

### XXI CONVEGNO NAZIONALE Sfide e opportunità: valore aggiunto dell'audit IT

di Silvano Ongetta

"Cammino sulle acque" così iniziava il mio editoriale del 2003 relativo al Convegno svoltosi a Orvieto (a mia difesa cercavo subito di non allarmare i lettori sul paventato rischio di miei, sino ad allora sottaciuti, incontrollabili livelli di onnipotenza). Quest'anno stante la sede del nostro Convegno se volessi ripercorrere quella colorita farsariga (ma sempre rimanendo con i piedi *ancorati* al suolo) potrei dire che abbiamo viaggiato **con il vento in poppa**.

Aldilà di immagini più o meno fantasiose, posso affermare, dopo aver ascoltato i commenti *a caldo* dei convenuti, corroborati in questi giorni da messaggi e-mail di qualche relatore e alcuni soci, che quello di Livorno è stato un ottimo Convegno.

(Continua a pagina 2)

### Assemblea Annuale AIEA

Il giorno martedì 17 luglio 2007, ad ore 18,30, presso la sede AIEA, Via Valla 16, Milano, è indetta in prima convocazione ed, occorrendo, in seconda convocazione, il giorno **Mercoledì 18 luglio 2007, ad ore 16.00, presso Unicredit Global Information Services (UGIS), via Livio Cambi 1 - Milano (MM1 Lampugnano)**

**L'Assemblea annuale** degli Associati AIEA per discutere e deliberare sul seguente ordine del giorno:

- ◇ Presentazione delle attività svolte dal Consiglio Direttivo nell'anno
- ◇ Presentazione delle attività previste nei prossimi mesi
- ◇ Approvazione del Rendiconto anno 2006
- ◇ Varie ed eventuali.

Si auspica la partecipazione di tutti. Gli associati sono invitati ad annunciare la propria partecipazione inviando il modulo accluso alla mail del 26.6.2007, debitamente compilato. Gli associati impossibilitati a partecipare, possono delegare un altro associato per essere rappresentati nelle operazioni di voto. Ogni delegato può accettare fino ad un massimo di tre deleghe.



Sommarrio:

numero 2 del 2007

<i>Sfide e opportunità: valore aggiunto dell'audit IT</i> di S. Ongetta	1
<i>Assemblea annuale AIEA</i>	1
<i>Un appuntamento importante: gli esami CISA e CISM</i>	3
<i>Formazione sui processi IT e su COBIT in collaborazione con SDA BOCCONI</i>	3
<i>AIEA e le altre associazioni:</i> AIIA AIPSI CLUSIT	4 8 10
<i>Percorsi formativi: settembre ed ottobre</i>	12
<i>COBIT e ITIL: due framework complementari</i>	13
<i>IT Control Objectives for BASEL II</i>	13
<i>Analisi di vulnerabilità applicative e Sviluppo Sicuro</i> di R. Ugolini	14

## XXI CONVEGNO

### Sfide e opportunità: valore aggiunto dell'audit IT

(Continua da pagina 1)

#### **I partecipanti**

Conteggiando gli iscritti, i relatori, i consiglieri e i preziosi e graditi ospiti è stata sfiorata quota 150. Anche se negli anni passati non siamo stati molto distanti da questo risultato, è indubbio che il Convegno di Livorno è al primo posto nella nostra hit parade di partecipazione. Questo risultato credo sia stato favorito da alcune premesse:

- a) La sede del Convegno – non capita tutti i giorni di poter accedere ed utilizzare le splendide strutture dell'Accademia Navale, ottenerne il patrocinio, ricevere il gratificante saluto di benvenuto dell'Ammiraglio comandante, essere supportati tecnicamente in sala da valenti militari, avere un Capitano di fregata come relatore, potere vedere da vicino la parte aerea di un brigantino e visitare la sala storica (dove sarebbe stato molto piacevole poter rimanere di più ad ascoltare le interessanti spiegazioni e vedere alcune testimonianze della Storia navale patria...ma le relazioni *premevano*)
- b) I relatori e i coordinatori – alcuni veri “animali da palcoscenico”
- c) Soprattutto l'importanza e l'attualità dei temi in agenda, favorita anche dal fatto che gli abstract delle relazioni sono stati resi noti con buon anticipo rendendo possibile una adeguata valutazione preventiva degli argomenti.

#### **L'anno prossimo ?**

Occorrerà ovviamente mantenere quantomeno il livello raggiunto in questi anni e quindi sarà necessario come sempre far tesoro dei vostri suggerimenti. Siate certi che approfondiremo con la massima attenzione i giudizi espressi nei “questionari per la rilevazione del grado di soddisfazione dei partecipanti” che i convenuti hanno compilato e da cui come sempre trarremo le indicazioni per far sì che il prossimo Convegno sia sempre più allineato alle vostre aspettative.

Consentitemi di riproporre una chiusa già usata in passato che esprime un modo di vedere l'Associazione che mi è proprio ed è endemico anche in altri consiglieri: “La fiamma del sacro fuoco è sempre accesa”. Da sette anni infatti la nostra più grande soddisfazione è il pensiero che il nostro lavoro nel suo insieme è da voi valutato positivamente e ciò ci dà la carica per cercare di essere sempre all'altezza delle vostre attese.

## Un appuntamento importante: gli esami CISA e CISM



Il 9 giugno 2007 hanno avuto luogo gli esami per gli aspiranti CISA e CISM. L'interesse per le certificazioni ISACA continua ad essere notevole anche in Italia.

71 candidati hanno messo alla prova la loro preparazione nella consueta cornice della Scuola Americana di Milano. Di questi 59 hanno affrontato la prova CISA, 12 hanno affrontato l'esame CISM.

