



Iniziativa :

**"Sessione di Studio" a Roma**

*Gentili Associati,*

*Il Consiglio Direttivo è lieto di informarVi che, proseguendo nell'attuazione delle iniziative promosse dall'Associazione Italiana Information Systems Auditors volte al processo di miglioramento, di formazione e informazione dei propri associati, ha organizzato un incontro che avrà luogo a:*

**Roma, 4 marzo 2008**

**Presso**

**Hotel Universo**

**Sala Convegni- Via Principe Amedeo, 5/B**

*come da agenda allegata.*

*La sessione, come sempre, è gratuita per gli associati; la partecipazione è estensibile, inoltre, ai non Soci, che intendano associarsi ad AIEA per l'anno 2009, vedi scheda d'iscrizione.*

*Per aderire all'iniziativa è richiesta la compilazione dell'allegata scheda di iscrizione che dovrà pervenire alla Segreteria dell'AIEA, **entro e non oltre il***

**2 marzo p.v.**

*Ricordiamo che la partecipazione all'evento corrisponde sino a 4 ore di credito nell'ambito del CISA/CISM Continuing Education (CPE).*

*In occasione della Sessione, verranno distribuiti:*

? *i PIN ai soci AIEA che si sono certificati CISA o CISM dal 2003 e che ISACA ha elencato come rispondenti ai requisiti richiesti da ISACA stessa*

? *le copie del quarto volume delle Guide AIEA "COBIT 4.1 E ISO 27001- Confronto quantitativo e qualitativo"*

*Vi Aspettiamo!*

Il Presidente  
(S. Ongetta)

Roma, febbraio 2009

## Abstract delle relazioni

Regole e normative sono sempre più numerose e vincolanti. Questo comporta che i temi legati alla compliance debbano essere affrontati in modo organico ed efficiente. Nel corso della sessione si parlerà di come impostare una gestione integrata di Compliance, capace di una visione complessiva di tutte le problematiche inerenti. Tale gestione integrata potrà permettere di meglio governare i cambiamenti, ridurre i rischi e contenere i costi, eliminando ridondanze e creando sinergie organizzative

### Nicoletta De Bonis (OPENTECH)

#### ? **La Compliance per la Governance in un sistema integrato di relazioni e di scambio di flussi informativi: presupposti ed esperienze**

La Compliance riveste sempre più un ruolo cruciale: non si tratta solo del rispetto di adempimenti alle normative esterne e alle policies e strategie interne, ma di affrontare in modo proattivo la complessità in cui opera l'Azienda e gestire l'evoluzione della organizzazione aziendale, con cui essa persegue i suoi obiettivi. In alcune realtà (Banche e Assicurazioni) è obbligatoria l'istituzione di una Funzione aziendale specifica e di un processo strutturato per il soddisfacimento della compliance. Nelle altre Aziende è comunque una esigenza sempre più forte tenere sotto controllo la "rete" complessa di normative, decreti, circolari e regolamenti interni.

Le Aziende devono passare ad una cultura di integrazione tra le diverse Funzioni aziendali, tramite la condivisione di processi e di asset e lo scambio di flussi informativi. L'Organizzazione e i Sistemi Informatici sono elementi essenziali per il raggiungimento degli obiettivi di Business: è necessario che siano progettati e monitorizzati e che garantiscano il rispetto dei principi di privacy e di sicurezza informatica.

### Marco Tulliani (SARA Assicurazioni)

#### ? **Utilizzo pratico di COBIT per gli obiettivi di IT Governance e di Compliance, come modello di governo integrato.**

La Compliance è una responsabilità della Direzione Aziendale e consiste nel garantire l'adeguamento a leggi, direttive interne e standard. In questo processo di adeguamento, data la sempre maggiore importanza dei sistemi informativi, la Direzione IT è direttamente coinvolta e spesso gioca un ruolo fondamentale.

