

## Sviluppo e innovazione

di Orillo Narduzzo

Il 2007 è stato un anno di ulteriore **sviluppo**. Nel nostro paese come nel mondo la professione dell'IS Auditor ha continuato ad affermarsi. Più richiesta dal mercato, più sfide nelle aziende, più associati, più certificati: una continua crescita. Il Presidente ha illustrato nella nostra assemblea annuale i risultati conseguiti e la discussione è stata aperta da un associato, iscritto da oltre vent'anni, che ha manifestato la sua soddisfazione per il miglioramento continuo perseguito con dedizione e concretezza. La Vostra soddisfazione è la nostra.

L'associazione eroga un servizio attraverso molteplici occasioni di confronto e formazione, molte sono le opportunità che abbiamo proposto. Abbiamo stretto rapporti con i nostri colleghi che svolgono attività affini e la nostra opinione è ricercata. Siamo orgogliosi del servizio fornito agli associati, ma siamo consapevoli che è possibile fare di più, con nuove modalità e contenuti.

*"Al servizio dei professionisti dell'IT Governance"*. Questo è il nostro pay off e vogliamo essere presenti favorendo la ricerca, proponendo nuovi contenuti originali per la nostra comunità professionale. **Innovazione.**

Un percorso impegnativo che la vostra fiducia e le vostre aspettative ci stanno chiedendo. Una sfida che accettiamo volentieri e che ci porterà ad elaborare nuove forme di studio, personalizzazione, comunicazione delle best practice professionali che ci caratterizzano. Pensiamo a progetti concreti che producano strumenti di lavoro per la nostra attività: valore aggiunto da utilizzare e condividere.

*Share your knowledge!* Cosa aspetti a darci una mano, il contributo di tutti è prezioso.

Siamo fortemente convinti che nel 2008 conseguiremo ulteriori risultati per affermare la nostra professione: auguri a tutti di un felice e proficuo anno nuovo.



Sommario:

numero 3 del 2007

Obiettivi di Silvano Ongetta	2
La certificazione CGEIT	8
AIEA e le altre associazioni: ANSSAIF	10
CobiT sale a 4.1 di Orillo Narduzzo	13
Attività AIEA	15
Calendario eventi 2008	16



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

## Obiettivi

**Intervista al Presidente AIEA, Silvano Ongetta, apparsa sul numero di settembre/dicembre 2007 di Internal Audit.**

**L'intervista è stata condotta dalla dott.ssa Claudia Vignati di Twister communications group**

*Considerata la rilevanza sempre maggiore dell'Information and Communication Technology nel modo delle imprese, è indispensabile che l'auditing dei Sistemi Informativi sia affidato a professionisti qualificati e aggiornati. L'Associazione Italiana Information System Auditors (AIEA), costituita nel 1979, ha scopo di promuovere, senza scopo di lucro, l'approfondimento dei problemi connessi al controllo del processo di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie, di standard e di tecniche nella loro realtà applicativa. Per conoscere più da vicino la sua storia e la sua attività, abbiamo rivolto alcune domande al suo Presidente, il dottor Silvano Ongetta.*

### **Presidente, potrebbe descriverci brevemente gli obiettivi e la mission dell'AIEA?**

Possiamo riassumere gli obiettivi della nostra Associazione in sette punti fondamentali:

- ◇ ampliare la conoscenza e l'esperienza dei suoi soci nel campo dell'Information System Auditing, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- ◇ provvedere a un'adeguata informazione e comunicazione reciproca, ai fini dell'aggiornamento nel campo delle tecniche di Auditing nell'Information and Communication Technology (ICT);
- ◇ promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo di affidabilità dell'organizzazione e di sicurezza dei sistemi;
- ◇ promuovere la formazione di base nell' Information System Auditing e l'aggiornamento professionale dei Soci mediante l'istituzione di corsi, seminari, convegni, redazione, traduzione e diffusione di pubblicazioni, nonché collaborazioni con le Università e le Scuole;
- ◇ cooperare con altre Associazioni o Fondazioni che abbiano per oggetto attività analoga o affine a quella AIEA, nel pieno rispetto della sua autonomia;
- ◇ facilitare i rapporti di scambio con analoghe Associazioni italiane ed estere;
- ◇ promuovere, a livello nazionale, la partecipazione degli Information System Auditors alla certificazione CISA (Certified Information System Auditor) e CISM (Certified Information Security Manager) e favorire il riconoscimento in Italia di queste qualificazioni professionali.

### **Quali sono stati i principali eventi che hanno scandito l'evoluzione di AIEA?**

Nel dicembre del 1979 alcuni esperti IT – anzi di EDP, come si diceva a quei tempi – e professionisti dell'Auditing colsero l'opportunità offerta dal mondo anglosassone e dalle grandi società di revisione (le cosiddette *Big Eight* di allora) che rispondevano ad una sollecitazione del mercato. L'idea di condividere standard e metodologie e di contribuire a costruire una nuova professionalità li ha portati a percorrere, per primi in Europa, una strada che nel tempo, si è rivelata vincente. Era nata l'Associazione Italiana EDP Auditors, il primo capitolo europeo riconosciuto dalla Information System Audit and Control Association & Foundation (ISACA).

