® Mapping: Mapping of PMBOK® With COBIT® 4.0

"A Guide to the Project Management Body of Knowledge (PMBOK® Guide)" è descritta come la somma delle conoscenze all'interno della professione di "Project Manager".

I requisiti posti da PMBOK, pubblicato dal PMI, in termini di informazioni richieste sono mappati sui criteri di controllo di COBIT. La struttura del documento segue i domini, i processi e gli obiettivi di controllo di COBIT.

Il documento è disponibile per il download per i Soci ISACA.

(Continua a pagina 15)

(Continua da pagina 14)

CobiT® Mapping: Mapping of PRINCE2 With CobiT® 4.0

PRINCE (Projects in Controlled Environments) è un metodo strutturato per la gestione progettuale. Il metodo è stato adottato per la prima volta nel 1989 da "UK Central Computer and Telecommunications Agency (CCTA)", oggi "UK Office of Government Commerce (OGC)".

I requisiti informativi richiesti da PRINCE2 sono dettagliatamente mappati su ciascun obiettivo di controllo di COBIT. La struttura del documento segue i domini, i processi e gli obiettivi di controllo di COBIT.

Il documento è disponibile per il download da settembre 2006 per gli Associati ISACA.

CobiT® Mapping: Mapping of TOGAF With CobiT® 4.0

TOGAF (The Open Group Architecture Framework) è un metodo dettagliato dotato di un insieme di strumenti di supporto per la sviluppo dell'architettura d'impresa. Fu sviluppato dai membri dell' "Open Group" attivi nel "Architecture Forum" ed è applicato dal 1995.

Il documento di ISACA contiene una mappatura dettagliata di TOGAF 8.1 su COBIT 4.0. La struttura del documento segue i domini, i processi e gli obiettivi di controllo di COBIT.

Il documento è disponibile per il download da settembre 2006 per gli Associati ISACA.

CobiT® Mapping: Mapping of ISO/IEC 17799:2005 With CobiT® 4.0

ISO/IEC 17799:2005 The Code of Practice for Information Security Management è uno standard internazionale basato su BS 7799-1/ISO/IEC 17799:2000. Lo standard è presentato come "best practice" per la realizzazione della gestione della sicurezza delle informazioni.

Il documento di ISACA contiene una mappatura dettagliata di ISO/IEC 17799:2005 su COBIT 4.0.

Il documento sarà reso disponibile per il download entro il 2006.

La Certificazione CISA

Molte domande? A ciascuna la sua risposta!

In questo numero riportiamo le Frequently Asked Questions sulla certificazione CISA. Nel prossimo numero ci sarà un analogo articolo su CISM.

Generalità sulla certificazione CISA

Cosa è la certificazione CISA?

La certificazione CISA, istituita e rilasciata da ISACA, riconosce formalmente esperienza e conoscenze in ambito di Audit di Sistemi Informativi. La Certificazione CISA è stata omologata dall'ANSI e dal DoD. Le certificazione è concessa ed amministrata direttamente dall'ISACA, sul cui sito sono disponibili informazioni più dettagliate ed ampie. Il sito è www.isaca.org.

Quali sono le condizioni per ottenere e conservare la certificazione CISA?

La certificazione CISA richiede

- un certo numero di anni di esperienza lavorativa negli ambiti per cui si è certificati
- il superamento di un esame specifico che richiede di rispondere a 200 domande "chiuse" (una tra quattro risposte)
- l'adesione ad un Codice Etico
- una volta conseguita la certificazione, un'attività di aggiornamento tecnico negli ambiti certificati, espressa in "CPE" (ore di aggiornamento tecnico), con dei minimi obbligatori calcolati su periodi annuali e triennali
- il pagamento di una quota annua di mantenimento.

Gli esami di Certificazione si tengono due volte all'anno, in giugno e dicembre, in una unica giornata in tutto il mondo. L'esame CISA è a scelta in inglese o in italiano. Non ci sono condizioni preliminari all'ottenimento delle certificazioni, eccetto quelle citate. L'esperienza di lavoro deve essere: 5 anni di audit IT (condizioni e sostitutivi: Requirements for CISA Certification

L'ISACA organizza dei corsi di preparazione all'esame CISA?

