

## Le elezioni del Consiglio Direttivo

Al'inizio di Gennaio hanno avuto luogo le elezioni per il Consiglio Direttivo AIEA. Attraverso un'ampia partecipazione al voto gli Associati hanno espresso la volontà di confermare le linee direttive che hanno caratterizzato l'Associazione negli ultimi tre anni.

Il nuovo Consiglio Direttivo, che sarà in carica per il periodo 2007—2009, è pertanto composto dai seguenti Associati, come comunicato dal Comitato Elettorale.

**Daniela Bolli, Francesco Ceccarelli, Daniela Cellino, Maria Dattoli,  
Alessandro Dellepiane, Francesco Galli, Orillo Narduzzo,  
Silvano Ongetta, Angelo Rodaro, Donatella Rosa, Enzo Toffanin.**

Ai nostri colleghi del Consiglio Direttivo vanno i più calorosi auguri di buon lavoro.



Sommario:  
**numero 1 del 2007**

<i>Editoriale del Presidente AIEA Silvano Ongetta</i>	2
<i>AIEA e le altre associazioni: AUSED e ACFE</i>	4 6
<i>Le buone letture</i>	9
<i>Gli Esami CISA /CISM Considerazioni e impressioni dei candidati</i>	10
<i>FAQ CISM</i>	14
<i>Da COBIT 4.0 A COBIT 4.1: le principali novità</i>	23
<i>Le occasioni formative di ISACA nel mondo</i>	24

## In questo numero

*Cosa è la certificazione CISM?*

*Perchè ISACA offre una certificazione  
della sicurezza dell'informazione?*

**Quali sono le condizioni per ottenere e con-  
servare la certificazione CISM?**

**L'ISACA organizza dei corsi di preparazione  
all'esame CISM?**

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

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

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

**Le risposte all'interno di questo numero!**

**AIEA e le altre Associazioni**

Continuano in questo nu-  
mero le interviste con i  
presidenti di Associazioni  
affini ad AIEA



**La redazione di INFOAIEA augura Buona Pasqua a tutti gli Associati!**

**EDITORIALE****La Presidenza dell'Associazione****Grazie della fiducia**

Ora che abbiamo, dietro le spalle, tutta la fase del rinnovo del Consiglio Direttivo, possiamo veramente pensare a tutto quello che abbiamo davanti.

Innanzitutto, un grande, caloroso grazie, da parte di tutto il CD, per la fiducia che ci avete accordato. Il numero dei votanti, quest'anno, è stato alto e questo dimostra come i soci sempre più si sentano parte attiva dell'Associazione.

Nel Consiglio, ora, siamo in 11, come previsto dallo Statuto, con ben tre nuovi consiglieri. Al di là del numero, è interessante notare che è raddoppiata (da 2 a 4) la presenza di "SOCIE" e che la distribuzione dei soci, sempre più alta, in tutto il territorio nazionale, ha portato ad un aumento di Consiglieri non "lombardi".

Il Consiglio, quindi, è ora in grado di garantire una ampia rappresentatività dei soci, con evidenti benefici per tutti gli associati. AIEA ha sempre più un respiro nazionale, rafforzato anche dai sempre più frequenti contatti con altre Associazioni similari.

Al di là delle cariche associative, ad ogni Consigliere è stato attribuito un ruolo ben definito, in modo da poter essere, per i soci, un riferimento preciso, su temi/attività definite.

Cosa ci aspetta il futuro e quali saranno gli impegni di tutto il Consiglio?

E' ovvio, ed è la mission di AIEA, cercare di soddisfare le aspettative professionali degli associati, tenendo conto anche di quelle che sono le aspettative "personali" degli stessi associati.

Questo vuol dire migliorare ed aumentare le occasioni di formazione, di incontro e di scambio di esperienze.

Diffondendo, inoltre, la conoscenza dell'Associazione a livello nazionale ed elevandone la leadership, come pure consolidando le intese con alcune associazioni professionalmente vicine, ogni socio troverà maggiori opportunità e riconoscimento professionale.

(Continua a pagina 3)

**EDITORIALE****La Presidenza dell'Associazione**

(Continua da pagina 2)

Siamo un Very Large Charter, ma questo è solo un punto di partenza: l'incremento continuo degli associati, l'ingresso di aziende diverse, potrà rendere più proficue le occasioni di incontro, permetterà interessanti confronti.

A questo punto, non resta altro che .....procedere e lavorare, con il supporto e le indicazioni che ci verranno dai soci, per mantenere gli impegni già assunti e quelli che decideremo di intraprendere.

Di nuovo un sentito "Grazie".

Silvano Ongetta

**Il nuovo Consiglio Direttivo: le cariche e le responsabilità**

Come già riportato nella AIEA Newsletter di febbraio, sono state attribuite le cariche associative e i compiti,. Di seguito il quadro complessivo dei consiglieri e delle aree di attività rispettivamente coperte.

Daniela Bolli	Responsabile relazioni con Università
Francesco Ceccarelli	Responsabile Percorsi Formativi
Daniela Cellino	Tesoriere
Maria Dattoli	Percorsi Formativi
Alessandro Dellepiane	Segretario
Francesco Galli	Responsabile relazioni con Associati
Orillo Narduzzo	Vicepresidente — Responsabile IT Governance / CobiT
Silvano Ongetta	Presidente
Angelo Rodaro	Responsabile Certificazione CISA / CISM
Donatella Rosa	Responsabile Comunicazione e promozione / Edizione Newsletter
Enzo Toffanin	Vicepresidente — Responsabile relazioni con i revisori



## AUSED

*Continuiamo 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 parola è ai Presidenti di AUSED, dott Erminio Severo, e ACFE , dott. Fabio Tortora, che ringraziamo per la disponibilità.*



L' **AUSED** - Associazione tra Utenti di Sistemi e Tecnologie dell'Informazione, indipendente e senza scopi di lucro, è nata nel 1976 per l'intuizione di alcune importanti aziende industriali e si è sviluppata progressivamente negli anni sino a essere riconosciuta come uno dei maggiori punti di riferimento dell'ICT in Italia.