*(Continua a pagina 3)*

## Obiettivi

*(Continua da pagina 2)*

Successivamente, nel 2001, è scaturita la decisione di modificare EDP (Electronic Data Processing) in IS (Information Systems), dalla constatazione dei mutamenti dell'ambiente di riferimento, sia tecnologico, sia professionale. L'evoluzione dei sistemi ed il sempre maggiore coinvolgimento delle strutture aziendali hanno portato ad allargare la propria area di intervento, a considerare il passaggio da "centro di calcolo" a "sistema aziendale", a comprendere professionalità specifiche sui temi della sicurezza.

La prospettiva si è ampliata progressivamente, passando dalla sicurezza all'efficiacia della gestione e all'efficienza e adeguatezza della progettazione, alla congruità dei costi, al monitoraggio ed al miglioramento continuo dei processi aziendali.

Numerosi eventi hanno accompagnato tale allargamento, sottolineandone la rilevanza strategica. Tra questi vogliamo ricordare la diffusione della cultura delle norme ISO e le relative proassi di certificazione, l'affermarsi della certificazione CISA (Certified Information System Auditor) e l'attenzione del legislatore a norme e leggi sul software, sulla privacy, sulla sicurezza ecc.

### **Com'è organizzata l'Associazione?**

Possono essere membri di AIEA tutti coloro che svolgono attività inerenti al controllo ed al governo della Tecnologia dell'Informazione e della Comunicazione o che sono interessati o esperti di settori connessi o comunque ad essa riferibili.

La sede per ragioni storiche è ubicata a Milano, dove l'Associazione è nata quasi trent'anni fa, ma AIEA è da sempre presente su tutto il territorio nazionale sia per quanto riguarda gli aderenti, sia ovviamente per gli eventi, che sono organizzati in diverse regioni per facilitare sempre più i contatti tra soci, le occasioni di informazione e di scambio esperienze. Il convegno nazionale di Information System Auditing (giunto nel 2007 alla sua XXII edizione) è annualmente organizzato in varie città, spaziando dal Piemonte alla Campania, dal Veneto alla Lazio, in una alternanza, sempre gradita dai Soci.

L'elezione del Consiglio Direttivo avviene sulla base di una lista di candidature raccolte prima della data di termine del mandato e distribuite a tutti gli associati; la raccolta delle candidature e l'organizzazione delle elezioni è curata da un Nominating Committee. Gli undici componenti del Consiglio Direttivo, eletti ogni tre anni dall'Assemblea dei Soci, provengono da varie regioni; da quest'anno la componente femminile rappresenta una consistente percentuale.

È inoltre costituito un Comitato dei Proibiviri, che ha il compito di attivarsi qualora un associato intenda sottoporre una richiesta di parere su fatti inerenti l'AIEA per una sua valutazione di conformità allo Statuto o al Regolamento Esecutivo.

*(Continua a pagina 4)*

L'evoluzione dei sistemi e il sempre maggiore coinvolgimento delle strutture aziendali hanno portato AIEA ad allargare la propria area di intervento, a considerare il passaggio da "centro di calcolo" a "sistema aziendale", a comprendere professionalità specifiche sui temi della sicurezza

## Obiettivi

*(Continua da pagina 3)*

### **A chi si rivolge principalmente l'AIEA? Quali sono le caratteristiche comuni dei suoi associati?**

I soci attuali rappresentano le diverse professionalità, all'interno e all'esterno delle imprese e degli enti, direttamente o indirettamente interessati al controllo dell'Information System: auditor, informatici, controller dell'area finanza, esperti di quality assurance, security administrator, esperti legali, ecc.

Le capacità di confronto e di soluzione delle problematiche più diverse e complesse derivano da un approccio multidisciplinare, caratteristico delle differenti professionalità presenti fra gli aderenti all'Associazione Italiana Information System Auditors.

### **Tra le attività dell'Associazione quali rappresentano un particolare valore aggiunto per i soci?**

Innanzitutto con un favorevole rapporto tra costo quota e ritorni formativi, i soci usufruiscono di un continuo aggiornamento professionale con le Sessioni di Studio, i Gruppi di Ricerca e i convegni; inoltre godono di facilitazioni su pubblicazioni e partecipazioni a convegni, corsi e seminari.

Ma vorrei sottolineare il grande valore aggiunto non solo per i soci, ma anche per le aziende alle quali i soci appartengono. In particolare:

- per le imprese che, nel processo di governo dei Sistemi ICT, ritengono importante che questa professione sia regolamentata, al fine di identificare e qualificare gli operatori che possiedono i requisiti necessari per lo svolgimento della professione;

- per le società di consulenza e i professionisti, per i quali è necessario un riconoscimento della professione che ufficializzi e renda pubblico il quadro delle competenze specifiche per le attività di consulenza di direzione;

per la comunità degli affari, per la quale è indispensabile l'esistenza di un'associazione professionale che controlli e garantisca il rispetto del codice di etica e i requisiti minimi di esperienza e di continuità nella professione.