L'ISACA mette a disposizione delle sue sedi locali (i "chapter") la documentazione e i sussidi necessari per tenere corsi di preparazione. L'AIEA è un "Chapter" dell'ISACA ed organizza dal 1992 corsi di preparazione all'esame CISA. Tali corsi si svolgono a Milano, Roma e Torino. I corsi ed i relativi programmi sono resi noti sul sito AIEA www.aiea.it

I Corsi di AIEA vengono distribuiti su alcune sessioni di due o tre giorni l'una. Le sessioni sono una ogni 2-3 settimane e sono programmate in modo che l'ultima si tenga 2-3 settimane prima dell'esame.

(Continua a pagina 17)

La Certificazione CISA

Molte domande? A ciascuna la sua risposta!

(Continua da pagina 16)

Quale altro tipo di assistenza offre l'AIEA per i candidati alla certificazione?

L'AIEA, in quanto Chapter ISACA coordina localmente, tramite un rappresentante formalmente individuato, le problematiche connesse con la Certificazione CISA

In ambito CISA AIEA:

- esegue attività di orientamento e supporto ai soci nella risoluzione di eventuali difficoltà per affrontare l'esame e ottenere / conservare la Certificazione, in particolare consigliando loro la linea di condotta da adottare
- traduce in italiano alcuni manuali di preparazione agli esami (Manuale tecnico, Manuale di esercitazione - supplemento annuale con le nuove domande)

Per sostenere l'esame CISA è necessario frequentare il corso AIEA?

No, l'esame può essere affrontato anche preparandosi da soli. Il vantaggio di iscriversi al corso è sostanziato dalla consolidata maggiore percentuale di promossi tra i partecipanti ai corsi, rispetto ai candidati che si preparano da soli.

L'iscrizione ai corsi AIEA implica che sono anche iscritto all'esame CISA?

L'iscrizione ai Corsi ed all'esame sono due cose distinte, l'una non implica l'altra. I corsi sono gestiti e tenuti da AIEA; l'iscrizione al corso avviene e viene pagata in euro, presso AIEA. L'esame è tenuto direttamente da ISACA, l'iscrizione all'esame si esegue e si paga in dollari, direttamente presso ISACA. Le due iscrizioni non sono eseguibili con un singolo atto o modulo.

Esame e requisiti di certificazione CISA

1. Qual è la fonte ufficiale d'informazione sui requisiti per certificarsi CISA?
2. Qual è la fonte ufficiale d'informazione sull'esame CISA?
3. Cosa è il foglio d'esame?
4. Non ho ricevuto il foglio d'esame e non sono sicuro di essere iscritto. Cosa devo fare?
5. Posso presentarmi all'esame senza avere il foglio d'esame?
6. Ho un problema con il pagamento del corso preparatorio AIEA, perché la mia organizzazione ha una regola istituzionale di pagamento di n giorni dopo la data della fattura. Posso seguire ugualmente il corso?
7. Conosco molto bene alcuni degli argomenti d'esame, ma credo di aver lacune su altri. Ho ugualmente delle discrete possibilità di promozione?
8. Ho trovato su un sito delle domande d'esercizio. Posso usarle per prepararmi all'esame?
9. All'esame c'era una domanda poco comprensibile, e credo di averla sbagliata. Come devo fare?

(Continua a pagina 18)

La Certificazione CISA

Molte domande? A ciascuna la sua risposta!

(Continua da pagina 17)

10. Mi sono sbagliato nel marcare la risposta esatta di una o più domande; alla fine il foglio era pasticciato ed aveva delle cancellazioni mal riuscite, Cosda devo fare?
11. Una parte sostanziale dell'esperienza che mi è richiesta per la certificazione è stata ottenuta come consulente abituale di una azienda, di cui pertanto non risulto dipendente. Cosa devo fare perchè sia convalidata?
12. Non dispongo dei requisiti minimi di certificazione in quanto mi manca una parte dell'esperienza richiesta. Devo aspettare a sostenere l'esame?
13. Ho deciso di cambiare lingua d'esame. Posso ancora modificare la mia scelta?
14. Mi sono iscritto all'esame ma non potrò prendervi parte. Posso ritirare l'iscrizione?
15. Mi sono iscritto all'esame ma non potrò prendervi parte. Posso rendere la documentazione e i sussidi d'esame già acquistati?
16. Quando sarò informato dei risultati dell'esame?