I numeri italiani sono in linea con quelli riportati da ISACA che annuncia, per il 2007, a livello mondiale, un aumento del 19% degli iscritti agli esami CISA, rispetto all'anno precedente. La crescita degli aspiranti CISM si attesta invece su un rotondo 25%. A tutti i candidati auguriamo di ottenere a breve notizie positive da ISACA.



## Formazione sui Processi ICT e su COBIT in collaborazione con SDA BOCCONI



AIEA è lieta di informare i soci dell'avvenuta sottoscrizione di un accordo con SDA BOCCONI per facilitare l'accesso ai corsi inerenti la promozione di una expertise sui processi ICT delle aziende.

I corsi "COBIT BASE" e "COBIT AVANZATO" fanno parte di un percorso didattico disegnato in collaborazione con SDA BOCCONI ed i loro contenuti sono complementari al corso SDA BOCCONI "Gestire per processi l'ICT in azienda".

Per questo motivo i partecipanti alle prossime edizioni del corso COBIT (sia base che avanzato) potranno usufruire di uno sconto pari al 10%, se al momento dell'iscrizione risulteranno iscritti anche al corso SDA BOCCONI "Gestire per processi l'ICT in azienda".

## Le nostre interviste: AIIA



*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 AIIA dott.ssa Carolyn Dittmeyer, di AIPSI dott. Elio Molteni e di CLUSIT dott. Gigi Tagliapietra, che ringraziamo per la disponibilità.*



**Associazione Italiana Internal Auditors**  
*Progress Through Sharing*

Nata nel 1972 l'AIIA, Associazione Italiana Internal Auditors, rappresenta il chapter italiano dell'Institute of Internal Auditors americano (IIA), con il suo fondamentale contributo al processo di miglioramento e consolidamento dei meccanismi di risk governance e controllo delle aziende presenti in Italia.

L'AIIA guarda al controllo interno come strumento dell'azione manageriale per il governo dell'operatività aziendale, al fine di pervenire ad un giusto equilibrio tra gli obiettivi economici e sociali, così come tra gli obiettivi aziendali e individuali.

Compito primario dell'Associazione è quello di promuovere lo sviluppo della professione di Internal Auditing, nonché la diffusione della cultura aziendale sulle tematiche di corporate governance, risk management e controllo interno, al fine di accrescere la consapevolezza di come il ruolo di Internal Auditing incida sul sistema "impresa", fornendo valore aggiunto e migliorando i processi dell'organizzazione.

In particolare, la *mission* dell'AIIA si esprime nei punti che seguono:

- ◇ Promuovere lo sviluppo della professione dell'Internal Auditing, formulando tra l'altro gli standard professionali di riferimento e prevedendo opportuni programmi formativi
- ◇ Aumentare la diffusione nelle aziende e nelle enti di conoscenze ed informazioni riguardanti la Corporate Governance, il Risk Management ed il Controllo Interno
- ◇ Sviluppare le modalità secondo le quali l'internal auditing incide sul valore del sistema impresa.

*(Continua a pagina 5)*

## AIIA

*(Continua da pagina 4)*

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

Associarsi all'AIIA significa diventare destinatario di una formazione professionale continua sui temi della "Corporate Governance" e della "Control Governance", grazie ad un'intensa attività di promulgazione e diffusione che si articola in pubblicazioni, corsi, workshop, convegni e tavole rotonde. L'obiettivo principale è quello di garantire ai soci un aggiornamento tempestivo sull'evoluzione degli standard, della normativa di riferimento e delle pratiche dell'Internal Auditing, nonché alimentare un costruttivo confronto tra le diverse esperienze professionali di cui i soci sono portatori, al fine di garantire un percorso di crescita professionale basato su una condivisione sinergica.

L'invito ad associarsi è pertanto rivolto ad una gamma eterogenea di figure accomunate dall'interesse, teorico o professionale, verso la pratica di Internal Auditing.

In particolare, la gamma dei soci AIIA è composta di:

- 1) persone che svolgono l'attività di Internal Auditing, consulenza e valutazione del sistema di controllo interno quali, ad esempio,:
  - ◇ sindaci
  - ◇ responsabili/addetti di funzioni aziendali preposte al controllo interno
  - ◇ specialisti in società di revisione e consulenza
  - ◇ componenti di enti regolatori
  - ◇ professionisti, dottori commercialisti
- 2) esponenti del mondo economico, finanziario e accademico
- 3) studenti e chi frequenta master/corsi di specializzazione in Internal Auditing

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

L'AIIA rappresenta l'Institute of Internal Auditors in Italia. Questa rappresentanza si manifesta già nella struttura organizzativa dell'associazione, speculare a quella dell'Institute americano. Oltre a questo, ciò che la contraddistingue fortemente è proprio l'attività di formazione e aggiornamento professionale continuo che, insieme alle certificazioni professionali, rappresentano il fulcro dell'attività dell'associazione. In merito alle certificazioni, vale la pena sottolineare che l'AIIA è il riferimento ufficiale e unico dell'Institute per il conseguimento delle certificazioni professionali (CIA, CCSA e CFSA) e per la certificazione dei validator per il programma di Quality Assurance.

Il ruolo dell'AIIA come punto di riferimento ufficiale per chi pratica questa professione è riconosciuto

*(Continua a pagina 6)*



**AIIA**

*(Continua da pagina 5)*

ovunque; tra i propri partners annovera infatti le più importanti aziende presenti in Italia, che si rivolgono all'associazione per tutto ciò che riguarda la pratica dell'internal auditing.