Oggi raccoglie circa duecento aziende operanti nei settori industriale, manifatturiero, dei servizi, aziende che operano nel settore dell'I.C.T nonché alcuni enti pubblici. Dal 1996 accetta tra i propri Associati anche persone fisiche che, per formazione o per esperienza aziendale, siano interessate agli scopi ed alle attività dell' Associazione.

L' **AUSED** non ha condizionamenti di tipo politico, non ha sponsorizzazioni di fornitori e "vive" della sola quota associativa.

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

L' attività dell' **AUSED** si realizza con l' organizzazione di incontri, seminari, corsi, gruppi di studio, indagini, che sono caratterizzati, oltre che da elevata professionalità, da estrema concretezza in quanto costantemente tesi alla risoluzione dei problemi di scelta, sviluppo e gestione dei Sistemi Informativi delle aziende.

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

Di particolare interesse per gli associati sono i Gruppi di Lavoro, "finestre" stabili su specifiche tematiche. Ad oggi i GdL attivi sono il GUPS –Gruppo Utenti e Prospect SAP-, quello delle

## AUSED

*(Continua da pagina 4)*

Aziende Farmaceutiche, l'Osservatorio Sicurezza, il Gruppo Telecomunicazioni, il Gruppo Open Source, l'Ict Sourcing & Governance e il Gruppo SOA - Service Oriented Architecture.

*Quali associazioni sono i parenti più prossimi ?*

Negli ultimi anni si è consolidata la collaborazione con altre Associazioni che, per comunanza di obiettivi e complementarietà di missione, hanno destato l'interesse degli Associati Aused. Tra queste quelle con le quali è attivo uno scambio continuo e diretto di esperienze in un rapporto di mutua collaborazione sono l'AIIA - Associazione Italiana Internal Auditors e il Clusit - Associazione Italiana per la sicurezza informatica.

Questa collaborazione, oltre che determinare l'estensione del "catalogo" degli eventi e delle opportunità di confronto per gli associati, si è esplicitata nell'organizzazione di attività congiunte, quali l'organizzazione di convegni ed eventi comuni.

*Come si sta evolvendo la professionalità dei soci? Quali sono i rischi di insufficiente definizione della mission ?*

La continua evoluzione della professionalità dei Soci, in maggioranza CIO, richiede l'allineamento on-time ai settori delle tecnologie più innovative, alla convergenza dei media e delle TLC nei prodotti e servizi, alle architetture dinamiche per le infrastrutture e i software applicativi, ma anche all'evoluzione degli skill del Personale IT, necessario per gestire i forti cambiamenti indotti dalla Globalizzazione, dall'Outsourcing e dall'Offshore, nell'ottica di mantenersi attore trainante dell'evoluzione del Business, garantendo la Governance dei Servizi e delle Soluzioni.

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

Il "mestiere" del CIO è sempre più difficile; l'aumento della condivisione di esperienze tra Aziende, Associazioni, Università, Media e Enti Pubblici è la risposta.

*(Continua a pagina 6)*



## ACFE



(Continua da pagina 5)

L'**ACFE** nasce nel 1988 negli Stati Uniti su iniziativa di un ex-agente della CIA, **Joseph T. Wells**, che tutt'ora ne è Presidente e uomo-immagine. L'associazione, che oggi conta 40.000 iscritti in tutto il mondo si è rapidamente evoluta anche grazie al carattere di novità: portare sul piano professionale e della consulenza un tema e una attività fino ad allora caratterizzata da un taglio più poliziesco che manageriale. Infatti, uno degli obiettivi più significativi voluti e raggiunti da Wells attraverso l'ACFE, è quello della creazione di una nuova figura professionale: il Fraud Examiner, figura per la quale è stato sviluppato un apposito percorso formativo culminante nella certificazione CFE (Certified Fraud Examiners). Negli USA, la certificazione CFE gode del riconoscimento ufficiale in tutti gli ambienti aziendali, da pubblico al privato e costituisce titolo preferenziale in fase di assunzione e per gli sviluppi di carriera. La motivazione principale risiede nei requisiti richiesti per accedere a tale certificazione, ai contenuti della formazione di base, agli obblighi di mantenimento della certificazione attraverso un impegno a conseguire, ogni anno, almeno 20 ore (CPE) di formazione specialistica. Il CFE e in genere ciascun membro di ACFE, è inoltre obbligato al rispetto del rigoroso codice etico che guida ed ispira l'operato degli associati in tutto il mondo.

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

Le motivazioni prevalenti, soprattutto per l'Italia, sono quelle della ricerca di opportunità di networking con colleghi che, in ambiti ed aziende diverse, svolgono la stessa professione. Le frodi e le attività di prevenzione, richiedono, nelle aziende, una pluralità di specializzazioni che vanno dal legale, al contabile dall'organizzativo, al tecnico all'informatico al criminologo. Non esiste una sola tipologia di fraud examiner dotato di uno skills specifico e polivalente, tale da affrontare da solo tutte le problematiche legate ai fenomeni fraudolenti, ma team di esperti che collaborano e si integrano tra loro con diversi gradi di intensità a seconda del "progetto" da sviluppare. Ecco perché il networking e la formazione continua e mirata sono l'elemento chiave della vita dei Chapter che, impiegano, in questa direzione, le principali energie.

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

(Continua a pagina 7)

## ACFE

*(Continua da pagina 6)*

L'ACFE è innanzitutto un network mondiale di professionisti provenienti dalle più diverse discipline. Inoltre rappresenta l'unica e la più credibile realtà no-profit per la lotta ed il contrasto delle frodi come fenomeno globale.

*Quali associazioni sono i parenti più prossimi ?*

Proprio alla luce delle considerazioni fatte sopra a proposito della "multidisciplinarietà" ACFE trova opportunità di collaborazione e interazione con le maggiori Associazioni professionali. Sicuramente, però, ACFE si relaziona con maggiore intensità ed efficacia con quelle associazioni, che come AIEA, condividono con ACFE i principi di etica, professionalità e formazione continua, puntando in via preferenziale al networking ed alla formazione non come forma speculativa o economica, ma come "mission" sociale e professionale.

*Quali sono i rischi di insufficiente definizione della mission ?*

Il principale è sicuramente il degrado della professionalità e la perdita di valore (in termini di riconoscimento) della certificazione. E' la differenza che passa tra un circolo culturale e un network di professionisti.