1 -cisa) La fonte ufficiale d'informazioni sui requisiti per certificarsi come CISA è la pagina: http://www.isaca.org/Template.cfm?Section=Requirements&Template=/ContentManagement/ContentDisplay.cfm&ContentID=20453 dal sito ISACA.

2 -cisa) La fonte ufficiale d'informazioni sull'esame CISA è il bollettino pubblicato sul sito ISACA. Il riferimento è: "http://www.isaca.org/cisaboi/" Questo documento definisce le date, le condizioni, i costi, le regole di iscrizione e di esecuzione dell'esame

3 -cisa) Il foglio d'esame è un documento in inglese, che riporta alcuni dati e informazioni che sono essenziali per permettere ai candidati di sottoporsi all'esame. Queste informazioni sono:

- il numero dell'esame
- l'indirizzo presso cui presentarsi
- l'ora dell'esame
- la lingua dell'esame

Senza queste indicazioni e, in particolare, senza il numero d'esame, non si viene ammessi in aula e non si può affrontare l'esame. Il foglio viene spedito ai candidati alcune settimane prima della data d'esame.

4 -cisa) Il foglio d'esame viene spedito quando gli elenchi dei candidati sono completi e, quindi, dopo la scadenza del termine d'iscrizione. Il problema può essere dovuto a:

- mancata iscrizione

(Continua a pagina 19)

La Certificazione CISA

Molte domande? A ciascuna la sua risposta!

(Continua da pagina 18)

- mancato pagamento

- mancata ricezione del foglio.

L'iscrizione viene effettuata direttamente presso l'ISACA e deve riportare la firma del candidato, oppure deve essere stata eseguita on-line sul sito indicando un numero di carta di credito per il pagamento. Se il candidato non ricorda di aver autorizzato a video o firmato alcunché, è probabile non sia iscritto.

- Mancata iscrizione: per stabilire se si è iscritti esistono le seguenti possibilità: se il candidato è socio dell'ISACA ed ha una password di accesso al sito "my isaca" -http://www.isaca.org/SecureTemplate.cfm?section=my_isaca, riservato ai membri, può stabilire immediatamente la propria posizione, consultando i suoi dati su questo sito; se non è iscritto oppure non ha la password di accesso può solo rivolgersi al CISA Coordinator, oppure direttamente all'ISACA (certification@isaca.org) per chiedere se risulta la sua iscrizione.

Se il candidato sa di essersi iscritto ed ha una prova dell'iscrizione stessa, ma non risulta iscritto, può mandarne questa prova all'ISACA e richiedere di essere comunque ammesso. Se la mancata iscrizione è stata una dimenticanza le possibilità di essere ammessi all'esame sono assai limitate.

- Mancato pagamento: Per stabilire se il pagamento è avvenuto si può consultare la propria pagina sul sito "my isaca" oppure richiedere direttamente questa informazione a certification@isaca.org. Se il pagamento non è stato eseguito, il candidato deve attivarsi immediatamente per regolarizzare la sua posizione. Gli altri problemi di pagamento (se il pagamento non è pervenuto, oppure se non si può stabilire a che titolo e per chi è stato eseguito) devono essere risolti direttamente dall'interessato. Ad esempio il candidato può inviare all'ISACA (certification@ISACA.org) i riferimenti del pagamento eseguito, specificando che si tratta della quota per la propria iscrizione. Se il pagamento per qualsiasi ragione manca, il candidato può comunque chiedere ad ISACA di ricevere il foglio d'esame e partecipare all'esame stesso. I risultati gli saranno comunicati solo a pagamento ricevuto.

- Mancata ricezione del foglio: se il foglio non è stato ricevuto il candidato può richiedere un duplicato elettronico tramite e-mail, e presentare la stampa del duplicato all'esame.

5 -cisa) In caso il foglio di esame non sia pervenuto o sia stato smarrito all'ultimo momento, si può tentare di ottenere il duplicato tramite e-mail richiedendolo a Certification@isaca.org. Presentarsi ugualmente all'esame con un documento comprovante la propria identità, senza sapere/esibire il proprio numero di partecipazione all'esame, è un tentativo con minime possibilità di successo. Al

(Continua a pagina 20)

La Certificazione CISA

Molte domande? A ciascuna la sua risposta!