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

Ad oggi, viste le caratteristiche dell'associazione e l'attività svolta, non è possibile individuare associazioni o altri tipi di organizzazioni che possano essere comparate all'AIIA. Il fatto stesso di essere l'unico interlocutore diretto dell'IIA in Italia, sede di certificazione e promotore ufficiale della divulgazione dell'*International Practices Framework*, definisce chiaramente il suo ambito d'intervento, rendendo di fatto nullo il rischio di insufficiente definizione.

Per contro, numerosi sono i punti di contatto - sotto il profilo degli interessi professionali e delle relative aree sinergiche - con altre associazioni di categoria e/o ordini professionali che rappresentano, di fatto, interlocutori continui dell'Associazione (quali, ad es., Confindustria, ANIA, ABI, Ordine Dott. Commercialisti, etc.).

Significative, infine, sono le aree di condivisione e di reciproco arricchimento esistenti tra l'AIIA e l'AIEA, presentando entrambe una radice comune data dall'attività di auditing, pur tenuto conto della focalizzazione specialistica di quest'ultima (governo e controllo dei sistemi ITC).

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

L'AIIA promuove numerose iniziative a valore aggiunto rivolte ai soci. In particolare:

- ◇ con un programma permanente di aggiornamento e formazione ai vari livelli si propone di coprire l'insieme dei bisogni espressi dai servizi di Internal Auditing e dalle funzioni preposte al Controllo delle aziende sul piano della preparazione tecnico-professionale dei loro componenti;
- ◇ con pubblicazioni periodiche qualificate e con incontri periodici (convegni, tavole rotonde, seminari) mantiene l'aggiornamento degli Internal Auditor in relazione alla crescente evoluzione dei singoli settori aziendali e favorisce un proficuo scambio di opinioni sugli argomenti di maggiore interesse professionale;
- ◇ provvede alla preparazione - ed è sede di esame - per la qualifica di CIA (Certified Internal Auditor), titolo riconosciuto in tutto il mondo e che conferisce una certificazione di qualità, di CCSA (Certificazione in Control Self-Assessment) e di CFSA (Certificazione in Financial Services Auditor);
- ◇ con i Comitati costituiti al proprio interno (tra cui il Comitato per lo Sviluppo Metodologico, il Comitato per la Ricerca e Studi, il Comitato per il Settore Finanziario, il Comitato per la Formazione, il Comitato per le Relazioni Esterne, il Comitato per lo sviluppo di iniziative con le Univer-

*(Continua a pagina 7)*



**AIIA**

(Continua da pagina 6)

sità, il Comitato per l'Area D.Lgs 231/01, etc.) ed i relativi gruppi di lavoro promuove la diffusione/affinamento nel contesto italiano del framework operativo e l'emanazione di position paper su tematiche di particolare attualità ed interesse;

- ◇ con la rete di relazioni gestita sia a livello nazionale che internazionale alimenta un'attività di benchmarking che consente alle singole realtà di confrontarsi continuamente con gli altri operatori. Tra le iniziative di recente avvio si ricordano:
  - ◇ il Chief Audit Executive Program a cui partecipano i responsabile delle funzioni Internal Audit delle maggiori aziende italiane;
  - ◇ il Gruppo di Lavoro con l'associazione AICOM sulla funzione Compliance;
  - ◇ il Gruppo di Lavoro con l'associazione ANDAF sulle novità introdotte dalla L. 262-/05 in relazione agli aspetti di informativa societaria e di responsabilità a carico del "Dirigente Preposto".

#### *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.

---



**IT Governance: The Tools of the Trade**  
**e-Symposium™**  
Live & Online: 31 July 2007  
[www.isaca.e-symposium.com](http://www.isaca.e-symposium.com)

*Continuano i seminari di ISACA. I prossimi appuntamenti sono previsti per martedì 31 luglio 2007 su "IT Governance: the tools of the trade" e per martedì 28 agosto 2007 su "Managing IT Risk for Compliance". Al termine di ciascun seminario è possibile sostenere l'esame che permette di guadagnare 3 ore per la Continuing Policy Education.*



## ***Le nostre interviste: AIPSI***

AIPSI – Associazione Italiana Professionisti Sicurezza Informatica, è il capitolo italiano di ISSA®, un'organizzazione internazionale no-profit di professionisti ed esperti praticanti.



Obiettivi:

- ◇ Organizzazione di forum educativi
- ◇ Redazione di documenti e pubblicazioni specializzate
- ◇ Interscambio di esperienze fra i professionisti del settore (nazionali e internazionali)
- ◇ Riferimento per la ricerca di professionisti di sicurezza IT
- ◇ Interazione con altre organizzazioni professionali
- ◇ Rilascio di attestati e certificazioni specifiche (non internazionali)

Anno di fondazione: 2005

Eventi chiave: ISSA European Security Conference nel 2006

Rinnovo del comitato direttivo e del presidente

Diffusione: AIPSI ha una diffusione a carattere nazionale con sede a Milano

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

- ◇ Lealtà e approccio collaborativi di tutti.
- ◇ Rappresentanza dei professionisti dell'Information Security.
- ◇ Networking con altri professionisti del settore.
- ◇ Possibilità di costituire gruppi di lavoro e di condivisione informazioni su tematiche d'interesse comune.
- ◇ Accesso e/o sconti a seminari, conferenze, training a carattere nazionale e internazionale.
- ◇ Pubblicazione di articoli e contenuti nell'Area soci del sito AIPSI.
- ◇ Possibilità di redigere articoli per conto di AIPSI/ISSA.