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

Innanzitutto la formazione e subito dopo la possibilità di disporre di un'area "franca" e "protetta" dove condividere le esperienze professionali. Questo è possibile attraverso l'organizzazione di momenti di incontro "strutturati" e finalizzati proprio all'incontro ed al confronto professionale.

*Come si sta evolvendo la professionalità dei soci?*

La professionalità sta seguendo l'evoluzione del fenomeno delle frodi, che oltre ad essere in costante crescita, richiede attività di contrasto via via sempre più sofisticate e organizzate. Inoltre sta crescendo la consapevolezza di un approccio alle frodi di taglio più manageriale e meno poliziesco e investigativo.

*(Continua a pagina 8)*

## ACFE

(Continua da pagina 7)

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

Stiamo lavorando per soddisfare una domanda crescente di formazione con un occhio costante alle opportunità di incontro e confronto tra professionisti. Inoltre riteniamo maturi i tempi per un coinvolgimento diretto delle aziende attraverso gli organi di governo e di controllo. Ma stiamo pensando anche al futuro. Nel 2007 lanceremo delle iniziative rivolte alle Università per la realizzazione di corsi e seminari di Fraud Examination, e accompagnare la formazione di aspiranti fraud examiners attraverso borse di studio e stage formativi.

Inoltre è allo studio una serie di proposte normative volte al riconoscimento della professione del Fraud Manager-Fraud Examiners alla stregua di quanto già oggi avviene per ruoli quali l'Internal Auditor ed il CFO.



## Novità dal sito ISACA

Continua l'attività di mappatura di COBIT® con altre metodologie e standard, infatti l'ITGI (The IT Governance Institute) annuncia la disponibilità delle seguenti pubblicazioni:

**COBIT® Mapping: Mapping of TOGAF With COBIT® 4.0—**

**COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0—**

**COBIT® Mapping: Mapping of COSO ERM With COBIT® 4.1—**

Il Bookstore registra le seguenti novità:

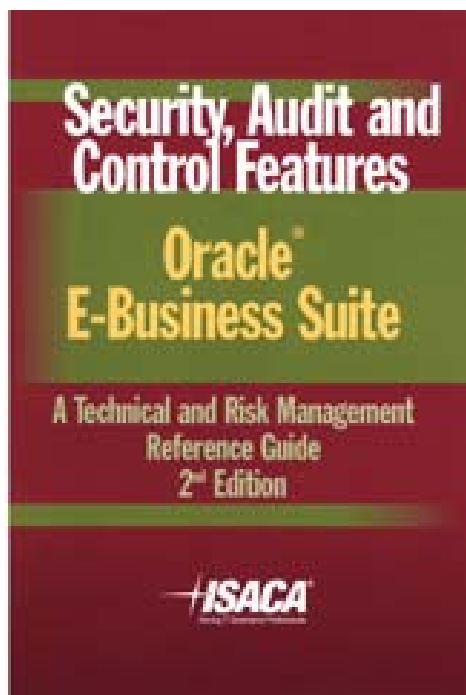
**IT Control Objectives for Sarbanes-Oxley, 2<sup>nd</sup> Edition**

**Security, Audit and Control Features SAP R/3, 2<sup>nd</sup> Edition**

**Security, Audit and Control Features PeopleSoft, 2<sup>nd</sup> Edition**

**Security, Audit and Control Features Oracle E-Business Suite, 2<sup>nd</sup> Edition**

... tutto su [www.isaca.org](http://www.isaca.org)

**Le Buone Letture:****Novità ISACA / ITGI**

**Security, Audit and Control Features Oracle Applications: A Technical and Risk Management Reference Guide, 2nd Edition**

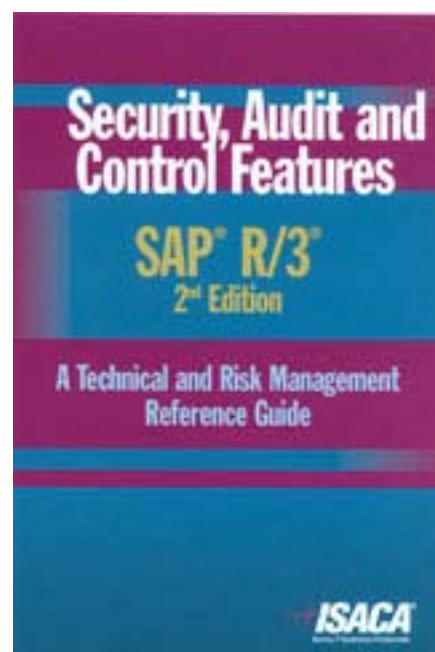
*This guide provides frameworks and methodologies for auditing and testing in an Oracle environment using Release 11i. It is written with the business manager in mind, as well as the IT and assurance professional, and has been updated to address:*

- *Third-party audit tools*
- *Investigatory tools, such as ACL's CCM technology*
- *New Oracle Applications facilities*
- *Audit programs and internal control questionnaires cross-referenced to COBIT 4.0*
- *The impact of Oracle Corporation's Project Fusion*

*This is the last guide in the series of technical and risk management reference guides to be updated to its second edition. They collectively cover enterprise resource planning (ERP) focusing on security, audit and control features of ERP systems.*

*Each guide concentrates on a different software program, but each also contains common chapters on ERP risk management and audit approach.*

***The second edition of the SAP®/R3®-based publication was published in March 2006 and is available in the ISACA Bookstore, [www.isaca.org/bookstore](http://www.isaca.org/bookstore)***





## **L'esame CISA e CISM: la parola ai protagonisti**

### **Milano, giugno 2006**

Il corso e la preparazione dell'esame mi hanno dato la possibilità di riflettere sull'impostazione del lavoro del Security Manager, di "orientare la testa" e interpretare più efficacemente le indicazioni relative all'organizzazione aziendale (argomento che, come tecnico, mi trova naturalmente spiazzata - da rinforzare con prosimi contributi di metodologia).

Quindi l'esperienza è positiva.

L'evoluzione degli argomenti professionali (norme ISO in testa) è rapida e convulsa, questo mi lascia spiazzata: è umanamente possibile restare al passo, professionalmente utili e vendibili in quest'area?