(Continua da pagina 19)

Commissario d'esame spetta in questo caso la decisione se ammettere o meno il candidato. La partecipazione sarà in ogni caso impossibile se esistono delle incertezze sul numero d'esame.

6 -cisa) Si, AIEA cerca di facilitare la partecipazione dei corsisti, purché il candidato porti una prova che il pagamento è stato richiesto e che la dilazione è dovuta al ritardo intrinseco della procedura aziendale di pagamento. Il candidato deve ovviamente sollecitare la propria organizzazione a velocizzare il pagamento, rispettando i termini di iscrizione.

7 -cisa) Come indicato anche nel manuale, il requisito fondamentale della preparazione è che questa si estenda a tutte le problematiche incluse nelle "job practice areas" cioè a tutti gli argomenti riportati sul manuale. Una preparazione "a macchie di leopardo" è quindi insufficiente per definizione. L'esame è definito in modo da assicurare una copertura uniforme, quindi coloro che lo affrontano impreparati su un determinato argomento, sanno in anticipo che hanno un'alta probabilità di rispondere male alle domande che riguardano quell'argomento.

8 -cisa) Si, ma il candidato che sceglie questi esercizi decide, a proprio rischio, di usare del materiale di preparazione che potrebbe indurlo in errore. Le domande di prova più appropriate sono indubbiamente quelle messe a disposizione dall'ISACA. Non è opportuno nemmeno usare domande di prova "vecchie": la dinamica di concetti ed argomenti in ambito IT è tale che le domande di esame possono cambiare sensibilmente da sessione a sessione. Un'apposita commissione non solo seleziona di volta in volta le domande d'esercizio più adatte, ma prepara degli insiemi numericamente bilanciati secondo i pesi dei vari argomenti. Inoltre le domande di prova sono corredate da una spiegazione che riflette le logiche da usare per le risposte d'esame. Leggere e capire queste spiegazioni è una parte fondamentale dell'esercizio.

9 -cisa) Se il problema è derivante dal testo o dall'argomento della domanda non occorre fare nulla. I risultati d'esame sono sottoposti ad un processo assai strutturato di revisione a posteriori, disegnato per mettere in evidenza difficoltà di questo genere e se necessario porvi rimedio, che viene svolto separatamente per le varie lingue d'esame.

10 -cisa) La lettura delle risposte è automatica, quindi è possibile che una marcatura pasticciata causi una errata rilevazione della risposta. Per questo motivo in tutti i manuali e i bollettini si sottolinea l'importanza di marcare con chiarezza i dati d'esame e le risposte, annerendo a matita lo spazio relativo. Se uno o più pallini dei dati o delle risposte sono stati cancellati e rifatti più volte, e il punteggio raggiunto è di poco inferiore a quello limite, esiste per il candidato la possibilità di richiedere, a pagamento, la verifica del foglio consegnato. Questo riesame viene eseguito manualmente. Se risultasse che a causa dei pasticci e delle cancellature la risposta è stata erroneamente

(Continua a pagina 21)

La Certificazione CISA

Molte domande? A ciascuna la sua risposta!

(Continua da pagina 20)

interpretata in prima sede di valutazione (ipotesi però poco probabile), la revisione potrebbe avere come risultato una correzione del voto.

11 -cisa) v Dipende dall'entità della collaborazione. Se è a tempo pieno o comunque molto significativa, non c'è motivo che quell'azienda, se interpellata, neghi a ISACA la conferma integrale dell'attività eseguita. E' opportuno però che il certificando preavvisi la persona di contatto che gli viene chiesto di indicare, in modo che acquisisca in anticipo la sua autorizzazione a citarlo come referente. La persona di contatto deve essere adeguatamente informata che l'esclusivo scopo delle possibili richieste di informazione di ISACA è quello di provare all'ISACA stessa l'effettivo svolgimento delle attività dichiarate, al fine della certificazione.

12 -cisa) L'esame può essere sostenuto anche senza già disporre dei requisiti di esperienza, e rimane valido per 5 anni. Pertanto l'esperienza richiesta deve essere acquisita e fatta valere entro 5 anni dall'esame. Diversamente l'esame decade.