*(Continua a pagina 9)*

## AIPSI

- ◇ Pubblicazione e ricerca di CV per agevolare l'attività di recruitment.
- ◇ Accesso al materiale riservato ai soci sul sito ISSA.
- ◇ Ricevimento della rivista mensile edita da ISSA (ISSA Journal).
- ◇ Accesso/ricevimento Webcast e newsletter di ISSA, newsletter italiana di AIPSI.
- ◇ Visibilità nazionale ed internazionale grazie al riconoscimento di ISSA nel mondo(oltre 13000 soci).
- ◇ Possibilità di partecipare a seminari e conferenze come speaker per conto di AIPSI/ISSA.
- ◇ Certificazione di competenze sulla sicurezza.

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

L'essere il capitolo italiano di una grande associazione world wide.

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

ISACA, a livello locale ed *international*

CLUSIT, a livello locale

AIPSA, in quanto l'evoluzione della sicurezza va nella direzione dell'integrazione fra sicurezza Fisica e Logica. Mentre AIPSI è rivolta alla sicurezza logica, AIPSA è un'associazione di sicurezza fisica.

Non vedo rischi di sovrapposizione fra le associazioni appena menzionate per i seguenti motivi:

- ◇ ISACA è un'associazione di professionisti esperti in Auditing
- ◇ CLUSIT è un'associazione di aziende più che di professionisti di sicurezza
- ◇ AIPSA, come anticipato, è sicurezza fisica, non IT

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

A parte le iniziative relativamente standard che accomunano, come tipologia, anche altre associazioni, quella di contribuire alla ricerca e selezione dei professionisti è un valore aggiunto non indifferente.



*A Francoforte si terranno dal 12 al 14 ottobre 2007 la Network Security Conference e la Information Security Management Conference.*



## Le nostre interviste: CLUSIT

Il Clusit nasce più di sette anni fa negli ambienti dell'Università di Milano dove già operava il primo CERT (Computer Expert Response Team) Italiano e si voleva dare vita anche in Italia a una organizzazione indipenden-

te che facesse crescere la cultura della sicurezza sul modello di altri CLUSI già operanti in Francia e in Svizzera. Oggi il Clusit conta più di 500 aderenti ed è la più autorevole associazione non-profit che opera nel campo della sicurezza con conferenze, pubblicazioni, collaborazioni con le università e le istituzioni, corsi di formazione e di preparazione alle certificazioni professionali.



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

Il Clusit è aperto sia alle aziende fornitrici che agli utenti, agli enti, alle istituzioni e anche ai singoli cittadini. Il requisito principale è quello di essere convinti che la sicurezza sia un tema importante e sostenere le attività dell'associazione nelle sue varie forme. Molti aderiscono per godere dei particolari vantaggi riservati ai soci in particolare nella formazione professionale e nella certificazione delle competenze.

La cultura della sicurezza ha fatto passi in avanti davvero significativi negli ultimi anni sia nella sfera privata che nel mondo delle imprese e delle istituzioni. Il problema è che affrontiamo un mondo in continuo dinamico cambiamento e all'aumento della sicurezza aumentano anche la velocità di connessione, il numero di utenti interconnessi, la quantità di informazioni scambiate, in sostanza aumenta la vulnerabilità complessiva del sistema.

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

La nostra attività principale è quella della promozione e della crescita della cultura della sicurezza informatica a tutti i livelli, mantenendo una elevata qualità e competenza nei contenuti perché siamo convinti che, se è pericoloso sottovalutare il tema della sicurezza, è altrettanto pericoloso banalizzare un argomento che invece richiede specifiche conoscenze e professionalità.

Credo sia importante sottolineare il fatto che il Clusit abbia tra le proprie caratteristiche peculiari la assoluta libertà di espressione, l'imparzialità e quindi l'equidistanza dai diversi interessi, la capacità di

*(Continua a pagina 11)*

## CLUSIT

*(Continua da pagina 10)*

prendere posizioni, a volte anche scomode, sia politicamente che nei confronti degli interessi economici in gioco; e ciò innanzi tutto a tutela dell'utente.

Siamo stati attivi promotori di una visione collaborativa della sicurezza e in particolare con il progetto ISAC intendiamo incoraggiare lo scambio di informazioni, con le dovute credenziali e confidenzialità, perchè sia sempre più tempestiva la scoperta di nuove minacce e attacchi.

Ci siamo da sempre occupati di tutela dei minori in rete e collaboriamo con le università italiane attraverso il "Premio Tesi" perchè sia incoraggiata l'innovazione nello specifico ambito della protezione delle informazioni.

Collaboriamo attivamente con gli altri CLUSI a livello europeo e siamo stati attivamente impegnati con ENISA, l'agenzia europea per la sicurezza delle informazioni, proprio sul tema della awareness.

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

In Italia collaboriamo con tutte le associazioni professionali che operano nel campo della tecnologia informatica e siamo parte attiva all'interno dell'associazione delle imprese industriali, la Confindustria. Abbiamo particolari collaborazioni con tutte le associazioni che direttamente operano nel campo più specifico della sicurezza e credo siano ben evidenti le diversità. Il Clusit non è una associazione di soli professionisti, nè un sindacato di imprese o un circolo culturale nè tanto meno una lobby: siamo una organizzazione che intende far crescere la cultura generale della sicurezza nel nostro Paese e agisce concretamente perchè questo avvenga a tutti i livelli.