L'aspetto più arricchente del percorso resta l'incontro con i compagni "di viaggio": condividendo esperienze diverse, apertamente e anche al di fuori e al di sopra delle parti e dei ruoli, hanno portato grande valore alle lunghe giornate di lavoro. Fare squadra sarà essenziale, dentro e fuori le aziende.

### **Milano, ottobre 2006**

L'attività professionale di informatico mi ha portato negli anni a seguire un percorso di crescita tecnica verso un profilo da Security Architect (consolidato nel 2005 con la certificazione CISSP).

Ho scelto il percorso CISM per riconciliare il mio interesse professionale per le architetture di infrastruttura e l'organizzazione operativa dei data center, con l'orientamento della società di consulenza per cui lavoro. L'obiettivo comune è di sviluppare una figura professionale di consulente in grado di mediare tra il mondo tecnico e quello organizzativo.

Da qualche anno una parte sempre maggiore del mio lavoro è legata a tematiche di gestione della sicurezza. La primavera del 2006 era il momento giusto per cercare di dare una forma a questa realtà.

Il corso CISM e l'associazione ad AIEA, con i seminari di approfondimento e la documentazione raccolta sul sito AIEA/ISACA, sono stati un passo fondamentale che mi hanno permesso di attingere direttamente all'esperienza maturata sul campo da professionisti del settore.

Il corso è fondamentalmente un ripasso in vista dell'esame, focalizzato ed efficace, da abbinare alla lettura della guida per acquisire il linguaggio e entrare nel ruolo. Ritengo utile che venga arricchito in modo da approfondire i contenuti con sessioni in cui si sviluppino business case. I materiali di studio e il sito ISACA sono ricchi di riferimenti quindi utilissimi per orientarsi.

*(Continua a pagina 11)*

**Rossella Favino**

## **L'esame CISA e CISM: la parola ai protagonisti**

*(Continua da pagina 10)*

La qualifica di CISM ancora non mi appartiene, a rigore, perchè il mio curriculum professionale non è stato ancora approvato da ISACA. Tuttavia il primo risultato è di certo una maggiore sicurezza nello svolgere il mio lavoro di Security Architect, che si sta estendendo nei confronti dei gruppi, non più solo tecnici, di sicurezza aziendale e ICT Governance, con i quali finalmente posso comunicare con un linguaggio coerente e comune, comprendendo meglio anche il loro punto di vista. Mi posso porre quindi come mediatore tra gli aspetti organizzativi e quelli tecnici di progettazione, implementazione e gestione.

L'esame è stato pesante ma il tempo a disposizione è adeguato alla complessità. Unici strumenti utilizzabili, matita e testa. Consiglio di portare snack gustosi e acqua.

Ringrazio infine AIEA per l'opera che sta svolgendo per lo sviluppo della professione e l'istruttore del corso CISM, l'ing. Luigi Vedani, per avere arricchito argomenti complessi e vasti con esempi di casi reali che hanno permesso di percepire il ruolo potenziale di una figura innovativa come quella dell'Information Security Manager.

=====

### **CISA : lettera da una neofita**

**Francesca Gatti**

Alla mia età, che non ho intenzione di dire, trovarsi a studiare per prepararsi all'esame CISA su un battello che scorre lentamente le rive del Nilo, bordesando paesini di un'altra civiltà e di un tempo lontano, in una giornata africana, di scontato sole e cielo blu, distraendosi ogni tanto dalla lettura per guardare le donne in nero sulla riva, gli uomini sui somari, i bambini giocare con l'acqua e più lontano le palme verdi e i (=) الجبل djebel=montagna in arabo) ocra e rosa e dietro le dune infinite è un'esperienza che consiglio caldamente.

Non consideravo i miei vicini di ponte più fortunati perché senza il fardello dei miei testi e in piscina a sguazzare. Forse mi sentivo solo un po' inconsueta, o almeno questo leggevo nelle facce "punto di domanda" che mi passavano vicino e che allungavano i colli e aguzzavano gli occhi per captare cosa di così interessante stavo leggendo per distrarmi da un paesaggio tanto magico.

In effetti i testi Standard per l'esame CISA non assomigliano per nulla a un romanzo, né per i contenuti né per il formato; ricordano le dispense universitarie sulle quali ho passato tanti anni e che, forse per l'età che continuo a non dichiarare, ho ripreso in mano con una certa nostalgia.

E comunque **l'esame CISA era molto vicino.**

Ebbene sì, mi sono divertita un mondo.

E tralasciando la settimana in Egitto, sulla quale mi sono già dilungata troppo e che **NON E'** un passo obbligatorio per la certificazione, (si può trovare conferma a quanto dico sul sito dell'AIEA), la considero un'esperienza tra quelle che ricorderò con piacere.

*(Continua a pagina 12)*

## ***L'esame CISA e CISM: la parola ai protagonisti***

*(Continua da pagina 11)*

Perché mi sono iscritta? Per enne motivi. Primo fra tutti perché sono fermamente convinta che la competenza sia il bagaglio necessario per ottenere un consenso diffuso, senza il quale è impensabile coinvolgere coloro con i quali condividere gli obiettivi comuni di sviluppo dell'impresa. E i pressapochisti non mi piacciono.

Quello dell'Auditor è un percorso ancora poco seguito dai Professionisti IT eppure è una competenza sempre più necessaria, anche nel mondo industriale.

La tensione delle Imprese verso la Compliance Totale nei confronti di un numero crescente e complesso di Normative, Standard, Best Practices ha prodotto l'esigenza di nuovi profili professionali, in grado di familiarizzare con le tecnologie all'avanguardia ma anche padroni di metodologie per l'implementazione di modelli di Governance dei processi.

Io ho deciso di frequentare il corso AIEA per sfruttare l'esperienza di chi meglio di chiunque altro aveva la padronanza della materia d'esame. Ed ho fatto la scelta giusta, non solo perché mi è andata bene alla prima ma perché in questa avventura ho conosciuto tanta gente eccezionale, sia tra il corpo docente che tra i colleghi. Abbiamo avuto modo di confrontarci sulle nostre esperienze lavorative, di farci coraggio, di aiutarci a capire. Ognuno ha dato il suo contributo. E il giorno dell'esame ho riprovato la strana sensazione dell'adrenalina che circola veloce e la complicità tipica di un gruppo di compagni di scuola il giorno dell'esame.