13 -cisa) Si, ma occorre richiedere questa variazione per tempo. Tipicamente le iscrizioni all'esame si chiudono circa 70 giorni prima del suo svolgimento. Una variazione della lingua può essere richiesta entro i 15 giorni successivi alla scadenza del termine d'iscrizione. Per i termini esatti, che possono variare di anno in anno, è necessario consultare il bollettino informativo d'esame.

14 -cisa) Sono previste due modalità diverse: cancellazione o rinvio.

la cancellazione dà diritto al rimborso della tariffa ma ISACA trattiene una quota di 100 dollari per spese amministrative

il rinvio, di cui si può usufruire una sola volta, permette di rimandare l'esame alla sessione successiva. In questo caso la quota d'iscrizione non può più essere resa, ed inoltre occorrerà versare un quota di reiscrizione di 50 dollari pagabili al momento di iscriversi alla successiva sessione d'esame.

Queste variazioni, come tutte le altre, devono essere richieste entro i pochi giorni successivamente alla chiusura delle iscrizioni. Per i termini esatti consultare il bollettino informativo d'esame.

15 -cisa) No, il materiale di studio già acquistato non può essere reso.

16 -cisa) I candidati saranno informati sul risultato degli esami sostenuti dopo 8-10 settimane dall'esame

La formazione AIEA

Un breve commento al corso sullo standard ISO 27001

di Federico Gozzi

Per l'Auditor gli standard sono un elemento essenziale, indipendentemente dal grado di utilizzo da parte dei soggetti sotto esame. Rilevanza è assunta in particolare dalle evoluzioni recenti che hanno interessato gli standard ISO con l'istituzione dell'area 27000, dedicata alla Sicurezza delle Informazioni.

Gli standard si "imparano" e AIEA ha inserito nel piano formativo del 2006 due edizioni: Roma 4, 11, 18 Aprile; Milano, 11, 18 e 25 Settembre..

Un Associato ci invia una breve sintesi della sua frequenza.

In estrema sintesi lo Standard ISO 27001:2005 è una norma internazionale che fornisce i requisiti di un Sistema di Gestione della Sicurezza nelle tecnologie dell'informazione (Information Security Management System—ISMS).

Lo standard è stato creato e pubblicato nell'ottobre 2005 a fini certificativi, in modo da costituire, assieme alla sua linea guida ISO/IEC 17799:2005, un sistema completo per garantire la gestione della sicurezza nella tecnologia dell'informazione.

Con la sua pubblicazione sostituisce la norma inglese BS 7799 - Information Security Management System ISMS, che sinora è stata la principale norma di riferimento per l'applicazione di un Sistema di Gestione per la sicurezza delle informazioni. Questo Standard Internazionale è stato approntato per fornire un modello il cui scopo è quello di impostare, implementare, utilizzare, monitorare, rivedere, manutenere e migliorare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) che è il cuore della ISO 27001.

L'adozione di un SGSI si colloca nell'ambito di un Isms Information Security Management System cioè di un processo Top Down di Governance della It Security che affronta non solo problemi tecnologici ma organizzativi e di processo con il Risk Assesment e Risk Management legato alla Sicurezza delle Informazioni e deve rappresentare per l'Alta Direzione una scelta strategica per un'Organizzazione.

La progettazione e l'implementazione di un SGSI è influenzata dalle necessità, dagli obiettivi, dai requisiti di sicurezza, dai processi impiegati e da dimensione e struttura dell'organizzazione.

L'obiettivo del nuovo standard ISO 27001:2005 è di stabilire le regole per la protezione dei dati e delle informazioni dalle minacce individuate, al fine di assicurarne l'integrità, la riservatezza e

(Continua a pagina 23)

(Continua da pagina 22)

la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (ISMS) finalizzato ad una corretta gestione dei dati sensibili dell'azienda.

La ISO 27001 e' universalmente valutata in modo positivo : è indubbiamente ben concepita ed è considerata dalle comunità tecniche mondiali nella soluzione di problematiche attinenti alla Sicurezza IT.