### **Quali sono i temi di attualità che l'Associazione sta affrontando, a livello locale e/o internazionale?**

In primo luogo, la IT Governance. Come è noto, l'allineamento strategico tra l'IT e gli obiettivi di business è essenziale affinché il business e la tecnologia che lo supporta, unitamente ai sistemi operativi e di gestione delle informazioni proseguano su percorsi paralleli.

Sebbene la possibilità di garantire che la strategia dei sistemi informativi sia allineata e operi in sintonia con le aspettative di business ricada tipicamente sul responsabile dei sistemi informativi, la IT Governance (che deve essere vista come un sottoinsieme della più ampia strategia aziendale) suggerisce che le re-

*(Continua a pagina 5)*

## Obiettivi

(Continua da pagina 4)

sponsabilità siano molti più ampie, per cui la definizione della direzione strategica non può che spettare all'Alta Direzione aziendale.

Quest'ultima dovrebbe quindi essere in grado di garantire che l'IT fornisca un valore definito e misurabile, che la strategia dell'IT sia allineata con la strategia aziendale e che gli scostamenti dagli obiettivi strategici siano gestiti con l'impostazione di chiare aspettative e risultati misurabili. In tale contesto l'Associazione sta da tempo operando affinché sempre più gli IS Auditor siano i "facilitatori" primari di questo processo.

Ma come è possibile pensare di gestire una parte importante della Governance dell'impresa senza prendere in considerazione l'indispensabilità del controllo e della Sicurezza? Occorre per questo individuare gli strumenti più adatti e coinvolgere gli attori più competenti, e noi come Associazione abbiamo pronte le risposte: CobiT – "Governance, Control and Audit for Information and Related Technology" è lo strumento e l'IS Auditor l'attore protagonista.

In secondo luogo, le aree di complementarietà CobiT e ITIL. Chi si occupa di Sistemi Informativi sa che deve fronteggiare esigenze spesso inconciliabili, dall'altra la necessità di presidiare con metodi e strumenti strutturati l'assetto tecnico-organizzativo del Sistema Informativo.

Da questa contrapposizione nasce il dilemma in merito al giusto compromesso tra la robustezza dell'architettura complessiva del Sistema Informativo (tecnologia, processi, organizzazione) e la necessità di dare risposte concrete alle esigenze aziendali.

La disponibilità e la conseguente adozione di standard e *best practice*, utilizzabili come riferimenti per la descrizione dei processi e il controllo del Sistema Informativo è una delle leve a disposizione per rendere meno stridente il contrasto tra teoria e realtà.

Poiché CobiT e ITIL sono le due *best practice* che stanno fornendo il maggiore contributo, diventa importante comprendere in quale contesto esse siano applicabili e con quali sinergie o sovrapposizioni. Grazie alla collaborazione tra AIEA, ITSMF Italia e SDA Bocconi è stato realizzato un white paper, "CobiT e ITIL, due framework complementari", che intende dare un primo contributo all'utilizzo sinergico e complementare di queste due fonti di conoscenza, che si stanno diffondendo come riferimenti *de facto* per l'Information Technology a livello internazionale e nazionale.

(Continua a pagina 6)

**L'Alta Direzione aziendale deve garantire che l'IT fornisca un valore definito e misurabile, che la strategia dell'IT sia allineata con la strategia aziendale e che gli scostamenti dagli obiettivi strategici siano gestiti con l'impostazione di chiare aspettative e risultati misurabili.**

## Obiettivi

*(Continua da pagina 5)*

### **A quali nuove sfide è chiamato un “moderno” Auditor ICT? E quali sono eventualmente le nuove competenze richieste?**

Come ho detto prima, l'IS Auditor e il Security Manager sono sempre più integrati nell'organizzazione aziendale. Il contributo dell'IS Auditor alla scelte aziendali e alla loro concretizzazione diventa sempre più necessario in un mondo in crescente dipendenza dalle tecnologie. L'ottica del controllo è importante, in quanto le stesse tecnologie che vengono utilizzate per il miglioramento del business e del servizio al cliente possono essere veicolo di un uso inappropriato, distorto o finanche illegale.

Molte sono le evoluzioni che in questi anni hanno portato in primo piano il Controlli Interno nei Sistemi Informativi, e di conseguenza la funzione di IS Auditing. La prospettiva si è ampliata progressivamente, passando dalla sicurezza all'efficacia ed efficienza della gestione, all'adeguatezza della progettazione, alla congruità dei costi, al monitoraggio e al miglioramento continuo dei processi aziendali.

Come ho già sottolineato, numerosi eventi hanno accompagnato tale allargamento, sottolineandone la rilevanza strategica. Tra questi vogliamo ricordare la diffusione della cultura delle norme ISO e le relative prassi di certificazione, l'affermarsi della certificazione CISA e l'attenzione del legislatore a norme e leggi sul software, sulla privacy, sulla sicurezza ecc.