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

Indubbiamente tutte le attività di formazione sono di grande utilità e vantaggio economico per i soci ma ci sono iniziative specifiche che sono particolarmente importanti per alcuni di essi. Penso ad esempio alla partecipazione a condizioni vantaggiose agli eventi a cui Clusit dà il patrocinio o le attività specifiche per mondo accademico come il "Premio Tesi". I "Quaderni del Clusit", vere e proprie monografie specialistiche, spesso su temi di assoluta novità, sono strumenti molto apprezzati come lo sono i workshop tecnologici a cui i soci possono partecipare a condizioni privilegiate. Infine credo sia un vantaggio per i soci ma anche per tutti coloro che hanno a cuore la crescita della sicurezza in Italia, il fatto che il Clusit abbia elaborato e sottoposto al nuovo Governo uno specifico documento con proposte concrete e priorità per porre mano alle iniziative più urgenti.



## Percorsi formativi

Il bimestre settembre / ottobre 2007

	SETTEMBRE 2007	OTTOBRE 2007
1		Corso ITIL Milano
2		Corso ITIL Milano / Corso CISA Roma
3		Sessione di Studio Milano / Corso Cisa Roma / Corso ITIL Milano
4		Sessione di Studio Roma / Corso ITIL Milano
5		
6		
7		
8		Corso Lead Auditor ISO 27001 Roma
9		Corso Lead Auditor ISO 27001 Roma
10		Corso Lead Auditor ISO 27001 Roma
11		Corso Lead Auditor ISO 27001 Roma
12		Corso CISA Milano/ Corso Lead Auditor ISO 27001 Roma
13		Corso CISA Milano
14		
15		
16		Corso CISA Roma
17		Corso CISA Roma
18		
19		Inizio Corso CISM Milano / Inizio Corso CISM Roma
20		Corso CISM Milano / Corso CISM Roma
21	Inizio Corso CISA Roma	
22	Corso CISA Roma	Corso Base IS Audit Milano
23		Corso Base IS Audit Milano/ Corso COBIT BASE Roma
24		Corso Base IS Audit Milano / Corso COBIT BASE Roma
25		Sessione di Studio Torino / Corso Base IS Audit Milano
26		Corso CISA Milano / Corso Base IS Audit Milano
27		Corso CISA Milano
28	Inizio Corso CISA Milano	
29	Corso CISA Milano	
30		

Il programma completo dei corsi AIEA è disponibile sul sito

<http://www.aiea.it/pdf/eventi/Calendario%20Eventi%20%20Semestre%202007.pdf>

**Le Buone Letture****COBIT® e ITIL®, due framework complementari**

AIEA è lieta di informare che è stato pubblicato il white paper "**COBIT® e ITIL®, due framework complementari**". Il documento, risultato della collaborazione attiva tra AIEA, itSMF Italia e SDA Bocconi, è un'utile guida per comprendere come utilizzare congiuntamente e proficuamente due tra i più importanti ed affermati framework per il governo e la gestione dell'IT. In particolare identifica chiaramente le aree di sinergia e, per esse, illustra quali parti dei modelli utilizzare in modo integrato e con quale approccio.

Utili esempi pratici, sviluppati per specifiche aree di processo, completano lo sviluppo degli argomenti. Il documento è anche un'utile guida per chi desidera una panoramica sui principali framework per la gestione dell'IT, oltre a COBIT e ITIL, e fornisce per questi ultimi una guida introduttiva per chi si avvicinasse ad essi per la prima volta.

Hanno contribuito per AIEA: Orillo Narduzzo, Andrea Pederiva, Stefano Niccolini. Il white paper è disponibile solo per gli associati. Chi fosse interessato, può inviare la richiesta alla segreteria AIEA presso [aiea@aiea.it](mailto:aiea@aiea.it). Siamo certi che il contenuto del documento sarà un interessante contributo all'attività professionale dei soci.

**Novità da ISACA****COBIT e BASILEA II**

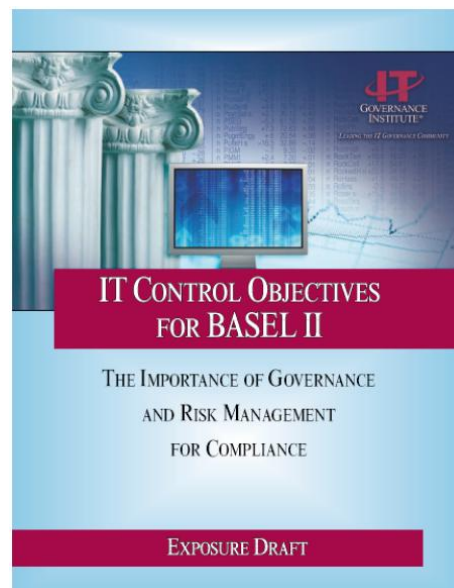
Il 16 maggio è stata pubblicata sul sito di ISACA e ITGI la Bozza del documento *IT Control Objectives for Basel II*.

Il documento fornisce un riferimento per la gestione dei rischi legati ai sistemi informativi nel contesto specifico delineato da Basilea 2.

Applicando il metodo proposto, le organizzazioni attive in ambito finanziario dovrebbero essere in grado di applicare processi e controlli adeguati nell'ambito dei sistemi informativi.

Gli obiettivi di controllo IT ed i processi di gestione descritti nel documento propongono un indirizzo per il ruolo dei sistemi informativi nell'ambito del rischio operativo e individuano i compiti risultanti per gli "informatici", per gli Auditor IT, per i Risk Manager e per i responsabili della Sicurezza.

Il termine per inviare a ISACA eventuali commenti e osservazioni si è chiuso il 18 giugno e il rilascio della versione definitiva del documento è previsto per il terzo trimestre del 2007.





## Analisi di vulnerabilità applicative e Sviluppo Sicuro\*

di Roberto Ugolini

L'attività di **analisi di vulnerabilità tecnologiche** è uno degli strumenti cardine per individuare le debolezze dei propri sistemi e pianificare una strategia di intervento.