Personalmente aspettavo da tempo un corso sulla ISO 27001 in quanto strettamente inerente con quanto concerne la mia attuale attività lavorativa presso l'Ufficio Politiche di Qualità e Sicurezza di Reale Mutua Assicurazioni da cui dipendo.

La platea del corso come sempre è formata da colleghi, alcuni ormai sono volti noti con i quali ho già trascorso molto tempo sia per la formazione AIEA del CISA sia in altri seminari passati.

Ritengo che i corsi AIEA siano stati e saranno sempre un momento culturale importante nella vita professionale fosse peraltro perchè a prescindere dai contenuti tematici di eccellenza sia del corso che del docente , si ha la fattiva possibilità di condividere e approfondire con altri colleghi le tematiche in oggetto e rendersi spesso conto della comunanza di certe problematiche.

Ruolo fondamentale è stato svolto dal docente, F. Cirilli, che ha saputo trasferire all'aula i concetti base dello standard, attraverso un approccio pragmatico, fondato su esperienze concrete.

Abbiamo quindi avuto modo di comprendere il senso della ISO 27001 e la sua applicabilità. Abbiamo approfondito inoltre l'uso congiunto dello Standard e delle Linee Guida per impostare correttamente in Azienda un sistema efficiente ed efficace di governo e controllo in ambito IT Security . Inoltre sono stati fatti ampi riferimenti al quadro legislativo di riferimento sia nazionale che internazionale.

Ruolo fondamentale è stato svolto dal docente, F. Cirilli, che ha saputo trasferire all'aula i concetti base dello standard, attraverso un approccio pragmatico, fondato su esperienze concrete.

Direi che … non è poco

La tutela dei marchi ISACA / ITGI e della proprietà intellettuale

ISACA è alla ricerca di assistenza per l'identificazione di rischi in merito a potenziali violazioni della proprietà intellettuale attraverso l'utilizzo non autorizzato o non appropriato del marchio ISACA/ITGI o di materiale sottoposto a copyright.

Chiunque fosse a conoscenza di fatti che in qualche modo si collocano nella tipologia descritta, è pregato di metterne a conoscenza AIEA all'indirizzo mail aiea@aiea.it. Sarà cura del Consiglio Direttivo AIEA valutare i successivi passi da intraprendere.

AIEA
Associazione Italiana Information Systems Auditors

ISACA
Information Systems Audit and Control Association

AIEA capitolo di Milano di ISACA
20141 Milano— Via Valla, 16
Tel 02 84742.365- Fax 02 84742212
E-mail: aiea@aiea.it
P.IVA 10899720154

InfoAIEA
2006, Volume 4 n.3 e 4
Registrazione al Tribunale di Milano
n. 372 del 9.6.2003
Direttore Responsabile Silvano Ongetta
Editore: AIEA, via Valla, 16
20141 MILANO

Redazione: Fabio Bramani, Daniela Cecagallina, Andrea Conrad, Federico Gozzi, Orillo Narduzzo, Silvano Ongetta, Stefano Niccolini, Angelo Rodaro

Siamo su Internet:
www.aiea.it

COLLABORATE!!
InfoAIEA ha bisogno della collaborazione di tutti gli associati: articoli, segnalazioni, quesiti, opinioni, vignette, ……. .
SCRIVETECI!!
E-mail : infoaiea@aiea.it, aiea@aiea.it
Sede: AIEA, Redazione InfoAIEA
Via Valla, 16 - 20141 Milano

Consiglio Direttivo 2004-2006

Presidente:	Silvano Ongetta
Vice presidenti:	Donatella Rosa, Orillo Narduzzo
Segretario:	Enzo Toffanin
Tesoriere:	Daniela Cellino

Consiglieri:
Mario Ballerini, Emanuele Boati, Francesco Ceccarelli, Francesco Galli, Angelo Rodaro.

Probiviri:
Francesco Blanco, Arturo Salvatici, Enrico Schiocchet

ISACA®
Al servizio dei professionisti dell'IT Governance

Capitolo di Milano

AIEA

Nota per i collaboratori.

Gli articoli scientifici pubblicati costituiscono una opportunità per guadagnare ore di credito nell'ambito del CISA e CISM Continuing Education.

I documenti debbono essere inoltrati in formato testo o word, le figure debbono essere inserite come immagini.