### **Secondo il suo parere, quali sono gli elementi che accomunano AIEA e AIIA?**

Ricordo quanto detto prima in merito alla funzione di auditor. Gli elementi comuni sono la capacità di confronto e di soluzione delle problematiche più diverse e complesse, la capacità di porsi come “consulente” per il management.

Mi piace sottolineare il fatto, inoltre, che il Sistema dei Controlli Interni può essere definito come l'insieme della struttura organizzativa, metodi e procedure adottato da un'azienda allo scopo di assicurare il rispetto delle politiche emanate dalla Direzione, di garantire che siano presenti le risorse (in senso lato) necessarie e che questo siano utilizzate in modo efficace (ed anche efficiente) per il raggiungimento degli obiettivi aziendali prefissati, tutelare la salvaguardia dei beni aziendali e assicurare l'accuratezza, affidabilità e correttezza delle informazioni trattate dai Sistemi Informativi.

### **Qual è secondo la sua opinione il grado di sensibilità delle imprese italiane al rischio tecnologico?**

Le aziende dipendono in misura diversa dall'ICT. Per quelle che hanno un ICT pervasivo al business, la sensibilità al rischio informatico è elevata.

Il settore finanziario è tradizionalmente all'avanguardia, perché da molto tempo tiene sotto controllo il rischio tecnologico, anche in seguito alle indicazioni degli Enti Formatori.

*(Continua a pagina 7)*

## Obiettivi

(Continua da pagina 6)

Le norme sono un importante stimolo anche per le aziende soggette alla SOX, direttamente o indirettamente. Anche le aziende, c.d. Utilità stanno dimostrando una sempre crescente attenzione al rischio informatico.

La sensibilità è focalizzata sulla sicurezza, cioè sulle contromisure per ridurre i rischi, ma vi sono esempi di approcci ben strutturati che coniugano diverse *best practice* integrate tra loro.

### **Quali sono le iniziative avviate dall'AIEA per sensibilizzare le imprese sui temi della governance dei Sistemi Informativi?**

Le iniziative di AIEA al riguardo sono molte e le abbiamo già richiamate nelle precedenti risposte. Le nostre proposte sono rivolte agli uomini d'azienda perché portino nel loro lavoro le *best practice* più adeguate. In pratica riguardano la formazione attraverso:

- ◇ sessioni di studio e il convegno nazionale, l'approfondimento di gruppo;
- ◇ i Gruppi di Ricerca che redigono dei White Paper;
- ◇ la promozione dei risultati ottenuti da ISACA (modelli, metodi, tecniche, pubblicazioni) che AIEA divulga, attraverso la traduzione e la presentazione dei casi aziendali di successo.

## Attività AIEA

### **AICQ-CI (Associazione Italiana Cultura Qualità - Centro Insulare)**

AIEA ha partecipato al seminario svolto il 12 novembre 2007 presso l'università di Roma La Sapienza - Facoltà di Ingegneria. Il seminario, organizzato dal sottocomitato AICQ-CI Qualità del software & Servizi ICT, ha avuto l'obiettivo di illustrare ulteriori esperienze italiane nell'uso del Capability Maturity Model Integration (CMMI), ma iniziare anche a presentare altri Maturity Model, relativi in questa occasione al dominio del Project Management e alla gestione dei processi IT.

In particolare AIEA ha presentato come il Maturity Model di COBIT possa essere di ausilio per l'assessment dei processi IT e per l'identificazione dei punti di miglioramento con l'obiettivo di definire gli step per migliorare il governo dell'IT.



## La Certificazione



### FOCUS sulla nuova certificazione ISACA: CGEIT

Per soddisfare alla crescente importanza di una efficace azione IT Governance e per rispondere alla richiesta di uno strumento che identifichi i professionisti con l'esperienza e le conoscenze necessarie, ISACA ha introdotto una nuova certificazione: CGEIT (Certified in the Governance of Enterprise IT) articolata nei seguenti domini:

- allineamento strategico
- gestione delle risorse
- controllo dei rischi
- misurazione delle prestazioni
- produzione di valore aggiunto.

Il profilo è stato costruito con il contributo dell'ITGI e del patrimonio metodologico dell'Institute e sulla scorta delle indicazioni e dell'opinione di esperti in materia, riconosciuti a livello mondiale.

CGEIT si focalizza, inoltre, su quegli strumenti metodologici (come CobIT e ITIL) che promuovono e supportano l'introduzione e l'esercizio della Governance IT aziendale / di Corporate.

La nuova Certificazione è rivolta a quei professionisti di Governance IT con funzioni direttive, consultive o di assurance, che desiderano veder riconosciuto il profilo professionale delle proprie conoscenze ed esperienze nel campo della Governance IT.