Infatti la pianificazione del processo di securizzazione dei sistemi di una azienda non può prescindere dalla conoscenza delle vulnerabilità e minacce a cui si può essere soggetti.

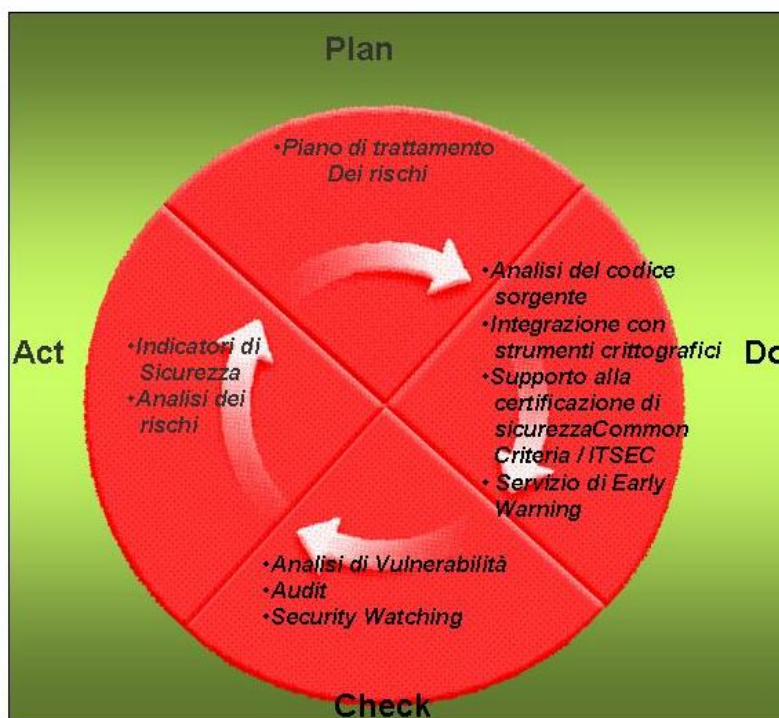
Solo conoscendo i rischi (opportuna valorizzazione delle vulnerabilità e delle minacce) a cui si è potenzialmente esposti è possibile attuare le opportune difese.

L'analisi di vulnerabilità non può essere una attività sporadica, ma deve essere svolta sistematicamente. Solo così è garantito il mantenimento della sicurezza. E deve essere inserita in un modello virtuoso di intervento in modo da fornire evidenze utili alla valorizzazione dei rischi tecnologici in una metodologia di analisi dei rischi (che comprenderà anche rischi organizzativi).

In altre parole, l'attività deve essere inserita nella logica del modello PDCA, fase CHECK - adottato dai sistemi di gestione tra i quali quelli a norma ISO 9001:2000 per la qualità e ISO/IEC 27001:2005 per la sicurezza (per aiutare le aziende a gestire, mantenere e migliorare il proprio sistema di sicurezza in linea con gli obiettivi identificati).

### Modello PDCA

Postecom ha sviluppato, realizzato ed affinato nel tempo, grazie anche alla capacità di integrazione di soluzioni tecnologiche, una serie di **strumenti ed attività** inquadrabili nelle fasi **Do e Check** del modello PDCA (Plan, Do, Check, Act).



Politiche e obiettivi di sicurezza definiti dall'azienda

(\*) L'articolo è stato pubblicato sul numero di marzo 2007 della rivista ICTSecurity. La riproduzione è autorizzata

## Analisi di vulnerabilità applicative e Sviluppo Sicuro

*(Continua da pagina 14)*

L'attività deve permettere di evidenziare le vulnerabilità sistemiche ed applicative, classificandole nel contesto ambientale e d'utilizzo, anche in relazione alla tipologia di dati trattati. Può essere svolto dall'interno così come dall'esterno della rete aziendale, così come in black box (senza conoscere i dettagli dell'obiettivo) od in white box.

Attraverso l'utilizzo di metodologie e di strumenti, e la produzione di documentazione a supporto (che, oltre a descrivere puntualmente le debolezze individuate e ad evidenziarne i livelli di rischio, offre soluzioni correttive e migliorative sia in ambito tecnico che organizzativo) **l'attività di analisi di vulnerabilità aiuta le aziende a migliorare il proprio sistema di sicurezza.**

Ma non basta, il ciclo virtuoso deve prevedere, fase DO, lo **sviluppo di codice sicuro**, per intervenire nella fase di creazione del codice, eliminando gli errori di programmazione prima della messa in esercizio.

L'approccio Postecom all'analisi di vulnerabilità

Di seguito un esempio di applicazione completa dell'approccio, che deve modulato in base all'esigenza ed all'ambito (applicazione, servizio, insieme di servizi). Gli strumenti utilizzati possono essere proprietari e liberi, privati e pubblici, individuati tra quelli disponibili come quelli più adatti all'esigenza ed all'ambito in esame.

### ANALISI NON INVASIVA

#### 1 IDENTIFICAZIONE E CLASSIFICAZIONE DELLE BANCHE DI DATI

Questa fase ha lo scopo di identificare e di classificare le banche di dati gestite con l'ambito oggetto dell'analisi (l'obiettivo). La classificazione è l'elemento chiave che permette di valutare il rischio effettivo di una vulnerabilità associata alla particolare banca di dati.

La classificazione sarà effettuata in base ai parametri riservatezza, integrità, disponibilità e tenendo conto gli aspetti legati alla privacy.