Prepararsi in solitudine è naturalmente possibile ma per accedere alle competenze e alle esperienze di un gruppo eterogeneo come il nostro credo bisognerebbe quantomeno allargare la bibliografia di riferimento. Io mi sono limitata a studiare i testi standard previsti dall'esame, a frequentare le lezioni, ripetere le esercitazioni e naturalmente non dimenticare a casa la mia esperienza lavorativa. In merito a questo ultimo argomento devo mettere in guardia i potenziali colleghi futuri: in generale l'esperienza mi ha aiutata ma molto spesso mi è stata nemica. Alcune tematiche che si prestano a differenti approcci devono essere STUDIAE così come i testi CISA le trattano, e studiate molto bene proprio perché l'esperienza potrebbe essere cattiva consigliera.

Chiudo questa mia lettera con un doveroso ringraziamento a tutti i docenti per la loro disponibilità ma soprattutto per la loro competenza.

= = = = =

*(Continua a pagina 13)*

## **L'esame CISA e CISM: la parola ai protagonisti**

### **La certificazione CISA: una sigla e tanti perché.**

Prima di entrare a far parte dell'auditing, CISA era per me soltanto il

passo che collega Parma a La Spezia, tristemente famoso, tra l'altro, per le frequenti chiusure invernali a causa della neve. CISA (Certified Information Systems Auditor) è viceversa una certificazione che attesta la capacità di utilizzare una metodologia e un linguaggio comune nel mondo informatico. Elementi indispensabili, nel lavoro di auditing, per essere sempre al passo con i tempi, specialmente in un mercato sempre più globalizzato, che ti porta a continui rapporti con colleghi italiani e stranieri.

In quest'ottica ho deciso di prendere la certificazione CISA e perciò mi sono iscritto al corso, pensando che fosse come la maggioranza delle analoghe iniziative, un modo come un altro per stare fuori dell'azienda e conoscere persone nuove.

Sin dal primo giorno mi sono accorto che però non era così. Gli argomenti trattati erano tutti molto interessanti. Si andava dalla Business Continuità alla sicurezza delle informazioni, dalla organizzazione delle strutture IT alla gestione e pianificazione dei progetti informatici.

In altre parole il corso ha fornito un approccio ed una metodologia immediatamente applicabile nel lavoro di tutti i giorni, peraltro proposti in maniera accattivante.

I docenti, molto preparati ed appassionati del proprio lavoro, sono riusciti, infatti, con esempi ed esperienze personali, a rendere piacevoli anche gli argomenti più ostici.

Tutto facile quindi? Affatto! Mi sono subito reso conto che, se volevo superare l'esame, dovevo rimbocarmi le maniche e mettermi a studiare non solo il manuale, ma anche gli articoli e gli approfondimenti sui diversi temi trattati.

Quindi ho provato e riprovato i test d'esame, con i risultati perennemente sotto la soglia minima prevista per l'ammissione. Mi hanno detto: "Questo è normale. Vedrai che quando farai quello vero sarà tutta un'altra cosa." Poi il giorno faticoso è arrivato e, come consuetudine, ho avuto la sensazione che, per sentirmi sicuro, avrei avuto bisogno di altro tempo.

L'esame si svolge a Milano presso la Scuola Americana. Sembra proprio di trovarsi nel paese a stelle e strisce. Mancano solo le majorette e la locale squadra di football.


Le quattro ore previste sono passate in fretta. Troppo in fretta! Sono state appena sufficienti per rispondere alle duecento domande. Quando ho finito avevo la testa confusa e, confrontandomi con gli altri, ho pensato che sicuramente non ce l'avrei fatta a superare l'esame. Invece...

Adesso a distanza di alcuni mesi, raccontando questa esperienza, mi rendo conto di quanto sia stata utile e di come abbia migliorato il modo di svolgere il mio lavoro.

Un esempio: recentemente ho avuto modo di confrontarmi con alcuni IT Auditor stranieri, certificati CISA. Il parlare un linguaggio comune e l'adottare una stessa metodologia, mi ha permesso di superare ogni difficoltà, semplificando notevolmente il compito da svolgere. Inoltre l'aver accresciuto le conoscenze informatiche mi permette di confrontarmi in modo più diretto e competente con il personale tecnico durante le attività di auditing.

Alla luce della personale esperienza, mi sento di consigliare la certificazione CISA a tutti quelli che svolgono questa attività. Impareranno a lavorare meglio e saranno sempre aggiornati con i continui progressi tecnologici.

*Stefano Aiello*



## La Certificazione CISM Molte domande? A ciascuna la sua risposta!

*In questo numero riportiamo le Frequently Asked Questions sulla certificazione CISM. Completiamo quindi un percorso iniziato sul precedente numero di INFOAIEA, riguardante il mondo CISA.*

### *Esame e requisiti di certificazione CISM*

1. Qual è la fonte ufficiale d'informazione sui requisiti per certificarsi CISM?
2. Qual è la fonte ufficiale d'informazione sugli esami CISM?
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?
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, Cosa 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 risulterebbe dipendente. Cosa devo fare perché 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?
17. Quanto dura l'esame?
18. Quale è il punteggio richiesto per superare l'esame?
19. Quali sono gli argomenti oggetto dell'esame?

*(Continua a pagina 15)*

## La certificazione CISM

### Molte domande? A ciascuna la sua risposta!

(Continua da pagina 14)

20. Posso dare nella medesima sessione anche l'esame CISA?
21. In cosa consiste la analisi della pratica lavorativa CISM e come è stata predisposta?
22. Chi è candidabile per la certificazione CISM e cosa la rende unica?
23. La certificazione CISA è riconosciuta per il CISM?
24. La certificazione CISSP ed altri attestati di sicurezza sono riconosciuti per il CISM?
25. Cosa caratterizza il CISM rispetto ad altre certificazioni di sicurezza?
26. Cosa caratterizza il CISM nei confronti del Certified Information Systems Security Professional (CISSP)?
27. Quali sono i requisiti da soddisfare nell'ambito del CISM continuing professional education program?