#### Condizioni di certificazione

Per poter ottenere questo riconoscimento, i candidati CGEIT devono:

Riempire l'apposito modulo (URL: [CGEIT Job Practice](#)), a comprova di un'esperienza di lavoro minima di:

5 anni di attività a supporto della Governance aziendale,

oppure

minimo 3 anni di attività a supporto della Governance aziendale e titoli sostitutivi di esperienza per un massimo di altri 2 anni

## La Certificazione



(Continua da pagina 8)

Superare l'esame CGEIT (la prima sessione è programmata nel dicembre 2008)

Aderire al codice etico ISACA (URL: [Code of Professional Ethics](#))

Aderire allo specifico programma di "sviluppo professionale continuo" (URL: [CGEIT Continuing Education Policy](#))

Per coloro che non hanno un codice identificativo ISACA, ma hanno un profilo professionale che corrisponde a quello richiesto, è possibile ottenere tale codice riempiendo un modulo on-line (URL: [www.isaca.org/profile](http://www.isaca.org/profile)) ed accedere, quindi, al sito My ISACA. In caso di difficoltà, contattare [feedback@isaca.org](mailto:feedback@isaca.org)

### Programma di Grandfathering

E' stato lanciato anche un programma temporaneo di *Grandfathering*, cioè di certificazione iniziale CGEIT per soli titoli, che non richiede il superamento dell'esame. Le condizioni di certificazione sono, in questo caso:

Minimo di 8 anni di esperienza di Governance IT con ruolo direttivo, consultivo o di assurance

Adesione al Codice di Etica Professionale ISACA

Adesione allo specifico programma di "sviluppo professionale continuo" CEP

Presentazione dell'apposita domanda compilata (URL: [CGEIT application](#))

Pagamento degli oneri di certificazione nella seguente misura:

Soci ISACA	US \$595
Certificati CISA e/o CISM ma non soci ISACA	US \$660
Tutti gli altri	US \$725



## ***Le nostre interviste: ANSSAIF***

*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 al presidente di ANSSAIF, ANTHONY CECIL WRIGHT*

ANSSAIF è nata nel 2003 con l'obiettivo primario di consentire lo scambio di informazioni fra i Soci, questi ultimi essendo impegnati sui temi della protezione degli asset aziendali.

L'Associazione è stata *costituita* per perseguire i seguenti obiettivi:

- 1) contribuire alla maturazione, in tutte le sedi oppor tune, anche universitarie, della consapevolezza dei problemi connessi alla necessaria protezione dei beni informatici, dei dati e delle informazioni, per garantirne la riservatezza, l'integrità e la disponibilità;
- 2) promuovere studi e ricerche nel campo della sicurezza ICT (Information and Communication Technology), curando altresì di individuare processi e momenti di integrazione della sicurezza logica e di quella fisica;
- 3) conservare il patrimonio di esperienze professionali degli specialisti di sicurezza del settore, anche al termine della loro attività lavorativa;
- 4) curare la condivisione di esperienze e conoscenze atte a migliorare l'attività professionale degli associati;
- 5) curare la promozione culturale e l'aggiornamento dei soci;

*(Continua a pagina 11)*

## ANSSAIF

*(Continua da pagina 10)*

6) concorrere alla formazione di giovani specialisti;

7) fornire informazioni sulla regolamentazione in ordine a tutti gli aspetti concernenti gli obblighi delle Aziende e dei Responsabili della sicurezza nei confronti delle norme.

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

Nel tempo ANSSAIF sta divenendo un punto d'incontro dei Soci con le Società impegnate nel fornire soluzioni agli intermediari finanziari.

Agli addetti ai lavori, si stanno ora aggiungendo coloro che hanno lasciato da poco l'Azienda, dopo tanti anni di esperienza nei Sistemi Informativi ed in Organizzazione; in tal modo, il bagaglio di conoscenza e la sensibilità acquisita non va dispersa, ma diventa fattore comune.

ANSSAIF è nata da un'idea del Presidente, manifestata ai colleghi delle altre banche al termine della scrittura del Rapporto "Il Rischio Informatico", successivamente pubblicato dalla CIPA (Banca d'Italia) dopo essere stato aggiornato con la normativa del 15 luglio 2004 sulla continuità operativa.

In quella sede erano rappresentate banche ed operatori di sistema provenienti da tante Regioni d'Italia: ciò ha suggerito l'idea di rimanere in contatto attraverso una modalità associativa, sfruttando tutti i possibili canali (telefono, email, audio conferenza, riunioni) ed organizzando un Convegno annuale nel quale incontrarsi assieme ai partner e, da un paio d'anni, con relativa prole!

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

*Quali associazioni sono i parenti più prossimi e quali sono i rischi di insufficiente definizione?*

*(Continua a pagina 12)*

## ANSSAIF

(Continua da pagina 11)

Si usa dire che la Sicurezza è una catena, ove ogni anello è importante. ANSSAIF è vicina alle preoccupazioni e ai “mal di testa” di chi si occupa di Sicurezza in ambiente finanziario e, al fine di fornire una sempre maggiore assistenza agli associati, coinvolge negli studi e nei dibattiti tutti gli attori in gioco: dalle Società Fornitrici agli Operatori di Sistema, dagli intermediari alle Associazioni dei Consumatori e, non ultime, altre importanti Associazioni di professionisti.