#### 2 ANALISI DELL'ARCHITETTURA

Questa fase ha lo scopo di raccogliere il maggior numero di informazioni sull'obiettivo che si intende attaccare senza "toccare" l'obiettivo stesso. In particolare in questa fase è importante determinare, se pertinenti: domini, blocchi di rete e gli indirizzi IP dei sistemi direttamente collegati ad internet. Sono effettuate interrogazioni ai seguenti servizi Internet (elenco non esclusivo):

- ◇ Search engine
- ◇ WHOIS database
- ◇ WAIS database
- ◇ DNS autoritativi primari e secondari (hidden)
- ◇ WWW (mapping, hyperlink traversal)

Inoltre sono analizzati, tramite interviste conoscitive e la documentazione di supporto, l'architettura del

*(Continua a pagina 16)*

## Analisi di vulnerabilità applicative e Sviluppo Sicuro

*(Continua da pagina 15)*

servizio, i protocolli di comunicazione, i protocolli di sicurezza, i web server, i data server, gli application server ed i linguaggi di programmazione utilizzati. In questa fase è anche definita la “piattaforma” di attacco, anche in termini di dislocazione di rete.

### **ANALISI INVASIVA**

#### **3 SCANNING**

L'obiettivo dello scanning è ottenere una verifica sulle informazioni ottenute nell'analisi dell'architettura, completandola con altre informazioni non ricavate precedentemente; ciò significa acquisire informazioni su quali IP dei blocchi di rete trovati nella fase precedente siano effettivamente contattabili, e, relativamente a tali IP, scoprire che servizi abbiano attivi e che sistemi operativi posseggano.

Le tecnologie impiegate sono (elenco non esclusivo):

- ◇ Network Ping sweeps
- ◇ ICMP queries
- ◇ Port scanning (TCP, UDP, RPC, stealth)
- ◇ Stack fingerprinting (remote OS detection)
- ◇ Application fingerprinting
- ◇ Firewalking (TTL modulation)
- ◇ TCP sequence number randomness
- ◇ Traceroute
- ◇ Transitive trust
- ◇ Network reverse mapping

#### **4 ENUMERATION**

Con questa fase si inizia “l'analisi invasiva” vera e propria, infatti si effettuano connessioni dirette ai server ed interrogazioni esplicite, il che potrebbe (a seconda della configurazione presente sui sistemi) originare dei log.

Attraverso l'enumerazione si vuole giungere a identificare, sulle macchine riscontrate come raggiungibili, degli account validi, delle risorse condivise e delle applicazioni attive sulle porte in ascolto.

Le tecniche utilizzate variano dai sistemi operativi delle macchine che vogliamo analizzare, di seguito una lista parziale:

- ◇ Finger
- ◇ Rusers
- ◇ X11
- ◇ SMB netbios shares
- ◇ SMB netbios resources

*(Continua a pagina 17)*

## Analisi di vulnerabilità applicative e Sviluppo Sicuro

*(Continua da pagina 16)*

- ◇ NFS shares
- ◇ RPC mapping (portmap, common ports)
- ◇ Default accounts (SMTP, finger,..)
- ◇ SNMP
- ◇ Banner grabbing
- ◇ WWW (CGI, cookies, HTML sources,...)
- ◇ SSL (certificates, encryption used, numero di bit)

### ATTACCO

#### 5 GAINING ACCESS

Una volta ottenute le informazioni del punto precedente inizia il vero e proprio attacco che ha come obiettivo il riuscire a compromettere la riservatezza, l'integrità e la disponibilità nel sistema remoto, delle informazioni e delle funzionalità gestite. Questa è la fase più delicata, che deve essere condivisa e concordata con l'owner dell'obiettivo, e potrà (dovrà) prevedere delle limitazioni in termini di "profondità" dell'attacco.

I metodi utilizzati anche in questo caso dipendono dal sistema operativo della macchina, ma si basano sostanzialmente sulla ricerca di password corrispondenti agli utenti trovati (password guessing), sullo sfruttamento di errori progettuali delle applicazioni e servizi attivi sul server (buffer overflow, attacchi data driven, ecc.) o del sistema operativo stesso.

La lista di tecniche e tecnologie impiegate in questa fase varia moltissimo a seconda dello scenario rilevato nelle fasi precedenti, un elenco non esaustivo è riportato di seguito:

- ◇ Cross-site scripting
- ◇ Parameter tampering
- ◇ Hidden field manipulation
- ◇ Backdoors e opzioni di debug
- ◇ Stealth commanding
- ◇ Forceful browsing
- ◇ Buffer overflow
- ◇ Cookie poisoning
- ◇ Configurazioni errate
- ◇ Vulnerabilità note
- ◇ SQL injection
- ◇ Attacchi http
- ◇ Attacchi Man-in-the-Middle
- ◇ Attacchi Denial Of Service

*(Continua a pagina 18)*

## Analisi di vulnerabilità applicative e Sviluppo Sicuro

(Continua da pagina 17)

La documentazione prodotta nella fase di assessment:

1. rileva le vulnerabilità e definisce il fattore di rischio assoluto e quello reale (al fine di eliminare i falsi positivi ed in riferimento al contesto ambientale e topologico in cui il sistema si trova, e con riferimento alla banca di dati coinvolta);
2. attribuisce ad ogni vulnerabilità una valutazione del grado di SEVERITA' (Alta / Media / Bassa). La severità delle vulnerabilità prese in considerazione è valutata ispirandosi alle classificazioni più diffuse in ambito internazionale (CVE, OSVDB, NESSUS ecc.);
3. raggruppa, ove possibile, le varie vulnerabilità in classi omogenee, al fine di poter confrontare risultati provenienti da attività diverse ed effettuate a distanza di tempo.