**1** La fonte ufficiale d'informazioni sui requisiti per certificarsi come CISM è la pagina "<http://www.isaca.org/TemplateRedirect.cfm?Template=/ContentManagement/ContentDisplay.cfm&ContentID=20681>" dal sito ISACA.

**2** La fonte ufficiale d'informazioni sull'esame CISM è il bollettino pubblicati sul sito ISACA. Il riferimento è <http://www.isaca.org/cismboi>. Questo documento definisce le date, le condizioni, i costi, le regole di iscrizione e di esecuzione dell'esame

**3** 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** 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 16)

## La certificazione CISM

**Molte domande? A ciascuna la sua risposta!**

*(Continua da pagina 15)*

- 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](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 CISM Coordinator, oppure direttamente all'ISACA ([certification@isaca.org](mailto: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](mailto: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](mailto: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** In caso il foglio di esame non sia pervenuto o sia stato smarrito all'ultimo momento, si può

*(Continua a pagina 17)*

## La certificazione CISM

**Molte domande? A ciascuna la sua risposta!**

*(Continua da pagina 16)*

tentare di ottenere il duplicato tramite e-mail richiedendolo a: [Certification@isaca.org](mailto: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 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** Sì, 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** Come indicato anche nel manuale, il requisito fondamentale della preparazione è che questa si estenda 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** Sì, 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** 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.

*(Continua a pagina 18)*

## La Certificazione CISM

**Molte domande? A ciascuna la sua risposta!**

*(Continua da pagina 17)*

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

**11** 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** 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** Sì, 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** 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 reinscrizione di 50 dollari pagabili al momento di iscriversi alla successiva sessione d'esame.

*(Continua a pagina 19)*

## La Certificazione CISM

### Molte domande? A ciascuna la sua risposta!

(Continua da pagina 18)

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** No, il materiale di studio già acquistato non può essere reso.

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

**17** Il candidato ha a disposizione 4 ore per rispondere a 200 domande a risposta multipla.

**18** Un candidato, per superare l'esame, deve ottenere un risultato minimo di 75.

**19** L'esame CISM verifica la conoscenza da parte del candidato di principi e prassi dell'IS Audit e le sue competenze tecniche. L'esame interessa sei aree (domini)

#### **Governo della sicurezza dell'informazione**

Definire e mantenere un contesto che garantisca che le strategie della sicurezza dell'informazione siano in linea con gli obiettivi di business e rispettino leggi e regolamenti che le riguardano

#### **Gestione del rischio**

Identificare e gestire i rischi nell'ambito della sicurezza dell'informazione e conseguire gli obiettivi di business.

#### **Gestione di programmi per la sicurezza dell'informazione**

Progettare, realizzare e gestire un programma per la sicurezza dell'informazione per attuare il contesto definito nell'ambito del 'Governo della sicurezza dell'informazione'

#### **Gestione della sicurezza dell'informazione**

Coordinare e dirigere attività che interessano sicurezza dell'informazione in modo da attuare il 'Programma per la sicurezza dell'informazione'.

#### **Gestione delle risposte**

Mettere in atto e gestire la capacità di risposta e recupero a fronte di eventi dannosi o disastrosi per la sicurezza dell'informazione.

**20** No, dal momento che i due esami si tengono contemporaneamente lo stesso giorno.

(Continua a pagina 20)

## La Certificazione CISM

**Molte domande? A ciascuna la sua risposta!**

*(Continua da pagina 19)*

**21** La filosofia ISACA per la certificazione consiste nel valutare abilità e conoscenze del candidato in relazione alle prestazioni lavorative. Per definire le attività svolte da un responsabile della sicurezza dell'informazione e le conoscenze che dovrebbe avere, ISACA ha costituito una 'task force' di leader del mondo del business, esperti in materia e professionisti per definire l'esperienza lavorativa su cui si basa l'esame di certificazione. In relazione all'importanza dell'analisi e alle evoluzioni nel settore della sicurezza dell'informazione, ISACA ha attualmente in corso una revisione dell'analisi. Ai qualificati CISM che sono impegnati nella attività di revisione dell'analisi si sono aggiunti rappresentanti di ISSA , dell'Information Security Forum e di ASIS International.

**22** La certificazione CISM si caratterizza rispetto ad altri attestati di sicurezza dell'informazione perché è concepita specificamente ed esclusivamente per coloro che hanno esperienza nella gestione di un programma di sicurezza dell'informazione. I requisiti di esperienza e l'esame CISM si basano sull'esperienza richiesta per svolgere, con competenza, i compiti e le funzioni di responsabile della sicurezza dell'informazione. Questi requisiti e le attività e competenze sottoposte a verifica sono state maturate da leader della sicurezza dell'informazione e quindi verificate da esperti e responsabili della sicurezza dell'informazione. I requisiti sono volti a misurare la esperienza di gestione di situazioni attinenti alla sicurezza dell'informazione, piuttosto che competenze di tipo generale.

**23** Il programma di certificazione CISM riconosce che le credenziali CISA confermano che l'interessato ha raggiunto un livello di conoscenza e di competenza generale di base nella sicurezza dell'informazione. In base a ciò, ai qualificati CISA è riconosciuto un attestato di competenza di due anni nella sicurezza dell'informazione. D'altra parte, i certificati CISA non si possono candidare alla qualifica CISM a meno che non possiedano l'esperienza richiesta e possano dimostrare competenza e conoscenze pratiche nel ruolo di responsabile della sicurezza dell'informazione.

**24** Il programma di certificazione CISM riconosce che le credenziali CISSP confermano che l'interessato ha raggiunto un livello di conoscenza e di competenza generale di base nella sicurezza dell'informazione. In base a ciò, ai certificati CISSP è riconosciuta una competenza di due anni nella sicurezza dell'informazione. D'altra parte, i certificati CISSP non si possono candidare alla qualifica CISM a meno che non possiedano l'esperienza richiesta e possano dimo-

*(Continua a pagina 21)*

## La Certificazione CISM

**Molte domande? A ciascuna la sua risposta!**

*(Continua da pagina 20)*

strare competenza e conoscenze pratiche nel ruolo di responsabile della sicurezza dell'informazione.