Se consideriamo che l'ABI è un socio sostenitore e la stessa Banca d'Italia partecipa agli incontri e Convegni, si ottiene in tal modo il completamento della cosiddetta “catena” della Sicurezza.

Le occasioni di incontro, da quest'anno quasi mensili, fa sì che ogni “anello” possa esprimere il suo parere, le sue esigenze, i suoi suggerimenti ed ascolta i pareri degli altri “anelli”. Tra le Associazioni con le quali vi è un ottimo contatto ci sono l'AIEA, il CLUSIT e l'ICAA.

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

Le indagini svolte o in svolgimento (ricordo quella sul Phishing con ICAA ed ISCOM; quella in corso su “i CIO e la Sicurezza” con l'Univ. Cattolica del Sacro Cuore; ecc.), i progetti con altre Associazioni (quale “l'auditing del BCP” condotta da AIEA), i suggerimenti all'ABI per l'emanazione di linee guida sulla Gestione dell'emergenza, le raccomandazioni ai Consumatori nell'accesso ad Internet e nella conservazione dei dati personali (pubblicata con ADI-CONSUM), le analisi dei fenomeni di cybercrime in corso e pubblicate nelle newsletters, ecc., tanto per citare i fatti più recenti, forniscono utili spunti ai Soci.

La recente esperienza acquisita nella realizzazione dei Piani di Business Continuity costituisce un altro “plus”.

Molto apprezzata è l'attenzione alle problematiche correnti e l'estremo equilibrio nel fornire suggerimenti e pareri. D'altra parte, chi si occupa di Sicurezza non è alla continua ricerca del giusto equilibrio fra rischio mitigato e rischio accettato?

## ***E COBIT sale a 4.1***

***Intervista al Vicepresidente Orillo Narduzzo  
apparsa su Computerworld del 25.6.2007***



Il 5 maggio scorso, un mese prima di ITIL Versione 3, è stata rilasciata la versione 4.1 del modello COBIT (Control Objectives for Information and related Technology) utilizzato per scopi di controllo dei processi IT e quindi soprattutto dagli auditor dei sistemi informatici aziendali.

COBIT è un framework composto da un insieme di pubblicazioni che contengono linee guida e modelli riconosciuti in tutto il mondo come il supporto per implementare un efficace governo dell'IT in una azienda. Il nucleo centrale è un modello che integra le risorse, i processi ed i criteri di valutazione delle informazioni tipici dell'ambito ICT, permettendo di effettuare assessment o avviare progetti di miglioramento della gestione con la garanzia di un quadro di riferimento completo e allineato alle best practice inerenti questo settore (ISO27001, BS20000, ITIL e le altre).

Delle principali novità di COBIT 4.1 abbiamo parlato con Orillo Narduzzo, vicepresidente dell'Associazione Italiana Information Systems Auditors (ISACA Milan Chapter) e responsabile dell'ufficio operativo Auditing ICT della Banca Popolare di Vicenza.

### **Quali sono le aziende in Italia e nel mondo che utilizzano COBIT?**

Nel mondo sono decine di migliaia le aziende ed i consulenti che utilizzano COBIT. I principali casi sono presentati sul sito [www.isaca.org](http://www.isaca.org). Nel 2005 la Comunità Europea ha riconosciuto COBIT, assieme ad altri due standard, come riferimento per la valutazione dei sistemi di controllo IT delle agenzie per il pagamento dei contributi alle aziende agricole. Audit o IT Governance in Italia sono sinonimi di COBIT per i principali gruppi bancari ed assicurativi, le principali utility, le società di revisione, i consulenti dell'Alta Direzione.

### **Quali sono le principali novità di COBIT 4.1?**

Sono stati esplicitati gli obiettivi di alto livello sia aziendali che IT che di processo creando dei legami fra di loro per definire dei percorsi di miglioramento focalizzati e a supporto del modello di IT Governance che ITGI (IT Governance Institute, l'ente che ha pubblicato COBIT per ISACA) ha sviluppato e pubblicato.

*(Continua a pagina 14)*

## **E COBIT sale a 4.1**

*(Continua da pagina 13)*

Gli "obiettivi di controllo", il cuore di COBIT finalizzato all'audit, sono stati riformulati per avvicinarsi di più alle linee guida gestionali. Il tema del controllo è stato collocato in "IT Assurance using COBIT" dove trovano spazio le descrizioni del valore aggiunto e dei rischi corrispondenti a ciascun obiettivo di controllo, oltre ai test necessari per verificarne l'adeguatezza. In "COBIT Control Practices", invece, vi è la descrizione di come si può progettare un buon sistema di controllo.

I "controlli generali", di tipo gestionale, sono sempre stati un punto di forza di COBIT; in questa versione sono stati indirizzati precisamente anche i "controlli applicativi" e i "controlli di processo". Sono stati proposti altri due supporti per le analisi di tipo organizzativo: l'elenco dei documenti che incorporano le interfacce tra i 34 processi censiti da COBIT, e le responsabilità ricoperte dalle principali figure professionali presenti in azienda e nell'IT in ciascun processo.