E' prodotto un documento contenente l'elenco dei sistemi/applicazioni testati, la descrizione delle vulnerabilità riscontrate con indicazione del livello di rischio e le soluzioni correttive, anche architetturali, suggerite per elevare il livello di sicurezza.

La documentazione prodotta indica inoltre, relativamente alle azioni correttive, l'eventuale prodotto, classe di prodotto, intervento software che possa risolvere il problema evidenziato.

Di fronte al problema di produrre **codice sorgente** che sia **sicuro**, in modo da eliminare all'origine la principale causa di vulnerabilità del software (dovute a errori di progettazione, implementazione, configurazione e deployment) un approccio è il seguente:

- ◇ Effettuare una valutazione del rischio dell'insieme delle proprie applicazioni, per determinare quali parti del proprio "parco software" siano le più critiche, rispetto alla natura dei dati trattati, rispetto alle vulnerabilità effettivamente presenti in relazione all'impatto (perdite economiche, di immagine, ecc.) e alla probabilità di un eventuale exploit. Dal risultato di questa valutazione si determineranno le priorità di intervento. Per determinare lo stato dell'intero insieme del proprio codice sorgente è consigliabile procedere in questa fase con un'analisi statica del codice sia manuale ma soprattutto automatizzate, e con attività di analisi di vulnerabilità, al fine di ottenere una mappa dei possibili problemi di security presenti (sostanzialmente una fotografia al tempo t0).
- ◇ Gestire le vulnerabilità, intervenendo nel ciclo di sviluppo software (SDLC), affinché siano collocati, configurati e utilizzati opportunamente tutti quegli strumenti metodologici, tecnologici, procedurali e organizzativi adeguati alla propria situazione. In primo luogo sarà necessario fissare le vulnerabilità che le attività di static code analysis e/o analisi di vulnerabilità precedenti hanno evidenziato. Non è opportuno prefiggersi di eliminarle tutte in una volta: l'output della valutazione è sostanzialmente il piano di intervento di questa prima sgrossatura. Da qui si possono già delineare quelle che saranno le regole di codifica che sono l'obiettivo della terza fase.
- ◇ Stabilire degli standard di sviluppo sicuro e limitare la produzione di codice insicuro. Sostanzialmente vuol dire imparare dall'esperienza e prevenire gli errori che portano a vulnerabilità nel software. Questo può avvenire tramite delle policy (che stabiliscono ruoli, processi, principi generali

(Continua a pagina 19)

## Analisi di vulnerabilità applicative e Sviluppo Sicuro

(Continua da pagina 18)

da seguire e responsabilità) e tramite dei tool a supporto. Questi consentono di creare/aggiornare delle regole di secure coding, il cui rispetto viene verificato, automaticamente, sul nuovo codice che da quel momento in poi si andrà a produrre. Questo passo non riguarda solo il codice sorgente. Si può estendere a livello di design: definendo delle specifiche di security per un determinato software (integrità, confidenzialità, autenticazione, autorizzazione, ecc.), utilizzando dei pattern di progettazione che non introducono difetti di sicurezza e soprattutto verificando la bontà di quanto fatto con un'analisi "threat modeling".

- ◇ Monitoring e auditing. Il processo di produzione di software sicuro va monitorato per evidenziare miglioramenti o peggioramenti in base sostanzialmente ad assessment condotti al tempo t1, t2, ecc. In questa fase rivestono particolare importanza le metriche di sicurezza, cioè la misurazione di una serie di parametri che vengono poi pesati per produrre degli indici che sintetizzino la situazione dei propri progetti e team di sviluppo. In questo modo si può capire se il numero di vulnerabilità, o la loro criticità, decresce in una certa applicazione, qual è il gruppo di sviluppatori meno performante, ecc. Le policy e le procedure adottate devono poi essere sottoposte periodicamente a revisione al fine di valutarne l'efficacia e apportare azioni correttive.

Tra gli strumenti di supporto per l'analisi del codice sorgente, assumono particolare rilevanza i source code analyzer, tool di analisi statica del codice (statica perché il codice non è in esecuzione), svolta su base sintattica e semantica.

Sono in grado di controllare il codice sorgente in base a delle regole built-in, ovviamente aggiornabili, e configurabili secondo la realtà del SDLC in cui sono inseriti. Possono lavorare su più linguaggi di programmazione e su più moduli dell'applicazione contemporaneamente.

Sono in grado di creare una mappa dei componenti dell'architettura di un software per controllare i collegamenti e il flusso di controllo, consentendo di capire dove impattano dei dati non validati.

I risultati delle loro analisi sono poi salvati in un opportuno database che alimenta un sistema di reportistica destinato:

- ◇ agli sviluppatori, per i dettagli delle singole vulnerabilità;
- ◇ ai development manager, per la gestione dei progetti e dei team;
- ◇ ai security manager, per controllare il trend e la tipologia delle vulnerabilità mitigate.

Tali strumenti, infine, possono essere integrati nell'ambiente di sviluppo (IDE) utilizzato dai programmatori in modo da segnalare la presenza di porzioni di codice non corrette, dal punto di vista della sicurezza, nello stesso istante in cui il codice sorgente stesso viene scritto.

## IT GOVERNANCE IMPLEMENTATION GUIDE

USING COBIT<sup>®</sup> AND VAL IT<sup>™</sup>

*E' disponibile nel bookstore ISACA un importante strumento operativo: la nuova guida per l'implementazione dell'IT Governance ed il relativo toolkit. E' possibile acquistarli o, per gli associati, scaricarli gratuitamente.*

**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: Orillo Narduzzo,  
 Stefano Niccolini, Silvano Ongetta,  
 Roberto Ugolini

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.*