Ai detentori di altri attestati più specialistici, come il GIAC (Global Information Assurance Certification di SANS, il MCSE (Microsoft Security Systems Engineer), il CompTIA Security + Credential e il CBCP (Certified Business Continuity Professional del Disaster Recovery Institute, è riconosciuto un attestato di esperienza di un anno nella sicurezza dell'informazione.

**25** Il CISM si differenzia da molte altre certificazioni di sicurezza per i suoi requisiti di esperienza e per la focalizzazione sulle attività svolte come responsabile della sicurezza dell'informazione.

Altre certificazioni di sicurezza sono caratterizzate per il focus sulle competenze tecniche o su conoscenze di specifici ambienti elaborativi o prodotti o sono rivolte a personale del settore nelle fasi iniziali della carriera. Solo il CISM si rivolge al responsabile della sicurezza dell'informazione, a colui cioè che, superata la fase di acquisizione di conoscenze, non è più interessato prioritariamente a competenze di tipo tecnico o specialistico, ma si è invece dedicato alla gestione del programma di sicurezza di un'azienda. La certificazione CISM è concepito per coloro che devono gestire e coordinare i programmi della sicurezza dell'informazione di un'azienda, e per i tecnici, molti dei quali possono essere detentori di altre certificazioni.

L'attenzione agli aspetti manageriali, che caratterizza il CISM, è testimoniata dai requisiti di esperienza, che richiedono un minimo di tre anni di responsabilità nella gestione della sicurezza dell'informazione e dall'esame, che si focalizza sulle attività di competenza dei responsabili della sicurezza.

**26** Sebbene vi siano parecchie differenze fra il 'common body of knowledge' del CISSP e le 'job practice areas' del CISM, quelle più evidenti riguardano i requisiti di esperienza. Le certificazioni CISSP e/o CISA sono complementari alla certificazione CISM e ne è incoraggiato il conseguimento.

**27** Per mantenere la certificazione CISM, si devono soddisfare i requisiti del CISM Continuing professional education (CPE) program. Questo programma richiede che l'interessato abbia svolto almeno venti (20) ore annuali e almeno centoventi (120) ore ogni tre anni di 'continuing professional education'. Inoltre è richiesto il pagamento di un canone annuale a ISACA dell'importo di 40\$ per i membri ISACA e di 60\$ per gli altri.

*(Continua a pagina 22)*

## La Certificazione CISM

**Molte domande? A ciascuna la sua risposta!**

(Continua da pagina 21)

### *Continuing Professional Education (CPE)*

1. Posso utilizzare le mie ore di CPE sia per il CISA sia per il CISM?
2. Ho sentito dire che le ore di CPE possono essere “auditare”. Di cosa si tratta?
3. Voglio sospendere per un certo periodo la mia qualifica di CISA, perché non posso ottenere le CPE. Come faccio?

**1-cpe)** Se si tratta di argomenti simultaneamente rilevanti nell'ambito dell'auditing e della gestione della sicurezza dei sistemi informativi, questo è certamente possibile.

**2-cpe)** Ogni anno ISACA seleziona un campione di persone che ha ottenuto la certificazione CISA e/o CISM per verificare la correttezza del processo di mantenimento della qualifica. Le persone selezionate dovranno produrre adeguata evidenza che comprovi l'effettuazione delle attività rispondenti ai criteri stabiliti dalla Qualifying Professional Education Activities. Il Board ISACA determinerà l'accettabilità delle ore specificate per ogni singola attività professionale formativa. I qualificati CISA e/o CISM che devono soddisfare ai requisiti CPE sono tenuti a richiedere e a conservare la documentazione pertinente alle attività educative svolte per un periodo minimo di 18 mesi dalla fine di ogni anno di attività. Per maggiori dettagli sulla Policy vedere il documento pdf in italiano alla pagina: [CISA Continuing Education Policy](#) e [CISM Continuing Education Policy](#)

**3-cpe)** Persone in condizioni particolari di impedimento temporaneo (esigenze di salute, stato di maternità, incidenti, altro) possono fare richiesta di ottenere temporaneamente la qualifica di CISA e/o CISM non in servizio attivo, salvo recuperare il loro stato attivo alla fine dell'emergenza. Le domande di cui sopra devono pervenire all'ISACA, unitamente al pagamento della quota annuale, entro e non oltre il 15 gennaio dell'anno per cui si desidera sospendere la condizione CPE. I professionisti CISA e/o CISM ai quali è concesso questo stato professionale non hanno più il dovere di adempiere agli obblighi di formazione continua, ma devono continuare a corrispondere la quota annuale di mantenimento della certificazione.

## Da COBIT<sup>®</sup> 4.0 a COBIT<sup>®</sup> 4.1

### Sintesi delle novità



#### COBIT 4.1 è un aggiornamento evolutivo di COBIT 4.0 che comprende:

1. Un' *Executive Summary* migliorato
2. L'illustrazione degli obiettivi e delle metriche nella sezione "framework"
3. Una migliore definizione dei concetti base. È importante sottolineare che la definizione di obiettivo di controllo è cambiata, spostandosi verso l'enunciato di una *practice* gestionale
4. Definizione degli obiettivi di controllo migliorata a seguito dell'aggiornamento e allineamento con le *control practices* e delle attività di sviluppo di ValIT. Alcuni obiettivi di controllo sono stati raggruppati o riformulati per evitare sovrapposizioni e rendere la sequenza degli obiettivi di controllo più coerente nell'ambito di ciascun processo con la conseguente rinumerazione degli obiettivi di controllo. Alcune espressioni sono state variate per rendere gli obiettivi di controllo più operativi e coerenti nella terminologia. In particolare gli obiettivi di controllo AI5.5 e AI5.6 sono stati inclusi nell'obiettivo AI5.4; gli obiettivi AI7.9, AI7.10 e AI7.11 sono stati inclusi nello obiettivo AI.7.8; nel processo ME3 sono stati inseriti i requisiti contrattuali in aggiunta a quelli normativi e legali.
5. I controlli applicativi sono stati rivisti per aumentare l'efficacia della loro strutturazione e per aumentare la loro capacità di supportare la valutazione dell'efficacia dei controlli stessi e la relativa documentazione. In conclusione si è ottenuta una lista di sei controlli applicativi in sostituzione dei 18 controlli applicativi illustrati nella versione 4.0, gli ulteriori dettagli sono stati portati nel fascicolo "*COBIT Control Practices, 2nd Edition*".
6. La lista degli obiettivi di business e di quelli IT contenuti nell'appendice I è stata migliorata, grazie agli spunti ottenuti dall'attività di validazione eseguita dalla University of Antwerp Management School (Belgium).
7. I supporti sono stati ampliati per fornire una lista sintetica dei processi di CobiT, inoltre lo schema che raffigura i domini è stato rivisto per includere gli elementi di controllo dei processi e di controllo delle applicazioni.
8. Sono stati opportunamente accolti ed inseriti i miglioramenti suggeriti dagli utilizzatori di CobiT 4.0 e di CobiT On line.