Il tema della compliance viene tipicamente affrontato come un male necessario ed è spesso percepito come un puro costo. Un approccio comprensivo, basato sulla Governance IT e quindi guidato dagli obiettivi di Allineamento Strategico, Valore delle Realizzazioni, Misurazione delle prestazioni, Gestione del Rischio e Gestione delle risorse, permette di adempiere alle richieste di Compliance, ottenendo risultati significativi e con costi contenuti.

Durante la presentazione saranno illustrati i contenuti dei framework di riferimento quali COSO e COBIT, i benefici attesi relativamente all'IT Governance come Modello Integrato e l'impatto organizzativo richiesto.

### Domenico De Angelis (OMNITECH)

#### ? **La Security Governance come processo all'interno dell'IT Governance**

L'IT rappresenta oggi un elemento radicato profondamente nei processi di business delle aziende e senza il quale spesso non sarebbe possibile neanche sviluppare nuove opportunità ed offerte da presentare sul mercato. La gestione in sicurezza dell'IT e di tutte le informazioni in esso contenute e amministrare rappresenta quindi una sfida, o in molti casi una scommessa, con la quale tutto il Management si trova a confrontarsi giornalmente.

L'intervento affronta le tematiche della Security Governance, presentando una metodologia di gestione integrata all'interno di una soluzione che consente di automatizzare il processo di sicurezza. Impiegata congiuntamente alla metodologia di analisi della sicurezza, la metodologia di gestione integrata può velocemente contribuire al rafforzamento della figura dell'IT Security Manager (CSO) all'interno dell'azienda.

## Relatori

### **Nicoletta De Bonis (OPENTECH)**

Ha conseguito la laurea in Matematica, alla Università “La Sapienza” nell’anno accademico 1980. E’ stata assunta nel 1981 da Syntax (Olivetti) ed ha proseguito il suo iter lavorativo, passando nel 1985 alla società Sistemi Informativi (Gruppo IBM) dove ha lavorato fino al 2005. Nello stesso anno ha iniziato la sua collaborazione con Opentech, rivestendo, in particolare, il ruolo di Direttore Sviluppo Prodotti; nell’ambito si è occupata della progettazione dei requisiti e nel coordinamento dello sviluppo di progetti di Compliance di Opentech.

Nel corso del tempo la sua carriera si è evoluta su due percorsi paralleli, maturati nel tempo. Uno è il percorso “tecnico” del software (progettazione e sviluppo soluzioni, delivery presso i Clienti, coordinamento di gruppi di lavoro su progetti differenti). L’altro è il percorso “metodologico” relativo ai processi di gestione e supporto per il software e per l’erogazione dei servizi correlati. Di seguito una sintesi delle Competenze e delle Certificazioni.

Ha acquisito vaste competenze in progetti complessi di Compliance, Governance-Risk-Compliance, IT Security, Assessment e Audit di Processo per processi ISO 9001:2000.

### **Marco Tulliani (SARA Assicurazioni)**

Ha conseguito la laurea in Ingegneria Elettronica (specializzazione Telecomunicazioni) nell’anno accademico 2001 presso l’Università di Roma Tre in Roma; nel medesimo anno ha conseguito l’abilitazione alla professione di Ingegnere ed è iscritto all’albo degli Ingegneri della Provincia di Roma.

E’ socio dell’ISACA (Information Systems Audit and Control Association) e del Clusit (Associazione Italiana per la Sicurezza Informatica).

Dopo una significativa esperienza come analista software presso una primaria società di consulenza informatica (Accenture) ha maturato un’esperienza triennale come responsabile di progetto presso l’Alenia Marconi System del Gruppo Finmeccanica, occupandosi anche di soluzioni di sicurezza end-to-end che indirizzano le necessità di sicurezza e privacy per i clienti internazionali.