### **Cosa risponde a chi ritiene COBIT, così come altre metodologie, uno strumento esclusivamente per poche grandi realtà?**

COBIT non è solo per le grandi aziende. Oltre ad avere una linea guida per l'utilizzo nell'ambito delle PMI, nella recente versione il modello è stato semplificato riducendo il numero degli obiettivi di controllo.

### **Come è stato affrontato il tema dell'integrazione con le altre metodologie complementari del mondo IT, prima tra tutte ITIL?**

Fin dalla prima versione di COBIT, le principali best practice inerenti il governo dell'ICT sono state considerate e incorporate. Questa attenzione è stata mantenuta costante e ogni aggiornamento ha migliorato l'utilizzo dei termini in modo da facilitare la comunicazione tra specializzazioni diverse e, in quest'ultimo anno, COBIT è stato formalmente mappato sulle principali best practice.

In particolare la pubblicazione del 2005 confronta COBIT 3.0 con ITIL 2, quella del 2006 COBIT 4.0 con ITIL 2 e passa in rassegna i due framework per sottolinearne la complementarietà. Aspettiamo a breve la nuova edizione che mapperà ITIL versione 3 su COBIT 4.1.

## **Attività AIEA**



### **FORUM PA (21 maggio 2007)**

AIEA ha partecipato, nell'ambito del Forum PA, al convegno Linee guida CNIPA sulla qualità delle forniture ICT. Il convegno nasce dalla constatazione del proliferare dei quadri di riferimento come COBIT, CMMI, ISO 9001, ISO 20000, ITIL, PMBOK, ecc. Obiettivo del convegno è stato quindi presentare le best practices COBIT, ITIL, PMBOK e CMMI e avviare un percorso di confronto tra i diversi approcci e le Linee Guida CNIPA.

### **Convegno AIPSI (6 giugno 2007)**

AIEA ha partecipato alla seconda edizione della ISSA European Security Conference che si è tenuta a Roma presso l'hotel Sheraton il 6 giugno 2007. L'evento, organizzato dall'AIPSI (Associazione Italiana Professionisti Sicurezza Informatica, capitolo italiano di ISSA), in collaborazione con Infosecurity, ha visto la partecipazione di AIEA alla roudtable finale sul tema "Risk of information leaving the enterprise", moderata da Stefano Zanero del Politecnico di Milano, a cui hanno partecipato Cosimo Comella (Garante Privacy), Rhonda MacLean (CEO della MacLean Risk Partners ed ex CISO di Bank of America) e Gerardo Costabile (Poste Italiane).

### **CNIPA (attività in corso)**

AIEA partecipa ad un tavolo di lavoro costituito dal CNIPA. Nell'ambito dell'evoluzione delle "Linee Guida sulla qualità dei beni e dei servizi ICT per la definizione e il governo dei contratti della pubblica amministrazione" messe a punto dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), anche con la collaborazione di Confindustria Servizi Innovativi e Tecnologici e AITE-CH/ASSINFORM, il CNIPA stesso ha richiesto la costituzione di un gruppo di lavoro che approfondisca i principali best practices framework allo scopo di diffonderne la conoscenza in ambito pubblico dandone una sintetica descrizione e tutte le informazioni per procurarseli ed approfondirne i contenuti, correlarli ai bisogni della pubblica amministrazione espressi dalle linee guida CNIPA in relazione all'acquisizione di forniture ICT ed infine esaminarne le eventuali certificazioni ad essi associate per valutarne l'utilizzabilità per la selezione del fornitore, la valutazione della qualità offerta, la definizione ed il governo dei contratti ICT.

Più precisamente CNIPA intende prendere in considerazione sia modelli per la qualità dei processi ICT che costituiscono raccolte organizzate (framework) di best practices, che raccolte di requisiti dei processi ICT codificate all'interno di standard. In particolare il gruppo di lavoro dovrebbe approfondire i seguenti framework e requisiti standard dei processi ICT: COBIT, ITIL, CMMI, PM BOK, PRINCE 2, EN ISO 9001:2000, ISO/IEC 20000:2005, ISO/IEC 27000:2005, UNI ISO 10006:2005.

AIEA partecipa al Gruppo di Lavoro quale sponsor del modello COBIT.