---

COBIT 4.1 sarà disponibile in formato pdf entro aprile 2007.

**Viaggiare e studiare  
Le occasioni formative di ISACA nel mondo**



### ISACA Training Week

<i>26-30 March 2007</i>	<i>Minneapolis, Minnesota, USA</i>
<i>7-11 May 2007</i>	<i>Denver, Colorado, USA</i>
<i>11-15 June 2007</i>	<i>Seattle, Washington, USA</i>
<i>15-19 October 2007</i>	<i>Montreal, Quebec, Canada</i>
<i>5-9 November 2007</i>	<i>San Antonio, Texas, USA</i>
<i>3-7 December 2007</i>	<i>Scottsdale, Arizona, USA</i>

Training week is a comprehensive training opportunity for information audit, assurance, security and governance professionals. Courses offered include: Fundamentals of IT Auditing, IT Audit Practices, and Information Security Management.

The Fundamentals of IT Auditing course is designed for new audit and control professionals responsible for IT audits and control reviews. The course is aligned with the CISA job practice areas and will be of particular interest to those intending to sit for the CISA exam.

The IT Audit Practices course has also been aligned with the CISA job practice areas. Presented at the intermediate level, the course builds upon the information and case studies presented in the fundamentals course to explore in greater depth the concepts, principles and practices of IT auditing.

The Information Security Management course is aligned with the CISM job practice areas. Participants will learn how to establish and maintain a framework that aligns information security strategies with business objectives; identify and manage information security risks; design, develop and manage an information security program; and develop and oversee a capability to manage incidents and recover from disruptive and destructive events.

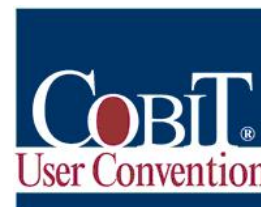
For more information on additional events and to register, please visit [www.isaca.org/trainingweek](http://www.isaca.org/trainingweek).

## Viaggiare e studiare Le occasioni formative di ISACA nel mondo

### **COBIT User Convention**

10-11 April 2007

Bogotá, Colombia



This unique educational event is exclusively designed for users of COBIT. The two-day event features case studies and facilitated discussion groups that address how COBIT is being used to identify, quantify and mitigate business risks; implement IT service improvements; satisfy control and regulatory needs; and establish performance measurement requirements. Experienced COBIT users will present implementation strategies, lead discussions, answer questions and provide COBIT updates. IT executives, assurance and control practitioners, and others who are currently using COBIT will benefit from attending this event. Participants will experience how organizations are implementing and using COBIT.

For more information and to register, please visit [www.isaca.org/cobituserconvention](http://www.isaca.org/cobituserconvention).

### **International Conference**

22-25 July 2007

Singapore



ISACA is pleased to present its 35<sup>th</sup> annual International Conference and Annual Meeting of the Membership, which will be held in Singapore. The International Conference has long been recognized throughout the world for providing in-depth coverage of the leading-edge technical and managerial issues facing IT audit, control, security, assurance and governance professionals. World-class presenters will bring together a wealth of experience and knowledge on best practices, system security, audit tools and processes, and other topics that impact not only those in a given geographic area, but all IT professionals worldwide.

For more information and to register, please visit [www.isaca.org/international](http://www.isaca.org/international).

### **Additional 2007 ISACA Conference Schedule**

10-12 September 2007—Information Security Management Conference, Las Vegas, Nevada, USA

10-12 September 2007—Network Security Conference, Las Vegas, Nevada, USA

21-24 October 2007—Latin America CACS, Monterrey, Mexico

## 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

2007, Volume 4 n.1  
Registrazione al Tribunale di Milano  
n. 372 del 9.6.2003

Direttore Responsabile Silvano Ongetta  
Editore: AIEA, via Valla, 16  
20141 MILANO

Redazione: Orillo Narduzzo, Stefano Niccolini

Hanno collaborato: Stefano Aiello, Rossella Favino, Francesca Gatti, Orillo Narduzzo, Stefano Niccolini, Silvano Ongetta

Tutti i diritti sono riservati. Il testo e le immagini non possono essere riprodotti senza autorizzazione. Le opinioni espresse dagli autori non rappresentano necessariamente le posizioni dell'AIEA. Ogni contributo sarà subordinato al vaglio di un Comitato Scientifico.

**Siamo su Internet:**

**[www.aiea.it](http://www.aiea.it)**

### COLLABORATE!!

InfoAIEA ha bisogno della collaborazione di tutti gli associati: articoli, segnalazioni, quesiti, opinioni, vignette, .....

### SCRIVETECI!!

E-mail : [infoaiea@aiea.it](mailto:infoaiea@aiea.it), [aiea@aiea.it](mailto:aiea@aiea.it)  
Sede: AIEA, Redazione InfoAIEA  
Via Valla, 16 - 20141 Milano

### Consiglio Direttivo 2007-2009

Presidente: Silvano Ongetta

Vice presidenti: Orillo Narduzzo  
Enzo Toffanin

Segretario: Alessandro Dellepiane

Tesoriere: Daniela Cellino

### Consiglieri:

Daniela Bolli, Francesco Ceccarelli, Maria Dattoli, Francesco Galli, Angelo Rodaro, Donatella Rosa.

### Probiviri:

Francesco Blanco, Arturo Salvatici, Enrico Schiocchet



Al servizio dei professionisti dell'IT Governance

**Capitolo di Milano**



### 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.*