Nel successivo biennio ha rivestito il ruolo di Senior Information System Auditor presso una primaria società di revisione contabile (KPMG), acquisendo conoscenze specialistiche nell’Information Risk Management oltre a svolgere audit sui processi informativi, operativi e contabili.

Nel corso del 2006 è stato assunto come Responsabile nell’ambito dell’IT Audit della Direzione Internal Audit di Gruppo di SARA Assicurazioni, al fine di curare il coordinamento delle verifiche sui processi informatici di SARA Assicurazioni e delle società appartenenti al Gruppo SARA, a supporto delle relative strutture di audit.

Nel 2006 ha partecipato in ISCOM - Istituto Superiore delle Comunicazioni (Ministero delle Comunicazioni) alla scrittura delle linee guida per la Certificazione di Sicurezza.

### **Domenico De Angelis (OMNITECH)**

Nato nel 1970, Domenico De Angelis inizia ad operare nel campo dell’Information Technology dal 1991 entrando in Sistemi Informativi Spa (gruppo IBM) e maturando le prime importanti esperienze sistemiche nel campo dei sistemi dipartimentali Unix, Oracle e Reti su un progetto di grande entità presso il cliente ENPALS.

Dopo l’esperienza nel gruppo IBM, opera sul mercato IT come libero professionista acquisendo



## Capitolo di Milano

competenze significative nell'ambito dei sistemi dipartimentali Unix e reti e approfondendo il proprio know-how nel settore della Sicurezza IT. E' proprio in quest'area che sin dal 1995 è impegnato come consulente presso grandi clienti nell'area Telco, Finance, PA, Utilities in progetti di sicurezza dove copre incarichi sia tecnico-specialistici che di responsabile di progetto. In particolare si occupa di Identity Management, Access Control, Strong Authentication, Vulnerability Assessment, PKI, Network Security, System Integration. Durante tale periodo sviluppa esperienze gestionali ed un network di conoscenze e relazioni con Aziende e Partner Nazionali ed Internazionali.

Nel 2001 è impegnato come socio fondatore nello start-up di Alpha Sistemi Srl (attuale Visiant Security), dove fa confluire le precedenti esperienze nel settore della sicurezza informatica consolidandole in una struttura di diversi collaboratori e di partnership con aziende fornitrici di soluzioni di sicurezza.

Dal 2007 collabora con Omnitech Srl, nuova start-up nell'ambito dell'Information Security operativa su Roma e Milano dove opera come Executive Consultant nella definizione delle strategie di marketing e vendite per lo sviluppo del Business. Da gennaio 2009 assume il ruolo di Responsabile dell'area Marketing & Vendite.

## PROGRAMMA

14.00	Registrazione dei partecipanti
14.15	Apertura dei lavori e saluto: <b>Donatella Rosa (Consiglio Direttivo AIEA)</b>
14.30	<b>Nicoletta De Bonis (Opentech)</b> <i>La Compliance per la Governance in un sistema integrato di relazioni e di scambio di flussi informativi: presupposti ed esperienze</i>
15.30	<b>Marco Tulliani (SARA Assicurazioni)</b> <i>Utilizzo pratico di COBIT per gli obiettivi di IT Governance e di Compliance, come modello di governo integrato</i>
16.30	<b>Domenico de Angelis (Omnitech)</b> <i>La Security Governance come processo all'interno dell'IT Governance</i>
17.30	<b>Domande e dibattito con i relatori</b>
17.50	<b>Aperitivo</b>
18.15	Termine dei lavori

In collaborazione con:



<sup>1</sup> La partecipazione all'evento in oggetto corrisponde sino a 4 ore di credito nell'ambito del CISA/CISM Continuing Education.

## Come arrivarci:

### Mezzi pubblici (raccomandato)

- Tutti i Bus ATAC con fermata e/o capolinea a Termini
- Metropolitana A e B, fermata Termini:
- Usciti dalla metropolitana si gira verso Via Cavour: seconda traversa a destra