# Calendario Eventi



## 1° SEMESTRE 2008

"Legenda Colori"		Roma	Milano	Torino	Lugano	
Gennaio	Febbraio	Marzo	Aprile	Maggio	Giugno	
1	Corso IS Audit Base Roma	Corso CISA Roma	<i>Sessione di Studio Roma</i>			
2			<i>Sessione di Studio Milano</i>			
3		ITIL Foundation v.3 Milano				
4		ITIL Foundation v.3 Milano	Corso CISM Milano			
5		ITIL Foundation v.3 Milano	Corso CISA Roma			
6		ITIL Foundation V.3 Milano	Corso CISM Milano			
7		Corso CISA Milano	Corso CISA Roma			
8		Corso CISA Torino	ITIL Foundation v.3 Roma			
9		Corso CISA Milano	ITIL Foundation v.3 Roma			
10		Corso CISA Torino	ITIL Foundation v.3 Roma	Corso CISA Roma		
11	Lead Auditor ISO27001 Milano	Corso COBIT Base Milano	ITIL Foundation v.3 Roma	Corso CISM Milano		
12	Lead Auditor ISO27001 Milano	Corso COBIT Base Milano	<i>Sessione di Studio Torino</i>	Corso CISA Roma		
13	Lead Auditor ISO27001 Milano	<i>Sessione di Studio Torino</i>	Corso CISA Milano	Corso CISA Roma		
14	Lead Auditor ISO27001 Milano	Corso CISA Roma	Corso CISA Torino	Corso CISM Milano		
15	Lead Auditor ISO27001 Milano	Corso CISA Roma	Corso CISA Milano	Corso CISA Roma		
16	<i>Sessione di Studio Lugano</i>		Corso COBIT Avanzato Milano	Corso COBIT Avanzato Milano	Corso CISA Milano	Information Security Management
17	<i>Sessione di Studio Torino</i>			Corso CISA Torino	Corso CISA Torino	
18				Corso CISM Roma	Corso CISM Roma	Information Security Management
19				Corso CISA Milano		
20				Corso CISA Torino		
21				Corso CISM Roma		
22		Corso CISA Milano		Corso CISA Roma		
23	<i>Sessione di Studio Roma</i>	Corso CISA Torino		Corso CISM Milano		
24				Corso CISA Roma		
25				Corso CISM Milano		
26				Corso CISA Roma		
27						
28	Corso IS Audit Base Roma		Corso CISA Milano			
29	Corso IS Audit Base Roma	Corso CISA Roma	Corso CISA Torino			
30	Corso IS Audit Base Roma	<i>Sessione di Studio Roma</i>	Corso CISA Milano			
31	Corso IS Audit Base Roma		Corso CISA Torino		Corso CISM Roma	



# Calendario Eventi

## 2° SEMESTRE 2008



"Legenda Colori"		Roma	Milano	Torino	Veneto	
	Luglio	Agosto	Settembre	Ottobre	Novembre	Dicembre
1						Information Security Management Milano
2						
3				Corso CISA Roma Corso CISM Milano	ITIL Foundation v.3 Roma	Information Security Management Milano
4				Corso CISA Roma Corso CISM Milano	ITIL Foundation v.3 Roma	
5					ITIL Foundation v.3 Roma	
6				ITIL Foundation v.3 Milano	ITIL Foundation v.3 Roma	
7				ITIL Foundation v.3 Milano	Corso CISA Milano Corso CISA Torino	
8				ITIL Foundation v.3 Milano <i>Sessione di Studio Milano</i>	Corso CISA Milano Corso CISA Torino	
9				ITIL Foundation v.3 Milano <i>Sessione di Studio Roma</i>		
10				Corso CISA Milano Corso CISA Torino Corso CISM Roma		
11				Corso CISA Milano Corso CISA Torino Corso CISM Roma	Corso Avanzato COBIT Roma <i>Sessione di Studio Roma</i>	<i>Sessione di Studio Roma</i>
12					Corso Avanzato COBIT Roma <i>Sessione di Studio Milano</i>	
13					<i>Sessione Veneto</i>	
14				Corso COBIT Base Roma	Corso CISA Roma Corso CISM Milano	
15				Corso COBIT Base Roma	Corso CISA Roma Corso CISM Milano	
16						<i>Sessione di Studio Milano</i>
17				Corso CISA Roma Corso CISM Milano	Lead Auditor ISO27001 Milano	
18				Corso CISA Roma Corso CISM Milano	Lead Auditor ISO27001 Milano	
19			Corso CISA Roma		Lead Auditor ISO27001 Milano	
20			Corso CISA Roma	Corso IS Audit Base Milano	Lead Auditor ISO27001 Milano	
21				Corso IS Audit Base Milano	Lead Auditor ISO27001 Milano Corso CISM Roma	
22			Lead Auditor ISO27001 Roma	Corso IS Audit Base Milano	Corso CISM Roma	
23			Lead Auditor ISO27001 Roma	Corso IS Audit Base Milano		
24			Lead Auditor ISO27001 Roma	Corso IS Audit Base Milano		
25			Lead Auditor ISO27001 Roma <i>Sessione di Studio Torino</i>			
26			Lead Auditor ISO27001 Roma Corso CISA Milano Corso CISA Torino			
27			Corso CISA Milano Corso CISA Torino		<i>Sessione di Studio Torino</i>	
28					Corso CISA Milano Corso CISA Torino Corso CISA Roma	
29					Corso CISA Milano Corso CISA Torino Corso CISA Roma	
30				Corso CISA Milano Corso CISA Torino Corso CISM Roma		
31				Corso CISA Milano Corso CISA Torino Corso CISM Roma		

**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

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, opi-  
 nioni, 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 op-  
 portunità 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 immagi-  
 ni.*